# Combinatorial Analysis of Block Ciphers With Trapdoors 

Arnaud Bannier

## To cite this version:

Arnaud Bannier. Combinatorial Analysis of Block Ciphers With Trapdoors. Cryptography and Security [cs.CR]. École Nationale Supérieure d'Arts et Métiers, 2017. English. NNT: . tel-03125786

HAL Id: tel-03125786
https://theses.hal.science/tel-03125786
Submitted on 29 Jan 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Doctorat ParisTech 

## THÈS E

pour obtenir le grade de docteur délivré par

## I'École Nationale Supérieure d'Arts et Métiers Spécialité "Automatique"

présentée et soutenue publiquement par

## Arnaud BANNIER

le 29 septembre 2017

## Combinatorial Analysis of Block Ciphers With Trapdoors

Directeur de thèse : Éric FILIOL

| Jury |  |  |
| :--- | :--- | :--- |
| M. Jean-Marc Steyaert | Professeur | École Polytechnique |
| M. Kenneth Paterson | Professeur | Royal Holloway, University of London |
| M. Massimiliano Sala | Professeur | University of Trento |
| Mme. Anne Canteaut | Professeur | Inria Paris |
| M. Alexei Zhukov | Professeur | Bauman Moscow State Technical University |
|  |  |  |
|  | Arts et Métiers ParisTech - Campus d'Angers |  |
|  |  | N\&S Numérique et Société |

## Remerciements

Tout d'abord, je tiens à remercier les membres du jury pour l'honneur qu'ils m'ont fait de lire et de questionner mon travail, ainsi que pour leurs travaux de recherche en lien avec cette thèse. M. Kenneth Paterson pour ses travaux remarquables sur les chiffrements à trappes imprimitives qui ont inspiré le présent manuscrit. M. Massimiliano Sala pour ses nombreuses contributions au développement et à la compréhension des algorithmes de chiffrement à trappes. Mme. Anne Canteaut pour ses travaux en cryptographie symétrique et ses précieux commentaires qui m'ont aidé à améliorer cette thèse. Je remercie enfin M. Jean-Marc Steyaert et M. Alexei Zhukov pour leur confiance et nos échanges pertinents durant ma soutenance.

Je remercie également mon directeur de thèse Eric Filiol, qui m'a fait confiance et m'a laissé une grande liberté dans mes recherches. Ce travail de recherche ne se serait pas concrétisé sans l'aide et le soutien de mes collègues du laboratoire CVO : Jean-Pierre Aubin, Richard Rey, Paul Irolla, Olivier Ferrand et Baptiste David. Je tiens à les remercier. En particulier, Nicolas Bodin, mon inséparable binôme de bureau et également très bon ami qui m'a pleinement aidé dans mes recherches, dans mes cours et qui a relu avec passion chaque ligne de ce manuscrit.

Je tiens aussi à remercier tout particulièrement Jean Labourdette, directeur de l'ESIEA, qui a su me soutenir, m'encourager et qui m'a fait confiance pour poursuivre l'aventure dans cette très belle école après ma thèse.

Je remercie également l'ensemble de mes collègues de l'ESIEA, notamment Elisabeth Davidson qui m'a beaucoup aidé pour la rédaction en anglais du manuscrit ainsi que pour la préparation de ma soutenance. Même s'ils n'ont évidemment pas tous participé directement à l'élaboration de cette thèse, les bons moments que je passe chaque jour en leur compagnie et leur soutien ont réellement contribué à la réussite de ce projet. Merci à eux.

Je remercie mes étudiants que pour une raison assez évidente je n'énumérerai pas ici mais qui m'ont fait découvrir ma passion pour l'enseignement et pour la bonne humeur apportée pendant les cours.

Enfin, je remercie du fond du cœeur celles et ceux présents pour moi depuis tant d'années. Mes amis Nicolas, Céline, Jérôme, Manon, Guillaume, Claire et Wilson. Un grand merci à mes parents Anita et Joseph qui ont toujours cru en moi et qui m'ont appris la persévérance, une qualité qui m'a été indispensable pour mener à bien mon doctorat. Pour finir, je remercie ma compagne Amélie qui a su me soutenir, surtout dans les moments les plus difficiles. Sans elle, je n'aurais pas apporté autant de soin à la finalisation de cette thèse. Merci infiniment.

## Overview

Trapdoors are a two-face key concept in modern cryptography. They are primarily related to the concept of trapdoor function used in asymmetric cryptography. A trapdoor function is a one-to-one mapping that is easy to compute, but for which the inverse function is difficult to compute without special information, called the trapdoor. Such a trapdoor is essential in public key encryption algorithms and digital signatures as it ensures that only the person who knows the secret information can decrypt or sign messages. In this case, the trapdoor mechanism is always public and fully detailed.

The second concept of trapdoor considers by-design mathematical backdoors and is a key issue in symmetric cryptography. In this case, the aim is to insert hidden mathematical weaknesses which enable one who knows them to break the cipher. The existence of a backdoor is hence a strongly undesirable property. While the term of trapdoor has been already used in the very few literature covering this issue, we suggest however to use the term of backdoor to describe hidden mathematical weaknesses in symmetric cryptography in order to avoid ambiguity. This thesis is focused on backdoors in block ciphers or, more specifically, on Substitution-Permutation Networks (SPN).

Inserting a backdoor in an encryption algorithm gives an effective cryptanalysis of the cipher to the designer. However, like any other cipher, this backdoor cipher may be vulnerable to classical cryptanalysis. If a classical attack can easily break it, the asymmetry between the designer and those who do not know the backdoor disappears; thus, the backdoor cipher is just a weak cipher.

Differential [13] and linear [74] cryptanalysis are considered as the most important attacks against block ciphers [64]. As mentioned in [41], any new cipher should at least be accompanied by a detailed analysis of its strength against these two attacks. The practical resistance of a block cipher against differential and linear cryptanalysis is assessed by the differential probability or linear potential of an optimal differential or linear trail respectively. When these values are low enough, the cipher is said to be practically secure. To prevent differential and linear cryptanalysis, the cipher designer chooses building blocks which provide high resistance against both these attacks. Nevertheless, the mathematical structure of the backdoor strongly reduces the choice of these building blocks and the usual strategies may no longer be useful.

In [76], Matsui presented an algorithm that computes an optimal trail in a Feistel cipher. In other words, the execution of this algorithm can prove the cipher practical security. The algorithm complexity remaining too high for the cipher

FEAL, two successive improvements have been proposed in [87] then [3]. Although an adaptation of Matsui's algorithm is straightforward for SPN, the block size of modern ciphers makes it computationally infeasible. The first contribution of this thesis is an improvement of this algorithm for SPN [8] and has received a best paper award. We introduce several optimizations paying special attention to SPN whose diffusion layer is a bit permutation. Because bit permutations do not provide high diffusion, the cipher security is hard to establish without a close analysis. Such mappings are generally chosen for efficiency purposes. On the contrary, diffusion layers providing high diffusion yield sufficient bounds to prove the cipher security but can be more computationally expensive. Therefore, such an algorithm is more useful for SPN using bit permutations.

Spending months computing the practical security of a known cipher is not a problem. However, the cipher designer has to repeat this search several times in order to optimize the choice of the cipher components or the number of rounds. Our algorithm meets this need since its execution time on the full Present [17] is below one second on a laptop computer.

Now we have a tool to evaluate the security of an SPN with regard to differential and linear cryptanalysis, we turn our attention to backdoor ciphers. The family of backdoor ciphers covered by this thesis is a generalization of the imprimitive ciphers introduced by Paterson in [88]. For such ciphers, the round function preserves a partition of the message space no matter the round keys used, and hence the same applies to the full cipher. This partition forms the backdoor and yields a powerful cryptanalysis with a suitably chosen key schedule. Even if the mathematical theory of the backdoor is given, no general algorithm details how to construct the building blocks of the cipher. Moreover, the author wondered what are the possible partitions for this backdoor. Caranti and al. [31] answered this question by proving that only linear partitions can be considered. Along a similar line, Harpes considered in his thesis [50] backdoor ciphers mapping a partition of the plaintexts to a partition of the ciphertexts. As these partitions are not necessarily equal, this family generalizes Paterson's one. These ciphers are called partition-based backdoor ciphers.

The main contribution of this thesis is an extension of Paterson and Harpes' works for SPN. In our study, we consider an SPN mapping a partition of the plaintexts to one of the ciphertexts, no matter what the round keys are. In other words, we assume that this property holds independently of the key schedule and the cipher key. Firstly, we prove that the round function of such an SPN must at least map a linear partition to another linear one. This result generalizes [31] since we consider the full cipher and not only the round function. It should be stressed that the apparent combinatorial aspect of our assumption is reduced to an algebraic one. Since it is easy to show that any linear transformation maps every linear partition to another one, the diffusion layer can be bypassed so that the substitution layer necessarily maps a linear partition to another one.

The substitution layer consists of several S-boxes evaluated in parallel. The natural problem that arises is to determine the properties that the previous result implies on each S-box. This refinement is far more complicated than the previous
one because it requires a deep analysis of the structure of the linear partitions with respect to the substitution layer. We eventually managed to prove that at least one of the S-boxes must map a linear partition to another one. To summarize, the study of the full cipher is reduced to that of the S-boxes.

In the light of this result, we are now interested in designing an S-box mapping a linear partition to another one with the best resistance against differential and linear cryptanalysis. We show how the Krasner-Kaloujnine embedding theorem yields an internal decomposition of such S-boxes. Using this decomposition, we manage to derive bounds for the differential and linear properties of backdoor S-boxes and we present an algorithm to design S-boxes which almost reach these bounds. Combining our reduction result with these bounds, we derive a criterion which can prove that an SPN does not belong to this family of backdoor ciphers. All these results were published in [9] and [12].

The last part puts into practice our theoretical treatment of partition-based backdoor ciphers. First, we present a toy backdoor SPN and break it with a keyschedule dependent attack suggested by Paterson but not detailed. Finally we present BEA-1 (standing for Backdoored Encryption Algorithm), a real-size backdoor cipher inspired by the current standard of symmetric encryption, namely the AES. Our cipher encrypts 80 -bit data blocks using using 120 -bit cipher key and is designed to resist linear and differential cryptanalysis. Conversely, the backdoor enables recovery of the full 120-bit cipher key in just a few seconds on a laptop computer using only $2^{16}$ chosen plaintext blocks. This cipher was presented in [11] as a challenge. Its cryptanalysis was then outlined in [11 and detailed in [12]. It should be mentioned that my teaching activity led me to consider Venn Diagrams. As a result, we published a new infinite family of Venn diagrams in [7].

This thesis is organized as follows. Firstly, Chapter 1 recalls the definition of substitution-permutation networks and the differential and linear cryptanalysis. An algorithm performing a security analysis with respect to these attacks is then described in Chapter 2. Backdoor ciphers are then the focus of this thesis from Chapter 3 to the end. In Chapter 3, we investigate the structure of partition-based backdoor ciphers and prove that their study can be reduced to their S-boxes. Next, Chapter 4 is devoted to the analysis of such S-boxes and ends with a toy backdoor cipher illustrating the results of these two chapters. Finally, Chapter 5 concludes our work by introducing BEA-1, a real-size backdoor cipher, and explains how its backdoor can be exploited to break it effectively.

## Contents

1 Substitution-Permutation Networks ..... 1
1.1 Preliminaries ..... 1
1.2 Substitution-Permutation Networks ..... 3
1.3 Differential Cryptanalysis ..... 9
1.3.1 General Idea of the Attack ..... 10
1.3.2 Differential Trails ..... 15
1.4 Linear cryptanalysis ..... 20
1.4.1 General Idea of the Attack ..... 20
1.4.2 Linear Approximations and Linear Trails ..... 24
1.5 Security Evaluation of SPN Building Blocks ..... 30
1.5.1 Perfect S-Boxes ..... 31
1.5.1.a Almost Perfect Nonlinear Functions ..... 31
1.5.1.b Almost Bent Functions ..... 32
1.5.1.c Known AB and APN Permutations ..... 33
1.5.2 Branch Number of the Diffusion Layer ..... 34
2 Security Evaluation of SPN ..... 37
2.1 Search for an Optimal trail ..... 38
2.1.1 General Principle ..... 40
2.1.2 Proof of the Algorithm ..... 41
2.2 A Detailed Example ..... 43
2.2.1 Search Algorithm for the First Round ..... 46
2.2.2 Search Algorithm for the Round Function ..... 49
2.2.3 Search Algorithm for the Last Round ..... 52
2.3 Optimizations ..... 53
2.3.1 Construction of the First Output Pattern ..... 53
2.3.2 The Round Function ..... 55
2.3.3 Active S-Boxes in the Next Round ..... 56
2.3.4 Test on the Bound ..... 58
2.3.5 Automatic Management of the Estimation ..... 60
2.4 Results ..... 60
3 Partition-Based Backdoor Ciphers ..... 63
3.1 Partition-Based Backdoor Ciphers ..... 65
3.1.1 Imprimitive Group Actions ..... 65

## Contents

3.1.2 Imprimitive Backdoor ciphers ..... 68
3.1.3 Exploiting the backdoor ..... 69
3.1.4 Generalizations ..... 71
3.1.5 Links With Other Attacks ..... 72
3.2 Substitution-Permutation Networks and Partitions ..... 73
3.2.1 Linear Partitions ..... 74
3.2.2 The Key Addition and Diffusion Layer ..... 77
3.2.3 From the Encryption Function to the Substitution Layer ..... 81
3.3 Structure of the Substitution Layer ..... 84
3.3.1 Truncating the substitution layer ..... 85
3.3.2 Structure of the Subspaces V and W ..... 88
3.3.3 Linked and Independent S-Boxes ..... 92
3.3.4 The Forbidden Case ..... 95
3.3.5 Reduction to one S-Box ..... 100
3.4 Conclusion ..... 103
4 Analysis of a Backdoor S-Box ..... 105
4.1 Structure of a Backdoor S-Box ..... 105
4.1.1 Wreath Product ..... 109
4.1.2 Krasner-Kaloujnine Embedding Theorem ..... 113
4.1.3 Application of the Embedding Theorem ..... 115
4.2 Differential and linear analyses ..... 116
4.2.1 Correlation Matrices and Linear Potentials ..... 119
4.2.2 Differential Probabilities ..... 121
4.2.3 Designing a Backdoor S-Box ..... 127
4.3 A Toy Partition-Based Backdoor Cipher ..... 129
4.3.1 Specification of TBC ..... 129
4.3.2 Differential and Linear Cryptanalysis ..... 131
4.3.3 The Backdoor ..... 132
4.3.3.a Basic and Multiple Partitions Attacks ..... 134
4.3.3.b Key Schedule Dependent Attack ..... 134
4.3.4 The Flaws of This Cipher ..... 136
4.4 Preventing Partition-Based Backdoors ..... 137
5 Backdoored Encryption Algorithm 1 ..... 141
5.1 Presentation of BEA-1 ..... 141
5.1.1 Specification of the Encryption Process ..... 141
5.1.2 Differential and Linear Cryptanalysis ..... 142
5.2 Design of the Backdoor ..... 145
5.2.1 The Linear Partitions Throughout the Encryption ..... 145
5.2.2 The Substitution Layer ..... 148
5.2.3 The Diffusion Layer ..... 149
5.3 Main Idea of the Cryptanalysis ..... 152
5.3.1 A Detailed Example ..... 152
5.3.2 Formalization of the Attack ..... 156
5.4 Cryptanalysis of BEA-1 Using the Backdoor ..... 157
5.4.1 Part 1: Finding the Right Output Coset ..... 158
5.4.2 Part 2: Obtaining Candidates for the Last Round Key ..... 160
5.4.3 Part 3: Finding the Last Round Key ..... 161
5.4.4 Part 4: Obtaining Candidates for the Remaining Bits ..... 164
5.4.5 Part 5: Deducing the Cipher Key ..... 165
5.5 Conclusion ..... 166
A Specifications of BEA-1 Building Blocks ..... 169
B Résumé long en français ..... 181
B. 1 Réseaux de substitutions-permutations ..... 181
B.1.1 Définitions ..... 182
B.1.2 Cryptanalyse différentielle ..... 184
B.1.2.a Idée générale de l'attaque ..... 184
B.1.2.b Pistes différentielles ..... 185
B.1.3 Cryptanalyse linéaire ..... 187
B.1.3.a Idée générale de l'attaque ..... 187
B.1.3.b Approximations et pistes linéaires ..... 189
B. 2 Évaluation de la sécurité des SPN ..... 190
B.2.1 Recherche d'une piste optimale ..... 192
B.2.1.a Rappels et définitions ..... 192
B.2.1.b Principe général ..... 193
B.2.2 Optimisations ..... 196
B.2.2.a Construction du premier motif de sortie ..... 196
B.2.2.b La fonction de ronde ..... 197
B.2.2.c Les S-Boxes actives à la ronde suivante ..... 198
B.2.2.d Le test sur la borne ..... 200
B.2.2.e Gestion automatique de l'estimation ..... 200
B.2.3 Résultats. ..... 201
B. 3 Chiffrements à trappes basées sur des partitions ..... 202
B.3.1 Généralisations ..... 203
B.3.2 Réseaux de substitutions-permutations et partitions ..... 204
B.3.3 De la fonction de chiffrement à la substitution ..... 205
B.3.4 Analyse des résultats ..... 207
B. 4 Analyse d'une S-box à trappe ..... 208
B.4.1 Structure d'une S-box à trappe ..... 208
B.4.2 Analyses différentielle et linéaire ..... 209
B.4.2.a Matrices de corrélations et potentiels linéaires ..... 210
B.4.2.b Probabilités différentielles ..... 211
B.4.2.c Conception d'une S-Box à trappe ..... 211
B.4.3 Se prémunir des trappes basées sur des partitions ..... 213
B. 5 Conclusion ..... 214

Contents


## Substitution-Permutation Networks

This chapter aims at offering an introduction of substitution-permutation networks and their cryptanalysis. We start with notation, some terminologies and basic results. Then, we present in Section 1.2 the main definitions concerning blocks ciphers and we focus particularly on Substitution-Permutation Networks (SPN). After given an example of such ciphers, we explore the two mains attacks of SPN, namely differential and linear cryptanalysis, in Sections 1.3 and 1.4 respectively. Finally, we conclude this chapter with a discussion on the security of SPN against these attacks.

### 1.1. Preliminaries

Let us begin with notation and some conventions. The cardinality of a finite set $E$ is denoted by $\# E$. The complement of a subset $F$ of $E$ consists of all elements in $E$ not in $F$ and is denoted by $F^{c}$. Let $f$ be a mapping from $E$ to $F$ and $g$ be a mapping from $F$ to $G$. The composition of $g$ on $f$ is the mapping $g \circ f$ from $E$ to $G$ which maps $x$ to $g(f(x))$. A permutation of $E$ is any bijective mapping from $E$ to $E$. If $\sigma$ and $\tau$ are permutations of $E$, then we often write $\sigma \tau$ instead of $\sigma \circ \tau$, namely we omit the small circle when composing permutations to fit the abstract formalism of permutation groups.

Let $n$ and $m$ be two positive integers. The Galois field of order two is denoted by $\mathbb{F}_{2}$. Every vector space considered in this thesis will be over the finite field $\mathbb{F}_{2}$. The set of all $n$-bit sequences is identified with the $n$-dimensional vector space $\mathbb{F}_{2}^{n}$. In this space, the addition denoted by + can be seen as a bitwise exclusive or (Xor). The zero vector $(0, \ldots, 0)$ is simply denoted by $0_{n}$. The concatenation of two binary vectors $x$ and $y$ is denoted $(x \| y)$. Similarly, if $f: \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ and $g: \mathbb{F}_{2}^{m} \rightarrow \mathbb{F}_{2}^{m}$ are two mappings, then $(f \| g)$ denote the mapping from $\mathbb{F}_{2}^{n+m}$ to $\mathbb{F}_{2}^{n+m}$ which maps $(x \| y)$ to $(f(x) \| g(y))$. Moreover, we should mentioned that the space $\mathbb{F}_{2}^{n m}$ will be often identified with $\left(\mathbb{F}_{2}^{n}\right)^{m}$ by gathering the bits in $m$ bundles of $n$ components.

Now, let us recall basic properties on linear algebra. For a complete introduction, the reader should refer to the work of Lang [68]. The dot product of two vectors $x$ and $y$ in $\mathbb{F}_{2}^{n}$, denoted by $\langle x, y\rangle$, is defined by the rule

$$
\langle x, y\rangle=x \times y^{\top}=y \times x^{\top}=\sum_{i=0}^{n-1} x_{i} y_{i}
$$

## Chapter 1 - Substitution-Permutation Networks

where $x^{\top}$ denotes the transpose of $x$. It is well-known that the dot product is a bilinear form, namely for all $x, y, z$ in $\mathbb{F}_{2}^{n}$ and all $\lambda$ in $\mathbb{F}_{2}$, it holds that

$$
\langle x+y, z\rangle=\langle x, z\rangle+\langle y, z\rangle, \quad\langle x, y+z\rangle=\langle x, y\rangle+\langle x, z\rangle, \quad\langle\lambda x, y\rangle=\langle x, \lambda y\rangle=\lambda\langle x, y\rangle .
$$

In addition, the dot product satisfies the followings two properties:

- (symmetric) for every $x$ and $y$ in $\mathbb{F}_{2}^{n},\langle x, y\rangle=\langle y, x\rangle$.
- (non-degenerate) for any $x$ in $\mathbb{F}_{2}^{n}$, if $\langle x, y\rangle=0$ for all $y$ in $\mathbb{F}_{2}^{n}$, then $x=0$.

If $E$ is a subset of $\mathbb{F}_{2}^{n}$, we denote by $E^{\perp}$ the set of all elements $x$ in $\mathbb{F}_{2}^{n}$ which are perpendicular to all elements of $E$ with respect to the dot product, that is to say,

$$
E^{\perp}=\left\{x \in \mathbb{F}_{2}^{n} \mid \forall y \in E,\langle x, y\rangle=0\right\} .
$$

It is easily seen from the properties of the dot product that $E^{\perp}$ is a subspace of $\mathbb{F}_{2}^{n}$. Therefore, $E^{\perp}$ is called the orthogonal space of $E$. Moreover, $E^{\perp}=\operatorname{span}(E)^{\perp}$.

Definition 1.1 (Transpose). Let $L: \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{m}$ be a linear mapping. There exists a unique mapping $L^{\top}: \mathbb{F}_{2}^{m} \rightarrow \mathbb{F}_{2}^{n}$, called the transpose of $L$, such that

$$
\langle L(x), y\rangle=\left\langle x, L^{\top}(y)\right\rangle
$$

for all $x$ in $\mathbb{F}_{2}^{n}$ and all $y$ in $\mathbb{F}_{2}^{m}$. Furthermore, if $A$ is the $n \times m$ matrix in $\mathbb{F}_{2}$ satisfying $L(x)=x \times A$, then $L^{\top}$ is given by $L^{\top}(y)=y \times A^{\top}$.

Proof. First, observe that for all elements $x$ and $y$ of $\mathbb{F}_{2}^{n}$ and $\mathbb{F}_{2}^{m}$, we have

$$
\langle L(x), y\rangle=L(x) \times y^{\top}=x \times A \times y^{\top}=x \times\left(y \times A^{\top}\right)^{\top}=\left\langle x, L^{\top}(y)\right\rangle .
$$

It remains to prove the uniqueness of this mapping. Suppose that $L^{\prime}$ and $L^{\prime \prime}$ are two mappings from $\mathbb{F}_{2}^{m}$ to $\mathbb{F}_{2}^{n}$ satisfying the required property. Let $x$ and $y$ be elements of $\mathbb{F}_{2}^{n}$ and $\mathbb{F}_{2}^{m}$. By assumption, it follows that $\left\langle x, L^{\prime}(y)\right\rangle=\left\langle x, L^{\prime \prime}(y)\right\rangle$, or equivalently, $\left\langle x, L^{\prime}(y)+L^{\prime \prime}(y)\right\rangle=0$ because of the bilinearity of the dot product. Therefore, $L^{\prime}(y)+L^{\prime \prime}(y)=0$ as this equality holds for all $x$ in $\mathbb{F}_{2}^{n}$ and as the dot product is non-degenerate. Consequently, $L^{\prime}(y)=L^{\prime \prime}(y)$ as desired.

Proposition 1.2. Let $L: \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{m}$ be a linear mapping. The kernel of $L^{\top}$ is the orthogonal space of the image of $L$, that is $\operatorname{Ker}\left(L^{\top}\right)=\operatorname{Im}(L)^{\perp}$.

Proof. By definition, the kernel of $L^{\top}$ is the set of elements of $\mathbb{F}_{2}^{m}$ mapped to $0_{n}$ by $L^{\top}$. If $y$ lies in $\mathbb{F}_{2}^{m}$, then $L^{\top}(y)=0$ if and only if $\left\langle x, L^{\top}(y)\right\rangle=0$ for every $x$ in $\mathbb{F}_{2}^{n}$ since the dot product is non-degenerate. Next,

$$
\begin{aligned}
\operatorname{Ker}\left(L^{\top}\right) & =\left\{y \in \mathbb{F}_{2}^{m} \mid \forall x \in \mathbb{F}_{2}^{n},\left\langle x, L^{\top}(y)\right\rangle=0\right\}=\left\{y \in \mathbb{F}_{2}^{m} \mid \forall x \in \mathbb{F}_{2}^{n},\langle L(x), y\rangle=0\right\} \\
& =\left\{y \in \mathbb{F}_{2}^{m} \mid \forall x \in \operatorname{Im}(L),\langle x, y\rangle=0\right\}=\operatorname{Im}(L)^{\perp} .
\end{aligned}
$$

The result is proven.

### 1.2. Substitution-Permutation Networks

Cryptology is the science of secrets. It aims at enabling two parties, called Alice and Bob, to communicate over an insecure channel. A channel can be any medium of communication, for instance a telephone line or a computer network. It is said insecure whenever a third party can intercept or modify the sent messages. Cryptology is divided into two complementary parts. On the one hand, cryptography gathers the methods to protect the information. Naturally, this includes confidentiality which ensures that an adversary intercepting the messages cannot gain information about the content of the communication. However, cryptography is equally interested in integrity (ensuring that the message you received was the message sent) and authenticity (ensuring the source of the messages). On the other hand, cryptanalysis intends to break the security provided by cryptography.

Confidentiality is provided using an encryption algorithm. In symmetric-key cryptography, Alice and Bob must share a secret key before they can communicate over an insecure channel. Assume that Alice wants to communicate with Bob. The message she wants to send is called the plaintext. Then, using the secret key, Alice encrypts the message. The resulting data is called the ciphertext and should conceal any information about the plaintext. Next, Alice sends the ciphertext to Bob. The latter can decrypt this ciphertext using the same secret key and hence recover the original message.

Symmetric-key encryption algorithms are divided into block ciphers and stream ciphers. In this thesis, we consider only block ciphers, for an overview of stream ciphers the reader can consult [77] for instance. A block cipher is an encryption algorithm processing fixed length blocks of data using a secret key, called the cipher key [39]. We introduce now its formal definition.

Definition 1.3 (Block Cipher). Let $n$ and $\kappa$ be positive integers. A block cipher is a mapping $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ that takes a $\kappa$-bit cipher key $K$ and an $n$-bit plaintext $p$ and returns the $n$-bit corresponding ciphertext $c=E(K, p)$.
Furthermore, for each cipher key $K$ in $\mathbb{F}_{2}^{\kappa}$, the mapping $E_{K}: p \mapsto E(k, p)$ is required to be a permutation of $\mathbb{F}_{2}^{n}$.

The integer $n$ is the block size of the cipher and $\kappa$ it its key length. The mapping $E_{K}$ is the encryption function associated with the cipher key $K$. Its inverse mapping is the decryption function and is denoted by $D_{K}$. It is worth observing that each encryption function $E_{K}$ must be bijective to enable decryption. Indeed, assuming that $E_{K}$ in not injective, there exist two different plaintexts $p$ and $p^{\prime}$ such that $c=E_{K}(p)=E_{K}\left(p^{\prime}\right)$. Then, the receiver who wants to decrypt $c$ cannot decide whether the corresponding plaintext is $p$ or $p^{\prime}$. Moreover, the mapping $E_{K}$ is either bijective or not injective because $\mathbb{F}_{2}^{n}$ is a finite set, justifying the definition.

A block cipher on its own cannot be used to encrypt any message. In fact, it processes only fixed length messages by definition. Generally the block size $n$ ranges between 64 and 128. In order to encrypt long messages whose lengths are not

## Chapter 1 - Substitution-Permutation Networks



Figure 1.1: Representation of an iterative block cipher (see Definition 1.4).
necessarily a multiple of the block size, we must specify how this primitive is used. These specifications are called modes of operation of a block cipher. Informally, a mode of operation splits the message into several $n$-bit blocks. Then, these blocks are linked together and encrypted using the block cipher. The first standardization of modes of operation was in [84, originally for the Data Encryption Standard (DES [83]). In this publication, four modes were presented called ECB, CBC, CFB and OFB. After the publication of the next standard of block ciphers, namely the Advanced Encryption Standard (AES [85]), another standardization was published by the National Institute of Standards and Technology in [86].

Block ciphers come in all shapes and sizes. Let us now introduce an important class which includes almost all modern block ciphers.

Definition 1.4 (Iterative Block Cipher). A block cipher $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n}$ is said to be an $r$-round iterative block cipher if it consists of the following two mappings.

- An algorithm called the key schedule which processes the cipher key $K$ in $\mathbb{F}_{2}^{\kappa}$ and produces $r$ round keys $k^{[0]}, \ldots, k^{[r-1]}$ in $\mathbb{F}_{2}^{l}$.
- A mapping $F: \mathbb{F}_{2}^{l} \times \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ called the round function, such that for any cipher key $K$, the encryption function can be written as

$$
E_{K}=F_{k[r-1]} \circ \cdots \circ F_{k[0]} .
$$

Remark 1.5. The integer $l$ is called the round key length. For a significant proportion of iterative block ciphers, the round key length is equal to the block size. The mapping $F_{k}$ from $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{n}$ which maps a block $x$ to $F(k, x)$ is called the round function associated with the round key $k$. Naturally, each mapping $F_{k}$ must be a permutation of $\mathbb{F}_{2}^{n}$. A diagrammatic representation of an iterative block cipher is given in Figure 1.1.


Figure 1.2: The round functions of iterative block ciphers, key-alternating block ciphers and SPNs (Definitions 1.4, 1.6 and 1.10).

Definition 1.6 (Key-Alternating Cipher). A key-alternating block cipher is an iterative block cipher such that

- the round key length is equal to the block size $n$,
- there exists an unkeyed permutation $F^{\prime}$ of $\mathbb{F}_{2}^{n}$ such that each round function $F_{k}$ maps a block $x$ to $F^{\prime}(x+k)$.

The round function of a key-alternating cipher is illustrated in Figure 1.2. As said in [40], a key-alternating cipher consists of an alternating sequence of unkeyed rounds and simple bitwise key additions. Indeed, when considering two elements of $\mathbb{F}_{2}^{n}$, their addition corresponds to the addition in the vector space $\mathbb{F}_{2}^{n}$, namely a bitwise addition in $\mathbb{F}_{2}$. Moreover, the addition in the finite field $\mathbb{F}_{2}$ is just an exclusive or (XOR). Consequently, this operation is often denoted by the symbol $\oplus$ in cryptography. However, since we will consider direct sums of vector spaces, we denote the sum in $\mathbb{F}_{2}^{n}$ by the symbol + to avoid confusion.

Remark 1.7. It should be mentioned that in the encryption process of a keyalternating block cipher, a round key is added after the last round. According to Kerckhoffs' Principle [59], the attacker knows every detail of the encryption, except of course the secret key. Therefore, if the encryption ends with the unkeyed permutation $F^{\prime}$, the attacker can undo this step. To save useless processing, the last step must be unknown to the cryptanalyst. Summarizing, the key schedule of an $r$-round key-alternating cipher derives $r+1$ round keys $k^{[0]}, \ldots, k^{[r]}$ in $\mathbb{F}_{2}^{n}$ from a cipher key $K$ in $\mathbb{F}_{2}^{\kappa}$ and the last key $k^{[r]}$ is added at the end of the encryption.

Denote by $\alpha_{k}$ the permutation of $\mathbb{F}_{2}^{n}$ which maps $x$ to $x+k$, that is to say $\alpha_{k}$ represents the addition of the round key $k$. Assume that $k^{[0]}, \ldots, k^{[r]}$ are the round keys derived from a cipher key $K$. Then, the encryption function is given by

$$
E_{k}=\alpha_{k[r]} \circ \underbrace{F^{\prime} \circ \alpha_{k[r-1]}}_{F_{k}[r-1]} \circ \cdots \circ \underbrace{F^{\prime} \circ \alpha_{k[0]}}_{F_{k[0]}}
$$

Closely related to key-alternating block ciphers is the concept of long-key cipher introduced by Daemen and Rijmen in [40].

Definition 1.8 (Long-Key Cipher). A long-key cipher is a key-alternating cipher with a trivial key schedule. The cipher key consists of the concatenation of the $r+1$ round keys, and hence is $n(r+1)$-bit long.

Certainly, long-key ciphers are not used in practice as they require too long cipher keys. They are used only to study key-alternating ciphers. By the long-key cipher associated with a key-alternating cipher, we mean the cipher obtained when we ignore its key schedule and consider independent round keys.

In his seminal paper in 1949 [91, Shannon introduced the main design principles used nowadays in block ciphers, namely confusion and diffusion. To quote Shannon, "The method of confusion is to make the relation between the simple statistics of the ciphertext and the simple description of the key a very complex and involved one" and "in the method of diffusion the statistical structure of the plaintext which leads to its redundancy is dissipated into long range statistics in the ciphertext". These concepts can be interpreted in several ways, a nice adaptation is due to Massey [73]:

Confusion: The ciphertext statistics should depend on the plaintext statistics in a manner too complicated to be exploited by the cryptanalyst.
Diffusion: Each digit of the plaintext and each digit of the secret key should influence many digits of the ciphertext.

A class of key-alternating block ciphers directly inspired by Shannon's work is the Substitution Permutation Networks (shorten as SPN). The round function of an SPN consists of three distinct stages: a key addition, a substitution layer and a permutation or diffusion layer. The key addition includes unknown material to the cryptanalyst, the substitution and diffusion layers provide respectively confusion and diffusion. One of the building blocks of any SPN is called a Substitution-box or simply an $S$-box.

Definition 1.9 (S-Box). An $n$-bit S-box is a mapping form $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{n}$. In this thesis, we require an S-box to be a permutation of $\mathbb{F}_{2}^{n}$.

In the substitution layer, the $n m$-bit data block is seen as $m$ bundles of $n$ bits. Then, $m$ S-boxes are evaluated in parallel on each bundle of the block. For this reason, the substitution layer is said to be a bricklayer function [39]. On the other hand, the diffusion layer consists of the evaluation of some linear mappings (generally one) but processes the data block as a whole since it is intended to provide diffusion.

Definition 1.10 (SPN). Let $m$ and $n$ be positive integers and let $S_{0}, \ldots, S_{m-1}$ be $n$-bit S-boxes.

- The substitution layer is denoted by $\sigma$ and maps $\left(x_{i}\right)_{0 \leq i<m}$ to $\left(S_{i}\left(x_{i}\right)\right)_{0 \leq i<m}$.
- The diffusion layer is a linear permutation denoted by $\pi: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$.

A Substitution-Permutation Network is a key-alternating block cipher such that the unkeyed round function $F^{\prime}$ is equal to $\pi \circ \sigma$.

Denoting by $k^{[0]}, \ldots, k^{[r]}$ the round keys derived from a cipher key $K$, the
encryption function of an SPN is hence defined to be

$$
E_{K}=\alpha_{k[r]} \circ \underbrace{\pi \circ \sigma \circ \alpha_{k[r-1]}}_{F_{k}[r-1]} \circ \cdots \circ \underbrace{\pi \circ \sigma \circ \alpha_{k[0]}}_{F_{k}[0]} .
$$

A comparison between the round function of an iterative cipher, a key-alternating cipher and an SPN is illustrated in Figure 1.2. It is worthwhile to note that the substitution layer is the only step which is not linear or affine. In order to make the cipher secure, the S-boxes must be highly nonlinear. The exact meaning of this statement will be detailed in Section 1.5.1.

Remark 1.11. We should mention that the last round of an SPN may not include the diffusion layer, see for instance the AES. Indeed, for all $k$ and $x$ in $\mathbb{F}_{2}^{n m}$ we have

$$
\alpha_{k} \circ \pi(x)=k+\pi(x)=\pi\left(\pi^{-1}(k)\right)+\pi(x)=\pi\left(\pi^{-1}(k)+x\right)=\pi \circ \alpha_{\pi^{-1}(k)}(x) .
$$

Thus, using an equivalent last-round key, the encryption process ends with a permutation known by the cryptanalyst. As a consequence, the diffusion layer in the last round does not offer any additional security and is often removed for efficiency purposes.

Before concluding this section with an example of SPN, we introduce a class of diffusion layers particularly used in lightweight block ciphers.

Definition 1.12 (bit permutation). A linear mapping $\pi: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ is said to be a bit permutation if there exists a permutation $\phi$ of $\llbracket 0, n m \llbracket$ such that

$$
\pi\left(x_{0}, \ldots, x_{n m-1}\right)=\left(x_{\phi^{-1}(0)}, \ldots, x_{\phi^{-1}(n m-1)}\right) .
$$

Remark 1.13. Despite appearances, using $\phi^{-1}$ on the indices is natural. The bit with index $i$ is mapped to the index $\phi(i)$. Equivalently, the bit mapped to the index $i$ was originally at the index $\phi^{-1}(i)$.
Example 1.14. Let us introduce a 5 -round SPN, called ToyCipher, which encrypts a 16 -bit block using a 16 -bit cipher key. Thus, for this cipher $r=5$ and $n m=\kappa=16$. The substitution layer $\sigma$ evaluates in parallel one 4 -bit S-box denoted by $S$. This S-box is given in hexadecimal notation at the bottom of Figure 1.3. For instance, $S$ maps 2 to D or equivalently $S(0010)=1101$. Similarly,

$$
\sigma(2, \mathrm{~F}, \mathrm{~F}, 1)=(S(2), S(\mathrm{~F}), S(\mathrm{~F}), S(1))=(\mathrm{D}, 6,6,3)
$$

The diffusion layer $\pi$ is the bit permutation associated with the permutation $\phi$ of $\llbracket 0,16 \llbracket$ defined by the formula

$$
\phi(i)=4(i \bmod 4)+\left\lfloor\frac{i}{4}\right\rfloor .
$$

This bit permutation is drawn from the block cipher Present [17] and its small scale variants Small-Present [69]. For instance $\phi(0)=0, \phi(1)=4, \phi(2)=8, \phi(3)=12$, $\phi(4)=1$ and

$$
\begin{aligned}
& =\left(\begin{array}{lllllllllllllllll}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1
\end{array}\right)=8 \mathrm{E} 79 .
\end{aligned}
$$

Chapter 1 - Substitution-Permutation Networks


Figure 1.3: The encryption algorithm ToyCipher.

| Key Schedule |  | Message encryption |  |
| :---: | :---: | :---: | :---: |
|  |  | $0000000000000000=0000$ | Plaintext |
| $\begin{aligned} & k^{[0]} \\ & S / \oplus 1 \end{aligned}$ | $0000000000000000=0000 \rightarrow$ | $0000000000000000=0000$ | After $\oplus k^{[0]}$ |
|  | $0111000100000000=7100$ | $0111011101110111=7777$ | After $\sigma$ |
|  |  | $0000111111111111=0 \mathrm{FFF}$ | After $\pi$ |
| $k^{[1]}$ | $0010000000001110=200 \mathrm{E} \rightarrow$ | $0010111111110001=2 \mathrm{FF} 1$ | After $\oplus k^{[1]}$ |
| $S / \oplus 2$ | 1101001000001110 = D20E | 1101011001100011 = D663 | After $\sigma$ |
|  |  | 1000111001111001 = 8E79 | After $\pi$ |
| $k^{[2]}$ | $0100000111011010=41 \mathrm{DA} \rightarrow$ | 1100111110100011 = CFA3 | After $\oplus k^{[2]}$ |
| $S / \oplus 3$ | 1100001011011010 = C2DA | 1110011000011001 = E619 | After $\sigma$ |
|  |  | 1001110011000011 = 9CC3 | After $\pi$ |
| $k^{[3]}$ | $0101101101011000=5 \mathrm{~B} 58 \rightarrow$ | $1100011110011011=$ C79B | After $\oplus k^{[3]}$ |
| $S / \oplus 4$ | $0010111101011000=2 \mathrm{~F} 58$ | $1110100010110000=$ E8BO | After $\sigma$ |
|  |  | $1110100010100010=$ E8A2 | After $\pi$ |
| $k^{[4]}$ | $1110101100000101=$ EBO5 $\rightarrow$ | $0000001110100111=0347$ | After $\oplus k^{[4]}$ |
| $S / \oplus 5$ | $0101111000000101=5 \mathrm{E} 05$ | $0111100100011000=7918$ | After $\sigma$ |
| $k^{[5]}$ | $1100000010101011=$ COAB $\rightarrow$ | 1011100110110011 = B9B3 | Ciphertext |

Figure 1.4: Encryption of 0000 with ToyCipher using the cipher key $K=0000$.

The round function $F_{k}$ consists of an addition with $k$, a substitution layer then a diffusion layer. With $k=200 \mathrm{E}$ and $x=0 \mathrm{FFF}$, we have

$$
F_{k}(x)=\pi \circ \sigma(0 \mathrm{FFF}+200 \mathrm{E})=\pi \circ \sigma(2 \mathrm{FF} 1)=\pi(\mathrm{D} 663)=8 \mathrm{E} 79 .
$$

As explained in Remark 1.11, the last round does not have a diffusion layer. An illustration of the whole encryption of ToyCipher function is given in Figure 1.3.

The key schedule derives 6 round keys $k^{[0]}, \ldots, k^{[5]}$ from the cipher key $K$. The first round key $k^{[0]}$ is equal to the cipher key $K$. To compute the round key $k^{[i+1]}$ form $k^{[i]}$, apply the S-box $S$ to the first bundle and add a round constant $r_{i}$ to the next bundle. The constant $r_{i}$ is just the binary decomposition of the integer $i+1$. Then rotate by 5 bit positions to the left all the bits to obtain $k^{[i+1]}$. In Figure 1.4, we describe step by step the whole encryption process of the plaintext block 0000 using the cipher key 0000.

### 1.3. Differential Cryptanalysis

One of the most important and powerful [39, 64] attacks against block ciphers is differential cryptanalysis, proposed by Biham and Shamir in [13, 14]. A formalization of this attack was then proposed by Lai, Massey and Murphy in [67]. Differential cryptanalysis is a chosen plaintext attack which requires the encryption of pairs of plaintexts that have a fixed difference. Then, the attack exploits a non-uniform distribution of the differences between pairs of outputs to recover partial information on the last-round key of the cipher. This section is organized as follows. First we

## Chapter 1 - Substitution-Permutation Networks

give the main idea of the attack and illustrate it with an example. Then, we explore the theoretical framework of this attack in Section 1.3.2

### 1.3.1. General Idea of the Attack

The difference between two elements $x$ and $x^{*}$ of $\mathbb{F}_{2}^{n}$ is defined to be $x-x^{*}$ but since each element is its own additive inverse in $\mathbb{F}_{2}^{n}$, it is simply equal to $x+x^{*}$. The main property used in differential cryptanalysis is that for every round key $k$, we have

$$
\begin{equation*}
(x+k)+\left(x^{*}+k\right)=x+x^{*} . \tag{1.1}
\end{equation*}
$$

In other words, the difference between $x$ and $x^{*}$ is invariant under the round key addition.

A successful differential cryptanalysis relies on the existence of a differential holding with high probability, which we define now. Let $f$ be a mapping from $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{n}$. A differential over $f$ is a pair $(a, b)$ of elements of $\mathbb{F}_{2}^{n}$. Given a differential $(a, b)$, the elements $a$ and $b$ are called the input and output difference patterns respectively. Then, a differential ( $a, b$ ) predicts that when two inputs $x$ and $x^{*}$ have difference $a$, then their images $f(x)$ and $f\left(x^{*}\right)$ have difference $b$ with a certain probability. It is easily seen that $x$ and $x^{*}$ have difference $a$ if and only if $x^{*}=x+a$. Equivalently, a differential $(a, b)$ predicts that when $x$ is uniformly distributed over $\mathbb{F}_{2}^{n}$, the value $f(x)+f(x+a)$ is equal to $b$ with a certain probability. This probability is naturally defined as follows.

Definition 1.15 (Differential Probability). Let $f: \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ be a mapping. The differential probability of $(a, b)$ over $f$ is denoted by $\mathrm{DP}_{f}(a, b)$ and defined to be

$$
\operatorname{DP}_{f}(a, b)=\frac{\#\left\{x \in \mathbb{F}_{2}^{n} \mid f(x)+f(x+a)=b\right\}}{2^{n}}
$$

Consider an $r$-round substitution permutation network $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ and assume that the last round does not have a diffusion layer. Given a cipher key $K$, we denote by $E_{K}^{(r-1)}$ the $r-1$ first rounds of the encryption function $E_{K}$. Therefore

$$
E_{K}^{(r-1)}=F_{k[r-2]} \circ \cdots \circ F_{k[0]} \quad \text { and hence } \quad E_{K}=\left(\alpha_{k[r]} \circ \sigma \circ \alpha_{k[r-1]}\right) \circ E_{K}^{(r-1)} .
$$

In a classical differential cryptanalysis of $E$, we do not use a differential over the $r$-round encryption function $E_{K}$, but on the ( $r-1$ )-round encryption $E_{K}^{(r-1)}$. Then, a differential $(a, b)$ over $r-1$ rounds can be exploited in a differential cryptanalysis when its average probability over all the cipher keys is large enough.

The main idea of the attack is the following. Assume that $(a, b)$ is an $(r-1)$-round differential which holds with probability $q$ for a significant proportion of the cipher keys. Let $K$ be the unknown cipher key. First, generate pairs $(p, p+a)$ of plaintexts and require their encryption under the cipher key $K$. The pairs obtained are denoted by $\left(c, c^{*}\right)$. In order to have some pairs $\left(c, c^{*}\right)$ satisfying $c+c^{*}=b$, we may use $C \times q^{-1}$ plaintext pairs with $C \geq 5$. Assume that $k$ is a candidate for the last-round key $k^{[r]}$.

Then we decrypt the last round of each pair $\left(c, c^{*}\right)$ using the candidate $k$ and we denote

$$
y=\sigma^{-1}(c+k) \quad \text { and } \quad y^{*}=\sigma^{-1}\left(c^{*}+k\right) .
$$

If the candidate key $k$ is the right key, then the equation $y+y^{*}=b$ should hold with probability $q$ since $(a, b)$ is an $(r-1)$-round differential. Otherwise, when $k$ is a wrong candidate, we hope that the equation $y+y^{*}=b$ holds with probability significantly less than $q$. This assumption is known as the hypothesis of wrong-key randomization [51. Indeed, it seems natural to think that the $(r+1)$-round differential $(a, b)$ holds with probability less than the $(r-1)$-round differential $(a, b)$, and when $k$ is a wrong key, the pair $\left(y, y^{*}\right)$ is equivalent to an $(r+1)$-round encryption of $(p, p+a)$.

To recover information on the last-round key, we may proceed as follows. For each candidate $k$ for the last-round key, decrypt the last round for each pair ( $c, c^{*}$ ) and save the number $N_{k}$ of pairs $\left(y, y^{*}\right)$ such that $y+y^{*}=b$. Then the key $k$ maximizing the value $N_{k}$ should be equal to the last-round key $k^{[r]}$. As will be seen in the next example, we only decrypt partially the last round in an effective cryptanalysis, and thus we recover a few bits of the last-round key.
Example 1.16. Let us now present a differential cryptanalysis of our SPN ToyCipher introduced in Example 1.14. Since this cipher consists of five rounds, we must first find a 4 -round differential holding with high probability. Finding such a differential is generally not easy because the vast majority of the differentials are useless in a differential cryptanalysis. For instance, the 4 -round differential ( $a, b$ ) with

$$
a=(0,8,0,0) \quad \text { and } \quad b=(0,0,7,0)
$$

has an average probability over the cipher keys equal to $1.22 \times 2^{-16}$. This value was computed via an exhaustive search, which is possible thanks to the small block size and key length of this cipher. A differential cryptanalysis based on this differential would require the encryption of more than $2^{16}$ different pairs of plaintexts $(x, x+a)$. However, there are only $2^{16}$ such pairs since there are $2^{16}$ different blocks.

We will explain in the next section and in Chapter 2 how to find high probability differentials, in this example we explain how such a differential can be used to recover key information. Consider the 4 -round differential $(a, b)$ where

$$
a=b=(0,4,0,0)
$$

The average probability of this differential over all the cipher keys is

$$
\frac{1}{2^{16}} \sum_{K \in \mathbb{F}_{2}^{16}} \mathrm{DP}_{E_{K}}(4)(0400,0400) \approx \frac{2688.2}{2^{16}} \approx 1.31 \times 2^{-5}
$$

The repartition of all the differential probabilities $\mathrm{DP}_{E_{K^{(4)}}}(0400,0400)$ is illustrated at the top of Figure 1.5. For instance, there are 1298 cipher keys $K$ such that

$$
\frac{2624}{2^{16}}<\mathrm{DP}_{E_{K^{(4)}}}(0400,0400) \leq \frac{2656}{2^{16}}
$$

Moreover, this differential holds with probability greater than $2^{-5}$ for $85 \%$ of the cipher keys. In view of these results, the differential $(a, b)$ holds with high probability

## Chapter 1 - Substitution-Permutation Networks

## Initialisation: Find a High Probability 4-Round Differential



Part 1: Get Plaintext/Ciphertext Pairs
Choose $N$ plaintext pairs $\left(p, p^{*}\right)$ such that $p+p^{*}=0400$ and request the corresponding ciphertext pairs $\left(c, c^{*}\right)$ encrypted under the unknown cipher key $K$.


Part 2: Recover Some Bits of the Last Round Key
For each candidate $\tilde{k}_{1}{ }^{[5]}$, decrypt partially the last round of the pairs $\left(c, c^{*}\right)$ such that $c_{i}=c_{i}^{*}$ for all $i$ in $\{0,2,3\}$ and $c_{1}+c_{1}^{*}$ lies in $\{1,4,6,9, \mathrm{~B}\}$. The key $\tilde{k}_{1}{ }^{[5]}$ maximizing the number of pairs $\left(y_{1}, y_{1}^{*}\right)$ satisfying $y_{1}+y_{1}^{*}=4$ should be equal to $k_{1}{ }^{[5]}$.


Figure 1.5: A differential cryptanalysis of ToyCipher.
(compared to $2^{-16}$ ) for a significant proportion of the cipher keys and can hence be used in a differential cryptanalysis.

As explained before, a differential cryptanalysis requires the encryption of $C \times q^{-1}$ pairs of plaintexts where $q$ is the average probability of the 4 -round differential. With $C=5$, this amounts to

$$
N=5 \times \frac{2^{16}}{2688.2} \approx 122 \approx 2^{7}
$$

pairs of chosen plaintexts. To generate these pairs, choose $N$ random plaintexts $p$ and form the pairs $(p, p+0400)$. Thus, all the bits of $p$ and $p^{*}=p+0400$ are equal except the bit with index 5 , starting from 0 . Let $K$ be the unknown cipher key and request for the encryption of all these pairs. Then, we obtain $N$ pairs $\left(c, c^{*}\right)$ such that

$$
c=E_{K}(p) \quad \text { and } \quad c^{*}=E_{K}(p+0400) .
$$

Let $\left(p, p^{*}\right)$ be one of these pairs and denote by $\left(x, x^{*}\right)$ its 4 -round encryption, that is $x=E_{K^{(4)}}(p)$ and $x^{*}=E_{K^{(4)}}\left(p^{*}\right)$. The following reasoning is illustrated in Part 1 of Figure 1.5. Assume that $x+x^{*}=0400$. Such a pair is called a right pair, or equivalently we say that ( $p, p^{*}$ ) follows the differential $(a, b)$. By extension, its corresponding ciphertext pair $\left(c, c^{*}\right)$ is also said to be a right pair. Adding the next round key, the pair ( $x, x^{*}$ ) becomes

$$
\left(y, y^{*}\right)=\left(x+k^{[4]}, x^{*}+k^{[4]}\right) .
$$

By assumption and according to Equation (1.1), the difference between $y$ and $y^{*}$ remains unchanged and is equal to 0400 . We must now understand how this difference propagates through the substitution layer. First, note that

$$
y_{0}=y_{0}^{*}, \quad y_{1}=y_{1}^{*}+4, \quad y_{2}=y_{2}^{*}, \quad y_{3}=y_{3}^{*} .
$$

Denote by $z$ and $z^{*}$ the images of $y$ and $y^{*}$ under $\sigma$. It goes without saying that for each $i$ in $\{0,2,3\}$, we have $z_{i}=z_{i}^{*}$ and hence $z_{i}+z_{i}^{*}=0$. It remains to explain what are the possible values for the difference $z_{1}+z_{1}^{*}$. This is done by computing the values $z_{1}+z_{1}^{*}$ for all possible $y_{1}$ and $y_{1}^{*}=y_{1}+4$ in $\mathbb{F}_{2}^{4}$ :

$$
\begin{array}{ll}
S(0)+S(4)=S(4)+S(0)=\mathrm{C}+7=\mathrm{B}, & S(8)+S(\mathrm{C})=S(\mathrm{C})+S(8)=\mathrm{E}+\mathrm{A}=4, \\
S(1)+S(5)=S(5)+S(1)=2+3=1, & S(9)+S(\mathrm{D})=S(\mathrm{D})+S(9)=\mathrm{F}+\mathrm{B}=4, \\
S(2)+S(6)=S(6)+S(2)=4+\mathrm{D}=9, & S(\mathrm{~A})+S(\mathrm{E})=S(\mathrm{E})+S(\mathrm{~A})=5+1=4, \\
S(3)+S(7)=S(7)+S(3)=8+9=1, & S(\mathrm{~B})+S(\mathrm{~F})=S(\mathrm{~F})+S(\mathrm{~B})=6+0=6 .
\end{array}
$$

Therefore, the difference $z_{1}+z_{1}^{*}$ lies in the set $\{1,4,6,9, \mathrm{~B}\}$. Finally, $c$ and $c^{*}$ are obtained by adding the last-round key $k^{[5]}$ to $z$ and $z^{*}$ respectively, so $c+c^{*}=z+z^{*}$. To summarize, we have proven that if $\left(p, p^{*}\right)$ is a right pair, then

$$
\begin{equation*}
c_{0}+c_{0}^{*}=c_{2}+c_{2}^{*}=c_{3}+c_{3}^{*}=0, \quad \text { and } \quad c_{1}+c_{1}^{*} \in\{1,4,6,9, \mathrm{~B}\} . \tag{1.2}
\end{equation*}
$$

To recover information on the last-round key, we must count for each candidate key $k$ the number of pairs $\left(c, c^{*}\right)$ satisfying the equation

$$
\sigma^{-1}(c+k)+\sigma^{-1}\left(c^{*}+k\right)=0400
$$

## Chapter 1 - Substitution-Permutation Networks



Figure 1.6: A differential cryptanalysis of ToyCipher.

According to the preceding discussion, if a pair ( $c, c^{*}$ ) does not satisfy (1.2), then this pair is necessarily a wrong pair. To avoid useless computing, we apply a filtering process which discards the wrong pairs and we denote by $\mathcal{F}$ the set of the filtered pairs. Let $k$ be a candidate key and let $i$ be a bundle index in $\{0,2,3\}$. For each filtered pair $\left(c, c^{*}\right)$, we have

$$
c_{i}=c_{i}^{*} \quad \text { and hence } S^{-1}\left(c_{i}+k_{i}\right)+S^{-1}\left(c_{i}^{*}+k_{i}\right)=0 .
$$

Therefore, this differential gives no information on $k_{i}{ }^{[5]}$ for each $i$ in $\{0,2,3\}$, so we can only recover information on $k_{1}{ }^{[5]}$. This is good news because we would otherwise have to decrypt the last round for all of the $2^{16}$ possible round keys, yielding a complexity greater than the brute force. Finally, the cryptanalysis ends as follows. For each $k_{1}$ in $\mathbb{F}_{2}^{4}$, compute its score

$$
N_{k_{1}}=\#\left\{\left(c, c^{*}\right) \in \mathcal{F} \mid S^{-1}\left(c_{1}+k_{1}\right)+S^{-1}\left(c_{1}^{*}+k_{1}\right)=4\right\} .
$$

Then, the higher the score $N_{k_{1}}$ is, the more likely $k_{1}$ is equal to $k_{1}{ }^{[5]}$. This step is illustrated in Part 2 of Figure 1.5. The experimental success probabilities of this differential cryptanalysis with respect to the constant $C$ are given in Figure 1.6. Define the rank of the right key $k_{1}{ }^{[5]}$ to be

$$
\operatorname{Rk}=\#\left\{k_{1} \in \mathbb{F}_{2}^{4} \mid N_{k_{1}} \geq N_{k_{1}[5]}\right\} .
$$

If the rank is equal to 1 , then the cryptanalysis recovers the right bundle within the set $\mathbb{F}_{2}^{4}$, giving four bits of information. When the rank is less than 2 , two choices remain for $k_{1}{ }^{[5]}$ instead of 16 . Thus, we have at least three bits of information. Similarly, we have (at least) two bits of information when $\mathrm{Nk} \geq 4$ and one bit if $\mathrm{Nk} \geq 8$. As can be seen in Figure 1.6, when $C=5$ this attack recovers one bit of information with probability $90.2 \%$, two and three bits with probability $74.7 \%$ and $65.2 \%$, and recovers the exact bundle with probability $50.9 \%$.

### 1.3.2. Differential Trails

Having explained how a high probability differential can be exploited in a cryptanalysis, now is the time to present the theory of differentials. This presentation is inspired by the works of Lai, Massey [67] and Daemen, Rijmen [39, 40]. In this section we consider a generic $r$-round SPN $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ such that for each cipher key $K$,

$$
E_{K}=F_{k[r-1]} \circ \cdots \circ F_{k[0]} \quad \text { with } \quad F_{k[i]}=\pi \circ \sigma \circ \alpha_{k[i]} .
$$

It is worth observing that the last round includes and ends with a diffusion layer. This definition makes sense here because the differentials used in an attack have fewer rounds that the whole cipher. Thus, the SPN considered here should be thought as a reduced-round version of the cipher attacked.

The standard method used to find a high probability differential relies on the study of a difference propagation through the components of the SPN. We have already seen that a difference remains unchanged by a key addition. The next proposition describes how a difference propagates through the substitution and diffusion layers.

Proposition 1.17. Let $a$ and $b$ be two difference patterns in $\mathbb{F}_{2}^{n m}$. Then

$$
\mathrm{DP}_{\sigma}(a, b)=\prod_{i=0}^{m-1} \mathrm{DP}_{S_{i}}\left(a_{i}, b_{i}\right) \quad \text { and } \quad \mathrm{DP}_{\pi}(a, b)= \begin{cases}1 & \text { if } \pi(a)=b \\ 0 & \text { otherwise }\end{cases}
$$

In other words, given an input difference pattern $a$, each S-box $S_{i}$ transforms independently $a_{i}$ to $b_{i}$ with a certain probability and the diffusion layer always maps $a$ to $\pi(a)=b$. Following the idea of propagation of a difference through the encryption process, we introduce the next definition.

Definition 1.18 (Differential Trail). An r-round differential trail is a family $\mathcal{T}=\left(a^{[0]}, \ldots, a^{[r]}\right)$ of $(r+1)$ difference patterns in $\mathbb{F}_{2}^{n m}$. Let $K$ be a cipher key. The fixed-key differential probability of $\mathcal{T}$ is defined to be

$$
\operatorname{DP}_{E_{K}}(\mathcal{T})=\frac{\#\left\{x \in \mathbb{F}_{2}^{n m} \mid \forall 1 \leq i \leq r, E_{K}^{(i)}(x)+E_{K}^{(i)}\left(x+a^{[0]}\right)=a^{[i]}\right\}}{2^{n m}}
$$

Let $\left(x, x^{*}\right)$ be a pair of plaintexts. We should say that $\left(x, x^{*}\right)$ follows the differential trail $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ if

- the difference between $x$ and $x^{*}$ is equal to $a^{[0]}$, and
- for each $1 \leq i \leq r$, the difference between the $i$-round encryptions of $x$ and $x^{*}$ is equal to $a^{[i]}$.

Using this vocabulary, the fixed-key differential probability of $\mathcal{T}$ can equivalently be defined as the probability that a pair chosen uniformly at random follows the trail $\mathcal{T}$ given that its difference is equal to the input pattern $a^{[0]}$. Therefore, the trail $\mathcal{T}$ predicts the evolution of an input difference after each round of the encryption

## Chapter 1 - Substitution-Permutation Networks

process whereas a differential only predicts its output difference. These two concepts are related via the following proposition.

Proposition 1.19. Let $(a, b)$ be an $r$-round differential and let $K$ be a cipher key. Denote by $E_{a, b}$ the set of all trails $\left(a^{[i]}\right)_{i \leq r}$ such that $a^{[0]}=a$ and $a^{[r]}=b$. Then

$$
\mathrm{DP}_{E_{K}}(a, b)=\sum_{\mathcal{T} \in E_{a, b}} \mathrm{DP}_{E_{K}}(\mathcal{T})
$$

This result is in fact quite intuitive since each pair following the differential naturally follows one and only one trail, namely the trail consisting of its intermediate differences. Conversely, a pair following a trail $\left(a^{[i]}\right)_{i \leq r}$ such that $a^{[0]}=a$ and $a^{[r]}=b$ obviously follows the $r$-round differential $(a, b)$. So far we have only considered fixedkey probabilities. However, these results may not describe what can be expected when attacking an unknown cipher key. For this purpose we introduce the next definition.

Definition $1.20(\mathrm{DP}(\mathcal{T}))$. The (expected) differential probability of a trail $\mathcal{T}$, denoted by $\operatorname{DP}(\mathcal{T})$, is the average fixed-key differential probability of $\mathcal{T}$ over the associated long-key cipher.

Recall that the long-key cipher associated with our SPN is the cipher obtained by disregarding the key schedule and considering independent round keys. Explicitly, the differential probability of $\mathcal{T}$ is given by

$$
\operatorname{DP}(\mathcal{T})=\frac{1}{\left(2^{n m}\right)^{r}} \times \sum_{K \in\left(\mathbb{F}_{2}^{n m}\right)^{r}} \operatorname{DP}_{E_{K}}(\mathcal{T})
$$

Remark 1.21. By virtue of Proposition 1.17, a difference can have a nondeterministic transition only during the substitution layer. Given a trail $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$, we denote by $b^{[i]}$ the element $\pi^{-1}\left(a^{[i+1]}\right)$ for each $i<r$. Thus, an $r$-round trail can alternatively be seen as the sequence $\left(\left(a^{[i]}, b^{[i]}\right)\right)_{i<r}$.

Theorem 1.22. Let $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ be a differential trail. The differential probability of $\mathcal{T}$ is given by

$$
\mathrm{DP}(\mathcal{T})=\prod_{i=0}^{r-1} \mathrm{DP}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=\prod_{i=0}^{r-1} \prod_{j=0}^{m-1} \mathrm{DP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right)
$$

where $b^{[i]}=\pi^{-1}\left(a^{[i+1]}\right)$ for each $i<r$.
This theorem has a significant practical impact since the differential probability of a trail can be computed by multiplying a few differential probabilities over the S-boxes. Computing the full differential probability matrix $\mathrm{DP}_{S_{j}}$ of the $n$-bit Sbox $S_{j}$ has complexity $O\left(2^{2 n}\right)$. Since substitution-permutation networks generally have $n$-bit $S$-boxes with $n$ less than or equal to 8 , all these matrices are easily computed. Moreover, the formula of the previous theorem can be simplified further by introducing the notion of active S-boxes.

Definition 1.23 (Active S-Box). Let $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ be a differential trail with a nonzero differential probability. The S-box $S_{j}$ is said to be active at round $i$ if the pattern $a_{j}{ }^{[i]}$ is nonzero, otherwise $S_{j}$ is inactive.

Proposition 1.24. Let $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ be a nonzero probability differential trail. Let $i<r$ and $j \leq m$ be nonnegative integers. Then $a_{j}{ }^{[i]}=0_{n}$ if and only if $b_{j}{ }^{[i]}=0_{n}$. Consequently, Theorem 1.22 can be restated as

$$
\mathrm{DP}(\mathcal{T})=\prod_{i, j \mid a_{j}[i] \neq 0} \operatorname{DP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right)
$$

Proof. To simplify the notation, denote by $a^{\prime}$ and $b^{\prime}$ the patterns $a_{j}{ }^{[i]}$ and $b_{j}{ }^{[i]}$. According to Theorem $1.22, \mathrm{DP}_{S_{j}}\left(a^{\prime}, b^{\prime}\right)$ is nonzero as $\mathrm{DP}(\mathcal{T})$ is nonzero by hypothesis. Because $S_{j}$ is one-to-one, $\operatorname{DP}_{S_{j}}\left(a^{\prime}, 0_{n}\right)$ is nonzero if and only if $a^{\prime}=0_{n}$. Further, $\operatorname{DP}_{S_{j}}\left(0_{n}, b^{\prime}\right)$ is nonzero only when $b^{\prime}=0_{n}$. Finally, observe that $\mathrm{DP}_{S_{j}}\left(0_{n}, 0_{n}\right)=1$. The result follows.

Definition 1.25 (EDP). The expected differential probability of an $r$-round differential $(a, b)$, denoted by $\operatorname{EDP}(a, b)$, is the average fixed-key differential probability of $(a, b)$ over the associated long-key cipher.

Theorem 1.26. Let $(a, b)$ be an $r$-round differential. Denote by $E_{a, b}$ the set of all trails $\left(a^{[i]}\right)_{i \leq r}$ such that $a^{[0]}=a$ and $a^{[r]}=b$. The expected differential probability of $(a, b)$ is given by

$$
\operatorname{EDP}(a, b)=\sum_{\mathcal{T} \in E_{a, b}} \operatorname{DP}(\mathcal{T})
$$

The expected differential probability of a differential is the theoretical value reflecting its usefulness. However, this notion has two downsides. First, the set $E_{a, b}$ generally grows exponentially with the number of rounds and it should be very difficult to enumerate all its trails. Consequently, in real size substitution permutation networks, it is almost impossible to compute an expected differential probability. However, this value can often be approximated using several high probability differential trials.

Secondly, the expected differential probability does not take into account the effect of the key schedule and provides only an average value. Thus, in a cryptanalysis, we tacitly assume that the fixed-key differential probability over the cipher key being attacked is approximately equal to its expected differential probability. This assumption is known as the hypothesis of stochastic equivalence [67].

Example 1.27. In Example 1.16, we have considered the 4-round differential $(a, b)$ with $a=b=0400$. Denote by $\left(x, x^{*}\right)$ the pair $(4100,4500)$ of plaintexts and consider the cipher key $K=0000$. Since $x+x^{*}$ is equal to 0400 , this input pair has the required input difference. Throughout the 4 -round encryption process, this pair is

$\begin{array}{ll}a^{[0]}=(0,4,0,0) & a^{[2]}=(0,1,0,0) \\ b^{[0]}=(0,1,0,0) & b^{[2]}=(0,4,0,0) \\ a^{[1]}=(0,0,0,4) & a^{[3]}=(0,4,0,0) \\ b^{[1]}=(0,0,0,4) & b^{[3]}=(0,4,0,0)\end{array}$

$$
\operatorname{DP}(\mathcal{T})=\frac{4}{16} \times \frac{6}{16} \times \frac{4}{16} \times \frac{6}{16}
$$

$$
=\frac{576}{16^{4}}=1.125 \times 2^{-7}
$$

|  | $2^{4} \times \mathrm{DP}_{S}(a, b)$ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 0 | 16 | . | . | . | . | . | . | . | . | . | . | . | . | . |  |  |
| 1 | . | 6 | . | 2 | 4 | . | . | . | . | . | . |  | 2 | . | 2 | . |
| 2 | . | . | . | . | . | . | . | . | 2 | 2 | 6 | 6 | . |  | . |  |
| 3 | . | . |  |  | 2 |  | 2 | . | 2 | . | 6 | . | . |  | 4 |  |
| 4 | . | 4 | . | . | 6 | . | 2 | . | . | 2 | . | 2 | . |  |  |  |
| 5 | . | . |  | . |  | 10 | . | 2 | . | . | . |  |  | 2 | . | 2 |
| 6 | . | 2 | . | 2 | . | . | . | . | . | . | . | 4 | . | 2 | . | 6 |
| 7 | . | . |  | . |  | 2 | . | 2 | . | . | . |  | 2 | . | 6 | 4 |
| 8 | . | 2 | 2 | . | . | . | . | . | 2 | 2 | . | . | 2 | 4 | 2 | . |
| 9 | . |  | 2 | 2 |  | . |  | - | 2 | 2 | . | . | 4 | 4 | . | . |
| A | . | . | 2 | 2 | 2 | . | 2 | 4 | . | 2 | 2 | . | . | . |  | . |
| B | . |  | 2 | 2 |  |  | 4 | 4 | . | . | 2 | 2 | . |  |  | . |
| C | . | . | . | . | . | 2 | 2 | . | 4 | 4 | . | . | 2 | . | . | 2 |
| D | . |  |  |  | 2 |  |  | 2 | 4 | 2 | . | 2 | 2 | 2 | . | . |
| E | . |  | 4 | 4 | . | 2 | 2 | . | . | . | . | . | . | 2 | 2 | . |
| F |  | 2 | 4 | 2 |  | . | 2 | 2 |  | . |  |  | 2 |  |  | 2 |

Figure 1.7: A differential trail included in the 4-round differential (0400, 0400).
transformed as follows:

|  | $x$ | $x^{*}$ |  | Difference |
| :---: | :---: | :---: | :---: | :---: |
|  | 4100 | 4500 | $\rightarrow$ | 0400 |
| $E_{K}{ }^{(1)}$ : | 8B77 | 8B73 | $\rightarrow$ | 0001 |
| $E_{K}{ }^{(2)}$ : | 3019 | 3119 | $\rightarrow$ | 0100 |
| $E_{K}{ }^{(3)}$ : | B265 | B665 | $\rightarrow$ | 0400 |
| $E_{K}{ }^{(4)}$ : | 795F | 7D5F | $\rightarrow$ | 0400 |

Since the output difference is equal to the output pattern $b$, this pair follows the differential $(a, b)$. More precisely, this pair follows the differential trail $\mathcal{T}=\left(a^{[i]}\right)_{i \leq 4}$ where

$$
a^{[0]}=0400, \quad a^{[1]}=0001, \quad a^{[2]}=0100, \quad a^{[3]}=0400, \quad a^{[4]}=0400 .
$$

This trial is illustrated in Figure 1.7 where $b^{[i]}=\pi^{-1}\left(a^{[i]}\right)$, as suggested by Remark 1.21. The active S-boxes are emphasized. Thus there are only four active S-boxes in this trial, which is the minimum. The differential probability matrix of $S$ is also given in the same figure. As seen in Example 1.16,

$$
S\left(y_{1}\right)+S\left(y_{1}+4\right)=\left\{\begin{array}{lll}
1 & \text { if } y_{1} \in\{1,3,5,7\}, & 9 \\
4 & \text { if } y_{1} \in\{2,6\}, \\
6 & \text { if } y_{1} \in\{8,9, \mathrm{~A}, \mathrm{C}, \mathrm{D}, \mathrm{E}\}, & \text { B } \\
\text { if } y_{1} \in\{0,4\} .
\end{array}\right.
$$

This relation explains the row indexed by 4 of the matrix $\mathrm{DP}_{S}$. By virtue of Corollary 1.24 , it suffices to multiply the probabilities of the active $S$-boxes to find that the (expected) probability of the trail $\mathcal{T}$ is equal to $1.125 \times 2^{-7}$, as shown in Figure 1.7.

It turns out that there are six trails associated with the differential $(a, b)$. These trails are given in Figure 1.8, sorted by differential probability. According to Theorem 1.26 , the expected differential probability of $(a, b)$ is the sum of the differential probabilities of these trails, that is

$$
\operatorname{EDP}(a, b)=\sum_{i=1}^{6} \operatorname{DP}\left(\mathcal{T}_{i}\right)=\frac{346133}{8388608} \approx 1.32 \times 2^{-5} .
$$

Recall that in the preceding example, we have found that the average fixed-key of this differential including the key schedule is approximately equal to $1.31 \times 2^{-5}$. Thus, the theoretical expected differential probability is very close to the real value in this example.

To conclude, it should be mentioned that the trail $\mathcal{T}_{1}$ is not the 4 -round trail which has the highest probability. Using the algorithm given in the next chapter, it can be proven that the optimal 4-round trial is the trail $\mathcal{T}_{o}^{(=)}\left(a^{[i]}\right)_{i \leq q}$ such that $a^{[i]}=0505$ for every $i \leq 4$. This trail has a differential probability equal to $\left(\frac{10}{16}\right)^{8} \approx 1.49 \times 2^{-6}$ which is greater than $\operatorname{DP}\left(\mathcal{T}_{1}\right) \approx 1.2 \times 2^{-6}$. However, we have computed that

$$
\frac{1}{2^{16}} \sum_{K \in \mathbb{F}_{2}^{16}} \mathrm{DP}_{E_{K}^{(4)}}(0505,0505) \approx \frac{1714.3}{2^{16}} \approx 1.67 \times 2^{-6}
$$

Therefore, the differential associated with an optimal trail is not necessarily an optimal differential.

|  | $\mathcal{T}_{1}$ | $\mathcal{T}_{2}$ | $\mathcal{T}_{3}$ | $\mathcal{T}_{4}$ | $\mathcal{T}_{5}$ | $\mathcal{T}_{6}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $a^{[0]}$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ |
| $b^{[0]}$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,1,0,0)$ | $(0,1,0,0)$ | $(0, \mathrm{~B}, 0,0)$ | $(0, \mathrm{~B}, 0,0)$ |
| $a^{[1]}$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,0,0,4)$ | $(0,0,0,4)$ | $(4,0,4,4)$ | $(4,0,4,4)$ |
| $b^{[1]}$ | $(0,4,0,0)$ | $(0,1,0,0)$ | $(0,0,0,4)$ | $(0,0,0,1)$ | $(4,0,4,9)$ | $(9,0,9,4)$ |
| $a^{[2]}$ | $(0,4,0,0)$ | $(0,0,0,4)$ | $(0,1,0,0)$ | $(0,0,0,1)$ | $(1, \mathrm{~A}, 0,1)$ | $(\mathrm{A}, 1,0, \mathrm{~A})$ |
| $b^{[2]}$ | $(0,4,0,0)$ | $(0,0,0,4)$ | $(0,4,0,0)$ | $(0,0,0,4)$ | $(4,4,0,4)$ | $(4,4,0,4)$ |
| $a^{[3]}$ | $(0,4,0,0)$ | $(0,1,0,0)$ | $(0,4,0,0)$ | $(0,1,0,0)$ | $(0, \mathrm{D}, 0,0)$ | $(0, \mathrm{D}, 0,0)$ |
| $b^{[3]}$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ |
| DP | $6^{4} / 16^{4}$ | $4^{2} \times 6^{2} / 16^{4}$ | $4^{2} \times 6^{2} / 16^{4}$ | $4^{4} / 16^{4}$ | $2^{4} \times 4^{2} \times 6^{2} / 16^{8}$ | $2^{6} \times 4 \times 6 / 16^{8}$ |
| $\approx$ | $1.2 \times 2^{-6}$ | $1.1 \times 2^{-7}$ | $1.1 \times 2^{-7}$ | $1.0 \times 2^{-8}$ | $1.1 \times 2^{-19}$ | $1.5 \times 2^{-22}$ |

Figure 1.8: The trails composing the 4 -round differential ( 0400,0400 ).

### 1.4. Linear cryptanalysis

After differential cryptanalysis, linear cryptanalysis is the main attack against block ciphers. This cryptanalysis was introduced by Matsui in [74, 75] for the DES and was the first attack which recovered experimentally a DES key. However, it should be mentioned that the idea of linear cryptanalysis was proposed earlier by Tardy-Corfdir and Gilbert [96] in an attack against the cipher FEAL-4.

Linear cryptanalysis is a known plaintext attack, which is an advantage over differential cryptanalysis. The main idea of this attack is to use a linear approximation of a reduced-round version of the cipher to recover information on some round keys. As was the case for the presentation of differential cryptanalysis, we first formalize the idea of linear cryptanalysis and give an example. Then we describe the theory of this attack in Section 1.4.2.

### 1.4.1. General Idea of the Attack

For a linear cryptanalysis to be successful, one must find a linear approximation of the cipher with high linear potential. First, let us define the concepts of linear approximation and linear potential. Let $f$ be a mapping from $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{n}$. Intuitively, we want to approximate a linear combination of the output bits of $f$ by a linear combination of its input bits. In other words, we want a relation of the form

$$
\begin{equation*}
\langle a, x\rangle=\langle b, f(x)\rangle, \tag{1.3}
\end{equation*}
$$

where the $n$-bit vectors $a$ and $b$ are called the input and output selection patterns of the approximation. Thus, a linear approximation over $f$ is simply defined to be a pair $(a, b)$ of elements of $\mathbb{F}_{2}^{n}$. Of course, such an approximation holds with a certain
probability. But it is worthwhile to note that, if Equation (1.3) quite never holds then the relation

$$
\begin{equation*}
\langle a, x\rangle=\langle b, f(x)\rangle+1 \tag{1.4}
\end{equation*}
$$

holds with high probability. From a cryptanalytic point of view, using Equation (1.3) or (1.4) does not matter as they yield the same amount of information. The worst case is when (1.3) holds for exactly the half of the inputs $x$. In this case, the left side gives no information on the right side, and hence on $f$. The usefulness of an approximation is characterized by its correlation or linear potential.

Definition 1.28 (Correlation and Linear Potential). Let $f: \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ be a mapping and $(a, b)$ be an approximation over $f$. The correlation of the approximation $(a, b)$ is defined to be

$$
\mathrm{C}_{f}(a, b)=2 \cdot \frac{\#\left\{x \in \mathbb{F}_{2}^{n} \mid\langle a, x\rangle=\langle b, f(x)\rangle\right\}}{2^{n}}-1
$$

The linear potential LP of $(a, b)$ is the square of its correlation, namely

$$
\mathrm{LP}_{f}(a, b)=\mathrm{C}_{f}(a, b)^{2}
$$

Remark 1.29. The definition of the correlation can be equivalently restated as

$$
\mathrm{C}_{f}(a, b)=2 \cdot \mathbb{P}_{x}(\langle a, x\rangle=\langle b, f(x)\rangle)-1
$$

Thus, the correlation of any approximation ranges from -1 to 1 included. Then, the linear potential of an approximation ranges from 0 to 1 . A correlation or linear potential equal to zero gives no information. The closer the absolute correlation or linear potential is to one, the more information it yields on $f$. Finally, it should be noted that several authors speak about linear probability rather than potential. We strongly encourage the term potential as this quantity is not a probability.

As for differential cryptanalysis, consider an $r$-round substitution permutation network $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ and assume that the last round does not have a diffusion layer, thus

$$
E_{K}=\left(\alpha_{k[r]} \circ \sigma \circ \alpha_{k[r-1]}\right) \circ E_{K}^{(r-1)}
$$

A classical linear cryptanalysis of $E$ is based on an approximation $(a, b)$ over the ( $r-1$ )-round encryption $E_{K}^{(r-1)}$ which has high linear potential for virtually all cipher keys $K$. Let $K$ be a cipher key. Then note that

$$
\begin{aligned}
\langle a, x\rangle & =\left\langle b, E_{K}^{(r-1)}(x)+k^{[r-1]}\right\rangle \\
\Longleftrightarrow \quad\langle a, x\rangle & =\left\langle b, E_{K}^{(r-1)}(x)\right\rangle+\left\langle b, k^{[r-1]}\right\rangle .
\end{aligned}
$$

Since $\left\langle b, k^{[r-1]}\right\rangle$ does not depend on $x$, the correlation of the approximation $(a, b)$ over $\alpha_{k[r-1]} \circ E_{K}^{(r-1)}$ is equal to the correlation of $(a, b)$ over $E_{K}^{(r-1)}$ up to the sign. Therefore,

$$
\begin{align*}
\mathrm{C}_{R^{\prime}}(a, b) & = \pm \mathrm{C}_{R}(a, b)  \tag{1.5}\\
\operatorname{LP}_{R^{\prime}}(a, b) & =\operatorname{LP}_{R}(a, b)
\end{align*} \quad \text { where } \quad\left\{\begin{array}{l}
R=E_{K}^{(r-1)}, \\
R^{\prime}=\alpha_{k k^{[r-1]}} \circ E_{K}^{(r-1)} .
\end{array}\right.
$$

## Chapter 1 - Substitution-Permutation Networks

Assume that $(a, b)$ is an $(r-1)$-round approximation with linear potential $q$ for a significant fraction of the cipher keys and let $K$ denote the unknown cipher key. For the cryptanalysis to be successful, it turns out that we need $N=C \times q^{-1}$ known plaintext/ciphertext pairs $(p, c)$. To recover information on the last-round key, proceed as follows. For each candidate key $k$ for $k^{[r]}$, compute the value

$$
P_{k}=\left(2 \times \#\left\{(p, c) \mid\langle a, p\rangle=\left\langle b, \sigma^{-1}(c+k)\right\rangle\right\}-N\right)^{2} .
$$

Then the key $k$ maximizing the value $P_{k}$ should be equal to the last-round key $k^{[r]}$. Again, the assumption that a wrong key $k$ should have a value $P_{k}$ less than $P_{k[r]}$ is called the hypothesis of wrong-key randomization [51].

Example 1.30. In this example we describe a linear cryptanalysis of our ToyCiPHER introduced in Example 1.14. Again we will not focus on how to find a suitable linear approximation of the reduced-round cipher but rather explain how to use one. Consider the 4-round linear approximation ( $a, b$ ) where

$$
a=b=(0,0,2,0) .
$$

The average linear potential of this approximation over every cipher key is

$$
\frac{1}{2^{16}} \sum_{K \in \mathbb{F}_{2}^{16}} \operatorname{LP}_{E_{K}{ }^{(4)}}(0020,0020) \approx \frac{6914.6}{2^{16}} \approx 1.69 \times 2^{-4} .
$$

This value was computed via an exhaustive search. The distribution of all linear potentials $\mathrm{LP}_{E_{K}(4)}(0020,0020)$ is given at the top of Figure 1.9. For instance, the inequalities

$$
\frac{4416}{2^{16}}<\operatorname{LP}_{E_{K}^{(4)}}(0020,0020) \leq \frac{4480}{2^{16}}
$$

hold for 2400 cipher keys. Compared with Figure 1.5, the repartition of theses potentials is more complicated and key-dependent than the repartition of the differential probabilities. We will explain this weird behavior in Section 1.4.2.

Let $K$ be an unknown cipher key. This linear cryptanalysis is known to be successful only when $C \times q^{-1}$ plaintext/ciphertext pairs are available. With $C=5$, this attack requires

$$
N=5 \times \frac{2^{16}}{6914.6} \approx 47 \approx 2^{6}
$$

known plaintexts. Assume we are given $N$ pairs $(p, c)$ such that $c=E_{K}(c)$. Let $k$ be a candidate of $k^{[5]}$. Following the principle of linear cryptanalysis, we must compute the value

$$
\begin{equation*}
P_{k}=\left(2 \times \#\left\{(p, c) \mid\langle a, p\rangle=\left\langle b, \sigma^{-1}(c+k)\right\rangle\right\}-N\right)^{2} . \tag{1.6}
\end{equation*}
$$

Observe that for each pair $(p, c)$, it holds that

$$
\begin{aligned}
\langle a, p\rangle=\left\langle b, \sigma^{-1}(c+k)\right\rangle & \Longleftrightarrow\langle 0020, p\rangle=\left\langle 0020, \sigma^{-1}(c+k)\right\rangle \\
& \Longleftrightarrow\left\langle 2, p_{2}\right\rangle=\left\langle 2, S^{-1}\left(c_{2}+k_{2}\right)\right\rangle .
\end{aligned}
$$

Initialisation: Find a High Potential 4-Round approximation


Part 1: Get Plaintext/Ciphertext Pairs
Choose $N$ plaintext pairs $\left(p, p^{*}\right)$ such that $p+p^{*}=0400$ and request the corresponding ciphertext pairs $\left(c, c^{*}\right)$ encrypted under the unknown cipher key $K$.


Part 2: Recover Some Bits of the Last Round Key
For each candidate $\tilde{k}_{2}{ }^{[5]}$, decrypt partially the last round for every ciphertext.
The key $\tilde{k}_{2}{ }^{[5]}$ maximizing $\left(2 \times \#\left\{\left(p_{2}, y_{2}\right) \mid\left\langle p_{2}, 2\right\rangle=\left\langle y_{2}, 2\right\rangle\right\}-N\right)^{2}$ should be equal to $k_{1}{ }^{[5]}$.


Figure 1.9: A linear cryptanalysis of TOYCiPher.

## Chapter 1 - Substitution-Permutation Networks



Figure 1.10: A differential cryptanalysis of ToyCipher.

Replacing in (1.6) yields

$$
\begin{equation*}
P_{k}=\left(2 \times \#\left\{(p, c) \mid\left\langle 2, p_{2}\right\rangle=\left\langle 2, S^{-1}\left(c_{2}+k_{2}\right)\right\rangle\right\}-N\right)^{2} . \tag{1.7}
\end{equation*}
$$

Since the value $P_{k}$ does not depend on $k_{0}, k_{1}$ and $k_{3}$, the cryptanalysis cannot give any information on the corresponding bundles of the last-round key. To recover information on $k_{2}{ }^{[5]}$, proceed as follows. For each candidate $k_{2}$ for $k_{2}{ }^{[5]}$, compute the value $P_{k_{2}}$ given in (1.7). Then the higher $P_{k_{2}}$ is, the more likely $k_{2}$ is equal to $k_{2}{ }^{[5]}$. This cryptanalysis is illustrated in Parts 1 and 2 of Figure 1.9 and its success probability is given in Figure 1.10. For instance, if $C=5$, the attack recovers one, two and three bits of information with probability $81.1 \%, 60.5 \%$ and $41.0 \%$ respectively. Unlike the differential cryptanalysis in Example 1.16, this attack never obtains four bits of information. This does not mean that the correct bundle $k_{2}{ }^{[5]}$ is never recovered but that there is at least another key with a score greater than or equal to its score.

### 1.4.2. Linear Approximations and Linear Trails

In this section, we explore the theory of linear approximations. All the results and definitions are drawn from the works of Daemen and Rijmen [39, 40]. Let $f$ be a mapping from $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{n}$. The matrix $\mathrm{C}_{f}$ formed by the correlations between all the selection patterns is called the correlation matrix of $f$. The next lemma explains how the correlation matrix of a composition can be derived from the correlation matrices of its components.

Lemma 1.31. Let $f$ and $g$ be two mappings from $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{n}$. The correlation matrix of the composite $g \circ f$ is equal to $\mathrm{C}_{f} \times \mathrm{C}_{g}$. Thus, for all $a, b$ in $\mathbb{F}_{2}^{n}$, we have

$$
\mathrm{C}_{g \circ f}(a, b)=\sum_{i \in \mathbb{F}_{2}^{n}} \mathrm{C}_{f}(a, i) \times \mathrm{C}_{g}(i, b)
$$

Consider a generic $r$-round substitution-permutation network $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ where the encryption function can be expressed for each cipher key $K$ as

$$
E_{K}=F_{k[r-1]} \circ \cdots \circ F_{k[0]} \quad \text { with } \quad F_{k[i]}=\pi \circ \sigma \circ \alpha_{k[i]} .
$$

Again, the last round includes and ends with a diffusion layer. First, we look at the correlation of an approximation over the basic steps of the round function, namely the key addition, the substitution layer and the diffusion layer.

Proposition 1.32. Let $a, b$ be two selection patterns in $\mathbb{F}_{2}^{n m}$ and let $k$ be a round key. The correlations of the approximation $(a, b)$ over each step of the round function are given by

$$
\mathrm{C}_{\alpha_{k}}(a, b)=\delta_{a, b}(-1)^{\langle a, k\rangle}, \quad \mathrm{C}_{\sigma}(a, b)=\prod_{i=0}^{m-1} \mathrm{C}_{S_{i}}\left(a_{i}, b_{i}\right), \quad \mathrm{C}_{\pi}(a, b)=\delta_{a, \pi^{\top}(b)} .
$$

By analogy with differential trails, let us introduce the concept of linear trails. Even if the applications of linear trails are similar to the ones of differential trails, these two concepts are by nature very different.

Definition 1.33 (Linear Trail). An $r$-round linear trail is a family $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ of $r+1$ selection patterns. The correlation contribution of $\mathcal{T}$ is defined to be

$$
\mathrm{C}(\mathcal{T})=\prod_{i=0}^{r-1} \mathrm{C}_{\pi \sigma}\left(a^{[i]}, a^{[i+1]}\right)
$$

When considering the fixed-key correlation of an $r$-round approximation or the average of these correlations, the correlation contribution of a linear trail is just an intermediate variable. Unlike differential trails, a linear trail does not have a concrete meaning. Indeed, a pair can follow a differential trail but it is meaningless to say that the messages (or worse one message) follow a linear trail. An approximation does not consider the messages individually but the whole encryption function.

Definition 1.34 (Active S-Box). Let $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ be a linear trail with a nonzero correlation contribution. The S-box $S_{j}$ is said to be active at round $i$ if the pattern $a_{j}{ }^{[i]}$ is nonzero, otherwise $S_{j}$ is inactive.

Remark 1.35. Generally, we say that $S_{j}$ is active when $b_{j}$ is nonzero. However, these two definitions are equivalent when considering bijective S-boxes, as ensured by the following proposition.

Proposition 1.36. Let $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ be a nonzero correlation linear trail. Let $i<r$ and $j \leq m$ be nonnegative integers. Denote by $b^{[i]}$ the element $\pi^{\top}\left(a^{[i+1]}\right)$. Then $a_{j}{ }^{[i]}=0_{n}$ if and only if $b_{j}{ }^{[i]}=0_{n}$. Consequently, Definition 1.33 can be restated as

$$
\mathrm{C}(\mathcal{T})=\prod_{i, j \mid a_{j}{ }^{[i]} \neq 0} \mathrm{C}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right) \quad \text { and } \quad \operatorname{LP}(\mathcal{T})=\prod_{i, j \mid a_{j}{ }^{[i]} \neq 0} \operatorname{LP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right)
$$

## Chapter 1 - Substitution-Permutation Networks

Proof. To simplify the notation, denote by $a^{\prime}$ and $b^{\prime}$ the patterns $a_{j}{ }^{[i]}$ and $b_{j}{ }^{[i]}$ and by $S$ the S-box $S_{j}$. Since $\mathrm{C}(\mathcal{T})$ is assumed to be nonzero, it must be the case that $\mathrm{C}_{S}\left(a^{\prime}, b^{\prime}\right)$ is nonzero. We contend that $\mathrm{C}_{S}\left(a^{\prime}, 0_{n}\right)=\delta_{a^{\prime}, 0_{n}}$, where $\delta$ is the Kronecker delta. To prove this, first observe that $\mathrm{C}_{S}\left(0_{n}, 0_{n}\right)=1$. Now, assume that $a^{\prime}$ is nonzero. By definition, $\left\langle 0_{n}, S(x)\right\rangle=0$ for any $x$ in $\mathbb{F}_{2}^{n}$. Next, the cardinality of $\left\{x \in \mathbb{F}_{2}^{n} \mid\langle a, x\rangle=0\right\}$ is equal to $2^{n-1}$ since any linear Boolean function is balanced. This proves that $\mathrm{C}_{S}\left(a^{\prime}, 0_{n}\right)=0$ whenever $a^{\prime}$ is nonzero. The same argument proves that $\mathrm{C}_{S^{-1}}\left(b^{\prime}, 0_{n}\right)=\delta_{b^{\prime}, 0_{n}}$. Then, it is well-known that $\mathrm{C}_{S^{-1}}\left(b^{\prime}, 0_{n}\right)=\mathrm{C}_{S}\left(0_{n}, b^{\prime}\right)$ (see [39, Equation 7.30]) and thus $\mathrm{C}_{S}\left(0_{n}, b^{\prime}\right)=\delta_{0_{n}, b^{\prime}}$. It follows that $a^{\prime}=0_{n}$ if and only if $b^{\prime}=0_{n}$. Finally, Lemma 1.31 and Proposition 1.32 imply that

$$
\begin{aligned}
\mathrm{C}_{\pi \sigma}\left(a^{[i]}, a^{[i+1]}\right) & =\sum_{c \in \mathbb{F}_{2}^{n m}} \mathrm{C}_{\sigma}\left(a^{[i]}, c\right) \times \mathrm{C}_{\pi}\left(c, a^{[i+1]}\right)=\sum_{c \in \mathbb{F}_{2}^{n m}} \mathrm{C}_{\sigma}\left(a^{[i]}, c\right) \times \delta\left(c, b^{[i]}\right) \\
& =\mathrm{C}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=\prod_{j=0}^{m-1} \mathrm{C}_{S_{j}}\left(a_{j}^{[i]}, b_{j}^{[i]}\right) .
\end{aligned}
$$

The result follows.
Let us now present the result relating linear trails and $r$-round linear approximations. The following proposition should be compared to Proposition 1.19, which is its counterpart about differential cryptanalysis.

Proposition 1.37. Let $(a, b)$ be an $r$-round approximation and let $K$ be a cipher key. Denote by $E_{a, b}$ the set of all trails $\left(a^{[i]}\right)_{i \leq r}$ such that $a^{[0]}=a, a^{[r]}=b$. Given a trail $\mathcal{T}$ in $E_{a, b}$, denote by $\langle\mathcal{T}, K\rangle$ the element $\sum_{i=0}^{r}\left\langle a^{[i]}, k^{[i]}\right\rangle$ of $\mathbb{F}_{2}$. Then the fixed-key correlation of $(a, b)$ is given by

$$
\mathrm{C}_{E_{K}}(a, b)=\sum_{\mathcal{T} \in E_{a, b}}(-1)^{\langle\mathcal{T}, K\rangle} \mathrm{C}(\mathcal{T})
$$

In contrast with differential, the correlation of an $r$-round approximation is a signed sum of the correlation contributions of its associated linear trails. When the high absolute correlation trails are added with the same sign, the amplitude of the whole correlation will be higher. In this case, we speak of constructive interference. Otherwise, when these trails have different signs, the whole correlation can be close or even equal to zero and we speak of destructive interference. This result explains the strange distribution of the correlations in Figure 1.9 of Example 1.30.

Definition 1.38 (ELP). The expected linear potential of an $r$-round approximation $(a, b)$, denoted by $\operatorname{ELP}(a, b)$, is the average fixed-key linear potential of $(a, b)$ over the associated long-key cipher.

Theorem 1.39. Let $(a, b)$ be an $r$-round approximation and denote by $E_{a, b}$ the set of all trails $\left(a^{[i]}\right)_{i \leq r}$ such that $a^{[0]}=a, a^{[r]}=b$. The expected linear potential of $(a, b)$ is given by

$$
\operatorname{ELP}(a, b)=\sum_{\mathcal{T} \in E_{a, b}} \operatorname{LP}(\mathcal{T})
$$

| LP | \#Trails | LP | \#Trails | LP | \#Trails |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $1.60 \times 2^{-4}$ | 1 | $1.80 \times 2^{-21}$ | 1 | $1.00 \times 2^{-28}$ | 2 |
| $1.27 \times 2^{-10}$ | 2 | $1.13 \times 2^{-21}$ | 2 | $1.13 \times 2^{-29}$ | 15 |
| $1.42 \times 2^{-11}$ | 4 | $1.27 \times 2^{-22}$ | 2 | $1.27 \times 2^{-30}$ | 21 |
| $1.00 \times 2^{-16}$ | 1 | $1.42 \times 2^{-23}$ | 1 | $1.00 \times 2^{-32}$ | 15 |
| $1.27 \times 2^{-18}$ | 1 | $1.00 \times 2^{-24}$ | 5 | $1.12 \times 2^{-33}$ | 44 |
| $1.42 \times 2^{-19}$ | 1 | $1.13 \times 2^{-25}$ | 3 | $1.00 \times 2^{-36}$ | 55 |
| $1.60 \times 2^{-20}$ | 2 | $1.27 \times 2^{-26}$ | 15 |  |  |
| $1.00 \times 2^{-20}$ | 4 | $1.42 \times 2^{-27}$ | 7 |  |  |

Figure 1.11: All linear potentials of the linear trails associated with the 4-round approximation (0020, 0020).

This time, the sum consists of nonnegative terms and thus there is no destructive interference. The expected linear potential is a powerful indicator of the cipher's security against linear cryptanalysis. Nonetheless, it must be kept in mind that the actual correlation is highly key-dependent as established by Proposition 1.37. Finally, the expected linear potential has the same downsides as the expected differential probability. This value is generally impossible to compute precisely and one should make the hypothesis of stochastic equivalence [51] to relate this notion with the cipher's security.
Example 1.40. Using the preceding theory of linear approximations, we now study the 4-round linear approximation $(a, b)$ with $a=b=0020$ introduced in Example 1.30. With an exhaustive search, we found that there are exactly 204 linear trails associated with the linear approximation $(a, b)$. In Figure 1.11, we gather the trails according to their linear potentials. The trail which has the best linear potential is simply the trail $\mathcal{T}=\left(a^{[i]}\right)_{i \leq 4}$ where $a^{[i]}=0020$. Since the diffusion layer is a bit permutation, its transpose is equal to its inverse, that is $\pi^{\top}=\pi^{-1}$. It is then easily seen that $b^{[i]}=0020$ for each $i<r$. By virtue of Proposition 1.36, the correlation of $\mathcal{T}$ can be computed using the correlation matrix of $S$, given in Figure 1.12. Thus,

$$
\mathrm{C}(\mathcal{T})=\prod_{i, j \mid a_{j}{ }^{[i]} \neq 0} \mathrm{C}_{S}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right)=\mathrm{C}_{S}(2,2)^{4}=\left(-\frac{12}{16}\right)^{4}=\left(\frac{9}{16}\right)^{2} .
$$

The linear potential of $\mathcal{T}$ is then $\left(\frac{9}{16}\right)^{4} \approx 1.60 \times 2^{-4}$. According to Theorem 1.39, the expected linear potential of the approximation $(a, b)$ can be computed as follows:

$$
\operatorname{ELP}(a, b)=\sum_{\mathcal{T} \in E_{a, b}} \operatorname{LP}(\mathcal{T})=1.63 \times 2^{-4}
$$

As we can see, this value is dominated by the linear potential of the best trail. In Example 1.30 we have found that the average fixed-key linear potential including the key schedule is equal to $1.69 \times 2^{-4}$, so is very close to the excepted linear potential. This shows that the linear potential of one high potential linear trail can well approximate the average potential of the associated approximation.

## Chapter 1 - Substitution-Permutation Networks




Figure 1.12: The correlation and linear potential matrices of $S$.

We will not explain here the complex and surprising distribution of the fixed-key correlations ( $a, b$ ) illustrated in Figure 1.9. Indeed, these correlations depend on the interaction between the expanded key and the 204 linear trails associated with $(a, b)$ However, we study another approximation whose linear potential distribution is even more surprising but simpler to explain.

In the remainder of this example, consider the 4 -round linear approximation $(a, b)$ where $a=b=0400$. It can be proven via an exhaustive search that the four linear trails $\mathcal{T}_{1}, \ldots, \mathcal{T}_{4}$ presented in Figure 1.13 are the only trails associated with ( $a, b$ ). At the left of Figure 1.14 is illustrated the distribution of the fixed-key correlations of $(a, b)$, including the key schedule. Therefore, the correlation $\mathrm{C}_{E_{K}(4)}(0400,0400)$ respectively is equal to $0,2^{-3}$ and $2^{-2}$ for a proportion of $\frac{3}{8}, \frac{1}{2}$ and $\frac{1}{8}$ of the cipher keys. According to Proposition 1.37, the fixed-key correlation of $(a, b)$ is a signed combination of the correlations of the $\mathcal{T}_{i}$, that is

$$
\mathrm{C}_{E_{K}}(0400,0400)=\sum_{i=1}^{4}(-1)^{\left\langle\mathcal{T}_{i}, K\right\rangle} \mathrm{C}\left(\mathcal{T}_{i}\right)
$$

Seeing the trails $\mathcal{T}_{i}$ as elements of $\left(\mathbb{F}_{2}^{16}\right)^{5}$, we have

$$
\begin{array}{ll}
\mathcal{T}_{1}=(0400,0400,0400,0400,0400), & \mathcal{T}_{3}=(0400,0004,0100,0400,0400), \\
\mathcal{T}_{2}=(0400,0400,0004,0100,0400), & \mathcal{T}_{4}=(0400,0004,0001,0100,0400) .
\end{array}
$$

Clearly, these four trails are linearly independent and thus, all the possible signed sums are equally likely when considering the long-key cipher. These sums are given at the right of Figure 1.14. This explains the distribution of the correlations of $(a, b)$.

|  | $\mathcal{T}_{1}$ | $\mathcal{T}_{2}$ | $\mathcal{T}_{3}$ | $\mathcal{T}_{4}$ |
| :---: | :---: | :---: | :---: | :---: |
| $a^{[0]}$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ |
| $b^{[0]}$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,1,0,0)$ | $(0,1,0,0)$ |
| $a^{[1]}$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,0,0,4)$ | $(0,0,0,4)$ |
| $b^{[1]}$ | $(0,4,0,0)$ | $(0,1,0,0)$ | $(0,0,0,4)$ | $(0,0,0,1)$ |
| $a^{[2]}$ | $(0,4,0,0)$ | $(0,0,0,4)$ | $(0,1,0,0)$ | $(0,0,0,1)$ |
| $b^{[2]}$ | $(0,4,0,0)$ | $(0,0,0,4)$ | $(0,4,0,0)$ | $(0,0,0,4)$ |
| $a^{[3]}$ | $(0,4,0,0)$ | $(0,1,0,0)$ | $(0,4,0,0)$ | $(0,1,0,0)$ |
| $b^{[3]}$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ | $(0,4,0,0)$ |
| C | $8^{4} / 16^{4}$ | $8^{4} / 16^{4}$ | $8^{4} / 16^{4}$ | $8^{4} / 16^{4}$ |
| $=$ | $2^{-4}$ | $2^{-4}$ | $2^{-4}$ | $2^{-4}$ |

Figure 1.13: The trails associated with the 4-round approximation (0400, 0400).


| Signs |  | Signs |  |
| :---: | :---: | :---: | :---: |
| $\mathcal{T}_{1} \mathcal{T}_{2} \mathcal{T}_{3} \mathcal{T}_{4}$ | C | $\mathcal{T}_{1} \mathcal{T}_{2} \mathcal{T}_{3} \mathcal{T}_{4}$ | C |
| + + + + | $2^{-2}$ | - + + + | $2^{-3}$ |
| + + + | $2^{-3}$ | + | 0 |
| + + - + | $2^{-3}$ | - + - + | 0 |
| + + | 0 | - + - | $-2^{-3}$ |
| + - + + | $2^{-3}$ | - - + + | 0 |
| + - + | 0 | - - + | $-2^{-3}$ |
| + - - + | 0 | - - - + | $-2^{-3}$ |
| + - - - | $-2^{-3}$ | - - - | $-2^{-2}$ |

Figure 1.14: Correlations of the 4-round approximation (0400, 0400 ).

### 1.5. Security Evaluation of SPN Building Blocks

As explained in Sections 1.3.2 and 1.4.2, the effectiveness of a differential is assessed by its expected differential probability and the effectiveness of a linear approximation by its expected linear potential. Naturally, a block cipher is resistant against differential and linear cryptanalysis when there exists no effective differential and approximation over the $(r-1)$-round encryption function. Equivalently, the cipher is secure when the maximum expected differential probability (MEDP) or linear potential (MELP) is low enough, namely if the corresponding attacks require more plaintext/ciphertext pairs than the block size allows.

According to Theorem 1.26, the expected probability of a given differential is hard to compute and Theorem 1.39 establishes the same result for linear cryptanalysis. Therefore, computing the MEDP and MELP are even harder. Nonetheless, we have seen that the expected probability of a differential can be approximated by the probability of its best trail and the same holds for a linear approximation. Relying on these facts, Kanda et al. [57] introduced four measures of security which can be divided into two categories according to the security they imply.

- The provable security of a cipher is evaluated by two measures called precise and theoretical. The precise measure gives the MEDP (resp. MELP) whereas the theoretical measure only gives an upper-bound of this value.
- The practical security of a cipher is assessed by two measures called heuristic and practical. The heuristic measure gives the maximum differential probability (resp. linear potential) of all trails while the practical measure upper-bounds this value.

Because computing even the heuristic measure can be a challenging problem, most of ciphers' security is assessed by the practical measure.

The standard strategy to design a secure cipher is to ensure that each differential or linear trail activates many S-boxes and that all the S-boxes of the cipher have good resistances against linear and differential cryptanalysis.

Definition 1.41. Let $S$ be an $n$-bit S-box. The maximum differential probability, correlation and linear potential of $S$, denoted respectively by $\mathrm{DP}_{S}^{\max }, \mathrm{C}_{S}^{\max }$ and $\mathrm{LP}_{S}^{\max }$, are defined to be

$$
\begin{aligned}
\mathrm{DP}_{S}^{\max } & =\max \left\{\mathrm{DP}(a, b) \mid a \in\left(\mathbb{F}_{2}^{n}\right)^{*}, b \in \mathbb{F}_{2}^{n}\right\}, \\
\mathrm{C}_{S}^{\max } & =\max \left\{|\mathrm{C}(a, b)| \mid a \in \mathbb{F}_{2}^{n}, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}, \\
\mathrm{LP}_{S}^{\max } & =\max \left\{\operatorname{LP}(a, b) \mid a \in \mathbb{F}_{2}^{n}, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}=\left(\mathrm{C}_{S}^{\max }\right)^{2} .
\end{aligned}
$$

Remark 1.42. According to Propositions 1.24 and 1.36, these maximums can be searched only for $a$ and $b$ both nonzero.

## 1.5 - Security Evaluation of SPN Building Blocks

### 1.5.1. Perfect S-Boxes

This section deals with the resistance of S-boxes with respect to differential and linear cryptanalysis. The theory covering this topic considers a larger class function. Following [33], an $(n, m)$-function is defined to be a mapping from $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{m}$. There are also known as vectorial Boolean function. Thus, according to our conventions, an $n$-bit S-box is a bijective ( $n, n$ )-function.

### 1.5. 1.a. Almost Perfect Nonlinear Functions

Let $F$ be an $(n, m)$-function. For each $a$ in $\mathbb{F}_{2}^{n}$ and $b$ in $\mathbb{F}_{2}^{m}$, denote by $\delta_{F}(a, b)$ the number of solutions to the equation $F(x)+F(x+a)=b$. These values are clearly related to the differential probabilities of $F$ by the formula

$$
\begin{equation*}
2^{n} \times \mathrm{DP}_{F}(a, b)=\delta_{F}(a, b) \tag{1.8}
\end{equation*}
$$

Remark 1.43. In Section 1.3.2, we have only defined the differential probabilities for $n$-bit S-boxes. This notion can naturally be extended to ( $n, m$ )-functions, precisely using Equation (1.8).

Definition 1.44 (differentially $\delta$-uniform function [80). Let $\delta$ be an integer. An $(n, m)$-function $F$ is said to be differentially $\delta$-uniform if for all nonzero $a$ in $\mathbb{F}_{2}^{n}$ and all $b$ in $\mathbb{F}_{2}^{m}$, it holds that $\delta_{F}(a, b) \leq \delta$. Equivalently, $F$ is differentially $\delta$-uniform if

$$
2^{n} \times \mathrm{DP}_{F}^{\max } \leq \delta
$$

Let $a$ be any nonzero element of $\mathbb{F}_{2}^{n}$. Obviously, for each $x$ in $\mathbb{F}_{2}^{n}$, there exists a unique $b$ in $\mathbb{F}_{2}^{m}$ such that $F(x)+F(x+a)=b$. Therefore

$$
\sum_{b \in \mathbb{F}_{2}^{m}} \delta_{F}(a, b)=2^{n} .
$$

In order to minimize the maximum of the $\delta_{F}(a, b)$ with $b$ in $\mathbb{F}_{2}^{m}$, their sum must be uniformly distributed over the all these values, proving the bound

$$
\begin{equation*}
\max _{a \in\left(\mathbb{F}_{2}^{n}\right)^{*}, b \in \mathbb{F}_{2}^{m}} \delta_{F}(a, b) \geq 2^{n-m} . \tag{1.9}
\end{equation*}
$$

Consequently, any $(n, m)$-function is at least $2^{n-m}$-uniform. An $(n, m)$-function which meets this bound is called perfect nonlinear [79]. Referring to Equation (1.8), we see that $F$ is perfect nonlinear if and only if $\mathrm{DP}_{F}^{\max }$ is minimal. Thus, perfect nonlinear functions provide optimal resistance against differential cryptanalysis.

It worthwhile to note that if $x$ is solution to the equation $F(x)+F(x+a)=b$, then so is $x+a$. Thus, when $a$ is nonzero, $\delta_{F}(a, b)$ is even (this result remains true when $a=0$, but requires another argument). It follows that

$$
\begin{equation*}
\max _{a \in\left(\mathbb{F}_{2}^{n}\right)^{*}, b \in \mathbb{F}_{2}^{m}} \delta_{F}(a, b) \geq 2 \tag{1.10}
\end{equation*}
$$

## Chapter 1 - Substitution-Permutation Networks

Assume that $F$ is an ( $n, n$ )-function. According to Equation (1.9), $F$ must be 1uniform to be perfect nonlinear. However, Equation (1.10) ensures that any function is at least 2-uniform. This proves that there does not exist perfect nonlinear ( $n, n$ )functions. Because ( $n, n$ )-functions are widely used in cryptography, particularly $n$-bit S-boxes, Nyberg introduced the following definition in [82].

Definition 1.45 (APN function). Any 2-uniform ( $n, n$ )-function is said to be almost perfect nonlinear (APN).

Remark 1.46. Using the notation introduced at the beginning of Section 1.5.1, an $(n, n)$-function $F$ is almost perfect nonlinear if and only if $\mathrm{DP}_{F}^{\max }=2^{-(n-1)}$. Additionally, we may stress that the term almost is ambiguous because APN functions are optimal for their size, as noted in [33].

### 1.5.1.b. Almost Bent Functions

Let $F$ be an $(n, m)$-function. For each $a$ in $\mathbb{F}_{2}^{n}$ and $b$ in $\mathbb{F}_{2}^{m}$, denote by $\lambda_{F}(a, b)$ the integer

$$
\sum_{x \in \mathbb{F}_{2}^{n}}(-1)^{\langle a, x\rangle+\langle b, F(x)\rangle} .
$$

The family $\Lambda_{F}$ consisting of all the values $\lambda_{F}(a, b)$ is called the Walsh spectrum of $F$. Up to scaling, the Walsh spectrum of $F$ is equivalent to its correlation matrix. More precisely, for all selection patterns $a$ and $b$ in $\mathbb{F}_{2}^{n}$ and $\mathbb{F}_{2}^{m}$ respectively, we have

$$
\lambda_{F}(a, b)=2^{n} \times \mathrm{C}_{F}(a, b) .
$$

Indeed, denoting by $E_{i}$ the set of all elements $x$ in $\mathbb{F}_{2}^{n}$ such that the sum $\langle a, x\rangle+$ $\langle b, F(x)\rangle$ is equal to $i$ in $\mathbb{F}_{2}$, we have

$$
\begin{equation*}
\lambda_{F}(a, b)=\sum_{x \in \mathbb{F}_{2}^{n}}(-1)^{\langle a, x\rangle+\langle b, F(x)\rangle}=\sum_{x \in E_{0}}(-1)^{0}+\sum_{x \in E_{1}}(-1)^{1}=\# E_{0}-\# E_{1} . \tag{1.11}
\end{equation*}
$$

Clearly, the set $E_{1}$ is the relative complement of $E_{0}$ in $\mathbb{F}_{2}^{n}$ and thus $\# E_{1}=2^{n}-\# E_{0}$. Replacing in (1.11), we obtain

$$
\begin{equation*}
\lambda_{F}(a, b)=2 \# E_{0}-2^{n} . \tag{1.12}
\end{equation*}
$$

Next, observe that the set $E_{0}$ is equal to $\left\{x \in \mathbb{F}_{2}^{n} \mid\langle a, x\rangle=\langle b, F(x)\rangle\right\}$. The result then follows from the definition of $\mathrm{C}_{F}(a, b)$.

The nonlinearity of an ( $n, m$ )-function $F$ was introduced by Nyberg in [81] and is defined to be

$$
\mathcal{N} \mathcal{L}(F)=2^{n-1}-\frac{1}{2} \max _{a \in \mathbb{F}_{2}^{m}, b \in\left(\mathbb{F}_{2}^{m}\right)^{*}}\left|\lambda_{F}(a, b)\right|=2^{n-1}\left(1-\mathrm{C}_{F}^{\max }\right) .
$$

Referring to (1.12), it is easily seen that each value $\lambda_{F}(a, b)$ in the Walsh spectrum of $F$ is even. Therefore, $\mathcal{N} \mathcal{L}(F)$ is an integer. In addition, it can be proven that the nonlinearity of $F$ is upper-bounded as follows:

$$
\mathcal{N} \mathcal{L}(F) \leq 2^{n-1}-2^{\frac{n}{2}-1} .
$$

## 1.5 - Security Evaluation of SPN Building Blocks

This inequality is known as the covering radius bound. An ( $n, m$ )-function meeting this bound with equality is said to be bent. Since the right side of this inequality is an integer if and only if $n$ is even, bent functions cannot exist when $n$ is odd. Using the maximum absolute correlation of $F$, the covering radius bound can be equivalently rewritten as

$$
2^{n} \times \mathrm{C}_{F}^{\max } \geq 2^{\frac{n}{2}}
$$

Thus, the function $F$ is bent if and only if $\mathrm{C}_{F}^{\max }$ is minimal. This restatement stresses that bent functions are exactly the $(n, m)$-functions which are the most resistant to linear cryptanalysis. However, Nyberg proved in [79] that such functions exist only if $n \geq 2 m$. Therefore, $n$-bit S-boxes cannot be bent.

Remark 1.47. It turns out that these bent functions are exactly the perfect nonlinear functions introduced in the previous section, as shown in [79]. Thus, bent functions are optimal with respect to differential and linear cryptanalysis.

Since the covering radius bound is not tight for every ( $n, m$ )-function, Chabaud and Vaudenay improved this inequality in [35, Theorem 4]. Their bound is now called the Sidelnikov-Chabaud-Vaudenay bound (shorten as SCV bound) because Sidelnikov had published earlier an equivalent result in [92. For the particular case of $(n, n)$-functions, this bound gives

$$
\begin{equation*}
\mathcal{N} \mathcal{L}(F) \leq 2^{n-1}-2^{\frac{n-1}{2}} \tag{1.13}
\end{equation*}
$$

Definition 1.48 (AB function [35). An $(n, n)$-function is said to be Almost Bent (AB) if its nonlinearity meets the bound (1.13) with equality.

Remark 1.49. Using the notation introduced at the beginning of Section 1.5.1, the SCV bound (1.13) can be restated in the following equivalent ways

$$
\begin{equation*}
2^{n} \times \mathrm{C}_{F}^{\max } \geq 2^{\frac{n+1}{2}}, \quad \mathrm{C}_{F}^{\max } \geq 2^{-\frac{n-1}{2}}, \quad \mathrm{LP}_{F}^{\max } \geq 2^{-(n-1)} \tag{1.14}
\end{equation*}
$$

Again, the term almost in the previous definition is ambiguous because AB functions are optimal.

When $n$ is even, the right side of the SCV bound (1.13) is not an integer. Therefore, almost bent functions exist only if $n$ is odd. To conclude, we should recall the result of Chabaud and Vaudenay [35] linking AB and APN functions.

Theorem 1.50. Any almost bent function is almost perfect nonlinear.

### 1.5.1.c. Known $A B$ and APN Permutations

By a power function, we mean an $(n, n)$-function $F$ which has the form $F(x)=x^{d}$ when we identify the space $\mathbb{F}_{2}^{n}$ with the finite field $\mathbb{F}_{2^{n}}$. Several almost perfect nonlinear power functions are known when $n$ is even, but they cannot be used as $S$-boxes in a substitution permutation network because they are not bijective. Indeed,

## Chapter 1 - Substitution-Permutation Networks

| Function | Exponent $d$ | Conditions | Proven in |
| :--- | :--- | :--- | :--- |
| Gold functions | $2^{i}+1$ | $\operatorname{gcd}(i, n)=1$ | [45, 80] |
| Kasami functions | $2^{2^{i}}-2^{i}+1$ | $\operatorname{gcd}(i, n)=1$ | $[58$, |
| Welch function | $2^{t}+3$ | $n=2 t+1$ | [28, 29, 44] |
| Niho function | $2^{t}+2^{\frac{t}{2}}-1, \quad t$ even | $n=2 t+1$ | [43, 53] |
|  | $2^{t}+2^{\frac{3 t+1}{2}}-1, t$ odd |  |  |

Figure 1.15: Known AB (and APN) power permutations $x \mapsto x^{d}$ over $\mathbb{F}_{2^{n}}$ with $n$ odd.

| Function | Exponent $d$ | Conditions | Proven in |
| :--- | :--- | :---: | :--- |
| Gold functions | $2^{i}+1$ | $\operatorname{gcd}(i, n)=1, n \equiv 2 \bmod 4$ | $[45,80]$ |
| Kasami functions | $2^{2^{i}}-2^{i}+1$ | $\operatorname{gcd}(i, n)=1, n \equiv 2 \bmod 4$ | $[58$ |
| Inverse function | $2^{n}-2$ | - | $[66]$ |

Figure 1.16: Known power permutations $F: x \mapsto x^{d}$ over $\mathbb{F}_{2^{n}}$ with $n$ even such that $F$ is 4-uniform and $2^{n} \times \mathrm{C}_{F}^{\max }=2^{\frac{n+2}{2}}$.
it is proven in [33, Section 2.1.3] that an APN power function is a permutation of $\mathbb{F}_{2}^{n}$ if and only if $n$ is odd.

In Figure 1.15, we enumerate the known almost bent power functions of $\mathbb{F}_{2^{n}}$ with $n$ odd. According to Theorem 1.50, these functions are also almost perfect nonlinear, which proves in particular that they are permutations of $\mathbb{F}_{2^{n}}$. In other words, these power permutations are $S$-boxes with optimal resistance against differential and linear cryptanalysis.

When $n$ is even, we already know that $A B$ functions, and hence $A B$ permutations do not exit. The existence of APN permutations with $n$ even has been a long-standing open question. However, in 2009 Dillon et al. [18 exhibited an APN permutation on 6 bits. So far, it is the only APN permutation of $\mathbb{F}_{2}^{n}$ known when $n$ is even, up to equivalence.

Therefore, when $n$ is even we generally use $n$-bit S-boxes $F$ with parameters close to AB and APN functions, namely 4-uniform permutations such that $2^{n} \times \mathrm{C}_{F}^{\max }=2^{\frac{n+2}{2}}$. All the 4 -bit S-boxes have been classified in [72] and we now know that these values are optimal for $n=4$. Figure 1.16 gives the known power permutations with these parameters. Observe that if $n$ is a multiple of 4 , the only known power permutation reaching these values is the inversion. This explains why the S-box of the AES is affine-equivalent to the inversion in $\mathbb{F}_{2^{8}}$.

### 1.5.2. Branch Number of the Diffusion Layer

In the previous section, we have describe how to design a substitution layer resistant to differential and linear cryptanalysis. Now we focus on the diffusion layer of an SPN. By virtue of Propositions 1.17 and 1.32 , the diffusion layer alone cannot provide any

## 1.5 - Security Evaluation of SPN Building Blocks

resistance to these attacks since it is linear. However, the diffusion layer can enhance the resistance provided by the substitution layer. The wide trail strategy is a design principle of block ciphers introduced by Daemen and Rijmen in [39]. Following this strategy, the diffusion layer should ensure that any linear of differential trail activate a large number of S-boxes.

The Hamming weight of an element $x$ of $\mathbb{F}_{2}^{n}$, denoted by $\mathrm{w}(x)$, is the number of nonzero components of $x$, that is $\mathrm{w}(x)=\#\left\{0 \leq i<n \mid x_{i} \neq 0\right\}$. By analogy, we define the bundle weight of an element $x$ in $\left(\mathbb{F}_{2}^{n}\right)^{m}$ to be the number $\mathrm{w}_{n}(x)$ of nonzero bundles of $x$, so $\mathrm{w}_{n}(x)=\#\left\{0 \leq i<m \mid x_{i} \neq 0_{n}\right\}$. The following definition characterizes the efficiency of the diffusion provided by the diffusion layer with respect to differential and linear cryptanalysis.

Definition 1.51 (Branch Number). Let $\lambda:\left(\mathbb{F}_{2}^{n}\right)^{m} \rightarrow\left(\mathbb{F}_{2}^{n}\right)^{m}$ be a $\mathbb{F}_{2}$-linear mapping. The differential branch number $\mathcal{B}_{\mathrm{D}}$ and the linear branch number $\mathcal{B}_{\mathrm{L}}$ of $\lambda$ (with respect to $\mathbb{F}_{2}^{n}$ ) are defined by

$$
\begin{aligned}
\mathcal{B}_{\mathrm{D}}(\lambda) & =\min \left\{\mathrm{w}_{n}(x)+\mathrm{w}_{n}(\lambda(x)) \mid x \in\left(\mathbb{F}_{2}^{n}\right)^{m}, x \neq 0\right\}, \\
\mathcal{B}_{\mathrm{L}}(\lambda) & =\min \left\{\mathrm{w}_{n}(x)+\mathrm{w}_{n}\left(\lambda^{\top}(x)\right) \mid x \in\left(\mathbb{F}_{2}^{n}\right)^{m}, x \neq 0\right\} .
\end{aligned}
$$

Clearly, the differential and linear branch numbers of $\lambda$ are upper-bounded by $m+1$. The linear mapping $\lambda$ whose branch numbers meet this bound with equality is said to be MDS or a perfect diffusion layer. In fact, perfect diffusions layers can be constructed from MDS codes, the reader can refer to [39, Sections 2.2 and 9.6].

Let us consider a generic SPN. The branch numbers of the diffusion layer can be used to derive important bounds on the maximal differential probability or linear potential of a trail. Therefore, the cipher's security can easily be assessed using the practical measure. The following theorem comes from [39, Theorem 9.3.1].

Theorem 1.52. Consider a generic SPN and denote by $S_{0}, \ldots, S_{m-1}$ its $n$-bit Sboxes and by $\pi: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ its diffusion layer. The maximum differential probability and linear potential of any 2 -round trail are respectively upper-bounded by

$$
\left(\max _{i<m} \mathrm{DP}_{S_{i}}^{\max }\right)^{\mathcal{B}_{\mathrm{D}}(\pi)} \quad \text { and } \quad\left(\max _{i<m} \mathrm{LP}_{S_{i}}^{\max }\right)^{\mathcal{B}_{\mathrm{L}}(\pi)}
$$

Chapter 1 - Substitution-Permutation Networks


## Security Evaluation of SPN

Differential [13] and linear [74] cryptanalysis are considered as the most important attacks against block ciphers [64]. As mentioned in [41], any new cipher should at least be accompanied by a detailed analysis of its strength against these two attacks. We have seen in Chapter 1 that the security of a cipher is assessed by the maximum expected differential probability (MEDP) or linear potential (MELP). When these values are low enough, the cipher is provably secure [57]. Nevertheless, computing the MEDP and MELP or even finding a useful upper bound remains a challenging open problem and the common proofs of security focus only on differential and linear trails. A cipher is then said to be practically secure when the maximum differential probability or linear potential of all trails gives rise to an ineffective cryptanalysis. Finally, it should be stressed that all these security measures tacitly assume that the round keys are independent. The cryptographer then assumes that these theoretical measures reflect the actual security when the round keys are fixed and derived from a key schedule. This hypothesis, called stochastic equivalence [67], seems to hold for almost all secure ciphers.

To prevent differential and linear cryptanalysis, the SPN designer must first choose S-boxes providing high resistance against both these attacks. These choices define the substitution layer of the cipher. Concerning the diffusion layer, two main families stand out. On one hand, the diffusion of the cipher can be done using a bit permutation. Even if bit permutations do not provide the best security, they are generally chosen for efficiency purposes. Indeed, in the last few years, many lightweight block ciphers using bit permutations have been suggested [17, 36, 95]. A recent survey of lightweight block ciphers can be found in [15]. On the other hand, the diffusion layer can involve a more complicated linear mapping defined for example as a matrix product over finite fields. Such mappings are generally more computationally expensive but they also provide high diffusion, ensuring that every trail activates a minimum number of S-boxes. Relying on this property, the designer can derive bounds on the maximum differential probability and linear potential of any trail and simply prove the practical security of its cipher.

However, the bounds obtained for an SPN which uses bit permutations may not suffice to prove its security. In fact, bit permutations have the smallest branch number possible among all linear permutations and the cipher security is hard to establish without a close analysis. The same observation may apply for backdoor

## Chapter 2 - Security Evaluation of SPN

ciphers since the mathematical structure of the backdoor strongly reduces the choice of the cipher's primitives. Thus, the usual strategies to thwart differential and linear cryptanalysis may no longer be useful. This motivates alternative methods to prove the security with respect to these attacks.

In this chapter, we describe a fully automatic algorithm finding an optimal differential or linear trail in an SPN. Our contribution was presented in [8]. The first algorithm finding optimal trails was introduced by Matsui in [76] for Feistel ciphers. Running his algorithm several times on the DES, Matsui found a permutation of the S-boxes making the DES stronger against differential and linear cryptanalysis. The algorithm complexity remaining too high for the cipher FEAL, two successive improvements have been proposed in [87] then [3]. Although an adaptation of Matsui's algorithm is straightforward for SPN, the block size (from 64 to 128 bits) of modern ciphers makes it computationally infeasible. This fact was also highlighted by Collard et al. [37] who then proposed a few improvements to use this algorithm on the cipher Serpent. In addition, it should be mentioned that another variation was exposed by Ali and Heys in [1]. They gave up finding an optimal trail to reduce the complexity. On the other side, their algorithm cannot prove the cipher practical security, but may still help the cryptanalyst to perform a differential or linear cryptanalysis. Our algorithm is an adaptation of [3, [76, 87] for SPN. We introduce several optimizations paying special attention to ciphers which have a bit permutation as diffusion layer.

After a brief summary of differential and linear cryptanalysis, the next section exposes a straightforward adaptation of Matsui's algorithm to compute optimal trails in substitution-permutation networks. An example of execution is then given in Section 2.2. All our optimizations are explained intuitively in this example and then formalized in Section 2.3. Finally, we present our results and close this chapter in Section 2.4 .

### 2.1. Search for an Optimal trail

Throughout this section, we consider a generic $r$-round substitution-permutation network $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ such that for each cipher key $K$,

$$
E_{K}=F_{k[r-1]} \circ \cdots \circ F_{k[0]} \quad \text { with } \quad F_{k[i]}=\pi \circ \sigma \circ \alpha_{k[i]} .
$$

As explained in Section 1.3.2 and 1.4.2, the last round includes and ends with a diffusion layer because the linear approximations or differentials used in an attack have fewer rounds that the whole cipher. We denote by $S_{0}, \ldots, S_{m-1}$ the $n$-bit S-boxes of the substitution layer. Recall that the differential probability and linear potential matrices of an S-box $S$ are defined for all $a, b$ in $\mathbb{F}_{2}^{n}$ by the formulae

$$
\begin{aligned}
\operatorname{DP}_{S}(a, b) & =2^{-n} \times \#\left\{x \in \mathbb{F}_{2}^{n} \mid S(x)+S(x+a)=b\right\}, \\
\operatorname{LP}_{S}(a, b) & =\left(2^{-(n-1)} \times \#\left\{x \in \mathbb{F}_{2}^{n} \mid\langle a, x\rangle=\langle b, S(x)\rangle\right\}-1\right)^{2} .
\end{aligned}
$$

The maximum differential probability and linear potential of $S$ are then defined to be

$$
\operatorname{DP}_{S}^{\max }=\max \left\{\operatorname{DP}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}, \quad \operatorname{LP}_{S}^{\max }=\max \left\{\operatorname{LP}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}
$$

According to Definitions 1.18 and 1.33, an $r$-round differential or linear trail is a family $\left(a^{[0]}\right)_{i \leq r}$ of $r+1$ patterns in $\mathbb{F}_{2}^{n m}$. In this chapter, it is however more convenient to specify for each round the input and output patterns of the substitution layer. Therefore, we equivalently define a differential or linear trail $\mathcal{T}$ to be a family $\left(\left(a^{[i]}, b^{[i]}\right)_{i<r}\right.$ of $r$ pairs of input/output patterns such that for each $i<r-1$,

$$
a^{[i+1]}= \begin{cases}\pi\left(b^{[i]}\right) & \text { for differential trails }, \\ \left(\pi^{\top}\right)^{-1}\left(b^{[i]}\right) & \text { for linear trails }\end{cases}
$$

The equivalence between these two definitions follows from Propositions 1.17 and 1.31. Additionally, if the diffusion layer $\pi$ is a bit permutation, it can be proven that $\left(\pi^{\top}\right)^{-1}=\pi$. In this case, the same structure can be seen as a differential or linear trail. Next, the differential probability and the linear potential of the trail $\mathcal{T}$ are given by

$$
\begin{aligned}
& \operatorname{DP}(\mathcal{T})=\prod_{i=0}^{r-1} \operatorname{DP}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=\prod_{i, j \mid a_{j}[i] \pm 0} \operatorname{DP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right), \\
& \operatorname{LP}(\mathcal{T})=\prod_{i=0}^{r-1} \operatorname{LP}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=\prod_{i, j \mid a_{j}[i] \pm 0} \operatorname{LP}_{S_{j}}\left(a_{j}^{[i]}, b_{j}^{[i]}\right),
\end{aligned}
$$

as established by Propositions 1.24 and 1.36. In other words, the differential probability of a trail is obtained by multiplying the differential probabilities of its active S-boxes.

Definition 2.1 (Optimal Trail). An $r$-round differential trail which has maximum probability among all $r$-round trails is said to be optimal. Naturally, we define an optimal linear trail to be a trail which has maximal linear potential. In this case, its probability (or potential) is denoted by $p_{o}^{(r)}$.

It is worth noting that there may exist more than one optimal trail. In the context of our search algorithm, a candidate for an input pattern $a$ in $\mathbb{F}_{2}^{n m}$ is an output pattern $b$ such that $\operatorname{DP}_{\sigma}(a, b)$ is nonzero. Of course, if we search for an optimal linear trail, this condition becomes $\operatorname{LP}_{\sigma}(a, b) \neq 0$. If $\mathcal{T}=\left(\left(a^{[i]}, b^{[i]}\right)\right)_{i<r}$ is an $r$-round trail, we denote by $\mathcal{T}{ }^{[i, j]}$ the sub-trail $\left(\left(a^{[k]}, b^{[k]}\right)\right)_{i \leq k \leq j}$. Finally, we will need the following definition.

Definition 2.2 (Trail Extension). Let $r_{1}$ and $r_{2}$ be integers such that $0 \leq r_{1} \leq r_{2}$. Let $\mathcal{T}_{1}$ and $\mathcal{T}_{2}$ be $r_{1}$ and $r_{2}$-round trails respectively. The trail $\mathcal{T}_{2}$ extends $\mathcal{T}_{1}$ if $\mathcal{T}_{2}{ }^{[0, r-1]}=\mathcal{T}$. In this case, $\mathcal{T}_{2}=\mathcal{T}_{1} \| \mathcal{T}_{2}^{\left[r, r^{\prime}-1\right]}$.

## Chapter 2 - Security Evaluation of SPN

### 2.1.1. General Principle

Let us now present a straightforward adaptation of Matsui's search algorithm for substitution-permutation networks. First, we explain how this algorithm computes an optimal differential trail. Then we will detail the changes that need to be made to compute an optimal linear trail.

Let us denote $R$ the actual number of rounds of the SPN. The algorithm presented in this chapter computes an optimal $R$-round trail without requiring any a priori knowledge. This algorithm is based on another search algorithm called OptTrailEst which takes as arguments:

- an integer $r \geq 2$ representing the current number of rounds,
- the probabilities $\left(p_{o}^{(i)}\right)_{1 \leq i<r}$ of optimal $i$-round trails,
- an estimation $p_{\mathrm{e}}^{(r)}$ of the probability $p_{\mathrm{o}}^{(r)}$ of the optimal trail searched,
and returns an optimal $r$-round trail denoted by $\mathcal{T}_{\mathrm{o}}{ }^{(r)}$. The knowledge of $\left(p_{\mathrm{o}}^{(i)}\right)_{1 \leq i<r}$ and $p_{\mathrm{e}}^{(r)}$ speeds up the search. Next, an automatic management of the estimation $p_{\mathrm{e}}^{(r)}$ will be proposed in Section 2.3.5 yielding the algorithm OptTrail. To summarize, the search algorithm OptTrail takes only $r$ and $\left(p_{o}^{(i)}\right)_{1 \leq i<r}$ as inputs and still outputs an optimal $r$-round trail.

Let us now explain how the algorithm OptTrail can be used to compute an optimal $R$-round trail from scratch. First, observe that $p_{\mathrm{o}}^{(1)}$ can be easily computed (cf Remark 2.8). Then, compute

$$
\mathcal{T}_{o}^{(r)}=\text { OptTrail }\left(r,\left(p_{\mathrm{o}}^{(i)}\right)_{1 \leq i<r}\right) \quad \text { and } \quad p_{o}^{(r)}=\operatorname{DP}\left(\mathcal{T}_{o}^{(r)}\right)
$$

for $r$ from 2 to $R$. The latter computation gives the desired result, as illustrated in Figure 2.1.

The rest of this section is dedicated to the algorithm OptTrailEst given in Figure 2.2. Let us explain how this algorithm works. First, suppose that the conditions on lines 9 and 18 are always true and that $p_{\mathrm{e}}^{(r)}$ is equal to 0 . Under this assumption, the algorithm runs implicitly through the trees of all $r$-round trails and saves one which has a maximum probability in the variable $\mathcal{T}_{o}{ }^{(r)}$. Observe that the first and last rounds have a special treatment that speeds up the search. When the program reaches the function Round ( $s, \mathcal{T}^{(s-1)}, p^{(s-1)}$ ), the current trail is

$$
\begin{aligned}
& \mathcal{T}^{(s-1)}=\left(\left(a^{[0]}, b^{[0]}\right), \ldots,\left(a^{[s-2]}, b^{[s-2]}\right)\right), \\
& \operatorname{DP}\left(\mathcal{T}^{(s-1)}\right)=\prod_{i=0}^{s-2} \operatorname{DP}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=p^{(s-1)} .
\end{aligned}
$$

The input pattern $a^{[s-1]}$ for this round equals $\pi\left(b^{[s-2]}\right)$. Then, for each candidates $b^{[s-1]}$ for $a^{[s-1]}$, the current trail $\mathcal{T}^{(s-1)}$ is extended by ( $\left.a^{[s-1]}, b^{[s-1]}\right)$ and the search for the next round is called. Therefore, the program performs a depth-first search. When the algorithm reaches the function LastRound (), it is not hard to compute the output pattern $b^{[r-1]}$ maximizing the probability of the last round. The trail is then saved only if its probability is greater than the probability $p_{e}^{(r)}$ of the best trail $\mathcal{T}_{\mathrm{o}}{ }^{(r)}$ found up to this point. It remains to explain the conditions on lines 9 and 18.


Input. The number $R$ of rounds of the cipher.
Output. An optimal $R$-round trail $\mathcal{T}_{0}^{(R)}$.
$p_{\mathrm{o}}^{(1)} \leftarrow \max \left\{\mathrm{DP}_{\sigma}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n}\right)^{m}\right\}$
For $r$ from 2 to $R$ do $\mathcal{T}_{\mathrm{o}}^{(r)} \leftarrow \operatorname{OptTrail}\left(r,\left(p_{\mathrm{o}}^{(i)}\right)_{1 \leq i<r}\right)$ $p_{o}^{(r)} \leftarrow \operatorname{DP}\left(\mathcal{T}_{o}^{(r)}\right)$
Return $\mathcal{T}_{\mathrm{o}}{ }^{(R)}$
Figure 2.1: Use of OptTrail.

Definition 2.3 (rank- $s$ bound). Let $\mathcal{T}$ be an $s$-round trail with $1 \leq s<r$. Its probability is said to be less than the rank-s bound if

$$
\operatorname{DP}(\mathcal{T})<\frac{p_{\mathrm{e}}^{(r)}}{p_{\mathrm{o}}^{(r-s)}}
$$

This condition on the probability of the current trail allows to prune the search tree without missing an optimal trail. It can be rewritten as

$$
\operatorname{DP}(\mathcal{T}) \times p_{o}^{(r-s)}<p_{\mathrm{e}}^{(r)}
$$

and means that even if the trail is extended by an optimal $(r-s)$-round trail, the probability of the whole trail would be less than $p_{e}^{(r)}$.

The significance of $p_{\mathrm{e}}^{(r)}$ is now clear. If $p_{\mathrm{e}}^{(r)}>p_{\mathrm{o}}^{(r)}$, a trail expandable into an optimal $r$-round trail can be cut. Furthermore, no trail will be saved because of the condition on line 25 . On the other hand, the closer $p_{\mathrm{e}}^{(r)}$ is from $p_{\mathrm{o}}^{(r)}$, the stronger is the pruning condition and the lower is the complexity of OptTrailEst.

Theorem 2.4. According to the results recalled in introduction of this section, the algorithm OptTrailEst can compute an optimal linear trail simply by replacing every DP by LP and every $\pi(\ldots)$ by $\left(\pi^{\top}\right)^{-1}(\ldots)$.

### 2.1.2. Proof of the Algorithm

Having explained the general principle of the algorithm, it remains now to prove the optimality of the trail returned.

## Chapter 2 - Security Evaluation of SPN

```
Algorithm 1 - OptTrailEst (r, ( poo (i)}\mp@subsup{)}{1\leqi<r,}{},\mp@subsup{p}{\textrm{e}}{(r)}
```

Input. The current number $r$ of rounds $(r \geq 2)$, the probabilities $\left(p_{\mathrm{o}}^{(i)}\right)_{1 \leq i<r}$ and an estimation $p_{\mathrm{e}}^{(r)}$ of $p_{\mathrm{o}}^{(r)}$
Output. Depending on the estimation $p_{\mathrm{e}}^{(r)}$, this algorithm returns :

- an optimal $r$-round trail $\mathcal{T}_{\mathrm{o}}^{(r)}$ if $p_{\mathrm{e}}^{(r)} \leq p_{\mathrm{o}}^{(r)}$;
- the empty trail if $p_{\mathrm{e}}^{(r)}>p_{\mathrm{o}}^{(r)}$.
$\mathcal{T}_{\mathrm{o}}{ }^{(r)} \leftarrow()$
For each non-zero output pattern $b^{[0]}$ do
Call FirstRound $\left(b^{[0]}\right)$
Return $\mathcal{T}_{\mathrm{o}}{ }^{(r)}$
Function FirstRound $\left(b^{[0]}\right)$
$a^{[0]} \leftarrow \arg \max \left\{\mathrm{DP}_{\sigma}\left(a, b^{[0]}\right) \mid a \in \mathbb{F}_{2}^{n m}\right\}$
$\mathcal{T}^{(1)} \leftarrow\left(\left(a^{[0]}, b^{[0]}\right)\right)$
$p^{(1)} \leftarrow \mathrm{DP}_{\sigma}\left(a^{[0]}, b^{[0]}\right)$
If $p^{(1)}$ is not less than the rank-one bound then
If $r>2$ then
Call Round $\left(2, \mathcal{T}^{(1)}, p^{(1)}\right)$ Else

Call LastRound( $\left.\mathcal{T}^{(1)}, p^{(1)}\right)$
Function Round $\left(s, \mathcal{T}^{(s-1)}, p^{(s-1)}\right)$
$a^{[s-1]} \leftarrow \pi\left(b^{[s-2]}\right)$
For each candidate $b^{[s-1]}$ for $a^{[s-1]}$ do $p^{(s)} \leftarrow p^{(s-1)} \times \mathrm{DP}_{\sigma}\left(a^{[s-1]}, b^{[s-1]}\right)$ If $p^{(s)}$ is not less than the rank-s bound then $\mathcal{T}^{(s)} \leftarrow \mathcal{T}^{(s-1)} \|\left(a^{[s-1]}, b^{[s-1]}\right)$ If $s+1<r$ then
Call Round $\left(s+1, \mathcal{T}^{(s)}, p^{(s)}\right)$
Else
Call LastRound $\left(\mathcal{T}^{(s)}, p^{(s)}\right)$
Function LastRound $\left(\mathcal{T}^{(r-1)}, p^{(r-1)}\right)$
$a^{[r-1]} \leftarrow \pi\left(b^{[r-2]}\right)$
$b^{[r-1]} \leftarrow \arg \max \left\{\mathrm{DP}_{\sigma}\left(a^{[r-1]}, b\right) \mid b \in \mathbb{F}_{2}^{n m}\right\}$
$p^{(r)} \leftarrow p^{(r-1)} \times \mathrm{DP}_{\sigma}\left(a^{[r-1]}, b^{[r-1]}\right)$
If $p^{(r)} \geq p_{\mathrm{e}}^{(r)}$ then
$\mathcal{T}^{(r)} \leftarrow \mathcal{T}^{(r-1)} \|\left(a^{[r-1]}, b^{[r-1]}\right)$
$\mathcal{T}_{0}^{(r)} \leftarrow \mathcal{T}^{(r)} \quad$ The current trail is saved
$p_{\mathrm{e}}^{(r)} \leftarrow p^{(r)}$

Figure 2.2: The search algorithm OptTrailEst for an optimal trail.

Lemma 2.5. Let $s$ be an integer such that $1 \leq s<r$. Let $\mathcal{T}$ be an $s$-round trail whose probability is less than the rank- $s$ bound. Then, there does not exist any $r$-round trail extending $\mathcal{T}$ with probability greater than or equal to $p_{\mathrm{e}}^{(r)}$.

Proof. By contradiction, assume that $\mathcal{T}_{r}$ is an $r$-round trail extending $\mathcal{T}$ such that $\operatorname{DP}\left(\mathcal{T}_{r}\right) \geq p_{\mathrm{e}}^{(r)}$. Then the probability of the $(r-s)$-round trail $\mathcal{T}_{r}{ }^{[s, r-1]}$ is

$$
\operatorname{DP}\left(\mathcal{T}_{r}^{[s, r-1]}\right)=\frac{\operatorname{DP}(\mathcal{T}) \times \operatorname{DP}\left(\mathcal{T}_{r}^{[s, r-1]}\right)}{\operatorname{DP}(\mathcal{T})}=\frac{\operatorname{DP}\left(\mathcal{T} \| \mathcal{T}_{r}^{[s, r-1]}\right)}{\operatorname{DP}(\mathcal{T})}=\frac{\operatorname{DP}\left(\mathcal{T}_{r}\right)}{\operatorname{DP}(\mathcal{T})}
$$

By assumption, $\operatorname{DP}(\mathcal{T})$ is strictly less than $p_{e}^{(r)} / p_{o}^{(r-s)}$. Note that this strict inequality implies that $p_{\mathrm{e}}^{(r)}$ is nonzero. It follows that

$$
\operatorname{DP}\left(\mathcal{T}_{r}^{[s, r-1]}\right)=\frac{\operatorname{DP}\left(\mathcal{T}_{r}\right)}{\operatorname{DP}(\mathcal{T})} \geq \frac{p_{\mathrm{e}}^{(r)}}{\operatorname{DP}(\mathcal{T})}>\frac{p_{\mathrm{e}}^{(r)}}{p_{\mathrm{e}}^{(r)} / p_{\mathrm{o}}^{(r-s)}}=p_{\mathrm{o}}^{(r-s)} .
$$

By definition of $p_{\mathrm{o}}^{(r-s)}$, this leads to a contradiction which proves the result.
Theorem 2.6 (validity of the algorithm). Depending on the estimation $p_{\mathrm{e}}^{(r)}$, the algorithm OptTrailEst returns

- an optimal $r$-round trail $\mathcal{T}_{\mathrm{o}}^{(r)}$ if $p_{\mathrm{e}}^{(r)} \leq p_{\mathrm{o}}^{(r)}$;
- the empty trail if $p_{\mathrm{e}}^{(r)}>p_{\mathrm{o}}^{(r)}$.

Proof. Suppose the condition on the bound to be removed. If $p_{\mathrm{e}}^{(r)}$ is less than $p_{\mathrm{o}}^{(r)}$, an optimal trail is saved in $\mathcal{T}_{\mathrm{o}}^{(r)}$, otherwise $\mathcal{T}_{\mathrm{o}}{ }^{(r)}$ remains empty. Then, Lemma 2.5 ensures that the pruning condition avoids only the trails which have probabilities strictly less than $p_{\mathrm{e}}^{(r)}$. The result still holds.

### 2.2. A Detailed Example

The algorithm OptTrailEst is a depth-first search within the trees of all $r$-round differential trails together with a pruning mechanism which cuts only non-optimal trails. Any enhancement of this pruning condition directly impacts the algorithm complexity. Thus, a good algorithmic optimization of OptTrailEst rests on the right balance between cost and efficiency of such an enhancement.

Before addressing the formal treatment of our optimizations in Section 2.3, we introduce an example explaining each of them intuitively. Let us consider a 16bit substitution permutation network quite similar to the TOYCIPHER presented in Example 1.14. First, it is worth recalling that the differential probability of a trail is computed over the associated long-key cipher. The key-schedule is thus disregarded throughout this chapter. To make this example more interesting, the substitution layer involves now four different 4-bit S-boxes denoted by $S_{0}, S_{1}, S_{2}$ and $S_{3}$. The definition of these S-boxes and their respective differential probability matrices are given in Figure 2.3. As can be seen, the S-box $S_{0}$ is optimal with respect

## Chapter 2 - Security Evaluation of SPN

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathrm{S}_{0}(x)$ | E | A | 1 | 2 | 7 | F | D | 6 | C | 3 | 0 | 9 | 8 | 4 | 5 | B |
| $S_{1}(x)$ | C | A | E | 0 | D | 3 | 1 | 8 | B | 2 | 9 | 4 | 5 | 6 | 7 | F |
| $S_{2}(x)$ | 5 | 9 | F | 8 | 6 | 0 | A | 3 | 7 | C | 4 | 1 | E | 2 | D | B |
| $S_{3}(x)$ | 9 | 5 | 7 | D | A | C | 2 | 4 | E | F | 6 | B | 0 | 1 | 8 | 3 |


|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 0 | 16 | . | . | . | . |  | . |  | . | . |  | . | . |  | . |  | 0 | 16 | . | . | . | . | . | . | . |  | . | . | . | . | . |  | . |
| 1 | . | . |  | 2 | 2 |  |  |  | 2 | 2 | . | 2 | 2 | . | 2 | 2 | 1 |  | . | . | 2 | . | . | 2 | . | 2 | 4 | . | . | . | 2 | 4 | . |
| 2 | . | . |  | . | . |  | . | . | 2 | 2 | 4 | . | 2 | 2 | . | 4 | 2 | . | . | 6 | . | . | . | 2 | . |  | 2 | 2 | 2 | 2 | . |  | . |
| 3 | . | 4 | 2 | 4 | . | 2 | . | . |  |  |  | 2 | 2 | . | . |  | 3 | . | 2 | 2 | . | 2 | 2 | . |  |  | . | 2 | 2 | 2 | . |  | 2 |
| 4 | . | . | 2 | . | 4 | 4 | . | 2 | . | 2 | . | . | 2 | . | . |  | 4 | . | 2 | . | . | 2 | . | . | . | 2 | 2 | . | 2 | . | . | 4 | 2 |
| 5 | . | 2 | . | . | . |  |  | 2 | 2 | . | . | 4 | 2 | 2 | . | 2 | 5 | . | 2 | . | 2 | . | . | 4 | 4 | . | . |  | . | . | 2 |  | 2 |
| 6 | . | . |  | 2 | . |  | 2 | . | 4 | 2 | . | . | 2 | 4 | . | . | 6 | . | . | 4 | 4 | . | . | . | . |  | . |  |  | 4 | 4 |  | . |
| 7 | - | 2 | - | . | 2 | 2 | 2 | 4 | 2 | . | . | . | . | . | 2 | . | 7 | . | 2 | . | . | 4 | 2 | . | . | . | . |  | 2 | . | 4 |  | 2 |
| 8 | . | 2 | 2 | . | . | . | . | . | 2 | 2 | . | 4 | . | 2 | . | 2 | 8 | . | . | . | . | 2 | 2 | 2 | 6 | 4 | . | . | . | . | . |  | . |
| 9 | . | . | 2 | 4 | . |  | 4 | 2 | 2 | . |  | . | . | 2 | . | . | 9 | . | 2 | . | . | . | . | 2 | . |  | 2 | 2 | 2 | . | . | 4 | 2 |
| A | . | 2 | 4 | 2 | 2 | 2 | . | . |  | . | . | . | . | 2 | 2 | . | A | . | . | 2 | . | 2 | 4 | . | . | . | . | 2 | . | 2 | . | 4 | . |
| B | . | . | 2 | . | . | . | . | 2 |  | 2 | 4 | . | 2 | . | 4 |  | B | . | . | 2 | 2 | 2 | . | . | 2 | 2 | . | . | 2 | 2 | 2 |  | . |
| C | . |  | . | . | 2 |  | 2 | . |  | 2 | . | 2 | 2 | 2 | 2 | 2 | C | . | 2 | . | . | . | . | 2 | . | 2 | 4 | . | . | 4 | . |  | 2 |
| D | . | . | 2 | 2 | 4 | . | 2 | 2 | . | . | 4 | . | . | . | . | . | D | . | 4 | . | . | . | 2 | . | 2 | 2 | . | 2 | . | . | . |  | 4 |
| E | - | 4 | . | . | . | 2 | 4 | 2 |  | 2 | . | 2 | . | - | . | - | E | . | . | . | . | 2 | 2 | 2 | 2 |  |  | 4 | 4 | . | . |  | . |
| F | $\cdot$ |  | - | - | . | 4 | . | . |  | . | 4 | . | . | . | 4 | 4 | F | . | . | - | 6 | . | 2 | . | . | 2 | 2 | 2 | . | . | 2 |  | . |
|  |  |  |  |  |  |  |  |  |  | $b$ |  |  |  |  |  |  |  |  |  |  |  | $2^{4}$ |  |  |  |  |  |  |  |  |  |  |  |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 0 | 16 | . |  | . | . |  | - |  |  | - |  | . | - | . | - | - | 0 | 16 | . | . | . | . | . | - | . |  |  | . | - | . | - |  |  |
| 1 | . |  |  | . |  | 2 | 4 | 2 |  | 2 |  | 2 | 4 | . | - |  | 1 |  | 4 | . | . | . | . | 4 | . |  |  | 2 | 2 | 2 | 2 |  |  |
| 2 | . | 2 | . | 6 | . | . | . | . |  | 2 | 2 | . | 2 | 2 | . | - | 2 | . | . | 2 | . | 2 | . | . | . | 10 | . | . | . | . | . | 2 | . |
| 3 | . | . | . | . | . | 4 | 4 | . | 2 | . | 2 | . | . | 2 | . | 2 | 3 | . | . | 2 | 2 | 2 | 2 | . | . |  | 4 | . | . | . | . | 4 |  |
| 4 | . |  |  | 2 | . | 2 | - |  |  | 6 | 2 | 2 |  |  | 2 |  | 4 |  |  | . | 2 | . | 2 | . | . | 2 | 4 | . |  | . | . | 6 | . |
| 5 | . | . | 4 | . | . | 4 | . | . | . | . | . | . | 4 | . | . | 4 | 5 | . | . | . | 4 | . | 4 | . | . | . | . | . | . | . | . |  | 8 |
| 6 | . |  |  | 2 |  |  |  | 2 | 2 | 2 | 6 |  | . |  |  | 2 | 6 |  | 4 | . | . | . |  | 4 | . |  |  | 2 | 2 | 2 | 2 |  |  |
| 7 | . | 2 |  | 2 | . |  | 4 | . |  |  |  |  | 2 |  | 2 | 4 | 7 |  |  | . | . | . | . | . | 8 |  |  | . | 4 | . | 4 |  |  |
| 8 | . | . | 4 | . | . | 2 | . | 2 | 4 | 2 | . | 2 | . | . | - | . | 8 | . | 2 | . | - | . | . | 2 | 4 | . |  | 6 | . | . | 2 |  |  |
| 9 |  | 2 |  |  | 2 |  |  |  |  | 2 |  |  | 2 |  | 8 |  | 9 |  | 2 | . |  | . |  | 2 | . |  |  |  | 6 | 6 | . |  |  |
| A | . | 4 | . | . | 4 |  | - |  | 4 | . |  | 4 | . | - | . | . | A | . | . | 6 | . | . | 2 | . | . |  | 2 | . | . | . | . | 2 | 4 |
| B | . | . | . | 2 | 2 | . | . | . | 2 | . | . | . | . | 8 | . | 2 | B | . | . | 2 | 6 | 4 | . | . | . | 2 | 2 | . | . | . | . |  | . |
| C |  | 2 | 4 | 2 |  |  |  |  |  |  |  | 4 | 2 |  | 2 |  | C |  |  |  | 2 | 6 |  |  |  |  | 2 |  |  | . |  | 2 | 4 |
| D | . | . |  | . | 2 | 2 | . | 8 | . |  | 2 | 2 | . | . | . | . | D | . | . | 4 | . | 2 | 6 | . | . | 2 | 2 | . | . | . | . |  |  |
| E | . | 4 | 4 |  | . |  | . | . | 2 |  | 2 |  |  | 2 | . | 2 | E |  | 2 |  |  |  |  | 2 | 4 |  |  |  | 2 | 6 |  |  |  |
| F |  |  |  |  | 6 |  |  | 2 |  |  |  |  |  | 2 | 2 |  | F |  | 2 |  |  |  |  | 2 |  |  |  | 6 |  |  | 6 |  |  |

Figure 2.3: The S-boxes and their difference probability matrices used in Section 2.2.
to differential cryptanalysis [72] whereas the others are not. More precisely, their maximal differential probabilities are given by

$$
\mathrm{DP}_{S_{0}}^{\max }=\frac{4}{16}, \quad \mathrm{DP}_{S_{1}}^{\max }=\frac{6}{16}, \quad \mathrm{DP}_{S_{2}}^{\max }=\frac{8}{16}, \quad \mathrm{DP}_{S_{3}}^{\max }=\frac{10}{16}
$$

The substitution layer of this cipher is the permutation $\sigma$ of $\left(\mathbb{F}_{2}^{4}\right)^{4}$ defined by the formula

$$
\sigma\left(x_{0}, x_{1}, x_{2}, x_{3}\right)=\left(S_{0}\left(x_{0}\right), S_{1}\left(x_{1}\right), S_{2}\left(x_{2}\right), S_{3}\left(x_{3}\right)\right)
$$

For instance, $\sigma$ maps 0000 to EC59. Next, the diffusion layer is the bit permutation associated with the permutation $\phi$ of $\llbracket 0,16 \llbracket$ defined by the rule

$$
\phi(i)=4(i \bmod 4)+\left\lfloor\frac{i}{4}\right\rfloor .
$$

Thus, this diffusion layer is exactly the same as the one of ToyCipher. We now know the full specification of the round function.

Clearly, an optimal 1-round differential trail activates only the S-box which has the highest differential probability, namely $S_{3}$ for this cipher. As can be seen in Figure 2.3, $\mathrm{DP}_{S_{3}}(2,8)=\frac{10}{16}$, so the pair $(2,8)$ of input/output difference patterns has the maximal probability over $S_{3}$. Consequently, the differential trail

$$
\mathcal{T}_{o}^{(1)}=\left(\left(a^{[0]}, b^{[0]}\right)\right)=(((0,0,0,2),(0,0,0,8)))
$$

is optimal and holds with probability $p_{o}^{(1)}=\frac{10}{16}$. In this example, the trail $\mathcal{T}_{o}^{(1)}$ happens to be the only 1-round optimal trail. However, if all the S-boxes are equal to $S_{0}$, it goes without saying that there are many optimal 1-round differential trails. For each $1 \leq w \leq 4$, we denote by $\mathrm{DP}_{(w)}^{\max }$ the maximal probability of a 1-round differential trail activating $w$ S-boxes. The previous discussion ensures that

$$
\operatorname{DP}_{(1)}^{\max }=\operatorname{DP}\left(\mathcal{T}_{o}^{(1)}\right)=\frac{10}{16}
$$

Naturally, a 1-round trail activating two $S$-boxes has maximum probability if and only if it activates $S_{2}$ and $S_{3}$ with their maximum differential probabilities. Therefore,

$$
\mathrm{DP}_{(2)}^{\max }=\mathrm{DP}_{S_{2}}^{\max } \times \mathrm{DP}_{S_{3}}^{\max }=\frac{8}{16} \times \frac{10}{16}=\frac{80}{16^{2}} .
$$

Similarly, we can compute that

$$
\mathrm{DP}_{(3)}^{\max }=\prod_{i=1}^{3} \mathrm{DP}_{S_{i}}^{\max }=\frac{480}{16^{3}} \quad \text { and } \quad \mathrm{DP}_{(4)}^{\max }=\prod_{i=0}^{3} \mathrm{DP}_{S_{i}}^{\max }=\frac{1920}{16^{4}}
$$

Assume that the SPN described above consists of seven rounds. To compute an optimal 7-round differential trail, the algorithm OptTrailEst requires the probabilities $p_{o}^{(i)}$ of optimal $i$-round trails for each $1 \leq i<7$ and an estimation $p_{e}^{(7)}$ of the probability of the 7 -round optimal trail searched. As explained in Section 2.1.1, the probabilities $\left(p_{o}^{(i)}\right)_{i<7}$ are obtained with five previous iterations of OptTrail. These

## Chapter 2 - Security Evaluation of SPN

|  | $\mathcal{T}_{o}^{(1)}$ | $\mathcal{T}_{o}^{(2)}$ | $\mathcal{T}_{o}^{(3)}$ | $\mathcal{T}_{o}^{(4)}$ | $\mathcal{T}_{o}^{(5)}$ | $\mathcal{T}_{o}^{(6)}$ |
| :--- | :---: | :---: | :---: | :---: | :---: | :---: |
| $a^{[0]}$ | $(0,0,0,2)$ | $(0,0, \mathrm{~A}, 0)$ | $(0,0, \mathrm{~F}, 0)$ | $(0,0, \mathrm{~F}, 0)$ | $(0,0,0,2)$ | $(0,0, \mathrm{~A}, 0)$ |
| $b^{[0]}$ | $(0,0,0,8)$ | $(0,0,1,0)$ | $(0,0,4,0)$ | $(0,0,4,0)$ | $(0,0,0,8)$ | $(0,0,1,0)$ |
| $a^{[1]}$ |  | $(0,0,0,2)$ | $(0,2,0,0)$ | $(0,2,0,0)$ | $(1,0,0,0)$ | $(0,0,0,2)$ |
| $b^{[1]}$ |  | $(0,0,0,8)$ | $(0,2,0,0)$ | $(0,2,0,0)$ | $(4,0,0,0)$ | $(0,0,0,8)$ |
| $a^{[2]}$ |  |  | $(0,0,4,0)$ | $(0,0,4,0)$ | $(0,8,0,0)$ | $(1,0,0,0)$ |
| $b^{[2]}$ |  |  | $(0,0,9,0)$ | $(0,0,9,0)$ | $(0,8,0,0)$ | $(4,0,0,0)$ |
| $a^{[3]}$ |  |  |  | $(2,0,0,2)$ | $(4,0,0,0)$ | $(0,8,0,0)$ |
| $b^{[3]}$ |  |  |  | $(\mathrm{A}, 0,0,8)$ | $(4,0,0,0)$ | $(0,8,0,0)$ |
| $a^{[4]}$ |  |  |  |  | $(0,8,0,0)$ | $(4,0,0,0)$ |
| $b^{[4]}$ |  |  |  |  | $(0,7,0,0)$ | $(4,0,0,0)$ |
| $a^{[5]}$ |  |  |  |  |  | $(0,8,0,0)$ |
| $b^{[5]}$ |  |  |  |  |  | $(0,7,0,0)$ |
| DP | ${ }^{10} / 16$ | $40 /{ }_{16}{ }^{2}$ | $6^{3} /{ }_{16^{3}}$ | $40 \times 6^{3} / 16^{5}$ | $120 \times 4^{2} / 16^{5}$ | $120 \times 4^{3} / 16^{6}$ |

Figure 2.4: The optimal trails of the example
Global variables

| $p_{o}^{(6)}={ }^{120 \times 4^{3}} / 16^{6}$ | $p_{e}^{(7)}=120 \times 4^{4} / 16^{7}$ |
| :---: | :---: |
| Max probabilities for $w$ S-boxes |  |
| $\mathrm{DP}_{(1)}^{\max }=10 / 16$ | $\mathrm{DP}_{(3)}^{\max }=480 / 1^{3}$ |
| $\mathrm{DP}_{(2)}^{\max }=80 / 16^{2}$ | $\mathrm{DP}_{(4)}^{\max }=1920 / 16^{4}$ |



6 rounds

Figure 2.5: Example of Run for OptTrailEst
optimal trails are given in Figure 2.4. Recall that their probabilities are computed by simply multiplying the differential probabilities of their active S-boxes. For instance,

$$
\begin{aligned}
\operatorname{DP}\left(\mathcal{T}_{0}^{(3)}\right) & =\mathrm{DP}_{S_{3}}(\mathrm{~F}, 4) \times \mathrm{DP}_{S_{2}}(2,2) \times \mathrm{DP}_{S_{3}}(4,9) \times \mathrm{DP}_{S_{0}}(2, \mathrm{~A}) \times \mathrm{DP}_{S_{4}}(2,8) \\
& =\left(\frac{6}{16}\right)^{3} \times \frac{4}{16} \times \frac{10}{16}=\frac{40 \times 6^{3}}{16^{5}} .
\end{aligned}
$$

Finally, we choose $p_{\mathrm{e}}^{(7)}=\left(120 \times 4^{4}\right) / 16^{7}$ as estimation of $p_{\mathrm{o}}^{(7)}$. Recall that an automatic management of this estimation will given later in Section 2.3.5. But for now, let us detail some carefully chosen steps of the algorithm OptTrailEst. The parameters of this execution are summarized in Figure 2.5.

### 2.2.1. Search Algorithm for the First Round

Following the algorithm OptTrailEst, we must try to extend all the output patterns $b^{[0]}$ of the first round. Intuitively, a trail activating $(w+1)$ S-boxes in the first

Global variables

| $\overline{p_{\mathrm{o}}^{(6)}=120 \times 4^{3} / 16^{6}} \quad p_{\mathrm{e}}^{(7)}=120 \times 4^{4} / 16^{7}$ |  |
| :--- | :--- |
| Sorted candidates |  |
| $\mathrm{DP}_{S_{0}}(3,1)=4 / 16$ | $\mathrm{DP}_{S_{0}}(7,1)=2 / 16$ |
| $\operatorname{DP}_{S_{0}}(\mathrm{E}, 1)=4 / 16$ | $\mathrm{DP}_{S_{0}}(8,1)=2 / 16$ |
| $\operatorname{DP}_{S_{0}}(5,1)=2 / 16$ | $\mathrm{DP}_{S_{0}}(\mathrm{~A}, 1)=2 / 16$ |



6 rounds

Figure 2.6: Example of Run for FirstRound() - Part 1
round is less likely to be optimal than a trail activating $w$ S-boxes in this same round. Therefore, the patterns $b^{[0]}$ should not be tested in the natural order but according to the number of S-boxes they activate, or equivalently to their bundle weights (see Section 1.5.2). Indeed, once a 7 -round trail with probability higher than the estimation $p_{\mathrm{e}}^{(7)}$ is found, this estimation is updated and the pruning condition is enhanced for the rest of the execution. Consequently, the earlier high probability trails are found, the lower is the complexity of this algorithm.

Thus, the first pattern we may try to extend is $b^{[0]}=(1,0,0,0)$. This step is illustrated in Figure 2.6. We are now executing the function FirstRound. First, an input pattern $a^{[0]}$ maximizing the probability $\mathrm{DP}_{\sigma}\left(a^{[0]}, b^{[0]}\right)$ must be picked out. Because $S_{0}$ is the only S-box activated by $b^{[0]}$, this amounts to find an element $a_{0}$ maximizing $\mathrm{DP}_{S_{0}}\left(a_{0}, 1\right)$ and then define $a^{[0]}=\left(a_{0}, 0,0,0\right)$. All the nonzero differential probabilities of the form $\operatorname{DP}_{S_{0}}\left(a_{0}, 1\right)$ are enumerated in Figure 2.6. These values are directly drawn from the difference probability matrix of $S_{0}$ previously given in Figure 2.3. Thus, $a_{0}$ can be equal to 3 or E , it does not matter. Our current trail $\mathcal{T}^{(1)}$ is then equal to

$$
\mathcal{T}^{(1)}=\left(\left(a^{[0]}, b^{[0]}\right)\right)=(((3,0,0,0),(1,0,0,0)))
$$

and $\operatorname{DP}\left(\mathcal{T}^{(1)}\right)=\frac{4}{16}$. To obtain a 7 -round trail, the current trail $\mathcal{T}^{(1)}$ must be extended by a 6 -round trail. In the best-case scenario, its 6 -round extension is optimal and the resulting 7 -round trail has probability

$$
\operatorname{DP}\left(\mathcal{T}^{(1)}\right) \times p_{o}^{(6)}=\frac{4}{16} \times \frac{120 \times 4^{3}}{16^{6}}=\frac{120 \times 4^{4}}{16^{7}}
$$

which is (greater than or) equal to the estimation $p_{e}^{(7)}$. Consequently, its probability is consistent with our estimation and it is worth trying to extend the trail $\mathcal{T}^{(1)}$. Assuming that our estimation is less than $p_{o}^{(7)}$, this means that the current trail can potentially be extended into an optimal 7 -round trail. This trail is then handled by the function Round (2) and the input pattern for this second round is

$$
a^{[1]}=\pi\left(b^{[0]}\right)=(0,0,0,8) .
$$

This function, helped by all its recursive calls, tries all possible extensions of $\mathcal{T}{ }^{(1)}$. Unfortunately any of them yields an optimal 7-round trail.

## Chapter 2 - Security Evaluation of SPN

Global variables
$p_{\mathrm{o}}^{(6)}={ }^{120 \times 4^{3}} / 16^{6} \quad p_{\mathrm{e}}^{(7)}=120 \times 4^{4} / 16^{7}$
Sorted candidates
$\operatorname{DP}_{S_{0}}(1,9)=2 / 16 \quad \operatorname{DP}_{S_{0}}(8,9)=2 / 16$
$\mathrm{DP}_{S_{0}}(2,9)=2 / 16 \quad \mathrm{DP}_{S_{0}}(\mathrm{~B}, 9)=2 / 16$
$\mathrm{DP}_{S_{0}}(4,9)=2 / 16 \quad \mathrm{DP}_{S_{0}}(\mathrm{C}, 9)=2 / 16$
$\mathrm{DP}_{S_{0}}(6,9)=2 / 16 \quad \mathrm{DP}_{S_{0}}(\mathrm{E}, 9)=2 / 16$


6 rounds

Figure 2.7: Example of Run for FirstRound() - Part 2

The next step of the algorithm OptTrailEst is simply to try to extend another difference pattern $b^{[0]}$. Certainly, we try $b^{[0]}=(2,0,0,0)$, then $b^{[0]}=(3,0,0,0)$ and so on. Let us skip these steps until we reach the pattern $b^{[0]}=(9,0,0,0)$, represented in Figure 2.7. Again, the function FirstRound requires to select an input pattern $a^{[0]}$ that maximizes the probability of the current trail. Since this step is repeated many times during the execution of OptTrailEst, all the input patterns

$$
\arg \max \left\{\mathrm{DP}_{S_{i}}\left(a_{i}, b_{i}\right) \mid a_{i} \in \mathbb{F}_{2}^{n}\right\}
$$

for every $i<n$ and every $b_{i}$ in $\mathbb{F}_{2}^{n}$ should be computed and stored before running the algorithm. This time, all the candidates $a_{0}$ have the same differential probability, so we choose $a_{0}=1$ and the current trail becomes

$$
\mathcal{T}^{(1)}=\left(\left(a^{[0]}, b^{[0]}\right)\right)=(((1,0,0,0),(9,0,0,0))) \quad \text { and } \quad \operatorname{DP}\left(\mathcal{T}^{(1)}\right)=\frac{2}{16} .
$$

If $\mathcal{T}^{(1)}$ is extended by an optimal 6 -round trail, the resulting trail has probability

$$
\operatorname{DP}\left(\mathcal{T}^{(1)}\right) \times p_{\mathrm{o}}^{(6)}=\frac{2}{16} \times \frac{120 \times 4^{3}}{16^{6}}=\frac{120 \times 2 \times 4^{3}}{16^{7}}
$$

which less than our estimation. Using the vocabulary introduced in Section 2.1.1, the probability of the current trail is less than the rank-1 bound and this trail (and thus all its extensions) can be discarded without missing an optimal 7-round trail.

Once all the patterns $b^{[0]}$ activating one S-box in the first round are handled, we consider the patterns activating two S-boxes. Before trying to extend all these patterns, we should test if this effort is worthwhile. Since $\mathrm{DP}_{(2)}^{\max }$ is equal to $\frac{80}{16^{2}}$, the best 1-round trail that can be obtained in the function FirstRound has probability $\frac{80}{16^{2}}$. By computing

$$
\mathrm{DP}_{(2)}^{\max } \times p_{\mathrm{o}}^{(6)}=\frac{80}{16^{2}} \times \frac{120 \times 4^{3}}{16^{6}}=\frac{20}{16} \times p_{\mathrm{e}}^{(7)}
$$

we see that this probability is greater than $p_{e}^{(7)}$ so these patterns must be considered. Nevertheless, applying the same test to the patterns which activate three S-boxes in the first round yields

$$
\mathrm{DP}_{(3)}^{\max } \times p_{\mathrm{o}}^{(6)}=\frac{480}{16^{3}} \times \frac{120 \times 4^{3}}{16^{6}}=\frac{120}{16^{2}} \times p_{\mathrm{e}}^{(7)}<p_{\mathrm{e}}^{(7)} .
$$

Global variables

| $p_{o}^{(3)}=6^{3} / 16^{3}$ | $p_{e}^{(7)}=120 \times 4^{4} / 16^{7}$ |
| :--- | :--- |
| $p_{o}^{(4)}={ }^{40 \times 6^{3}} / 16^{5}$ |  |

## Sorted Candidates

$$
\begin{array}{ll}
\mathrm{DP}_{S_{0}}(2, \mathrm{~A})=4 / 16 & \mathrm{DP}_{S_{3}}(2,8)=10 / 16 \\
\mathrm{DP}_{S_{0}}(2, \mathrm{~F})=4 / 16 & \mathrm{DP}_{S_{3}}(2,2)=2 / 16 \\
\mathrm{DP}_{S_{0}}(2,8)=2 / 16 & \mathrm{DP}_{S_{3}}(2,4)=2 / 16 \\
\mathrm{DP}_{S_{0}}(2,9)=2 / 16 & \mathrm{DP}_{S_{3}}(2, E)=2 / 16 \\
\mathrm{DP}_{S_{0}}(2, \mathrm{C})=2 / 16 & \\
\mathrm{DP}_{S_{0}}(2, \mathrm{D})=2 / 16 &
\end{array}
$$



4 rounds

Figure 2.8: Example of Run for Round (3) - Part 1

Consequently, it is useless to consider the patterns $b^{[0]}$ activating three or four S -boxes in the first round. To conclude, using this additional costless test, we have considered

$$
\binom{4}{1} \times 16^{1}+\binom{4}{2} \times 16^{2}=1600
$$

patterns instead of $2^{16}=65536$.

### 2.2.2. Search Algorithm for the Round Function

To explain our optimizations of the function Round, assume that we have already handle the first two rounds and that the current trail $\mathcal{T}^{(2)}$ is as illustrated in Figure 2.8. This trail has a differential probability equal to $\frac{6^{2}}{16^{2}}$ and the input pattern of the third round is

$$
a^{[2]}=\pi\left(b^{[1]}\right)=(2,0,0,2) .
$$

According to the function Round (3), every candidate $b^{[2]}$ for $a^{[2]}$ must be considered and then tested by the pruning mechanism. However, we will create these candidates recursively bundle by bundle. For this purpose, the output candidate patterns of the two active S -boxes are sorted according to their probabilities. First, we choose the best output pattern for $S_{0}$, namely $b_{0}{ }^{[2]}=\mathrm{A}$, represented in Figure 2.9. Before selecting the output pattern for the other active S-box, this first choice should be tested as follows. The current probability for this round is $\mathrm{DP}_{S_{0}}(2, \mathrm{~A})$ and it

## Chapter 2 - Security Evaluation of SPN



4 rounds


Permutation +3 rounds

Figure 2.9: Example of Run for Round (3) - Part 2
remains one active S-box. The differential probability of this other S-box is clearly upper-bounded by $\mathrm{DP}_{(1)}^{\max }$ and thus the probability of the round is upper-bounded by the product $\mathrm{DP}_{S_{0}}(2, \mathrm{~A}) \times \mathrm{DP}_{(1)}^{\max }$. Since it remains four rounds before reaching a 7 -round trail, the probability of any extension can be upper-bounded by

$$
\begin{equation*}
\operatorname{DP}\left(\mathcal{T}^{(2)}\right) \times\left(\operatorname{DP}_{S_{0}}(2, \mathrm{~A}) \times \mathrm{DP}_{(1)}^{\max }\right) \times p_{\mathrm{o}}^{(4)}=\frac{6^{2}}{16^{2}} \times \frac{4}{16} \times \frac{10}{16} \times \frac{40 \times 6^{3}}{16^{5}} \tag{2.1}
\end{equation*}
$$

This value is greater than the estimation $p_{\mathrm{e}}{ }^{(7)}$, and hence our first choice $b_{0}{ }^{[2]}=\mathrm{A}$ seems to be a good one.

We now introduce a second pruning condition for this same candidate. This new condition applies whenever the diffusion layer of the SPN is a bit permutation. Observe that the candidate $b_{0}{ }^{[0]}=\mathrm{A}$ activates two S -boxes in the next round. And no matter what the choice of second candidate is, the input pattern of the next round will activate at least two S-boxes. We have already upper-bounded the probability of this round by $\mathrm{DP}_{S_{0}}(2, \mathrm{~A}) \times \mathrm{DP}_{(1)}^{\max }$. The probability of the next round is at most equal to $\mathrm{DP}_{(2)}^{\max }$ and it remains three rounds to reach the seven rounds. Therefore, the probability of any extension is upper-bounded by

$$
\begin{equation*}
\operatorname{DP}\left(\mathcal{T}^{(2)}\right) \times\left(\operatorname{DP}_{S_{0}}(2, \mathrm{~A}) \times \mathrm{DP}_{(1)}^{\max }\right) \times \mathrm{DP}_{(2)}^{\max } \times p_{\mathrm{o}}^{(3)}=\frac{6^{2}}{16^{2}} \times \frac{4}{16} \times \frac{10}{16} \times \frac{10}{16} \times \frac{6^{3}}{16^{3}} \tag{2.2}
\end{equation*}
$$

This probability is greater than the estimation and our first choice is now completely confirmed.

Next, we focus on the second active S-box, namely $S_{3}$. Referring to Figure 2.8, the first candidate that must be chosen is $b_{3}{ }^{[2]}=8$. With this choice, the output pattern $b^{[2]}$ of this round is complete and equal to ( $\mathrm{A}, 0,0,8$ ). However, this pattern must pass the two pruning tests before the current trail can be extended. It is easily checked from Figure 2.10 that these tests involve the same computation as in (2.1) and (2.2), so they accept the output pattern $b^{[2]}$. Finally, the pattern $a^{[3]}=\pi\left(b^{[2]}\right)=(9,0,8,0)$ is handled by the function Round (4).


Figure 2.10: Example of Run for Round (3) - Part 3

Once all the extensions of $a^{[3]}$ are explored, the other candidates for $a^{[2]}$ need to be considered. According to Figure 2.8, the second best candidate for $a_{3}{ }^{[2]}$ is $b_{3}{ }^{[2]}=2$. Again, the probability of any 4 -round extension of the current trail is upper-bounded by

$$
\operatorname{DP}\left(\mathcal{T}^{(2)}\right) \times\left(\operatorname{DP}_{S_{0}}(2, \mathrm{~A}) \times \operatorname{DP}_{S_{3}}(2,2)\right) \times p_{\mathrm{o}}^{(4)}=\frac{6^{2}}{16^{2}} \times \frac{4}{16} \times \frac{2}{16} \times \frac{40 \times 6^{3}}{16^{5}}
$$

This time, this upper bound is less than the estimation $p_{\mathrm{e}}^{(7)}$ and this candidate is discarded. In other words, the probability of the current trail is less than the rank-3 bound. Recall that the candidates are sorted according to their probabilities. Hence the remaining two candidates 4 and E for $a_{3}{ }^{[2]}$ can also be discarded without any additional computing. Since every candidate of the second active S-box has been considered, this recursive call ends and we go back to the first active S-box.

Referring to Figure 2.8, the next candidate for $a_{0}{ }^{[2]}$ is $b_{0}{ }^{[2]}=F$. Since this new candidate has the same differential probability as its predecessor, the first pruning mechanism computes the same upper bound as in (2.1) and validates this choice. However, Figure 2.11 illustrates that this candidate activates every S-box in the next round. The second upper bound is hence

$$
\left.\operatorname{DP}\left(\mathcal{T}^{(2)}\right) \times\left(\operatorname{DP}_{S_{0}}(2, F) \times \operatorname{DP}_{(1)}^{\max }\right)\right) \times \operatorname{DP}_{(4)}^{\max } \times p_{\mathrm{o}}^{(3)}=\frac{6^{2}}{16^{2}} \times \frac{4}{16} \times \frac{10}{16} \times \frac{1920}{16^{4}} \times \frac{6^{3}}{16^{3}},
$$

which is less than the estimation, discarding this candidate. The next candidate is $b_{0}{ }^{[2]}=8$. The probability of any complete extension of this trail is upper-bounded by

$$
\left.\operatorname{DP}\left(\mathcal{T}^{(2)}\right) \times\left(\operatorname{DP}_{S_{0}}(2,8) \times \operatorname{DP}_{(1)}^{\max }\right)\right) \times p_{\mathrm{o}}^{(4)}=\frac{6^{2}}{16^{2}} \times \frac{2}{16} \times \frac{10}{16} \times \frac{40 \times 6^{3}}{16^{5}}
$$

This bound is less than the estimation. As a consequence this and the three remaining candidates for $a_{0}{ }^{[2]}$ are all rejected, which completes the search for all extensions of the trail $\mathcal{T}^{(2)}$ and this recursive call to Round(3).

## Chapter 2 - Security Evaluation of SPN



4 rounds


Permutation +3 rounds

Figure 2.11: Example of Run for Round(3) - Part 4

To conclude, let us compare the number of patterns considered by the optimized and non-optimized versions of Round. Following the algorithm OptTrailEst given in Section 2.1.1, we would have to try every candidate $b^{[2]}$ for $a^{[2]}$, namely the 24 patterns in

$$
\left\{\left(b_{0}{ }^{[2]}, 0,0, b_{3}{ }^{[2]}\right) \mid b_{0}{ }^{[2]} \in\{8,9, \mathrm{~A}, \mathrm{C}, \mathrm{D}, \mathrm{~F}\}, b_{3}{ }^{[2]} \in\{2,4,8, \mathrm{E}\}\right\} .
$$

In this optimized version, we have considered only the two complete output patterns (A, $0,0,8$ ), (A, $, 0,2$ ) and the two half patterns ( $\mathrm{F}, 0,0, ?$ ), ( $2,0,0, ?$ ). Moreover, it is worth observing that all the sorted output candidates over each S-box with their respective differential probabilities should be computed and stored before starting the search. Similarly, all the rank-s bounds $p_{\mathrm{e}}^{(r)} / p_{\mathrm{o}}^{(r-s)}$ are updated and stored after each modification of the estimation. Finally, the probability of the current trail is computed recursively. Therefore, each pruning test requires at most two multiplications and one comparison.

### 2.2.3. Search Algorithm for the Last Round

To finish this example, we should consider the function LastRound. Nevertheless, this function is called only few times during the execution of OptTrailEst and is already very efficient. Assume that the current 6 -round trail $\mathcal{T}^{(6)}$ is as in Figure 2.12. The corresponding input pattern of this last round is

$$
a^{[6]}=\pi\left(b^{[5]}\right)=\pi(4,0,0,0)=(0,8,0,0) .
$$

Therefore there is only one S-box activated in the last round. Its best output candidate is also obtained by choosing the best output candidate for each active S-box. In this case, we must choose an element $b_{1}{ }^{[6]}$ maximizing the probability $\mathrm{DP}_{S_{1}}\left(8, b_{1}{ }^{[6]}\right)$. According to the difference probability matrix of $S_{1}$ given in Figure 2.3, the only choice is $b_{1}{ }^{[6]}=7$. Thus, the final output pattern $b^{[6]}$ is equal to

| $a^{[0]}=(0,0,0,2)$ | $a^{[3]}=(4,0,0,0)$ |
| :--- | :--- |
| $b^{[0]}=(0,0,0,8)$ | $b^{[3]}=(4,0,0,0)$ |
| $a^{[1]}=(1,0,0,0)$ | $a^{[4]}=(0,8,0,0)$ |
| $b^{[1]}=(4,0,0,0)$ | $b^{[4]}=(0,8,0,0)$ |
| $a^{[2]}=(0,8,0,0)$ | $a^{[5]}=(4,0,0,0)$ |
| $b^{[2]}=(0,8,0,0)$ | $b^{[5]}=(4,0,0,0)$ |



Figure 2.12: Example of Run for LastRound ()
$(0,7,0,0)$. It remains to compute the differential probability of this 7-round trail and compare it with the estimation. We have

$$
\mathrm{DP}\left(\mathcal{T}^{(7)}\right)=\mathrm{DP}\left(\mathcal{T}^{(6)}\right) \times \operatorname{DP}_{\sigma}\left(a^{[6]}, b^{[6]}\right)=\frac{20 \times 4^{4}}{16^{6}} \times \frac{6}{16}=\frac{120 \times 4^{4}}{16^{7}}
$$

Therefore, its probability is equal to the estimation, so this trail is saved in $\mathcal{T}_{\mathrm{o}}{ }^{(7)}$. The estimation $p_{\mathrm{e}}^{(7)}$ is then updated even if in this case its value does not change. The call to the function LastRound and the algorithm continues the execution of Round (6).

### 2.3. Optimizations

This section is dedicated to give a theoretical framework to the optimizations introduced in the previous example. First observe that the first loop of OptTrailEst requires to call the function FirstRound for all non-zero output differences $b^{[0]}$. Since there are $2^{n m}-1$ such differences, we can lower-bound its complexity by $2^{64}$ or $2^{128}$ for real-sized substitution-permutation networks. Therefore, this algorithm must be optimized for any practical execution.

### 2.3.1. Construction of the First Output Pattern

As we have said above, the number of calls to the function FirstRound () is a problem that must be solved. To optimize this step, a partition of the set of all non-zero differences is defined. Then, we give an effective way to test whether no difference in one part can be the beginning of an optimal trail.

For each integer $w$ such that $1 \leq w \leq m$, we denote by $\mathrm{DP}_{(w)}^{\max }$ the maximal probability of any 1 -round trail activating $w$ S-boxes. In other words,

$$
\mathrm{DP}_{(w)}^{\max }=\max \left\{\mathrm{DP}_{\sigma}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n}\right)^{m} \text { such that } \mathrm{w}_{n}(a)=w\right\},
$$

where $\mathrm{w}_{n}(a)$ denotes the bundle weight of $a$. Then, let us sort the differential probabilities $\mathrm{DP}_{S_{i}}^{\max }$ in the decreasing order. This is equivalent to define a permutation $\tau$ of $\llbracket 0, m \llbracket$ such that for each $i<m-1$, it holds that

$$
\mathrm{DP}_{S_{\tau(i)}}^{\max } \geq \mathrm{DP}_{S_{\tau(i+1)}}^{\max }
$$

## Chapter 2 - Security Evaluation of SPN

Proposition 2.7. Let $w$ be an integer such that $1 \leq w \leq m$. Then,

$$
\mathrm{DP}_{(w)}^{\max }=\prod_{i=0}^{w-1} \mathrm{DP}_{S_{\tau(i)}}^{\max }
$$

Proof. Let $a$ be an input pattern activating $w$ S-boxes and $b$ be an output pattern. For each $0 \leq i<m$, denote by $p_{i}$ the differential probability $\mathrm{DP}_{S_{i}}\left(a_{i}, b_{i}\right)$. Let $\rho$ be a permutation of $\llbracket 0, m \llbracket$ such that $p_{\rho(i)} \geq p_{\rho(i+1)}$ for all $i<m-1$. Since the pattern $a$ activates $w$ S-boxes, it must be the case that $p_{\rho(i)}=0$ for each $i \geq w$. Thus,

$$
\operatorname{DP}_{\sigma}(a, b)=\prod_{i=0}^{m-1} \operatorname{DP}_{S_{i}}\left(a_{i}, b_{i}\right)=\prod_{i=0}^{m-1} p_{i}=\prod_{i=0}^{m-1} p_{\rho(i)}=\prod_{i=0}^{w-1} p_{\rho(i)} \leq \prod_{i=0}^{w-1} \mathrm{DP}_{S_{\rho(i)}}^{\max }
$$

By definition of $\tau, \mathrm{DP}_{S_{\rho(i)}}^{\max } \leq \mathrm{DP}_{S_{\tau(i)}}^{\max }$ for each $0 \leq i<w$. Therefore,

$$
\begin{equation*}
\operatorname{DP}_{\sigma}(a, b) \leq \prod_{i=0}^{w-1} \mathrm{DP}_{S_{\tau(i)}}^{\max } \tag{2.3}
\end{equation*}
$$

As this inequality holds for every $a$ and $b$ in $\left(\mathbb{F}_{2}^{m}\right)^{n}$ such that $\mathrm{w}_{n}(a)=w$, it follows that

$$
\max \left\{\mathrm{DP}_{\sigma}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{m}\right)^{n}, \mathrm{w}_{n}(a)=w\right\} \leq \prod_{i=0}^{w-1} \mathrm{DP}_{S_{\tau(i)}}^{\max }
$$

Clearly, there exists a pair $(a, b)$ of input/output patterns with $\mathrm{w}_{n}(a)=w$ such that $\mathrm{DP}_{\sigma}(a, b)$ meets the bound (2.3) with equality, proving our proposition.
Remark 2.8. It goes without saying that $\mathrm{DP}_{(1)}^{\max } \geq \ldots \geq \mathrm{DP}_{(m)}^{\max }$ hold. Thus, the probability of an optimal one-round trail is

$$
p_{o}^{(1)}=\max \left\{\mathrm{DP}_{\sigma}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n m}\right)^{*}\right\}=\mathrm{DP}_{(1)}^{\max }=\mathrm{DP}_{S_{\tau(0)}}^{\max } .
$$

Of course, the differential probability matrices $\mathrm{DP}_{S_{i}}$ and the probabilities $\mathrm{DP}_{S_{i}}^{\max }$ and $\mathrm{DP}_{(i)}^{\max }$ are computed and stored before starting the search.

Theorem 2.9. Let $w$ and $w^{\prime}$ be two integers such that $1 \leq w \leq w^{\prime} \leq m$. If $\mathrm{DP}_{(w)}^{\max }$ is less than the rank-one bound, then there exists no $r$-round trail activating $w^{\prime}$ S-boxes in the first round with probability greater than or equal to $p_{\mathrm{e}}^{(r)}$.

Proof. Assume that $\mathrm{DP}_{(w)}^{\max }$ is less than the rank-one bound. Let $\mathcal{T}$ be a one-round trail activating $w^{\prime}$ S-boxes. By definition, $\mathrm{DP}(\mathcal{T}) \leq \mathrm{DP}_{\left(w^{\prime}\right)}^{\max }$. Then, the inequality $\mathrm{DP}_{\left(w^{\prime}\right)}^{\max } \leq \mathrm{DP}_{(w)}^{\max }$ obviously holds, and thus $\mathrm{DP}(\mathcal{T}) \leq \mathrm{DP}_{(w)}^{\max }$. Therefore, $\mathrm{DP}(\mathcal{T})$ is less than the rank-one bound and Lemma 2.5 ensures that there does not exist any $r$-round trail extending $\mathcal{T}$ with probability greater than or equal to $p_{\mathrm{e}}^{(r)}$. This concludes the proof.

This theorem states that whenever $\mathrm{DP}_{(w)}^{\max }$ is less than the rank-one bound, we only have to test the output differences $b^{[0]}$ activating at most ( $w-1$ ) S-boxes. There are

$$
\sum_{i=1}^{w-1}\binom{m}{w}\left(2^{n}-1\right)^{i}
$$

```
Algorithm 2 - OptTrailEst
    \mp@subsup{\mathcal{T}}{\textrm{o}}{(r)}}\mp@subsup{}{}{(r)}\leftarrow(
For }w\mathrm{ from 1 to m do
        If DP 
        Exit the loop
        Else
            For each output pattern b[0] activating w S-boxes do
            Call FirstRound(b[0])
Return }\mp@subsup{\mathcal{T}}{0}{(r)
```

Figure 2.13: First optimization - construction of the first difference
such differences, compared to $2^{n m}-1$ without this optimization.
We have run the final algorithm with several SPN having a bit permutation as linear layer. With $m=16$ and $n=4, \mathrm{DP}_{(4)}^{\max }$ was always less than the rank-one bound, and hence there was at most $2^{21}$ difference patterns $b^{[0]}$ to test instead of $2^{64}$. With $m=16$ and $n=8$, the gap is even larger since $\mathrm{DP}_{(3)}^{\max }$ was always less than the rank-one bound, yielding $2^{21}$ difference patterns to test instead of $2^{128}$. The algorithm optimized with Theorem 2.9 is described in Figure 2.13.

### 2.3.2. The Round Function

Following Matsui's algorithm [76], the output candidates of the function Round are constructed recursively. Let $a$ denote the input difference of the current round. According to Propositions 1.24 and 1.36, any candidate $b$ for $a$ can be constructed by selecting an output pattern for each S-box activated by $a$. The following theorem establishes that the pruning mechanism can be applied bundle by bundle.

Theorem 2.10. Let $s$ be an integer such that $1 \leq s \leq r$ and $\mathcal{T}$ be an $s$-round trail. Denote by $x_{0}<\ldots<x_{w-1}$ the indices of the S-boxes activated by $a^{[s-1]}$ where $w=\mathrm{w}_{n}\left(a^{[s-1]}\right)$. Let $v$ be an integer satisfying $1 \leq v \leq w$. If

$$
\operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right)\left(\prod_{i=0}^{v-1} \mathrm{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \operatorname{DP}_{(w-v)}^{\max }
$$

is less than the $s$-rank bound, then for every pattern $c$ satisfying:

- $c_{x_{i}}=b_{x_{i}}{ }^{[s-1]}$ for each $i<v-1$, and
- $\operatorname{DP}_{S_{x_{v-1}}}\left(a_{x_{v-1}[s-1]}, c_{x_{v-1}}\right) \leq \operatorname{DP}_{S_{x_{v-1}}}\left(a_{x_{v-1}[s-1]}, b_{x_{v-1}}{ }^{[s-1]}\right)$,
there does not exist any $r$-round trail extending $\mathcal{T} \mathcal{T}^{[0, s-2]} \|\left(a^{[s-1]}, c\right)$ with probability greater than or equal to $p_{\mathrm{e}}^{(r)}$.

Proof. Let $c$ be an output pattern satisfying the required conditions. If $c$ is not a candidate for $a^{[s-1]}$, then $\mathrm{DP}_{\sigma}\left(a^{[s-1]}, c\right)=0$ and any trail extending the current trail $\mathcal{T}^{[0, s-2]} \|\left(a^{[s-1]}, c\right)$ has also zero probability. Therefore, we assume that $c$ is a

## Chapter 2 - Security Evaluation of SPN

candidate for $a^{[s-1]}$ in the following. By hypothesis,

$$
\begin{aligned}
\mathrm{DP}_{\sigma}\left(a^{[s-1]}, c\right) & =\prod_{i=0}^{w-1} \mathrm{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, c_{x_{i}}\right) \\
& =\left(\prod_{i=0}^{v-1} \mathrm{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, c_{x_{i}}\right)\right) \times\left(\prod_{i=v}^{w-1} \mathrm{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, c_{x_{i}}\right)\right),
\end{aligned}
$$

And thus

$$
\begin{aligned}
\operatorname{DP}_{\sigma}\left(a^{[s-1]}, c\right) & \leq\left(\prod_{i=0}^{v-1} \operatorname{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times\left(\prod_{i=v}^{w-1} \mathrm{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, c_{x_{i}}\right)\right) \\
& \leq\left(\prod_{i=0}^{v-1} \operatorname{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \mathrm{DP}_{(w-v)}^{\max } .
\end{aligned}
$$

Next, we have the inequality

$$
\begin{aligned}
\operatorname{DP}\left(\mathcal{T}^{[0, s-2]} \|\left(a^{[s-1]}, c\right)\right) & =\operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right) \times \operatorname{DP}_{\sigma}\left(a^{[s-1]}, c\right) \\
& \leq \operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right) \times\left(\prod_{i=0}^{v-1} \operatorname{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \operatorname{DP}_{(w-v)}^{\max } .
\end{aligned}
$$

Consequently, the probability of $\mathcal{T}{ }^{[0, s-2]} \|\left(a^{[s-1]}, c\right)$ is less than the $s$-rank bound. The result then is a consequence of Lemma 2.5.

### 2.3.3. Active S-Boxes in the Next Round

Throughout this part, the linear layer $\pi$ is assumed to be a bit permutation. Denote by $\mathrm{L}_{\mathrm{ASB}}$ the mapping from $\left(\mathbb{F}_{2}^{n}\right)^{m}$ to $\mathbb{F}_{2}^{m}$ which maps a pattern $c$ to the $m$-bit vector $\mathrm{L}_{\mathrm{ASB}}(c)=\left(x_{i}\right)_{i<m}$ where $x_{i}$ is equal to one if and only if the bundle $c_{i}$ is nonzero. In other words, $\mathrm{L}_{\mathrm{ASB}}(c)$ is a compact representation of the S-boxes activated by the pattern $c$ and $\mathrm{L}_{\mathrm{ASB}}$ should be read "List of the Active S-Boxes".

Given two elements $L$ and $L^{\prime}$ of $\mathbb{F}_{2}^{m}$, we denote by $L \vee L^{\prime}$ their bitwise OR. Moreover, we say that two patterns $c$ and $c^{\prime}$ seen as elements of $\mathbb{F}_{2}^{n m}$ are disjoint if for all bit indices $i \leq n m$, the equation $c_{i}=c_{i}^{\prime}$ implies that $c_{i}=c_{i}^{\prime}=0$. It should be noted that if two disjoint patterns $c$ and $c^{\prime}$ are seen as elements of $\left(\mathbb{F}_{2}^{n}\right)^{m}$, then $c_{i}=c_{i}^{\prime}$ also implies that $c_{i}=c_{i}^{\prime}=0_{n}$ for each $i<m$. Let $c$ be a pattern and $i<m$ be a nonnegative integer. By $c_{i}$ we mean the element of $\left(\mathbb{F}_{2}^{n}\right)^{m}$ where all bundles are zero, except the one of index $i$ which is equal to $c_{i}$. In other words,

$$
\left(x_{j}\right)_{j<m}=\left.c\right|_{i} \Longleftrightarrow \begin{cases}x_{i}=c_{i} & \text { and } \\ x_{j}=0_{n} & \text { if } j \neq i .\end{cases}
$$

Before stating and proving the pruning condition involving the active $S$-boxes in the next round, we introduce two preliminary results.

Lemma 2.11. Let $c^{0}, \ldots, c^{w-1}$ be $w$ pairwise mutually disjoint patterns. Then

$$
\mathrm{L}_{\mathrm{ASB}}\left(\sum_{i=0}^{w-1} c^{i}\right)=\bigvee_{i=0}^{w-1} \mathrm{~L}_{\mathrm{ASB}}\left(c^{i}\right)
$$

Proof. The result is certainly true when $w=1$, so assume that $w=2$. Denote by $L^{0}$, $L^{1}$ and $L$ the lists of S-boxes activated by $c^{0}, c^{1}$ and $\left(c^{0}+c^{1}\right)$ respectively. Let $i<m$ be an integer. Next, we have the following equivalences

$$
L_{i}=0 \Leftrightarrow c_{i}^{0}+c_{i}^{1}=0_{n} \Leftrightarrow c_{i}^{0}=c_{i}^{1}=0_{n} \Leftrightarrow L_{i}^{0}=L_{i}^{1}=0
$$

Therefore, $L=L^{0} \vee L^{1}$. The result follows by induction on $w$ as $c^{w-1}$ and $\left(\sum_{i=0}^{w-2} c^{i}\right)$ are clearly mutually disjoint.

Corollary 2.12. Let $b$ be an output pattern. Let $1 \leq w \leq m$ be an integer and let $0 \leq x_{0}<\ldots<x_{w-1}<m$ be $w$ indices. Then,

$$
\mathrm{L}_{\mathrm{ASB}}\left(\pi\left(\left.\sum_{i=0}^{w-1} b\right|_{x_{i}}\right)\right)=\bigvee_{i=0}^{w-1} \mathrm{~L}_{\mathrm{ASB}}\left(\pi\left(\left.b\right|_{x_{i}}\right)\right)
$$

Proof. Since the diffusion layer $\pi$ is linear, it holds that

$$
\pi\left(\left.\sum_{i=0}^{w-1} b\right|_{x_{i}}\right)=\sum_{i=0}^{w-1} \pi\left(\left.b\right|_{x_{i}}\right) .
$$

Clearly, the patterns $\left.b\right|_{x_{i}}$ are mutually disjoint. Since $\pi$ is a bit permutation, it must be the case that the $\pi\left(\left.b\right|_{x_{i}}\right)$ are also disjoint. Finally, the relation

$$
\mathrm{L}_{\mathrm{ASB}}\left(\sum_{i=0}^{w-1} \pi\left(\left.b\right|_{x_{i}}\right)\right)=\bigvee_{i=0}^{w-1} \mathrm{~L}_{\mathrm{ASB}}\left(\pi\left(\left.b\right|_{x_{i}}\right)\right)
$$

follows from Lemma 2.11, which concludes the proof.
Theorem 2.13. We use the same notation as in Theorem 2.10 except that $s<r-1$. Let $w^{\prime}$ denote the Hamming weight of $\bigvee_{i=0}^{v-1} \mathrm{~L}_{\mathrm{ASB}}\left(\pi\left(\left.b^{[s-1]}\right|_{x_{i}}\right)\right)$. If

$$
\left[\operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right)\left(\prod_{i=0}^{v-1} \mathrm{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \mathrm{DP}_{(w-v)}^{\max }\right] \times \mathrm{DP}_{\left(w^{\prime}\right)}^{\max }
$$

is less than the rank- $(s+1)$ bound, then for every output pattern $c$ satisfying

$$
c_{x_{i}}=b_{x_{i}}{ }^{[s-1]} \text { for each } i<v,
$$

there does not exist any $r$-round trail extending $\mathcal{T}^{[0, s-2]} \|\left(a^{[s-1]}, c\right)$ with probability greater than or equal to $p_{e}^{(r)}$.

Proof. Following the proof of Theorem 2.10, we can assume that $c$ is a candidate for $a^{[s-1]}$ and deduce the upper bound

$$
\operatorname{DP}\left(\mathcal{T}^{[0, s-2]} \|\left(a^{[s-1]}, c\right)\right) \leq \operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right) \times\left(\prod_{i=0}^{v-1} \operatorname{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \operatorname{DP}_{(w-v)}^{\max }
$$

Define $a^{[s]}=\pi(c)$. Let $b^{[s]}$ be any output pattern. Similarly, we can assume that $b^{[s]}$ is a candidate for $a^{[s]}$. Let $w^{\prime \prime}$ denote the bundle weight of $a^{[s]}$ which is clearly

## Chapter 2 - Security Evaluation of SPN

equal to the Hamming weight of $\mathrm{L}_{\mathrm{ASB}}\left(a^{[s]}\right)$. According to Corollary 2.12,

$$
\begin{aligned}
\mathrm{L}_{\mathrm{ASB}}\left(a^{[s]}\right) & =\mathrm{L}_{\mathrm{ASB}}\left(\pi\left(b^{[s-1]}\right)\right)=\mathrm{L}_{\mathrm{ASB}}\left(\pi\left(\sum_{i=0}^{w-1} b^{[s-1]}| |_{x_{i}}\right)\right)=\bigvee_{i=0}^{w-1} \mathrm{~L}_{\mathrm{ASB}}\left(\pi\left(\left.b^{[s-1]}\right|_{x_{i}}\right)\right) \\
& =\left(\bigvee_{i=0}^{v-1} \mathrm{~L}_{\mathrm{ASB}}\left(\pi\left(\left.b^{[s-1]}\right|_{x_{i}}\right)\right)\right) \vee\left(\bigvee_{i=v}^{w-1} \mathrm{~L}_{\mathrm{ASB}}\left(\pi\left(\left.b^{[s-1]}\right|_{x_{i}}\right)\right)\right) .
\end{aligned}
$$

As a consequence,

$$
w^{\prime \prime}=\mathrm{w}\left(\mathrm{~L}_{\mathrm{ASB}}\left(a^{[s]}\right)\right) \leq \mathrm{w}\left(\bigvee_{i=0}^{v-1} \mathrm{~L}_{\mathrm{ASB}}\left(\pi\left(\left.b^{[s-1]}\right|_{x_{i}}\right)\right)\right)=w^{\prime},
$$

and thus $\mathrm{DP}_{\left(w^{\prime \prime}\right)}^{\max } \geq \mathrm{DP}_{\left(w^{\prime}\right)}^{\max }$. Eventually,

$$
\begin{aligned}
\operatorname{DP} & \left(\mathcal{T}^{[0, s-2]}\left\|\left(a^{[s-1]}, c\right)\right\|\left(a^{[s]}, b^{[s]}\right)\right)=\operatorname{DP}\left(\mathcal{T}^{[0, s-2]} \|\left(a^{[s-1]}, c\right)\right) \times \operatorname{DP}_{\sigma}\left(a^{[s]}, b^{[s]}\right) \\
& \leq\left[\operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right) \times\left(\prod_{i=0}^{v-1} \operatorname{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \operatorname{DP}_{(w-v)}^{\max }\right] \times \operatorname{DP}_{\left(w^{\prime \prime}\right)}^{\max } \\
& \leq\left[\operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right) \times\left(\prod_{i=0}^{v-1} \mathrm{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \mathrm{DP}_{(w-v)}^{\max }\right] \times \mathrm{DP}_{\left(w^{\prime}\right)}^{\max } .
\end{aligned}
$$

Therefore, the probability of $\mathcal{T}{ }^{[0, s-2]}\left\|\left(a^{[s-1]}, c\right)\right\|\left(a^{[s]}, b^{[s]}\right)$ is less than the rank$(s+1)$ bound and there exists no $r$-round trail extending it with probability greater than or equal to $p_{\mathrm{e}}^{(r)}$. Using the fact that this property holds for all $b^{[s]}$, the desired result is proven.

The search procedure Round optimized with Theorems 2.10 and 2.13 is described in Figure 2.14 .

### 2.3.4. Test on the Bound

All the previous results can be preserved while strengthening the condition on the bound. Suppose we have found a trail with probability greater than or equal to $p_{\mathrm{e}}^{(r)}$. The estimation $p_{\mathrm{e}}^{(r)}$ is then equal to the differential probability of this trail. Now, assume that the probability of the current $s$-round trail $\mathcal{T}$ satisfies $\mathrm{DP}(\mathcal{T}) \cdot p_{\mathrm{o}}^{(r-s)}=p_{\mathrm{e}}^{(r)}$. In this case, the probability $\operatorname{DP}(\mathcal{T})$ is not less than the rank- $s$ bound and the algorithm tries all its possible extensions. However, the previous equality implies that in the best-case scenario, we find an $r$-round trail with probability $p_{\mathrm{e}}^{(r)}$. Because such a trail is already known, the extension of $\mathcal{T}$ can be aborted. This discussion proves that Definition 2.3 can be enhanced as follows.

Definition 2.14 (rank- $s$ bound). Let $\mathcal{T}$ be a $s$-round trail with $s<r$. Its probability is less than the rank-s bound if

$$
\left(\mathcal{T}_{\mathrm{o}}^{(r)}=() \text { and } \operatorname{DP}(\mathcal{T})<\frac{p_{\mathrm{e}}^{(r)}}{p_{\mathrm{o}}^{(r-s)}}\right) \quad \text { or } \quad\left(\mathcal{T}_{\mathrm{o}}^{(r)} \neq() \text { and } \operatorname{DP}(\mathcal{T}) \leq \frac{p_{\mathrm{e}}^{(r)}}{p_{\mathrm{o}}^{(r-s)}}\right)
$$

```
Algorithm 3 - \(\operatorname{Round}\left(s, \mathcal{T}^{(s-1)}, p^{(s-1)}\right)\)
Input. \(\mathcal{T}=\left(\left(a^{[0]}, b^{[0]}\right), \ldots,\left(a^{[s-2]}, b^{[s-2]}\right)\right)\)
\(a^{[s-1]} \leftarrow \pi\left(a^{[s-2]}\right)\)
\(b^{[s-1]} \leftarrow 0_{n m}\)
\(p^{(s, 0)} \leftarrow p^{(s-1)}\)
\(\mathcal{T}^{(s)} \leftarrow \mathcal{T}^{(s-1)} \|\left(a^{[s-1]}, b^{[s-1]}\right)\)
\(w \quad \leftarrow \mathrm{w}_{n}\left(a^{[s-1]}\right)\)
Denote \(x_{0}<\ldots<x_{w-1}\) the indices of the S -boxes activated by \(a^{[s-1]}\).
\(X \leftarrow\left(x_{0}, \ldots, x_{w-1}\right)\)
\(L^{(0)} \leftarrow 0_{m}\)
Call RoundRec \(\left(s, 1, \mathcal{T}^{(s)}, p^{(s, 0)}, L^{(0)}, X\right)\)
Function \(\operatorname{RoundRec}\left(s, v, \mathcal{T}^{(s)}, p^{(s, v-1)}, L^{(v-1)}, X\right)\)
    If \(v=w\) then
        \(p^{(s)} \leftarrow p^{(s, w-1)}\)
        If \(s+1<r\) then
            Call Round \(\left(s+1, \mathcal{T}^{(s)}, p^{(s)}\right)\)
        Else
            Call LastRound \(\left(\mathcal{T}^{(s)}, p^{(s)}\right)\)
        Else
            \(x \leftarrow x_{v-1}\)
            For each \(b_{x}^{[s-1]}\) sorted in decreasing order according to
                \(\mathrm{DP}_{S_{x}}\left(a_{x}^{[s-1]}, \cdot\right)\) do
            \(p^{(s, v)} \leftarrow p^{(s, v-1)} \times \operatorname{DP}_{S_{x}}\left(a_{x}^{[s-1]}, b_{x}^{[s-1]}\right)\)
            If \(p^{(s, v)} \times \mathrm{DP}_{(w-s)}^{\max }\) is less than the rank-s bound then
                Exit the loop
                                    Theorem 2.10
            If \(\pi\) is a bit permutation then
                \(L^{(v)} \leftarrow L^{(v-1)} \vee \mathrm{L}_{\mathrm{ASB}}\left(\pi\left(\left.b^{[s-1]}\right|_{x}\right)\right)\)
                \(w^{\prime} \leftarrow \mathrm{w}\left(L^{(v)}\right)\)
                If \(p^{(s, v)} \times \mathrm{DP}_{(w-s)}^{\max } \times \mathrm{DP}_{\left(w^{\prime}\right)}^{\max }\) is not less than the rank- \((s+1)\)
                    bound then
                    Call RoundRec \(\left(s, v+1, \mathcal{T}^{(s)}, p^{(s, v)}, L^{(v)}, X\right) \quad\) Theorem 2.13
            Else
            Call RoundRec \(\left(s, v+1, \mathcal{T}^{(s)}, p^{(s, v)}, L^{(v)}, X\right)\)
```

Figure 2.14: Second optimization - the search function Round

## Chapter 2 - Security Evaluation of SPN

```
Algorithm 4 - OptTrail(r, ( }\mp@subsup{p}{0}{(i)}\mp@subsup{)}{1\leqi<r}{}
```

Input. The current number $r$ of rounds and the probabilities $\left(p_{o}^{(i)}\right)_{1 \leq i<r}$
Output. An optimal $r$-round trail $\mathcal{T}_{\mathrm{o}}^{(r)}$

```
\(\mathcal{T}_{o}^{(r)} \leftarrow()\)
\(p_{e}^{(r)} \leftarrow p_{o}^{(r-1)}\)
While \(\mathcal{T}_{\mathrm{o}}^{(r)}\) is empty do
\(p_{\mathrm{e}}^{(r)} \leftarrow p_{\mathrm{e}}^{(r)} / 2\)
\(\mathcal{T}_{\mathrm{o}}^{(r)} \leftarrow \operatorname{OptTrailEst}\left(r,\left(p_{\mathrm{o}}^{(i)}\right)_{1 \leq i<r}, p_{\mathrm{e}}^{(r)}\right)\)
Return \(\mathcal{T}_{o}^{(r)}\)
```

Figure 2.15: Automatic estimation management

### 2.3.5. Automatic Management of the Estimation

As explained in Section 2.1.1, the estimation $p_{e}^{(r)}$ determines the complexity of the algorithm OptTrailEst. Several methods yield good estimations of $p_{o}^{(r)}$. For instance, an iterative trail can be used. Following an idea of Ohta, Moriai and Aoki [87], let us introduce the algorithm OptTrail. The latter has two main advantages. Firstly, the estimation management is completely automatic, that is to say, no knowledge is required on the SPN. Secondly, its complexity has the same order of magnitude as OptTrailEst runs with $p_{e}^{(r)}=p_{\mathrm{o}}^{(r)} / 2$.

The algorithm OptTrail is presented in Figure 2.15. To understand how it works, it is worth recalling that OptTrailEst finds no trail whenever $p_{e}^{(r)}>p_{o}^{(r)}$ as ensured by Theorem 2.6. In this case, the best trail $\mathcal{T}_{\mathrm{o}}{ }^{(r)}$ remains empty at the end of the execution of this algorithm. Since $p_{o}^{(r)} \leq p_{o}^{(r-1)}$, we begin by running OptTrailEst with the estimation $p_{e}^{(r)}=p_{o}^{(r-1)} / 2$. Then, this estimation is divided by two after each execution OptTrailEst until an optimal trail is found. This happens whenever the condition $p_{\mathrm{e}}^{(r)} \leq p_{\mathrm{o}}^{(r)}$ becomes true. It is not hard to see that we have the following proposition.

Proposition 2.15. The complexity of OptTrailEst decreases as the input $p_{\mathrm{e}}^{(r)}$ increases.

In addition, we have observed experimentally that the complexity of the algorithm OptTrailEst executed with $p_{\mathrm{e}}^{(r)} \geq 2^{4} \cdot p_{\mathrm{o}}^{(R)}$, is negligible compared to its complexity when running with $p_{\mathrm{e}}^{(r)}=p_{\mathrm{o}}^{(R)} / 2$. This discussion justifies that OptTrail has roughly the same complexity as OptTrailEst.

### 2.4. Results

Experiments and simulations have been performed by a AMD Phenom II X4 965 Black Edition 3.4 GHz processor. The running time for a $R$-round cipher includes the precomputations and $R-1$ calls to OptTrail, as explained in Section 2.1.1.

To prove the practical security of Present [17] against differential cryptanalysis, the authors have shown that the probability of any 5 -round trail is upper-bounded by $2^{-20}$ and had exhibited a 5 -round trail of probability $2^{-21}$. The algorithm presented here allows us to prove in 0.3 second that this upper bound is met with equality. They have then deduced that any 25 -round trail probability is upper-bounded by $2^{-100}$. Our algorithm shows that the optimal trail probability is $2^{-110}$ in 0.5 second. The number of rounds is not a problem since an optimal 64-round trail is computed in just 2 seconds. Note that Present has 32 rounds.

The permutation used in SmallPresent [69] (and in Present) can be generalized for all positive integers $n$ and $m$. Denote by $\phi_{n, m}$ the permutation of $\llbracket 0, n m \llbracket$ defined by the rule

$$
\phi(i)=m(i \bmod n)+\left\lfloor\frac{i}{m}\right\rfloor .
$$

We have constructed a 128 -bit SPN on the same model as Present to test our algorithm efficiency. Define $\pi$ to be the bit permutation associated with $\phi_{8,16}$ and the S-boxes to be all equal to the AES S-box [39]. Using this algorithm, an optimal 13 -round differential trail with probability $2^{-89}$ was obtained in 7.1 seconds.

To analyze Puffin security against differential cryptanalysis, Cheng et al [36] have upper-bounded the probability of an optimal 31 -round trail by $2^{-62}$. In 0.02 second, we have computed a trail meeting this bound.

Finally, we have tested our algorithm on Iceberg [95]. However, its diffusion layer is not a bit permutation so the optimization presented in Section 2.3.3 is no longer applicable. The authors have upper-bounded the probability of an optimal 16 -round differential trail by $2^{-160}$. We proved that it is in fact $2^{-171,6}$ in 2.3 seconds. All these results are outlined in Figure 2.16.

|  | Block <br> size | Round <br> number | Upper- <br> bound | Best <br> probability | Running <br> time |
| :--- | :---: | :---: | :---: | :---: | :---: |
| Present | 64 | 5 | $2^{-20}$ | $2^{-20}$ | 0.3 s |
| Present | 64 | 25 | $2^{-100}$ | $2^{-110}$ | 0.5 s |
| Present-like | 128 | 13 | - | $2^{-89}$ | 7.1 s |
| PuFFin | 64 | 31 | $2^{-62}$ | $2^{-62}$ | 0.02 s |
| Iceberg | 64 | 16 | $2^{-160}$ | $2^{-171.6}$ | 2.3 s |

Figure 2.16: Summary of Results
To conclude, we have presented in this chapter a generic algorithm that computes an optimal differential or linear trail in an SPN. Running this algorithm may allow to prove the practical security of the block cipher. In the opposite case of a weak cipher, the returned trail gives rise to a powerful differential or linear cryptanalysis of the cipher. Especially optimized for SPN whose diffusion layer is a bit permutation, we are able to find an optimal differential trail of Present and Puffin within one second. Block cipher designers have then a powerful tool which can be run several times in order to improve their cipher primitives.

Chapter 2 - Security Evaluation of SPN


## Partition-Based Backdoor Ciphers

One of the first backdoor ciphers was created in 1997 by Rijmen and Preneel [89]. Their S-boxes are constructed to have one high correlation between the zero mapping and a sum of certain output bits. The knowledge of this correlation yields a high potential linear trail which is used to recover a part of the key with linear cryptanalysis. Such a weakness is generally pointed out by the first line of the S-boxes' correlation matrices. Yet, if the output size of the S-boxes is large enough, their computation is too expensive. Relying on this fact, the authors claimed that their backdoor is undetectable, even if one knows its global design. Nevertheless, Wu and al. [100] disproved this by discovering a way to recover the backdoor. It is worthwhile to mention that in practice, if a real cipher containing a backdoor is given, the presence of the backdoor will certainly not be revealed.

More recently in [2], the authors created non-surjective S-boxes embedding a parity check to create a backdoor cipher. The message space is thus divided into cosets and leads to an attack on this DES-like cipher in less than $2^{23}$ operations. The security of the whole algorithm, particularly against linear and differential cryptanalysis is not given and the authors admit that their attack is dependent on the first and last permutation of the cipher. Finally, the non-surjective S-boxes may lead to detect easily the backdoor by simply calculating the image of each input vector. This problem is naturally avoided in a Substitution-Permutation Network in which S-boxes are bijective by definition.

Our approach is mainly a generalization of the ideas presented by Paterson in [88]. In this article, a DES-like backdoor cipher exploiting a weakness induced by the round functions is presented. The group generated by the round functions acts imprimitively on the message space. In other words, the round function preserves a partition of the message space no matter the round keys used, and hence the same applies to the full cipher. This partition forms the backdoor. Paterson then introduced a backdoor cipher composed of 32 rounds and using an 80-bit cipher key. The backdoor can seriously compromise the cipher security using $2^{32}$ chosen plaintexts. Moreover, when combined with a carefully chosen key schedule, the backdoor enables recovery of the key using $2^{41}$ operations and a few known plaintexts. Even if the mathematical material to build the backdoor is given, no general algorithm details the S-boxes' construction. As the author acknowledges, the S-boxes of his backdoor cipher are incomplete: half of the ciphertext bits are independent of half of the plaintext bits

## Chapter 3 - Partition-Based Backdoor Ciphers

and the security against a differential attack is not as high as one might expect. Moreover, the author wondered whether the partition of the message space had to be linear, that is to say made up with every coset of a linear subspace. Caranti and al. 31 answered Paterson's question by proving that if the group generated by the round functions is imprimitive, then the partition of the message space must be linear.

In his thesis [50], Harpes considered backdoor ciphers mapping a partition of the plaintexts to a partition of the ciphertexts independently of the cipher key used. As these partitions are not necessarily equal, this family generalizes Paterson's one. These ciphers are called partition-based backdoor ciphers throughout this thesis. When the input and output partitions are equal, we speak of imprimitive backdoor ciphers to fit Paterson's work. More generally, a probabilistic partition-based backdoor cipher is a cipher which behaves like a partition-based cipher with high probability. Harpes suggested using such a backdoor with its partitioning cryptanalysis [52 to recover some bits of the cipher key using known or chosen plaintext/ciphertext pairs.

Along a similar line to Paterson's imprimitive ciphers, the group generated by the round functions has required much attention. This group was first studied by Coppersmith and Grossman in [38]. Then, Kaliski et al. asked whether the DES is a group and provided strong evidence that it is not the case [56. This group was proved to be the alternating group later in [97]. The next standard block cipher, namely the AES, was proven to generate also the alternating group in [94, 98]. Even if a secure cipher must generate a large group, it has been shown that this condition is not sufficient in [78]. Indeed, the authors described a very weak block cipher generating the symmetric group. More recently, Caranti et al. [31] introduced a class of block ciphers for which it is easier to prove that the group generated by the round functions is primitive. To demonstrate the efficiency of their framework, they applied it to the AES. Their results were then improved in [30, [32, 5, 4] and can then be used to prove that this group is either the alternating group or the symmetric group. Finally, we should mention another active area of research about backdoor ciphers which considers the so-called hidden sum [24, 25, 19]. This family of backdoor ciphers relies on an alternative vector space structure which can be used to break the cipher.

The backdoor ciphers covered by this thesis, namely imprimitive and partitionbased ciphers with their probabilistic variants, are introduced formally in the next section. We also recall several ways to exploit the backdoors of imprimitive ciphers but these attacks can easily be extended to partition-based backdoors. A cryptanalysis of a probabilistic backdoor cipher will be detailed later in Chapter 5 .

The remainder of this chapter focuses only on non-probabilistic partition-based backdoor substitution-permutation networks. More precisely, we study the structure of such ciphers when the backdoor holds no matter the round keys used, that is to say independently of the key schedule. We explore in Section 3.2 how the partition of the message space evolves through each step of the encryption process and prove that the study of the whole cipher can be reduced to the study of its substitution layer. Then, we spend quite a bit of time in Section 3.3 showing that this study can
be restricted further to that of one single S-box. Lastly, our results are summarized in Section 3.4 which concludes this chapter. The content of this chapter was first published in [9] and then developed in [12].

### 3.1. Partition-Based Backdoor Ciphers

This section introduces every family of backdoor ciphers covered by this thesis. To detail these backdoors, we may recall some classical results and definitions in Section 3.1.1. Readers acquainted with basic facts on imprimitive groups may jump immediately to Section 3.1.2 which presents imprimitive backdoor ciphers. Then Section 3.1.3 recalls how to take advantage of such a backdoor while Section 3.1.4 deals with its generalizations. To conclude this introduction, other closely related attacks are given in Section 3.1.5.

### 3.1.1. Imprimitive Group Actions

The symmetric group on $X$, denoted by $\operatorname{Sym}(X)$, is the set of all permutations of $X$ together with the operation of composition. Even if it is quite common to define the composition of two permutations $\sigma, \tau$ in $\operatorname{Sym}(X)$ by $\sigma \circ \tau: x \mapsto \tau(\sigma(x))$ when studying permutation groups, we will keep the convention that $\sigma \circ \tau(x)=\sigma(\tau(x))$ throughout this and the following chapters. In other words, permutations are still evaluated from right to left in a composition.

Definition 3.1 (Group Action). Let $G$ be a group and let $X$ be a set. A (left) group action is a mapping $G \times X \rightarrow X,(g, x) \mapsto g \cdot x$ such that the following statements hold:

- $e \cdot x=x$ for any $x$ in $X,(e$ denotes the identity element of $G)$;
- $g \cdot(h \cdot x)=(g h) \cdot x$ for all $g, h$ in $G$ and all $x$ in $X$.

Alternatively, a group action can be defined as a group homomorphism $\phi$ from $G$ to the symmetric group $\operatorname{Sym}(X)$.

Let us explain the equivalence between these two definitions of a group action. Let $G$ be a group acting on $X$. Define the mapping $\phi$ from $G$ to $\operatorname{Sym}(X)$ which maps an element $g$ of $G$ to the permutation

$$
\phi_{g}: X \rightarrow X, x \mapsto g \cdot x .
$$

Let $g$ be an element of $G$. It is easily seen that $\phi_{g^{-1}} \circ \phi_{g}=\phi_{g} \circ \phi_{g^{-1}}=\mathrm{Id}_{X}$ and hence $\phi_{g}$ is a permutation of $X$, ensuring that $\phi$ is well-defined. It remains to prove that $\phi$ is a homomorphism. Let $h$ be an element of $G$. For any $x$ in $X$, it holds that

$$
\left(\phi_{g} \circ \phi_{h}\right)(x)=\phi_{g}\left(\phi_{h}(x)\right)=\phi_{g}(h \cdot x)=g \cdot(h \cdot x)=(g h) \cdot x=\phi_{g h}(x) .
$$

Thus, the action of $G$ on $X$ yields a homomorphism $\phi$ from $G$ to $\operatorname{Sym}(X)$.

## Chapter 3 - Partition-Based Backdoor Ciphers

Conversely, let $\phi$ be a homomorphism from a group $G$ to the symmetric group on a set $X$. Define the mapping $\cdot$ from $G \times X$ to $X$ by the rule $g \cdot x=\phi_{g}(x)$. Let $g$ and $h$ be two elements of $G$. Then, for every $x$ in $X$, we have

$$
\begin{aligned}
& e \cdot x=\phi_{e}(x)=\operatorname{Id}_{X}(x)=x \quad \text { and } \\
& g \cdot(h \cdot x)=\phi_{g}\left(\phi_{h}(x)\right)=\left(\phi_{g} \circ \phi_{h}\right)(x)=\phi_{g h}(x)=(g h) \cdot x .
\end{aligned}
$$

This discussion establishes the equivalence between the two definitions.
A permutation group on $X$ is a subgroup of $\operatorname{Sym}(X)$. Permutation groups are closely tied to group actions. Indeed, a permutation group $G$ on $X$ naturally acts on $X$ by $g \cdot x=g(x)$ for all $g$ in $G$ and all $x$ in $X$. In this case, the corresponding homomorphism from $G$ to $\operatorname{Sym}(X)$ is simply the inclusion mapping.

Inversely, let $G$ be a group acting on $X$ and let $\phi$ denote the corresponding homomorphism. Then, the image $\phi(G)$ is a permutation group on $X$ called the permutation group induced on $X$ by $G$. Moreover, if $\phi$ is one-to-one, $G$ is isomorphic to $\phi(G)$ and the action of $G$ on $X$ is said to be faithful. In such a case, the notions of permutation groups and group actions are the same.

Before defining imprimitive group actions, we need to introduce the following two definitions.

Definition 3.2 (Transitivity). The action of a group $G$ on a set $X$ is said to be transitive if for all $x_{1}$ and $x_{2}$ in $X$, there exists an element $g$ of $G$ such that $g \cdot x_{1}=x_{2}$.

Definition 3.3 (G-invariant Partition). Let $G$ be a group acting on a set $X$. A partition $\mathcal{B}$ of $X$ is said to be a $G$-invariant partition (or a block system of $G$ ) if every element $g$ of $G$ preserves $\mathcal{B}$, that is to say, if $\mathcal{B}=\{g \cdot B \mid B \in \mathcal{B}\}$ where $g \cdot B$ denotes the set $\{g \cdot x \mid x \in B\}$.

Any group $G$ acting on a set $X$ has at least two $G$-invariant partitions, namely $\mathcal{B}=\{X\}$ and $\mathcal{B}=\{\{x\} \mid x \in X\}$. These partitions are said to be trivial.

Definition 3.4 (Imprimitivity). Let $G$ be a group acting transitively on $X$. The action of $G$ on $X$ is said to be imprimitive if there exists a non-trivial $G$-invariant partition of $X$. Otherwise, the group is said to act primitively.

A permutation group $G$ on $X$ is naturally said to be imprimitive when its induced action on $X$ is imprimitive. Moreover, it should be noted that any subgroup of an imprimitive permutation group is also imprimitive.

Lemma 3.5. Let $G$ be a group acting imprimitively on a set $X$ and let $\mathcal{B}$ be a non-trivial $G$-invariant partition. For all parts $B_{1}$ and $B_{2}$ in $\mathcal{B}$, there exists $g$ in $G$ such that $g \cdot B_{1}=B_{2}$.

Proof. Let $B_{1}$ and $B_{2}$ be two parts of $\mathcal{B}$. Let $x_{1}$ and $x_{2}$ be elements of $B_{1}$ and $B_{2}$ respectively. As the action of $G$ on $X$ is transitive, there exists an element $g$ of $G$ such that $g \cdot x_{1}=x_{2}$. Thus, $x_{2}$ belongs to both $g \cdot B_{1}$ and $B_{2}$. Note that $g \cdot B_{1}$ is a
part of $\mathcal{B}$ because $\mathcal{B}$ is $G$-invariant. It follows that $g \cdot B_{1}=B_{2}$ since these two parts have a non-empty intersection.

Remark 3.6. Any part $B$ of a $G$-invariant partition $\mathcal{B}$ is called a block. Generally, permutation group books [42, 55, 99] deal with blocks rather than $G$-invariant partitions because such partitions are uniquely determined by any of their blocks. Indeed, Lemma 3.5 implies that $\mathcal{B}=\{g \cdot B \mid g \in G\}$. Alternatively, a block $B$ of $G$ can be defined to be a non-empty subset of $X$ such that for every $g$ in $G$, the subsets $g \cdot B$ and $B$ are either disjoint or equal. For this reason, it is common to define an imprimitive group action to be a transitive action which has a non-trivial block. Finally, note that $G$-invariant partitions are called block systems in [6, 42, 55], imprimitive systems in (90] and complete block systems in [88, 99].

Let $G$ be a group acting on $X$ and assume that $\mathcal{B}$ is a $G$-invariant partition. Denote by $B$ a fixed block in $\mathcal{B}$. Given any block $B^{\prime}$, Lemma 3.5 ensures that there exists an element $g$ of $G$ such that $g \cdot B=B^{\prime}$. Denoting by $\phi$ the homomorphism associated with the action of $G$ on $X$, we know that the mapping $\phi_{g}: x \mapsto g \cdot x$ is a permutation of $X$. As a consequence, $B$ and $B^{\prime}$ have the same cardinality. This discussion proves the following corollary.

Corollary 3.7. Let $G$ be a group acting imprimitively on a set $X$ and let $\mathcal{B}$ be a nontrivial $G$-invariant partition. Every part of $\mathcal{B}$ have the same cardinality. Assuming that $X$ is finite, we have the relation $\# X=\# B \times \# \mathcal{B}$ where $B$ is any block of $\mathcal{B}$.

In mathematics, we generally ties together different objects which are similar when considering their structures. These similar objects are then said to be isomorphic. Let $G$ and $H$ be two groups acting respectively on $X$ and $Y$. For these actions to be isomorphic, the groups $G$ and $H$ must have the same structure, namely being isomorphic as groups. However, this condition cannot be sufficient since it disregards how the groups $G$ and $H$ act on their respective sets. For instance, the group $\operatorname{Sym}(\{1,2\})$ acts naturally on $\{1,2\}$ but can also act trivially on $\{1,2\}$ by always fixing every element. These two actions are very different while they have the same group and set. For this reason, we introduce the following stronger notion.

Definition 3.8 (Permutation Isomorphism). Let $G$ act on $X$ and let $H$ act on $Y$. The action of $G$ on $X$ is permutation isomorphic to $H$ on $Y$ if there exists an isomorphism $\varphi: G \rightarrow H$ and a bijection $\lambda: X \rightarrow Y$ satisfying for every $g$ in $G$ and every $x$ in $X$ the relation

$$
\lambda(g \cdot x)=\varphi(g) \cdot \lambda(x)
$$

Remark 3.9. The condition that the relation $\lambda(g \cdot x)=\varphi(g) \cdot \lambda(x)$ holds for every $x$ in $X$ is equivalent to saying that the diagram in Figure 3.1 commutes. The terminology permutation isomorphism is also used in [42, pp. 17] and [6]. However, the same notion is called a $G$-space isomorphism in [26, pp. 6], and more simply an isomorphism in [90, pp. 282].

Assume that the action of $G$ on $X$ is permutation isomorphic to $H$ on $Y$. Then, this action is uniquely determined by the other action. Indeed, for any $g$ in $G$ and

## Chapter 3 - Partition-Based Backdoor Ciphers



Figure 3.1: Diagrammatic representation of a permutation isomorphism (see Definition 3.8). Note that $g$ denotes the mapping $X \rightarrow X, x \mapsto g \cdot x$ and similarly, $\varphi(g)$ denotes $Y \rightarrow Y, y \mapsto \varphi(g) \cdot y$.
any $x$ in $X$, we have

$$
g \cdot x=\lambda^{-1}(\varphi(g) \cdot \lambda(x)) .
$$

Let $\mathcal{B}$ be any $G$-invariant partition. For every $h$ in $H$, we have

$$
h \cdot \lambda(\mathcal{B})=\varphi\left(\varphi^{-1}(h)\right) \cdot \lambda(\mathcal{B})=\lambda\left(\varphi^{-1}(h) \cdot \mathcal{B}\right)=\lambda(\mathcal{B})
$$

Thus, $\lambda(\mathcal{B})$ is a $H$-invariant partition. Consequently, if the action of $G$ on $X$ is imprimitive, then so is the action of $H$ on $Y$.

### 3.1.2. Imprimitive Backdoor ciphers

Backdoors based on imprimitive permutation groups were introduced by Paterson in [88. We restate here their theoretical framework using our notation. This family of backdoor ciphers belongs to the class of iterated block ciphers. We may recall that the encryption process of an iterated block cipher (see Definition 1.4) consists of the composition of round functions applied to the plaintext with different round keys. More formally, the message, cipher key and round key spaces are respectively $\mathbb{F}_{2}^{n}, \mathbb{F}_{2}^{\kappa}$ and $\mathbb{F}_{2}^{l}$, where $n$ is the block size, $\kappa$ the cipher key length and $l$ the round key length. The round function is a family $\left(F_{k}\right)_{k \in \mathbb{F}_{2}^{l}}$ of keyed permutations of the message space $\mathbb{F}_{2}^{n}$. Then, the $r$-round encryption function $E$ associated with the round keys $k^{[0]}, \ldots, k^{[r-1]}$ is given by

$$
E_{k[0], \ldots, k[r-1]}=F_{k[r-1]} \circ \cdots \circ F_{k[0]} .
$$

In practice, the round keys $\left(k^{[i]}\right)_{i<r}$ are derived from a cipher key $K$ using a key schedule. Nevertheless, the key schedule is disregarded by the main framework of imprimitive backdoor ciphers, which considers only independent round keys. As will be seen at the end of Chapter 4, a carefully designed key schedule can remarkably improve the backdoor, but for now it is simpler to ignore this part of the cipher.

By the group generated by the round functions, we mean the subgroup $G$ of $\operatorname{Sym}\left(\mathbb{F}_{2}^{n}\right)$ defined to be

$$
G=\left\langle F_{k} \mid k \in \mathbb{F}_{2}^{l}\right\rangle .
$$

Being a permutation group on $\mathbb{F}_{2}^{n}$, it naturally acts on the message space by the rule $g \cdot x=g(x)$ for every $g$ in $G$ and $x$ in $\mathbb{F}_{2}^{n}$. Even if we will only consider this group in

## 3.1 - Partition-Based Backdoor Ciphers

the remainder of this section, we may introduce two other similar groups to stress its relevance. First, let $G_{r}$ be the group generated by the $r$-round encryption functions with independent round keys, namely

$$
G_{r}=\left\langle E_{k[0]}, \ldots, k^{[r-1]} \mid k^{[0]}, \ldots, k^{[r-1]} \in \mathbb{F}_{2}^{l}\right\rangle .
$$

Then $G_{\text {cipher }}$ is defined in the same way as $G_{r}$ except that the round keys are derived from all possible cipher keys using the cipher's key schedule. In other words, $G_{\text {cipher }}$ is generated by all the encryption functions of the cipher. In [54, Lemma 1], it has been proven that $G_{\text {cipher }}$ is a subgroup of $G_{r}$, itself being a subgroup of $G$. As a consequence, if $G$ is an imprimitive permutation group, then so are $G_{r}$ and $G_{\text {cipher }}$.

An imprimitive backdoor cipher is an iterated block cipher such that the permutation group $G$ generated by its round functions is imprimitive. Naturally, the cipher's designer has to be aware of this property, otherwise we should not talk about backdoor. Now, suppose that $G$ is an imprimitive permutation group on $\mathbb{F}_{2}^{n}$. Then, there exists by definition a non-trivial $G$-invariant partition $\mathcal{B}$ of $\mathbb{F}_{2}^{n}$. Corollary 3.7 establishes that the number of blocks in $\mathcal{B}$ divides the cardinality of $\mathbb{F}_{2}^{n}$, that is $2^{n}$. Thus, the partition $\mathcal{B}$ contains $2^{d}$ blocks with $1<d<n$ and we can write

$$
\mathcal{B}=\left\{B_{0}, \ldots, B_{2^{d}-1}\right\} .
$$

Furthermore, each block $B_{i}$ has cardinality $2^{n-d}$. Let $g$ be an element of $G$. Since the partition $\mathcal{B}$ is $G$-invariant, the image of any block under $g$ is still a block. Equivalently, the permutation $g$ of $\mathbb{F}_{2}^{n}$ induces a permutation $\bar{g}$ of $\llbracket 0,2^{d} \llbracket$ which maps $i$ to the unique index $j$ satisfying $g\left(B_{i}\right)=B_{j}$. Using this notation, a block $B_{i}$ is mapped to $B_{\bar{g}(i)}$ by $g$.

### 3.1.3. Exploiting the backdoor

There are several ways to take advantage of this backdoor. We begin with the most basic, but also the one which works for every imprimitive backdoor cipher. As explained above, $G_{\text {cipher }}$ is a subgroup of $G$, so every encryption function lies in $G$. Let $K$ be a cipher key and let $g$ denote its associated encryption function $E_{K}$. This means that when several plaintexts lying in a same block $B_{i}$ are encrypted with $g$, the corresponding ciphertexts lie in the same block $B_{\bar{g}(i)}$. Such a property can be used by the following chosen-plaintext attack. For each index $0 \leq i<2^{d}$, choose a plaintext $p_{i}$ in $B_{i}$ and request their corresponding ciphertexts $c_{i}$. With those data, we can recover the induced permutation $\bar{g}$. Indeed, the image of any index $i$ under $\bar{g}$ is the index of the block containing $c_{i}$.

Now, assume that we are given a ciphertext $c$ whose corresponding plaintext is unknown. First, we must find the index $j$ of the block $B_{j}$ containing $c$. Next, we know that the plaintext lies in the block $B_{\bar{g}^{-1}(j)}$, that is to say, in a subset of size $2^{n-d}$. If we know that $p$ is a meaningful message, our uncertainty on $p$ can be further restricted by canceling the meaningless messages in $B_{\bar{g}^{-1}(j)}$. If $d$ is large, typically when $\frac{n}{2}<d<n$, then this cryptanalysis requires a huge amount of chosen plaintexts but also gives precise information on the plaintext. Similarly, if $d$ is small, this attack gives little information on the plaintext but only needs a few chosen plaintexts.

## Chapter 3 - Partition-Based Backdoor Ciphers

Relying only on this basic cryptanalysis, the cipher designer needs to choose between quantity of data required and efficiency of the backdoor. However, such a choice can be avoided if the imprimitive cipher has several non-trivial $G$-invariant partitions. Assume that

$$
\mathcal{A}=\left\{A_{0}, \ldots, A_{2^{a}-1}\right\} \quad \text { and } \quad \mathcal{B}=\left\{B_{0}, \ldots, B_{2^{b}-1}\right\}
$$

are two $G$-invariant partitions. Up to a rearrangement of the blocks, it can be assumed that $0_{n}$ lies in both $A_{0}$ and $B_{0}$. It is well-known that a non-empty intersection of two blocks of $G$ is still a block (see for instance [99, Proposition 6.1]). Then, $A_{0} \cap B_{0}$ is a block and

$$
\mathcal{A} \cap \mathcal{B}=\left\{g\left(A_{0} \cap B_{0}\right) \mid g \in G\right\}=\{A \cap B \mid A \in \mathcal{A}, B \in \mathcal{B}\} \backslash\{\varnothing\}
$$

is a (possibly trivial) $G$-invariant partition. This result will be generalized later in Proposition 3.20. Denote by $2^{d}$ the number of elements in the intersection $A_{0} \cap B_{0}$. Then, we know that each block of $\mathcal{A} \cap \mathcal{B}$ has also cardinality $2^{d}$.

The basic cryptanalysis detailed above can be enhanced as follows. Again, denote by $g$ the encryption function associated with the unknown cipher key. Using $2^{a}$ chosen plaintexts and the corresponding ciphertexts, recover the permutation $\bar{g}_{A}$ induced by $g$ on the partition $\mathcal{A}$. Similarly, recover the permutation $\bar{g}_{B}$ induced on $\mathcal{B}$ with $2^{b}$ other chosen plaintexts. Next, given a ciphertext $c$, find the indices $j_{A}$ and $j_{B}$ such that $c$ lies in both $A_{j_{A}}$ and $B_{j_{B}}$. Finally, the plaintext corresponding to $c$ lies in

$$
A_{i_{A}} \cap B_{i_{B}} \quad \text { where } i_{A}=\left(\bar{g}_{A}\right)^{-1}\left(j_{A}\right) \text { and } i_{B}=\left(\bar{g}_{B}\right)^{-1}\left(j_{B}\right) .
$$

To summarize, this cryptanalysis requires $2^{a}+2^{b} \leq 2^{\max (a, b)+1}$ chosen plaintexts and yields $2^{d}$ possible plaintexts for each ciphertext.

Maybe the most interesting set of parameters for this cryptanalysis are $a=b=\frac{n}{2}$ and $d=0$. In this case, the partitions $\mathcal{A}$ and $\mathcal{B}$ consist of $2^{\frac{n}{2}}$ blocks, each of cardinality $2^{\frac{n}{2}}$. The intersection $A_{0} \cap B_{0}$ contains only $2^{d}=1$ element, so the partition $\mathcal{A} \cap \mathcal{B}$ is equal to $\left\{\{x\} \mid x \in \mathbb{F}_{2}^{n}\right\}$. Once the permutations $\bar{g}_{A}$ and $\bar{g}_{B}$ have been recovered with $2^{\frac{n}{2}+1}$ chosen plaintexts, the cryptanalyst can decrypt any ciphertext. In other words, the cryptanalyst has an alternative decryption algorithm as he does not recover the cipher key. Using the common vocabulary introduced in [62, 63], this attack performs a global deduction. Intuitively, the messages in $\mathbb{F}_{2}^{n}$ are arranged in a $2^{\frac{n}{2}} \times 2^{\frac{n}{2}}$ matrix. Each block $A$ of $\mathcal{A}$ represents a row and each block $B$ of $\mathcal{B}$ a column of this matrix. The mappings $\bar{g}_{A}$ and $\bar{g}_{B}$ describe how $g$ permutes the rows and columns respectively. Given a ciphertext, this attack recovers the row and the column of the plaintext, and hence the plaintext itself. An example of such a backdoor cipher is given in [88, Section 3.3].

Finally, let us explain the key-schedule-dependent attack outlined by Paterson in his article. Even if this attack can be generalized using several $G$-invariant partitions, we consider hereinafter only one $G$-invariant partition $\mathcal{B}$ for simplicity. The main idea is to design a key schedule such that every induced permutation $\overline{E_{K}}$ of $\mathcal{B}$ is uniquely determined by a part of the cipher key $K$. Equivalently, we require the

## 3.1 - Partition-Based Backdoor Ciphers

existence of a (non-trivial) partition $\mathcal{K}=\left\{I_{0}, \ldots, I_{m-1}\right\}$ of $\mathbb{F}_{2}^{\kappa}$ such that all the cipher keys belonging to a same part of $\mathcal{K}$ induce the same permutation of $\mathcal{B}$, that is to say

$$
\forall K, K^{\prime} \in \mathbb{F}_{2}^{\kappa}, \quad\left(\exists I \in \mathcal{K}, K \in I \text { and } K^{\prime} \in I\right) \Longrightarrow\left(\overline{E_{K}}=\overline{E_{K^{\prime}}}\right) .
$$

Such a property can be used to carry out a key recovery attack. Let $K$ be an unknown cipher key. Assume that the cryptanalyst has a few plaintext/ciphertext pairs $\left(p_{i}, c_{i}\right)$. It is worthwhile to mention that this attack does not require a lot of data, only two or three pairs could be sufficient. Denote by $[x]$ the block of $\mathcal{B}$ containing the message $x$ in $\mathbb{F}_{2}^{n}$. Then, proceed as follows.

- For each class $I$ in $\mathcal{K}$, choose a cipher key $\tilde{K}$ in $I$ and test whether the equalities $\overline{E_{\tilde{K}}}\left(\left[p_{i}\right]\right)=\left[c_{i}\right]$ hold for all pairs $\left(p_{i}, c_{i}\right)$. Observe that $\overline{E_{\tilde{K}}}\left(\left[p_{i}\right]\right)=\left[c_{i}\right]$ holds if and only if $E_{\tilde{K}}\left(p_{i}\right)$ lies in the same block as $c_{i}$. This equivalent statement is more convenient for a real implementation.
- Then, for each candidate class $I$, check for every cipher key $\tilde{K}$ in $I$ if $E_{\tilde{K}}\left(p_{i}\right)=c_{i}$ hold for all pairs ( $p_{i}, c_{i}$ ).
Although this cryptanalysis was sketched by Paterson, no real example was given in his paper. In [9, Section 6], we introduced a toy imprimitive backdoor cipher vulnerable to this key schedule cryptanalysis. The cipher key space is divided into $2^{\frac{\kappa}{2}}$ classes, each containing $2^{\frac{\kappa}{2}}$ keys. When this attack is performed with two plaintext/ciphertext pairs, the first step requires at most $2 \times 2^{\frac{\kappa}{2}}$ encryptions. Generally, only one candidate class has to be tested in the second step, thereby requiring at most $2 \times 2^{\frac{\kappa}{2}}$ encryptions. Thus, the average-case complexity of this attack is $\mathcal{O}\left(2^{\frac{\kappa}{2}}\right)$, compared with the exhaustive search which requires $2^{\kappa}$ encryptions. In Section 4.3, we will detail a toy backdoor cipher combining several $G$-invariant partitions with a key schedule dependent cryptanalysis.


### 3.1.4. Generalizations

Now we turn our attention to generalizations of imprimitive backdoor ciphers proposed by Harpes in his thesis [50]. So far, we have considered backdoor ciphers preserving a partition $\mathcal{B}$ of the message space. More generally, a Partition-Based Backdoor Cipher is a cipher mapping a partition of the plaintext space to a partition of the ciphertext space, no matter the cipher key used. An imprimitive cipher is then a partition-based cipher whose input and output partitions are equal. More formally, we introduce the following definition.

Definition 3.10 (Partition-Based Backdoor Cipher). An iterated $n$-bit block cipher $E$ is called a partition-based backdoor cipher if there exist two partitions $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{F}_{2}^{n}$ such that for every cipher key $K$ in $\mathbb{F}_{2}^{\kappa}$ the following relationship holds:

$$
\left\{E_{K}(A) \mid A \in \mathcal{A}\right\}=\mathcal{B}
$$

Since $E_{K}$ must be a permutation of $\mathbb{F}_{2}^{n}$ to allow decryption, it is easily seen that the partitions $\mathcal{A}$ and $\mathcal{B}$ necessarily have the same number of parts. Such backdoor ciphers are the focus of this and the next chapter. The toy backdoor cipher given at the end of Chapter 4 will also illustrate this generalization.

## Chapter 3 - Partition-Based Backdoor Ciphers

Partitioning Cryptanalysis is an attack on iterated block ciphers introduced by Harpes in [52]. As differential cryptanalysis uses a pair $(a, b)$ of difference patterns, partitioning cryptanalysis considers a pair of partitions $(\mathcal{A}, \mathcal{B})$, where $\mathcal{A}$ is a partition of the plaintexts and $\mathcal{B}$ a partition of the set of inputs of the last round. A pair $(\mathcal{A}, \mathcal{B})$ is effective if for almost all cipher keys, the inputs of the last round function are non-uniformly distributed over the blocks of $\mathcal{B}$ when the plaintexts are uniformly chosen among one fixed block $A$ of $\mathcal{A}$. Then, the attack exploits this non-uniform behavior to recover information on the last round key, in the same way as linear and differential cryptanalysis do.

In the light of this attack, we should relax the definition of partition-based backdoor ciphers to include any iterated cipher designed to be vulnerable to partitioning cryptanalysis. To avoid confusion, we suggest the following definition.

Definition 3.11 (Probabilistic Partition-Based Backdoor Cipher).
An $r$-round iterative block cipher $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ is said to be a probabilistic partition-based backdoor cipher if there exists a pair $(\mathcal{A}, \mathcal{B})$ of partitions of $\mathbb{F}_{2}^{n}$ satisfying the following property: for almost all cipher keys $K$ in $\mathbb{F}_{2}^{\kappa}$ and for each part $A$ of $\mathcal{A}$, there exists a part $B_{A, K}$ of $\mathcal{B}$ such that for every other part $B$ it holds that

$$
\mathbb{P}_{x \in A}\left(E_{K}^{(r-1)}(x) \in B_{A, K}\right) \gg \mathbb{P}_{x \in A}\left(E_{K}^{(r-1)}(x) \in B\right) .
$$

In other words, for almost all cipher keys $K$ in $\mathbb{F}_{2}^{\kappa}$ and for each part $A$ of $\mathcal{A}$, the ( $r-1$ )-round encryption function $E_{K}^{(r-1)}$ maps a significant proportion of the plaintexts lying in $A$ to a part $B_{A, K}$ of $\mathcal{B}$ and the remaining plaintexts in $A$ should be spread over the other parts of $\mathcal{B}$. Again, this property must be intended by the designer to call it a backdoor. Chapter 5 will be dedicated to BEA-1, our backdoor cipher inspired by Paterson and Harpes' work and by the theory developed in this and the next chapters.

### 3.1.5. Links With Other Attacks

Before addressing the formal treatment of partition-based backdoor ciphers, we may digress a little from backdoors and expose a cryptanalysis closely related to our topic. In [70], Leander et al. developed a new cryptanalysis, called invariant subspace attack, breaking the PRINTCiPher [61] for a significant fraction of its keys. Its efficiency has then been proven on several ciphers [21, 49, 71]. The general idea of this attack can be outlined as follows. Let $F$ denote the SP-layer of a SubstitutionPermutation network, that is, the round function without the key addition. Then, assume that $F$ maps a coset of a given subspace $V$ to another coset of $V$. In other words, there exist $a$ and $b$ such that $F(a+V)=b+V$. Here, the addition is made in $\mathbb{F}_{2}^{n}$, and hence corresponds with the XOR operation. The round function associated with the round key $k$ is then defined by $F_{k}: x \mapsto F(x+k)$. If the round key $k$ belongs to the coset $a+b+V$, then it holds that

$$
F_{k}(b+V)=F(b+k+V)=F(a+V)=b+V,
$$

## 3.2 - Substitution-Permutation Networks and Partitions

hence the name of invariant subspace. Therefore, if every round key lies in this particular coset, the affine subspace $b+V$ is preserved by the full encryption process. Such a property enables a very efficient distinguisher. As additional results, they also showed that the invariant subspace attack

- implies a truncated differential attack to be possible (the probability of the truncated differential characteristic is however highly key-dependent);
- implies the existence of strongly biased linear approximations for weak keys (independently of the number of rounds).

This attack was generalized in 2015 by Leander, Minaud and Rønjom [71]. They proposed a generic algorithm that is able to detect invariant subspaces. Indeed, their initial invariant subspaces on PRINTCIPHER were found empirically.

Following the idea of the invariant subspace attack, Grassi et al. [47, 48 introduced the subspace trail cryptanalysis. Given $r+1$ subspaces $V^{[0]}, \ldots, V^{[r]}$, it is assumed that the image of any coset of $V^{[i]}$ under the SP-network is included in a coset of $V^{[i+1]}$. That is to say, for each $a^{[i]}$, there exists $a^{[i+1]}$ such that the following inclusion holds

$$
F\left(a^{[i]}+V^{[i]}\right) \subseteq a^{[i+1]}+V^{[i+1]} .
$$

In this case, it is easy to see the all the round functions $F_{k}$ inherit such a property. The family of subspaces $\left(V^{[i]}\right)_{i \leq r}$ is said to be a subspace trail. Naturally, the dimension of $V^{[i]}$ must be less than or equal to the dimension of $V^{[i+1]}$. In contrast to the invariant subspace attack, Grassi et al. relaxed the assumption that the coset has to be invariant. Here, the considered subset becomes the coset of possibly different increasingly dimensional subspaces throughout the encryption. However, the authors also required this property to hold for each coset of $V^{[0]}$ instead of one. Therefore, this cryptanalysis is not a generalization, but a variation of the invariant subspace attack. As will become clear in the next section, the family of backdoors covered in this thesis is closely related to constant-dimensional subspace trails.

### 3.2. Substitution-Permutation Networks and Partitions

This section aims at studying an SPN which maps a partition of the plaintexts to a partition of the ciphertexts. When the cipher key $K$ is fixed, the encryption function $E_{K}$ is just a permutation of the message space. Therefore, any partition $\mathcal{A}$ of the plaintexts is mapped to the partition $E_{K}(\mathcal{A})$ of the ciphertexts. Nonetheless, to exploit the backdoor, the designer needs to know the pair of partitions $\left(\mathcal{A}, E_{K}(\mathcal{A})\right)$. The problem is that the output partition $E_{K}(\mathcal{A})$ depends a priori on the cipher key $K$, which is unknown to the attacker. The simplest way to solve this problem is to require that the partitions $E_{K}(\mathcal{A})$ are independent of the cipher keys $K$. In other words, we want all the partitions $E_{K}(\mathcal{A})$ to be equal to a fixed partition $\mathcal{B}$.

As with differential and linear cryptanalysis, taking account of the exact effect of the key schedule seems to be a challenging problem. Therefore, the key schedule will deliberately be omitted throughout this chapter. This amounts to consider an SPN

## Chapter 3 - Partition-Based Backdoor Ciphers

mapping a partition $\mathcal{A}$ to a fixed partition $\mathcal{B}$, independently of the round keys used. In the following subsection, we introduce some definitions and preliminary results.

### 3.2.1. Linear Partitions

Since we are concerned with ciphers which associate a partition of the ciphertext space to another partition of the plaintext space, let us introduce the following definition.

Definition 3.12. Let $f$ be a permutation of $E$ and $\mathcal{A}, \mathcal{B}$ be two partitions of $E$. Let $f(\mathcal{A})$ denote the set $\{f(A) \mid A \in \mathcal{A}\}$. We say that $f$ maps $\mathcal{A}$ to $\mathcal{B}$ if $f(\mathcal{A})=\mathcal{B}$. If $\mathcal{A}=\mathcal{B}$, we says that $f$ preserves the partition $\mathcal{A}$.

The two partitions $\{\{x\} \mid x \in E\}$ and $\{E\}$ are called the trivial partitions of $E$. Observe that, for any permutation $f$ of $E$,

$$
f(\{\{x\} \mid x \in E\})=\{\{x\} \mid x \in E\} \quad \text { and } \quad f(\{E\})=\{E\} .
$$

That is, every permutation preserves the two trivial partitions. Moreover it should be highlighted that if $f$ maps $\mathcal{A}$ to $\mathcal{B}$ and if $\mathcal{A}$ is non-trivial, then so is $\mathcal{B}$.

Example 3.13. Let $E$ denote the set $\llbracket 0,8 \llbracket$ and consider the two partitions $\mathcal{A}, \mathcal{B}$ of $E$ defined to be $\mathcal{A}=\{\{0,1,4\},\{2,6\},\{3,7\},\{5\}\}$ and $\mathcal{B}=\{\{0,2,7\},\{1\},\{3,5\},\{4,6\}\}$. Let $f$ be the permutation of $E$ defined as follows:

$$
0 \mapsto 7, \quad 1 \mapsto 0, \quad 2 \mapsto 3, \quad 3 \mapsto 6, \quad 4 \mapsto 2, \quad 5 \mapsto 1, \quad 6 \mapsto 5, \quad 7 \mapsto 4 .
$$

By definition,

$$
\begin{aligned}
f(\mathcal{A})=\{f(A) \mid A \in \mathcal{A}\} & =\{f(\{0,1,4\}), f(\{2,6\}), f(\{3,7\}), f(\{5\})\} \\
& \left.=\left\{\begin{array}{c} 
\\
\end{array}, 0,2\right\}, \quad\{3,5\}, \quad\{6,4\}, \quad\{1\}\right\} .
\end{aligned}
$$

The equality $f(\mathcal{A})=\mathcal{B}$ holds, and thus $f$ maps the partition $\mathcal{A}$ to $\mathcal{B}$.
Lemma 3.14. Let $f$ be a permutation of $E$ and $\mathcal{A}, \mathcal{B}$ be two partitions of $E$. If for any part $A$ of $\mathcal{A}, f(A)$ is a part of $\mathcal{B}$, then $f$ maps $\mathcal{A}$ to $\mathcal{B}$.

Proof. Suppose that for all $A$ in $\mathcal{A}, f(A)$ lies in $\mathcal{B}$. By hypothesis, $f(\mathcal{A})$ is included in $\mathcal{B}$. It remains to show that $\mathcal{B}$ is a subset of $f(\mathcal{A})$. Let $B$ be a part of $\mathcal{B}$ and let $y$ be an element of $B$. Since $f$ is surjective, there exists $x$ in $E$ such that $f(x)=y$. Furthermore, there exists a unique part $A$ of $\mathcal{A}$ which contains $x$ as $\mathcal{A}$ is a partition de $E$. Then, $y$ belongs to $f(A)$ and $B$. Observe that $f(A)$ and $B$ are two non-disjoint parts of $\mathcal{B}$. Consequently, $f(A)=B$ and $B$ belongs to $f(\mathcal{A})$. The result follows.

In this chapter, we will consider a special kind of partitions which is composed of all the cosets of a linear subspace. Such partitions have already been introduced by Harpes [50, Definition 4.4] and are recalled below.

|  |  | .0 | .1 | .2 | .3 | .4 | .5 | .6 | .7 | .8 | .9 | .$A$ | .$B$ | .$C$ | .$D$ | .$E$ | .$F$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $f(x)$ | 0 | 1 E | 08 | 04 | 13 | 0 F | 18 | 14 | 10 | 19 | 15 | 0 E | 0D | 03 | 1 C | 07 | 17 |
|  | 1. | 12 | 11 | 0 B | 1 B | 09 | 05 | 1 F | 00 | 0 A | 01 | 02 | 1 A | 06 | 0 C | 1 D | 16 |

Figure 3.2: The permutation $f$ of Example 3.17.


Figure 3.3: The permutation $f$ mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$ where $V=\operatorname{span}(07,1 \mathrm{~A})$ and $W=\operatorname{span}(0 \mathrm{E}, 12)$.

Definition 3.15 (linear partition). Let $\mathcal{A}$ be a partition of $\mathbb{F}_{2}^{n}$. Let $V$ denote its part containing $0_{n}$. The partition $\mathcal{A}$ is said to be linear if $V$ is a subspace of $\mathbb{F}_{2}^{n}$ and if every part of $\mathcal{A}$ is a coset of $V$ in $\mathbb{F}_{2}^{n}$, in other words, if

$$
\mathcal{A}=\left\{x+V \mid x \in \mathbb{F}_{2}^{n}\right\}=\mathbb{F}_{2}^{n} / V
$$

We denote by $\mathcal{L}(V)$ such a partition.
Remark 3.16. It turns out that the linear partitions associated with the two trivial subspaces of $\mathbb{F}_{2}^{n}$, that is $\left\{0_{n}\right\}$ and $\mathbb{F}_{2}^{n}$, correspond with the two trivial partitions of $\mathbb{F}_{2}^{n}$. Moreover, if $V$ is a non-trivial subspace of $\mathbb{F}_{2}^{n}$, then the linear partition $\mathcal{L}(V)$ is also non-trivial.
Example 3.17. Consider the subspaces $V$ and $W$ of $\mathbb{F}_{2}^{5}$ defined to be

$$
V=\operatorname{span}(07,1 \mathrm{~A})=\{00,07,1 \mathrm{~A}, 1 \mathrm{D}\} \quad \text { and } \quad W=\operatorname{span}(0 \mathrm{E}, 12)=\{00,0 \mathrm{E}, 12,1 \mathrm{C}\}
$$

Since both $V$ and $W$ are 2-dimensional subspaces of $\mathbb{F}_{2}^{5}$, the quotient spaces $\mathcal{L}(V)=$ $\mathbb{F}_{2}^{5} / V$ and $\mathcal{L}(W)=\mathbb{F}_{2}^{5} / W$ are 3-dimensional. In other words, the two linear partitions $\mathcal{L}(V)$ and $\mathcal{L}(W)$ have $2^{3}=8$ parts. It can be verified that

$$
\begin{aligned}
& \mathcal{L}(V)=\{V, 01+V, 02+V, 03+V, 08+V, 09+V, 0 \mathrm{~A}+V, 0 \mathrm{~B}+V\}, \\
& \mathcal{L}(W)=\{W, 01+W, 02+W, 03+W, 04+W, 05+W, 06+W, 07+W\} .
\end{aligned}
$$

For instance, the part $0 \mathrm{~B}+V$ of the linear partition $\mathcal{L}(V)$ is the coset of $V$ with respect to $0 B$. Explicitly, it is equal to

$$
0 B+V=\{0 B+00,0 B+07, O B+1 A, 0 B+1 D\}=\{0 B, 0 C, 11,16\} .
$$

Now, consider the permutation $f$ of $\mathbb{F}_{2}^{5}$ given in Figure 3.2. The image of $0 \mathrm{~B}+V$ under $f$ is

$$
\begin{aligned}
f(0 \mathrm{~B}+V) & =f(\{0 \mathrm{~B}, 0 \mathrm{C}, 11,16\})=\{0 \mathrm{D}, 03,11,1 \mathrm{~F}\} \\
& =\{03+0 \mathrm{E}, 03+00,03+12,03+1 \mathrm{~F}\}=03+W .
\end{aligned}
$$

## Chapter 3 - Partition-Based Backdoor Ciphers

Observe that $f(0 \mathrm{~B}+V)$ is a coset of $W$ so a part of $\mathcal{L}(W)$. The images of all cosets of $V$ under $f$ are displayed in Figure 3.3. Since any of them is a part of $\mathcal{L}(W)$, the permutation $f$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. It is worthwhile to observe that a permutation mapping a linear partition to another one does not need to be itself linear or even affine. Indeed, $f$ is certainly not linear as $f(00)=1 \mathrm{E} \neq 00$. By contradiction, suppose that $f$ is an affine transformation. Then, there exist a linear mapping $L: \mathbb{F}_{2}^{5} \rightarrow \mathbb{F}_{2}^{5}$ and an element $c$ of $\mathbb{F}_{2}^{5}$ such that $f(x)=L(x)+c$ holds for all $x$ in $\mathbb{F}_{2}^{5}$. Therefore,

$$
f(x)+f(y)+f(z)=L(x)+c+L(y)+c+L(z)+c=L(x+y+z)+c=f(x+y+z)
$$

for all $x, y$ and $z$ in $\mathbb{F}_{2}^{5}$. Observe that

$$
f(00)+f(01)+f(02)=1 \mathrm{E}+08+04=12 \neq 13=f(00+01+02) .
$$

Thus, $f$ is not an affine transformation.
Lemma 3.18. Let $V, W$ be two subspaces of $\mathbb{F}_{2}^{n}$ and $f$ be a permutation of $\mathbb{F}_{2}^{n}$ which maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. For any $x$ in $\mathbb{F}_{2}^{n}, f$ maps $x+V$ to $f(x)+W$.

Proof. Let $x$ be an element of $\mathbb{F}_{2}^{n}$. By hypothesis, there exists $y$ in $\mathbb{F}_{2}^{n}$ such that $f(x+V)=y+W$. Observe that $x$ lies in $x+V$, so $f(x)$ lies in both $y+W$ and $f(x)+W$. Since $y+W$ and $f(x)+W$ are two non-disjoint parts of $\mathcal{L}(W)$, they must be equal. Thus, $f(x+V)=f(x)+W$.

Example 3.19. In Example 3.17, we have seen that $f(0 B+V)=03+W$. Since $f$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$, the previous lemma states that $f(O \mathrm{~B}+V)=f(\mathrm{OB})+W=0 \mathrm{D}+W$. There is however no contradiction here because 0 D belongs to $03+W$. Consequently, the cosets $03+W$ and $0 \mathrm{D}+W$ are equal.

The following two propositions are interesting properties of linear partitions which will be used in the rest of this chapter.

Proposition 3.20. Let $V_{1}, V_{2}, W_{1}, W_{2}$ be four subspaces of $\mathbb{F}_{2}^{n}$ and $f$ be a permutation of $\mathbb{F}_{2}^{n}$ which maps $\mathcal{L}\left(V_{1}\right)$ to $\mathcal{L}\left(W_{1}\right)$ and $\mathcal{L}\left(V_{2}\right)$ to $\mathcal{L}\left(W_{2}\right)$. Then $f$ maps $\mathcal{L}\left(V_{1} \cap V_{2}\right)$ to $\mathcal{L}\left(W_{1} \cap W_{2}\right)$.

Proof. Let $x+\left(V_{1} \cap V_{2}\right)$ be a part $\mathcal{L}\left(V_{1} \cap V_{2}\right)$. Observe that $x+\left(V_{1} \cap V_{2}\right)=\left(x+V_{1}\right) \cap$ $\left(x+V_{2}\right)$. Now,

$$
f\left(x+\left(V_{1} \cap V_{2}\right)\right)=f\left(\left(x+V_{1}\right) \cap\left(x+V_{2}\right)\right)=f\left(x+V_{1}\right) \cap f\left(x+V_{2}\right)
$$

as $f$ is one-to-one. Then, Lemma 3.18 ensures that $f\left(x+V_{1}\right)=f(x)+W_{1}$ and $f\left(x+V_{2}\right)=f(x)+W_{2}$. Next,

$$
f\left(x+\left(V_{1} \cap V_{2}\right)\right)=\left(f(x)+W_{1}\right) \cap\left(f(x)+W_{2}\right)=f(x)+\left(W_{1} \cap W_{2}\right) .
$$

This show that the image of any part of $\mathcal{L}\left(V_{1} \cap V_{2}\right)$ under $f$ lies in $\mathcal{L}\left(W_{1} \cap W_{2}\right)$. The result is then a consequence of Lemma 3.14

Proposition 3.21. Let $V, W$ be two subspaces of $\mathbb{F}_{2}^{n}$ and $f$ be a permutation of $\mathbb{F}_{2}^{n}$ which maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. There exists an automorphism $L$ of $\mathbb{F}_{2}^{n}$ such that $L(V)=W$. In particular, $V$ and $W$ are isomorphic.

Proof. By definition, $f(V)$ belongs to $\mathcal{L}(W)$. Thus, there exists an element $x$ of $\mathbb{F}_{2}^{n}$ such that $f(V)=x+W$. Consequently, $V$ and $W$ have the same finite cardinality. Hence, $V$ and $W$ have the same dimension denoted by $d$. Let $\left(v_{i}\right)_{0 \leq i<d}$ and $\left(w_{i}\right)_{0 \leq i<d}$ be two bases of $V$ and $W$ respectively. According to the incomplete basis theorem, there exist two families $\left(v_{i}\right)_{d \leq i<n}$ and $\left(w_{i}\right)_{d \leq i<n}$ such that $\mathcal{B}_{V}=\left(v_{i}\right)_{0 \leq i<n}$ et $\mathcal{B}_{W}=\left(w_{i}\right)_{0 \leq i<n}$ are two bases of $\mathbb{F}_{2}^{n}$. Denoting by $L$ the linear mapping which maps $v_{i}$ to $w_{i}$ for all $0 \leq i<n$, we get an automorphism of $\mathbb{F}_{2}^{n}$ satisfying the equality $L(V)=W$.
Example 3.22. Consider again the permutation $f$ of $\mathbb{F}_{2}^{5}$ defined as in Figure 3.9. As seen in the previous example, the permutation maps the linear partition $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Then, Proposition 3.21 ensures that there exists a linear permutation $L$ of $\mathbb{F}_{2}^{5}$ such that $L(V)=W$. Following its proof, consider the bases $(07,1 \mathrm{~A})$ and $(0 \mathrm{E}, 12)$ of $V$ and $W$ respectively and complete them into the following bases of $\mathbb{F}_{2}^{5}$

$$
\mathcal{B}_{V}=\left(v_{i}\right)_{i<5}=(07,1 \mathrm{~A}, 01,02,08) \quad \text { and } \quad \mathcal{B}_{W}=\left(w_{i}\right)_{i<5}=(0 \mathrm{E}, 12,01,02,04)
$$

Then, the mapping $L$ can be defined by the rule $L\left(v_{i}\right)=w_{i}$ for each $i<5$. This linear transformation will be used in the next chapter.

### 3.2.2. The Key Addition and Diffusion Layer

Before tackling the full SPN, we look at its basic operations and building-blocks. Recall that the round function is made up of a key addition, a substitution layer and a diffusion layer. The attacker knows the specifications of the substitution and diffusion layers but he does not know the round key used in the key addition. Therefore, the key addition should not be considered as one operation but rather as a family of permutations. To get back to the subject at hand, we must first determine the partitions $\mathcal{A}$ which are mapped to a unique partition under the action of all round keys.

The next proposition explains the fundamental property of linear partitions according to the key addition. This result was introduced by Harpes in [50, Lemma 4.3] and [52, Theorem 4]. Later, Caranti et al. gave a similar result expressed for imprimitive groups in [31]. For convenience, we restate and prove this result with our own notation.

Proposition 3.23. Let $n$ be a positive integer. Let $\mathcal{A}$ and $\mathcal{B}$ be two partitions of $\mathbb{F}_{2}^{n}$. For each $k$ in $\mathbb{F}_{2}^{n}$, let $\alpha_{k}$ denote the permutation of $\mathbb{F}_{2}^{n}$ defined by the rule $\alpha_{k}(x)=x+k$. Then, the permutation $\alpha_{k}$ maps $\mathcal{A}$ to $\mathcal{B}$ for any $k$ in $\mathbb{F}_{2}^{n}$ if and only if $\mathcal{A}=\mathcal{B}$ and $\mathcal{A}$ is a linear partition.

Proof. Firstly, suppose that $\alpha_{k}(\mathcal{A})=\mathcal{B}$ for any $k$ in $\mathbb{F}_{2}^{n}$. Especially, choosing $k=0_{n}$ gives $\alpha_{0_{n}}(\mathcal{A})=\mathcal{B}$, and thus $\mathcal{A}=\mathcal{B}$ since $\alpha_{0_{n}}$ is the identity mapping. Let $V$ denote the part of $\mathcal{A}$ containing $0_{n}$. It is sufficient to show that $V$ is a subgroup of $\mathbb{F}_{2}^{n}$

## Chapter 3 - Partition-Based Backdoor Ciphers

because any subgroup of $\mathbb{F}_{2}^{n}$ is also a $\mathbb{F}_{2}$-linear subspace of $\mathbb{F}_{2}^{n}$. Let $v_{1}$ and $v_{2}$ be two elements of $V$. Since $\alpha_{v_{1}}\left(0_{n}\right)=v_{1}$, the intersection $\alpha_{v_{1}}(V) \cap V$ is non-empty. We know that $\alpha_{v_{1}}$ maps $\mathcal{A}$ to $\mathcal{A}$, so $\alpha_{v_{1}}(V)$ lies in $\mathcal{A}$. Thus, $\alpha_{v_{1}}(V)=V$ since $\mathcal{A}$ is a partition. It follows that $\alpha_{v_{1}}\left(v_{2}\right)=v_{1}+v_{2}$ is an element of $V$. Therefore, the subset $V$ of $\mathbb{F}_{2}^{n}$ is closed under the operation of addition and because every element of $\mathbb{F}_{2}^{n}$ is its own inverse, $V$ is a subgroup of $\mathbb{F}_{2}^{n}$. Furthermore, for any $x$ in $\mathbb{F}_{2}^{n}, \alpha_{x}(V)=x+V$ must be a part of $\mathcal{A}$. Thus, $\mathcal{A}$ is linear.

Conversely, suppose that the partition $\mathcal{A}$ is linear and that $\mathcal{A}=\mathcal{B}$. Let $V$ denote the part of $\mathcal{A}$ containing $0_{n}$ and let $x$ be an element of $\mathbb{F}_{2}^{n}$. Then,

$$
\alpha_{x}(\mathcal{A})=\alpha_{x}\left(\left\{y+V \mid y \in \mathbb{F}_{2}^{n}\right\}\right)=\left\{(x+y)+V \mid y \in \mathbb{F}_{2}^{n}\right\}=\mathcal{A} .
$$

The result is proven.
Even if this result was easily obtained, it has maybe the most important impact on our study. Due to this result and its generalization given later in the next section, only linear partitions will be considered. By definition, the linear partitions are quotient spaces, and hence highly structured algebraic objects. Consequently, the apparent combinatorial aspect of our study is reduced to an algebraic problem. This result is indeed quite restrictive since the linear partitions account for a small proportion of all partitions.

Example 3.24. Let $n$ and $k$ be non-negative integers and $q$ be a prime power. The $q$-binomial (or Gaussian) coefficient is defined to be

$$
\left[\begin{array}{l}
n \\
d
\end{array}\right]_{q}=\prod_{i=1}^{d} \frac{1-q^{n-i+1}}{1-q^{i}} .
$$

It can be proven that this coefficient counts the number of $d$-dimensional subspaces of an $n$-dimensional vector space over the finite field $\mathbb{F}_{q}[46]$. Therefore, the number of subspaces of $\mathbb{F}_{2}^{3}$ is given by

$$
\begin{aligned}
\sum_{d=0}^{3}\left[\begin{array}{l}
3 \\
d
\end{array}\right]_{2} & =1+\frac{1-2^{3}}{1-2}+\frac{\left(1-2^{3}\right)\left(1-2^{2}\right)}{(1-2)\left(1-2^{2}\right)}+\frac{\left(1-2^{3}\right)\left(1-2^{2}\right)\left(1-2^{1}\right)}{(1-2)\left(1-2^{2}\right)\left(1-2^{3}\right)} \\
& =1+7+7+1=16 .
\end{aligned}
$$

Since a linear partition of $\mathbb{F}_{2}^{3}$ is uniquely determined by a subspace of $\mathbb{F}_{2}^{3}$, there are exactly 16 linear partitions. All these partitions are represented graphically at the top of Figure 3.4. For instance, the linear partition associated with the subspace $\operatorname{span}(2,4)=\{0,2,4,6\}$ is $\mathcal{L}(\operatorname{span}(2,4))=\{\{0,2,4,6\},\{1,3,5,7\}\}$. The On-line Encyclopedia of Integer Sequences (OEIS [93]) includes almost all known integer sequences. The 2-binomial coefficients are given in the sequence A022166 and their sums are given in A006116.

Proposition 3.23 states that, among the set of all the partitions of $\mathbb{F}_{2}^{n}$, only the linear ones yield a unique output partition for every key. The Bell number $B_{m}$ counts the number of partitions of a set of size $m$ (see sequence A000110). Thus, the number of partitions of $\mathbb{F}_{2}^{n}$ is $B_{2^{n}}$. For $n=3$, there are $B_{8}=4140$ partitions in all. Hence, the

Every linear partitions over $\mathbb{F}_{2}^{3}$
All the key additions


Figure 3.4: All linear partitions and key additions in $\mathbb{F}_{2}^{3}$.

## Chapter 3 - Partition-Based Backdoor Ciphers



Figure 3.5: The key additions preserving the partition $\mathcal{L}(\operatorname{span}(6))$.
linear partitions represent a fraction of $16 / B_{8} \approx 2^{-8.0}$. This ratio falls greatly as $n$ increases. In fact, for $n=4$, only $67 / B_{16} \approx 2^{-27.2}$ are linear and for $n=5$, this ratio becomes $374 / B_{32} \approx 2^{-78.2}$. This underlines how Proposition 3.23 is restrictive.

All the key additions are given at the bottom of Figure 3.4. The reverse implication of Proposition 3.23 states that any linear partition is preserved by all the key additions. For instance,

$$
\begin{aligned}
& \alpha_{2}(\mathcal{L}(\operatorname{span}(6))=\{f(\{0,6\}), f(\{1,7\}), f(\{2,4\}), f(\{3,5\})\} \\
& =\{\{2,4\},\{3,5\},\{0,6\},\{1,7\}\}=\mathcal{L}(\operatorname{span}(6)) \text {. }
\end{aligned}
$$

Thus, the permutation $\alpha_{2}$ preserves $\mathcal{L}(\operatorname{span}(6))$. Figure 3.5 illustrates graphically that this linear partition is preserved by all the key additions. It is then not hard to check that the same holds for every linear partition given in Figure 3.4.

Now that we know linear partitions are of major importance, we focus on how the diffusion layer deals with these partitions.

Proposition 3.25. Let $n$ be a positive integer. Let $L$ be an automorphism of $\mathbb{F}_{2}^{n}$ and $V$ a subspace of $\mathbb{F}_{2}^{n}$. Then, $L(\mathcal{L}(V))=\mathcal{L}(L(V))$. In particular, $L$ maps a linear partition to another one.

Proof. Since $L$ is an automorphism, we have

$$
\begin{aligned}
L(\mathcal{L}(V)) & =L\left(\left\{x+V \mid x \in \mathbb{F}_{2}^{n}\right\}\right)=\left\{L(x+V) \mid x \in \mathbb{F}_{2}^{n}\right\} \\
& =\left\{L(x)+L(V) \mid x \in \mathbb{F}_{2}^{n}\right\}=\left\{x^{\prime}+L(V) \mid x^{\prime} \in \mathbb{F}_{2}^{n}\right\} .
\end{aligned}
$$

Moreover, $L(V)$ is a subspace of $\mathbb{F}_{2}^{n}$ because $L$ is a linear mapping. Consequently, $L(\mathcal{L}(V))=\mathcal{L}(L(V))$.

If $V$ and $W$ are two subspaces of $\mathbb{F}_{2}^{n}$, it is straightforward to design a linear permutation $L$ of $\mathbb{F}_{2}^{n}$ mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Indeed, Proposition 3.25 establishes that $L$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ if and only if $L(V)=W$. In other words, we only need to consider the image of $V$ and not the whole linear partition $\mathcal{L}(V)$.

## 3.2 - Substitution-Permutation Networks and Partitions

### 3.2.3. From the Encryption Function to the Substitution Layer

Along with the two results of the previous section, we can now address our main issue. For the rest of this chapter, we consider a generic SPN whose parameters are defined as follows.

Let $m, n$ and $r$ be positive integers.
Let $S_{0}, \ldots, S_{m-1}$ be $n$-bit S-boxes.

- The addition of the round key $k$ is denoted by $\alpha_{k}: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}, x \mapsto x+k$.
- The substitution layer is denoted by $\sigma$ and maps $\left(x_{i}\right)_{0 \leq i<m}$ to $\left(S_{i}\left(x_{i}\right)\right)_{0 \leq i<m}$.
- The diffusion layer is a linear permutation denoted by $\pi: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$.

The round function $F_{k}$ associated with the round key $k$ is defined to be $F_{k}=\pi \sigma \alpha_{k}$. The encryption function associated with the round keys $K=\left(k^{[0]}, \ldots, k^{[r]}\right)$ in $\left(\mathbb{F}_{2}^{n m}\right)^{r+1}$ is defined to be

$$
E_{K}=\alpha_{k[r]} F_{k[r-1]} \ldots F_{k[0]} .
$$

We can now prove the following result.
Theorem 3.26. Let $\mathcal{A}$ and $\mathcal{B}$ be two partitions of $\mathbb{F}_{2}^{n m}$. Suppose for any $(r+1)$ tuples of round keys $K=\left(k^{[0]}, \ldots, k^{[r]}\right)$ in $\left(\mathbb{F}_{2}^{n m}\right)^{r+1}$ that the encryption function $E_{K}$ maps $\mathcal{A}$ to $\mathcal{B}$. Define $\mathcal{A}^{[0]}=\mathcal{A}$ and for all $1 \leq i \leq r, \mathcal{A}^{[i]}=(\pi \sigma)^{i}(\mathcal{A})$. Then,

- $\mathcal{A}^{[r]}=\mathcal{B}$;
- for any $0 \leq i<r$ and for any $k^{[i]}$ in $\mathbb{F}_{2}^{n m}, F_{k}\left[{ }^{[i]}\left(\mathcal{A}^{[i]}\right)=\mathcal{A}^{[i+1]}\right.$;
- for any $0 \leq i \leq r, \mathcal{A}^{[i]}$ is a linear partition.

Proof. Observe that for the round key $k=0_{n m}$, the key addition $\alpha_{0_{n m}}$ is the identity mapping on $\mathbb{F}_{2}^{n m}$, and thus $F_{0_{n m}}=\pi \sigma \alpha_{0_{n m}}=\pi \sigma$. Now, choosing $K=\left(k^{[0]}, \ldots, k^{[r]}\right)=$ $\left(0_{n m}, \ldots, 0_{n m}\right)$ gives

$$
\begin{aligned}
\mathcal{B} & =E_{K}\left(\mathcal{A}^{[0]}\right)=\alpha_{k[r]} F_{k[r-1]} \ldots F_{k[0]}\left(\mathcal{A}^{[0]}\right)=\alpha_{0_{n m}}\left(F_{0_{n m}}\right)^{r}\left(\mathcal{A}^{[0]}\right) \\
& =(\pi \sigma)^{r}\left(\mathcal{A}^{[0]}\right)=\mathcal{A}^{[r]} .
\end{aligned}
$$

Let $0 \leq i<r$ be an integer. Let $k^{[i]}$ be any element of $\mathbb{F}_{2}^{n m}$. Define $k^{[j]}=0_{n m}$ for all $0 \leq j \leq r$ such that $j \neq i$. By hypothesis, the equality $\alpha_{k[r]} F_{k[r-1]} \ldots F_{k[0]}\left(\mathcal{A}^{[0]}\right)=\mathcal{A}^{[r]}$ holds. Thus,

$$
F_{k[i]} \ldots F_{k[0]}\left(\mathcal{A}^{[0]}\right)=\left(\alpha_{k[r]} F_{k[r-1]} \ldots F_{k[i+1]}\right)^{-1}\left(\mathcal{A}^{[r]}\right) .
$$

On one hand,

$$
\begin{aligned}
F_{k[i]}^{[i]} \ldots F_{k[0]}\left(\mathcal{A}^{[0]}\right) & =F_{k^{[i]}}\left(F_{k}[i-1] \ldots F_{k[0]}\right)\left(\mathcal{A}^{[0]}\right)=F_{k k^{[i]}}\left(F_{0_{n m}}\right)^{i}\left(\mathcal{A}^{[0]}\right) \\
& =F_{\left.k^{[i]}\right]}(\pi \sigma)^{i}\left(\mathcal{A}^{[0]}\right)=F_{k^{[i]}}\left(\mathcal{A}^{[i]}\right) .
\end{aligned}
$$

On the other hand,

$$
\begin{aligned}
\left(\alpha_{k[r]} F_{k[r-1]} \ldots F_{k[i+1]}\right)^{-1}\left(\mathcal{A}^{[r]}\right) & =\left(\alpha_{0_{n m}}\left(F_{0_{n m}}\right)^{r-(i+1)}\right)^{-1}\left(\mathcal{A}^{[r]}\right) \\
& =\left((\pi \sigma)^{r-(i+1)}\right)^{-1}\left(\mathcal{A}^{[r]}\right)=\mathcal{A}^{[i+1]} .
\end{aligned}
$$

## Chapter 3 - Partition-Based Backdoor Ciphers

Therefore, $F_{k k^{[i]}}\left(\mathcal{A}^{[i]}\right)=\mathcal{A}^{[i+1]}$, or equivalently $\alpha_{k[i]}\left(\mathcal{A}^{[i]}\right)=(\pi \sigma)^{-1}\left(\mathcal{A}^{[i+1]}\right)$. Since this equality holds for every $k^{[i]}$, Proposition 3.23 states that the partition $\mathcal{A}^{[i]}$ is linear.

It remains to show that $\mathcal{A}^{[r]}$ is linear as the previous argument holds only for $i<r$. Let $k^{[r]}$ be an element of $\mathbb{F}_{2}^{n m}$. Define $k^{[i]}=0_{n m}$ for each $0 \leq i<r$. Then,

$$
\mathcal{A}^{[r]}=\alpha_{k[r]} F_{k[r-1]} \ldots F_{k[0]}\left(\mathcal{A}^{[0]}\right)=\alpha_{k[r]}\left(F_{0_{n m}}\right)^{r}\left(\mathcal{A}^{[0]}\right)=\alpha_{k[r]}\left(\mathcal{A}^{[r]}\right) .
$$

Again, Proposition 3.23 implies that $\mathcal{A}^{[r]}$ is linear and the result is proven.
This theorem can be restated in the following way. Firstly, the input partition $\mathcal{A}$ and the output partition $\mathcal{B}$ must be linear. This result generalizes Proposition 3.23 in the sense that it applies to the full cipher and not only to the key addition. As was pointed in Example 3.24, linear partitions are very specific partitions. This means that our combinatorial hypothesis implies to consider only algebraic objects.

Secondly, we have only supposed that the encryption function maps $\mathcal{A}$ to $\mathcal{B}$ after $r$ rounds. Nevertheless, Theorem 3.26 ensures that each iteration of the round function also maps a fixed linear partition to another one. As a consequence, the study of the full cipher is reduced to the study of the round function. Additionally, this result can be strengthened as follows.

Corollary 3.27. Keep the notation of Theorem 3.26. For all $0 \leq i \leq r$, let $V^{[i]}$ denote the part of $\mathcal{A}^{[i]}$ containing 0 . According to Theorem 3.26, $\mathcal{A}{ }^{[i]}=\mathcal{L}\left(V^{[i]}\right)$. Let $0 \leq i<r$ be an integer. Then,

$$
\sigma\left(\mathcal{L}\left(V^{[i]}\right)\right)=\mathcal{L}\left(W^{[i]}\right) .
$$

where $W^{[i]}$ denotes the subspace $\pi^{-1}\left(V^{[i+1]}\right)$. In particular, the substitution layer must at least map one linear partition to another one.

Proof. By definition, $\pi \sigma\left(\mathcal{A}^{[i]}\right)=\mathcal{A}^{[i+1]}$ or, equivalently, $\sigma\left(\mathcal{A}^{[i]}\right)=\pi^{-1}\left(\mathcal{A}^{[i+1]}\right)$. This equality can be restated as

$$
\sigma\left(\mathcal{L}\left(V^{[i]}\right)\right)=\pi^{-1}\left(\mathcal{L}\left(V^{[i+1]}\right)\right) .
$$

As $\pi$ is an automorphism of $\mathbb{F}_{2}^{n m}$, then so $\pi^{-1}$ is. Next, Proposition 3.25 ensures that $\pi^{-1}\left(\mathcal{L}\left(V^{[i+1]}\right)\right)=\mathcal{L}\left(\pi^{-1}\left(V^{[i+1]}\right)\right)$. The result follows.

A diagrammatic representation of Theorem 3.26 and Corollary 3.27 is given in Figure 3.6. This highlights that the input partition is always transformed in the same way through each basic operation of the encryption process. The results obtained so far can be summarized as follows: if an SPN maps a partition $\mathcal{A}$ of the plaintext space to a partition $\mathcal{B}$ of the ciphertext space no matter the round keys used, then the substitution layer has to map at least one linear partition to another one. This shows that our study can be reduced to the substitution layer without loss of generality.


Figure 3.6: Results of Section 3.2.3

|  |  | . 0 | 1 | . 2 | . 3 | 4 | 5 | 6 | 7 | . 8 | 9 |  | . B |  | D | E | .F |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $S_{0}(x)$ | 0 | 1 F | 19 | 03 | 05 | 1D | 1B | 01 | 07 | 14 | 12 | 1 C | 1A | 16 | 10 | 1E | 18 |
|  | 1 | OE | 08 | 09 | OF | OC | OA | OB | OD | 04 | 02 | 17 | 11 | 06 | 00 | 15 | 13 |
| $S_{1}(x)$ | 0 | 02 | 19 | 11 | 14 | 1B | OE | OC | 07 | 15 | OA | 01 | 00 | OD | 1C | 1D | 12 |
|  |  | 06 | 1 E | 10 | 16 | 05 | 13 | 17 | 1 F | 18 | 04 | 09 | OB | 1A | 08 | OF | 03 |
| $S_{2}(x)$ | 0 | 1 E | 08 | 04 | 13 | OF | 18 | 14 | 10 | 19 | 15 | OE | OD | 03 | 1 C | 07 | 17 |
|  |  | 12 | 11 | OB | 1 B | 09 | 05 | 1 F | 00 | OA | 01 | 02 | 1A | 06 | OC | 1D | 16 |
| $S_{3}(x)$ | 0. | 03 | OA | 10 | 1A | 15 | 04 | 1 C | OE | 12 | 18 | 02 | OB | 06 | 14 | OC | 1D |
|  | 1. | 1B | 09 | 11 | 00 | OF | 05 | 1F | 16 | 08 | 19 | 01 | 13 | 1 E | 17 | OD | 07 |

Figure 3.7: Specification of the S-boxes used throughout Section 3.3.

### 3.3. Structure of the Substitution Layer

In the remainder of this chapter, $V$ and $W$ will denote two subspaces of $\left(\mathbb{F}_{2}^{n}\right)^{m}$.
As explained in the previous section, it remains to understand how the substitution layer can map the linear partition $\mathcal{L}(V)$ to $\mathcal{L}(W)$. This problem is far more complex for the substitution layer than it was for the diffusion layer. The reasons for this are twofold. First, the substitution layer is non-linear. It is even the only part of the SPN which is not affine. As a consequence, to map the linear partition $\mathcal{L}(V)$ to $\mathcal{L}(W)$, we have to consider all the parts of both partitions and not only the subspaces $V$ and $W$, as was the case for the diffusion layer (see Proposition 3.25).

Secondly, the substitution layer should not be considered as a whole, but as the parallel application of its S-boxes. Therefore our problem becomes the following. Given two subspaces $V$ and $W$, what are the necessary and/or sufficient conditions on the S-boxes for the substitution layer to map $\mathcal{L}(V)$ to $\mathcal{L}(W)$.

Before going any further, let us introduce an example that we will continue throughout this section.

Example 3.28. Consider the substitution layer made up of the four 5 -bit S-boxes $S_{0}, S_{1}, S_{2}$ and $S_{3}$ described in Figure 3.7. Its parameters are then $m=4$ and $n=5$. Observe that the S-box $S_{2}$ was previously studied in Example 3.17. Define the two families $\mathcal{E}_{V}=\left(v_{i}\right)_{0 \leq i<7}$ and $\mathcal{E}_{W}=\left(w_{i}\right)_{0 \leq i<7}$ of elements of $\left(\mathbb{F}_{2}^{5}\right)^{4}$ as follows:

$$
\begin{array}{rlr}
v_{0}=(10,00,00,17), v_{3}=(02,00,00,1 \mathrm{C}), & w_{0}=(10,00,00,15), w_{3}=(02,00,00,08), \\
v_{1}=(08,00,00,17), v_{4}=(01,00,00,1 \mathrm{C}), & w_{1}=(08,00,00,1 \mathrm{D}), w_{4}=(01,00,00,00), \\
v_{2}=(04,00,00,0 \mathrm{~B}), v_{5}=(00,00,1 \mathrm{~A}, 00), & w_{2}=(04,00,00,15), w_{5}=(00,00,12,00), \\
v_{6}=(00,00,07,00) . & w_{6}=(00,00,0 \mathrm{E}, 00) .
\end{array}
$$

Finally, define $V$ and $W$ to be the subspaces spanned by $\mathcal{E}_{V}$ and $\mathcal{E}_{W}$ respectively. Note that the family $\mathcal{E}_{V}$ is linearly independent because it is echelonized. Hence, $\mathcal{E}_{V}$
is a basis of $V$. The same applies for $\mathcal{E}_{W}$ and $W$. As a consequence, $V$ and $W$ are both 7 -dimensional subspaces of $\left(\mathbb{F}_{2}^{5}\right)^{4}$.

We claim that the substitution layer $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Naturally, we will not verify this statement by hand because it requires to check for each of the $2^{13}$ cosets of $V$ that the $2^{7}$ images of its elements under $\sigma$ lies in the same coset of $W$. However, the reader who is reluctant to accept this claim is encouraged to check it with a computer.

### 3.3.1. Truncating the substitution layer

To understand how the substitution layer can maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$, we will adopt a divide and conquer strategy. That is to say, we want to break down this problem into several independent sub-problems, each involving fewer S-boxes than the full substitution layer. The first idea is to truncate the substitution layer and the subspaces $V$ and $W$ to get a local view of what happens on some S-boxes.

Definition 3.29 (Truncation and Substitution Layer). Let $E$ be any nonempty subset of $\llbracket 0, m \llbracket$ and define the following mappings

$$
\begin{aligned}
\mathrm{T}_{E}:\left(\mathbb{F}_{2}^{n}\right)^{m} & \longrightarrow\left(\mathbb{F}_{2}^{n}\right)^{E} & \sigma_{E}:\left(\mathbb{F}_{2}^{n}\right)^{E} & \longrightarrow\left(\mathbb{F}_{2}^{n}\right)^{E} \\
\left(x_{i}\right)_{0 \leq i<m} & \longmapsto\left(x_{i}\right)_{i \in E} & \left(x_{i}\right)_{i \in E} & \longmapsto\left(S_{i}\left(x_{i}\right)\right)_{i \in E} .
\end{aligned}
$$

If $E$ has cardinality $p$, then we identify $\left(\mathbb{F}_{2}^{n}\right)^{E}$ with $\left(\mathbb{F}_{2}^{n}\right)^{p}$.
The mapping $\mathrm{T}_{E}$ allows to shorten a vector of $\left(\mathbb{F}_{2}^{n}\right)^{m}$ to keep only the coordinates whose indices belong to $E$. The application $\sigma_{E}$ is a substitution layer truncated to the S-boxes whose indices lie in $E$.

Remark 3.30. Note that $\mathrm{T}_{E}$ is a linear mapping. Observe that $\sigma_{\llbracket 0, m \llbracket}$ is the substitution layer of the SPN. Moreover, the truncated substitution layer $\sigma_{\{i\}}$ and the S-box $S_{i}$ are equal for all $0 \leq i<m$.

Proposition 3.31 (Truncating to a few S-boxes). Suppose that $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Let $E$ be a non-empty subset of $\llbracket 0, m \llbracket$. Then, the permutation $\sigma_{E}$ maps $\mathcal{L}\left(\mathrm{T}_{E}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{E}(W)\right)$.

Proof. Let $x=\left(x_{i}\right)_{i \in E}$ be an element of $\left(\mathbb{F}_{2}^{n}\right)^{E}$. Let $y$ be the element of $\left(\mathbb{F}_{2}^{n}\right)^{m}$ defined by the rule $y_{i}=x_{i}$ if $i$ belongs to $E$ and $y_{i}=0_{n}$ otherwise. Thus, $\mathrm{T}_{E}(y)=x$. By hypothesis, $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Hence, Lemma 3.18 implies that, $\sigma(y+V)=$ $\sigma(y)+W$. Next,

$$
\mathrm{T}_{E}(\sigma(y+V))=\mathrm{T}_{E}(\sigma(y))+\mathrm{T}_{E}(W)
$$

since $\mathrm{T}_{E}$ is a linear mapping. Furthermore,

$$
\begin{aligned}
\mathrm{T}_{E}(\sigma(y+V)) & =\mathrm{T}_{E} \sigma(\{y+v \mid v \in V\})=\left\{\mathrm{T}_{E} \sigma(y+v) \mid v \in V\right\} \\
& =\left\{\sigma_{E}\left(\mathrm{~T}_{E}(y+v)\right) \mid v \in V\right\}=\sigma_{E}\left(\left\{\mathrm{~T}_{E}(y+v) \mid v \in V\right\}\right) \\
& =\sigma_{E}\left(\left\{\mathrm{~T}_{E}(y)+\mathrm{T}_{E}(v) \mid v \in V\right\}\right)=\sigma_{E}\left(\mathrm{~T}_{E}(y)+\mathrm{T}_{E}(V)\right) .
\end{aligned}
$$

| $(07,03)+\mathrm{T}_{\{0,3\}}(V)$ | $\rightarrow$ | $(07,1 \mathrm{~A})+\mathrm{T}_{\{0,3\}}(W)$ | $(07,03)+\mathrm{T}_{\{0,3\}}(V)$ |  | $(07,1 \mathrm{~A})+\mathrm{T}_{\{0,3\}}(W)$ |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $(07,03)+(00,00)$ |  | $(07,1 \mathrm{~A})+(00,00)$ | $(07,03)+(10,17)$ |  | $(07,1 \mathrm{~A})+(0 \mathrm{~A}, 15)$ |
| $(07,03)+(01,1 C)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(06,1 \mathrm{D})$ | $(07,03)+(11,0 B)$ |  | $(07,1 \mathrm{~A})+(0 \mathrm{C}, 08)$ |
| $(07,03)+(02,1 C)$ |  | $(07,1 \mathrm{~A})+(1 \mathrm{C}, 1 \mathrm{D})$ | $(07,03)+(12,0 B)$ |  | $(07,1 \mathrm{~A})+(0 \mathrm{D}, 08)$ |
| $(07,03)+(03,00)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(1 \mathrm{~A}, 00)$ | $(07,03)+(13,17)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(0 \mathrm{~B}, 15)$ |
| $(07,03)+(04,0 \mathrm{~B})$ | $\longrightarrow$ | $(07,1 \mathrm{~A})+(02,08)$ | $(07,03)+(14,1 C)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(08,1 \mathrm{D})$ |
| $(07,03)+(05,17)$ |  | $(07,1 \mathrm{~A})+(04,15)$ | $(07,03)+(15,00)$ |  | $(07,1 \mathrm{~A})+(0 \mathrm{E}, 00)$ |
| $(07,03)+(06,17)$ |  | $(07,1 \mathrm{~A})+(1 \mathrm{E}, 15)$ | $(07,03)+(16,00)$ |  | $(07,1 \mathrm{~A})+(0 \mathrm{~F}, 00)$ |
| $(07,03)+(07,08)$ |  | $(07,1 \mathrm{~A})+(18,08)$ | $(07,03)+(17,1 C)$ |  | $(07,1 \mathrm{~A})+(09,1 \mathrm{D})$ |
| $(07,03)+(08,17)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(1 \mathrm{~F}, 15)$ | $(07,03)+(18,00)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(14,00)$ |
| $(07,03)+(09,08)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(19,08)$ | $(07,03)+(19,1 C)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(12,1 \mathrm{D})$ |
| $(07,03)+(0 A, 0 B)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(17,08)$ | $(07,03)+(1 \mathrm{~A}, 1 \mathrm{C})$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(07,1 \mathrm{D})$ |
| $(07,03)+(0 B, 17)$ |  | $(07,1 \mathrm{~A})+(11,15)$ | $(07,03)+(1 \mathrm{~B}, 00)$ |  | $(07,1 \mathrm{~A})+(01,00)$ |
| $(07,03)+(0 C, 1 C)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(1 \mathrm{D}, 1 \mathrm{D})$ | $(07,03)+(1 \mathrm{C}, 0 \mathrm{~B})$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(16,08)$ |
| $(07,03)+(0 D, 00)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(1 \mathrm{~B}, 00)$ | $(07,03)+(1 \mathrm{D}, 17)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(10,15)$ |
| $(07,03)+(0 \mathrm{E}, 00)$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(15,00)$ | $(07,03)+(1 \mathrm{E}, 17)$ |  | $(07,1 \mathrm{~A})+(05,15)$ |
| $(07,03)+(0 \mathrm{~F}, 1 \mathrm{C})$ |  | $(07,1 \mathrm{~A})+(13,1 \mathrm{D})$ | $\underline{(07,03)+(1 F, 0 B)}$ | $\longmapsto$ | $(07,1 \mathrm{~A})+(03,08)$ |

Figure 3.8: $\sigma_{\{0,3\}}$ mapping a coset of $\mathrm{T}_{\{0,3\}}(V)$ to a coset of $\mathrm{T}_{\{0,3\}}(W)$.

Therefore, $\sigma_{E}\left(x+\mathrm{T}_{E}(V)\right)=\mathrm{T}_{E}(\sigma(y))+\mathrm{T}_{E}(W)$. In other words, the image of any part of $\mathcal{L}\left(\mathrm{T}_{E}(V)\right)$ under $\sigma_{E}$ lies in $\mathcal{L}\left(\mathrm{T}_{E}(W)\right)$. The result is a consequence of Lemma 3.14 .

Example 3.32. By choosing $E=\{0,3\}$, the previous proposition ensures that the truncated substitution layer $\sigma_{\{0,3\}}$ maps $\mathcal{L}\left(\mathrm{T}_{\{0,3\}}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{\{0,3\}}(W)\right)$. First, it is easy to see that

$$
\begin{aligned}
& \mathrm{T}_{\{0,3\}}(V)=\operatorname{span}((10,17),(08,17),(04,0 \mathrm{~B}),(02,1 \mathrm{C}),(01,1 \mathrm{C})), \\
& \mathrm{T}_{\{0,3\}}(W)=\operatorname{span}((10,15),(08,1 \mathrm{D}),(04,15),(02,08),(01,00)) .
\end{aligned}
$$

Again, we will not explicitly check that $\sigma_{\{0,3\}}$ maps $\mathcal{L}\left(\mathrm{T}_{\{0,3\}}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{\{0,3\}}(W)\right)$ but limit ourselves to prove that the coset $(07,03)+\mathrm{T}_{\{0,3\}}(V)$ is mapped to one coset of $\mathrm{T}_{\{0,3\}}(W)$. Its image can be found using Lemma 3.18 as follow

$$
\begin{aligned}
\sigma_{\{0,3\}}\left((07,03)+\mathrm{T}_{\{0,3\}}(V)\right) & =\sigma_{\{0,3\}}((07,03))+\mathrm{T}_{\{0,3\}}(W) \\
& =(07,1 \mathrm{~A})+\mathrm{T}_{\{0,3\}}(W) .
\end{aligned}
$$

The images of every element of this coset are given in Figure 3.8. For instance,

$$
\begin{aligned}
\sigma_{\{0,3\}}((07,03)+(01,1 \mathrm{C})) & =\sigma_{\{0,3\}}(06,1 \mathrm{~F})=\left(S_{0}(06), S_{3}(1 \mathrm{~F})\right)=(01,07) \\
& =(07,1 \mathrm{~A})+(06,1 \mathrm{D}) .
\end{aligned}
$$

This explains the second image.
Choosing $E=\{i\}$ in Proposition 3.31 gives that the S -box $S_{i}$ maps $\mathcal{L}\left(\mathrm{T}_{\{i\}}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{\{i\}}(W)\right)$. As this result holds for each index $i$ in $\llbracket 0, m \llbracket$, we deduce that

$$
\begin{equation*}
\sigma(\mathcal{L}(V))=\mathcal{L}(W) \quad \Longrightarrow \quad \forall i \in \llbracket 0, m \llbracket, S_{i}\left(\mathcal{L}\left(\mathrm{~T}_{\{i\}}(V)\right)\right)=\mathcal{L}\left(\mathrm{T}_{\{i\}}(W)\right) \tag{3.1}
\end{equation*}
$$



Figure 3.9: The S-box $S_{3}$ mapping $\mathcal{L}\left(V^{\prime}\right)$ to $\mathcal{L}\left(W^{\prime}\right)$ where $V^{\prime}=\operatorname{span}(0 \mathrm{~B}, 17)$ and $W^{\prime}=\operatorname{span}(08,15)$.

However, the equivalence does not hold in general. Hence, this only gives a necessary condition on each S-box. In other words, this means that we can lose information when considering each S-box independently. The next example stresses this fact.
Example 3.33. In our example, the truncated subspaces $\mathrm{T}_{\{i\}}(V)$ and $\mathrm{T}_{\{i\}}(W)$ are the following:

$$
\begin{aligned}
& \mathrm{T}_{\{0\}}(V)=\mathbb{F}_{2}^{5}, \mathrm{~T}_{\{1\}}(V)=\{00\}, \\
& \mathrm{T}_{\{2\}}(V)=\operatorname{span}(07,1 \mathrm{~A}), \mathrm{T}_{\{3\}}(V)=\operatorname{span}(0 \mathrm{~B}, 17), \\
& \mathrm{T}_{\{0\}}(W)=\mathbb{F}_{2}^{5}, \mathrm{~T}_{\{1\}}(W)=\{00\}, \\
& \mathrm{T}_{\{2\}}(W)=\operatorname{span}(0 \mathrm{~B}, 17), \mathrm{T}_{\{3\}}(W)=\operatorname{span}(08,15) .
\end{aligned}
$$

First, observe that the truncated subspaces for $S_{0}$ and $S_{1}$ are trivial. Hence, the associated linear partitions are also trivial and no information on $S_{0}$ or $S_{1}$ can be drawn from (3.1). Yet, the last two truncated subspaces are non-trivial and (3.1) gives the following equalities:

$$
\begin{aligned}
& S_{2}(\mathcal{L}(\operatorname{span}(07,1 \mathrm{~A})))=\mathcal{L}(\operatorname{span}(0 \mathrm{~B}, 17)), \\
& S_{3}(\mathcal{L}(\operatorname{span}(0 \mathrm{~B}, 17)))=\mathcal{L}(\operatorname{span}(08,15))
\end{aligned}
$$

The first property has already been highlighted in Example 3.17 and in Figure 3.3. The second one is represented in Figure 3.9.

Let us now show that the converse of Implication 3.1 does not hold in general. Consider the substitution layer $\sigma^{\prime}$ made up of the four S-boxes $S_{0}^{\prime}, S_{1}^{\prime}, S_{2}^{\prime}$ and $S_{3}^{\prime}$ where

$$
S_{\mathbf{0}}^{\prime}=S_{\mathbf{1}}, \quad S_{1}^{\prime}=S_{1}, \quad S_{2}^{\prime}=S_{2}, \quad S_{3}^{\prime}=S_{3} .
$$

Thus, this new substitution layer differs from $\sigma$ by only one S-box. Recall that the linear partition associated with $\mathrm{T}_{\{0\}}(V)=\mathrm{T}_{\{0\}}(W)$ is trivial. Therefore, $S_{0}^{\prime}$ necessarily preserves this partition. As the other S-boxes remain the same, the right side of (3.1) still holds for $\sigma^{\prime}$, that is

$$
\forall i \in \llbracket 0,4 \llbracket, S_{i}^{\prime}\left(\mathcal{L}\left(\mathrm{T}_{\{i\}}(V)\right)\right)=\mathcal{L}\left(\mathrm{T}_{\{i\}}(W)\right)
$$

However, we will prove that $\sigma^{\prime}$ does not map $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Suppose by contradiction that it does. Then Proposition 3.31 ensures that $\sigma_{\{0,3\}}^{\prime}$ maps $\mathcal{L}\left(\mathrm{T}_{\{0,3\}}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{\{0,3\}}(W)\right)$. By Lemma 3.18,

$$
\begin{aligned}
\sigma_{\{0,3\}}^{\prime}\left((07,03)+\mathrm{T}_{\{0,3\}}(V)\right) & =\sigma_{\{0,3\}}^{\prime}(07,03)+\mathrm{T}_{\{0,3\}}(W) \\
& =\left(S_{0}^{\prime}(07), S_{3}^{\prime}(03)\right)+\mathrm{T}_{\{0,3\}}(W) \\
& =\left(S_{1}(07), S_{3}(03)\right)+\mathrm{T}_{\{0,3\}}(W)=(07,1 \mathrm{~A})+\mathrm{T}_{\{0,3\}}(W) .
\end{aligned}
$$

## Chapter 3 - Partition-Based Backdoor Ciphers

Then

$$
\begin{aligned}
\sigma_{\{0,3\}}^{\prime}((07,03)+(01,1 \mathrm{C})) & =\sigma_{\{0,3\}}^{\prime}(06,1 \mathrm{~F})=\left(S_{0}^{\prime}(06), S_{3}^{\prime}(1 \mathrm{~F})\right)=\left(S_{1}(06), S_{3}(1 \mathrm{~F})\right) \\
& =(0 \mathrm{C}, 07)=(07,1 \mathrm{~A})+(0 \mathrm{~B}, 1 \mathrm{D}) .
\end{aligned}
$$

This is a contradiction since $(0 \mathrm{~B}, 1 \mathrm{D})$ does not belong to $\mathrm{T}_{\{0,3\}}(W)$ as it can be seen in Figure 3.8. As a consequence, the substitution layer $\sigma^{\prime}$ does not map $\mathcal{L}(V)$ to $\mathcal{L}(W)$.

As shown in the previous example, truncating the substitution layer and the subspaces $V$ and $W$ to each S-box independently of the others is too restrictive in general. This suggests that some S-boxes can in a way be linked together. That is to say, considering them independently results in a loss of information on the subspaces $V$ and $W$. Recall that we are interested in splitting the problem of finding all the substitution layers $\sigma$ mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$ into several independent smaller problems. Taking into account that some S-boxes can be linked together, we require the following:

- a sub-problem can involve several S-boxes;
- the same S-box cannot be involved in two different sub-problems (in other words, the sub-problems are independent);
- each S-box is involved in one sub-problem (possibly trivial).

This is naturally formalized by a partition $\mathcal{I}$ of $\llbracket 0, m \llbracket$. Each part $I$ of $\mathcal{I}$ represents a sub-problem and its elements are the indices of the S-boxes involved in. By virtue of Proposition 3.31, it holds that

$$
\begin{equation*}
\sigma(\mathcal{L}(V))=\mathcal{L}(W) \quad \Longrightarrow \quad \forall I \in \mathcal{I}, \sigma_{I}\left(\mathcal{L}\left(\mathrm{~T}_{I}(V)\right)\right)=\mathcal{L}\left(\mathrm{T}_{I}(W)\right) . \tag{3.2}
\end{equation*}
$$

The next section aims to find a sufficient condition on the partition $\mathcal{I}$ to obtain the equivalence. In such a case, this means that combining the solutions of these sub-problems yields a substitution layer mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$ and vice versa.

### 3.3.2. Structure of the Subspaces $V$ and $W$

With the aim of finding partitions for which the converse of (3.2) holds, let us introduce a few definitions and notation.

Definition 3.34 (Wall, $V_{E}$ and $W_{E}$ ). Let $E$ be a subset of $\llbracket 0, m \llbracket$. The wall associated with $E$, denoted by $\mathrm{Wall}_{E}$, is defined to be

$$
\operatorname{Wall}_{E}=\left\{x \in\left(\mathbb{F}_{2}^{n}\right)^{m} \mid \forall i \in E^{c}, x_{i}=0_{n}\right\} .
$$

Moreover, we denote by $V_{E}$ the intersection of $V$ and $\operatorname{Wall}_{E}$, that is $V_{E}=V \cap \operatorname{Wall}_{E}=$ $\left\{v \in V \mid \forall i \in E^{c}, v_{i}=0_{n}\right\}$. The subspace $W_{E}$ is defined in the same way.

Remark 3.35. The notion of wall was introduced by Aragona and Calderini [4, 22. It is easily seen that

$$
\mathrm{Wall}_{E}=\prod_{i=0}^{m-1} \operatorname{Wall}_{E}^{[i]} \quad \text { with } \quad \operatorname{Wall}_{E}^{[i]}= \begin{cases}\left\{0_{n}\right\} & \text { if } i \in E^{c} \\ \mathbb{F}_{2}^{n} & \text { if } i \in E\end{cases}
$$

$$
\begin{aligned}
v_{0}=(15,00,00,00), v_{3}=(04,00,00,0 \mathrm{~B}), & w_{0}=(14,00,00,00), w_{3}=(04,00,00,15), \\
v_{1}=(0 \mathrm{D}, 00,00,00), v_{4}=(01,00,00,1 \mathrm{C}), & w_{1}=(0 \mathrm{E}, 00,00,00), w_{4}=(02,00,00,08), \\
v_{2}=(03,00,00,00), v_{5}=(00,00,1 \mathrm{~A}, 00), & w_{2}=(01,00,00,00), w_{5}=(00,00,12,00), \\
v_{6}=(00,00,07,00) . & w_{6}=(00,00,0 \mathrm{E}, 00) .
\end{aligned}
$$



$$
\begin{aligned}
& A_{V}=\operatorname{span}\left(v_{5}, v_{6}\right) \\
& B_{V}=\operatorname{span}\left(v_{0}, v_{1}, v_{2}\right) \\
& C_{V}=\operatorname{span}\left(v_{0}, v_{1}, v_{2}, v_{3}, v_{4}\right) \\
& D_{V}=\operatorname{span}\left(v_{0}, v_{1}, v_{2}, v_{5}, v_{6}\right)
\end{aligned}
$$

$$
\begin{aligned}
& A_{W}=\operatorname{span}\left(w_{5}, w_{6}\right) \\
& B_{W}=\operatorname{span}\left(w_{0}, w_{1}, w_{2}\right) \\
& C_{W}=\operatorname{span}\left(w_{0}, w_{1}, w_{2}, w_{3}, w_{4}\right) \\
& D_{W}=\operatorname{span}\left(w_{0}, w_{1}, w_{2}, w_{5}, w_{6}\right)
\end{aligned}
$$

Figure 3.10: The subspaces $V_{E}, W_{E}$ for each subset $E$ of $\{0,1,2,3\}$.

Thus, a wall is the Cartesian product of trivial spaces for each S-box. Additionally, if $E \subseteq F$, then $\mathrm{Wall}_{E} \subseteq \mathrm{Wall}_{F}$ and hence $V_{E} \subseteq V_{F}$ and $W_{E} \subseteq W_{F}$.

The subspaces Wall $_{E}$ are essential in the study of the substitution layer because the latter always preserves the partition $\mathcal{L}\left(\mathrm{Wall}_{E}\right)$ regardless of its S-boxes. This result, together with Proposition 3.20, establishes the following corollary.

Corollary 3.36. Let $E$ be a subset of $\llbracket 0, m \llbracket$. If $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$, then $\sigma$ also maps $\mathcal{L}\left(V_{E}\right)$ to $\mathcal{L}\left(W_{E}\right)$.

Example 3.37. All the subspaces $V_{E}$ are graphically represented in Figure 3.10. For instance,

$$
V_{\{0\}}=\operatorname{span}((15,00,00,00),(0 \mathrm{D}, 00,00,00),(03,00,00,00)) .
$$

Additionally, this figure also highlights the expected inclusions given by Remark 3.35. Observe that $\mathcal{B}_{V}=\left(v_{i}\right)_{0 \leq i<7}$ is a basis of $V$. This new basis is more convenient than the standard basis $\mathcal{E}_{V}$ previously introduced in Example 3.28 since all the $V_{E}$ are

## Chapter 3 - Partition-Based Backdoor Ciphers



Figure 3.11: The S-box $S_{0}$ mapping $\mathcal{L}\left(V^{\prime}\right)$ to $\mathcal{L}\left(W^{\prime}\right)$ where $V^{\prime}=\operatorname{span}(03,0 \mathrm{D}, 15)$ and $W^{\prime}=\operatorname{span}(01,0 \mathrm{E}, 14)$.
then easily described. It is worth noting that the same picture remains valid for the subspace $W$. For example,

$$
W_{\{0\}}=\operatorname{span}((14,00,00,00),(0 \mathrm{E}, 00,00,00),(01,00,00,00)) .
$$

This emphasizes that when the substitution layer maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$, the subspaces $V$ and $W$ have the same structure.

According to Corollary 3.36 , the substitution layer maps $\mathcal{L}\left(V_{\{0\}}\right)$ to $\mathcal{L}\left(W_{\{0\}}\right)$. Next, truncate to $E=\{0\}$ using Proposition 3.31 to obtain

$$
S_{0}(\mathcal{L}(\operatorname{span}(03,0 \mathrm{D}, 15)))=\mathcal{L}(\operatorname{span}(01,0 \mathrm{E}, 14))
$$

This property is depicted in Figure 3.11. Finally, it should be underlined that with Proposition 3.31 alone, no property can be established on the S-box $S_{0}$ (see Example 3.33).

Definition 3.38 (Projection $\mathrm{P}_{E}$ ). Let $E$ be a subset of $\llbracket 0, m \llbracket$. The projection $\mathrm{P}_{E}$ from $\left(\mathbb{F}_{2}^{n}\right)^{m}$ onto $\mathrm{Wall}_{E}$ is defined to be $\mathrm{P}_{E}\left(x_{0}, \ldots, x_{m-1}\right)=\left(y_{0}, \ldots, y_{m-1}\right)$ where $y_{i}=x_{i}$ if $i$ belongs to $E$ and $y_{i}=0_{n}$ otherwise.

Remark 3.39. It is not hard to see that $\mathrm{P}_{E}$ is a linear mapping and that $V_{E}$ is always a subspace of $\mathrm{P}_{E}(V)$. Moreover, it holds that $\mathrm{T}_{E}(V)=\mathrm{T}_{E}\left(\mathrm{P}_{E}(V)\right)$.

The next lemma gives some relations between the previous definitions. It is quite important and will be used several times by the end of the current chapter.

Lemma 3.40. Let $\mathcal{I}$ be a partition of $\llbracket 0, m \llbracket$. Then $V$ equals the internal direct sum $\oplus_{I \in \mathcal{I}} V_{I}$ if and only if $V_{I}=\mathrm{P}_{I}(V)$ for any part $I$ of $\mathcal{I}$. In this case, the decomposition of an element $v$ of $V$ is $v=\sum_{I \in \mathcal{I}} \mathrm{P}_{I}(v)$.

Proof. Suppose that $V=\oplus_{I \in \mathcal{I}} V_{I}$. Let $I$ be a part of $\mathcal{I}$. Since $V_{I}$ is always included in $\mathrm{P}_{I}(V)$, only $\mathrm{P}_{I}(V) \subseteq V_{I}$ needs to be verified. Let $v=\left(v_{0}, \ldots, v_{m-1}\right)$ be an element of $V$. We must prove that $\mathrm{P}_{I}(v)$ lies in $V_{I}$. By hypothesis, $v$ can be uniquely written as $\sum_{J \in \mathcal{I}} v_{J}$ where $v_{J}$ belongs to $V_{J}$. For every $i$ in $I$, we have

$$
\left(\mathrm{P}_{I}(v)\right)_{i}=v_{i}=\sum_{J \in \mathcal{I}}\left(v_{J}\right)_{i}=\left(v_{I}\right)_{i},
$$

since $\left(v_{J}\right)=0_{n}$ for all parts $J$ of $\mathcal{I}$ distinct from $I$. As $\mathrm{P}_{I}(v)_{i}=0_{n}=\left(v_{I}\right)_{i}$ for each $i$ in $I^{c}$, we have $\mathrm{P}_{I}(v)=v_{I}$. Thus, $\mathrm{P}_{I}(v)$ is included in $V_{I}$.

Conversely, suppose that $V_{I}=\mathrm{P}_{I}(V)$ for all $I$ in $\mathcal{I}$. Let $v$ be an element of $V$. Clearly, $v=\sum_{I \in \mathcal{I}} \mathrm{P}_{I}(v)$. By hypothesis, $\mathrm{P}_{I}(v)$ belongs to $V_{I}$ for any $I$ in $\mathcal{I}$. The uniqueness of this decomposition directly follows from the definition of the $V_{I}$. Therefore, $V=\oplus_{I \in \mathcal{I}} V_{I}$.

Remark 3.41. Suppose that $\mathcal{I}$ is a partition of $\llbracket 0, m \llbracket$ such that $V=\bigoplus_{I \in \mathcal{I}} V_{I}$. The previous lemma, together with Remark 3.39, establishes that $\mathrm{T}_{I}(V)=\mathrm{T}_{I}\left(V_{I}\right)$ for each part $I$ of $\mathcal{I}$.

Proposition 3.42 (Substitution layer structure). Let $\mathcal{I}$ be a partition of $\llbracket 0, m \llbracket$ satisfying both $V=\bigoplus_{I \in \mathcal{I}} V_{I}$ and $W=\bigoplus_{I \in \mathcal{I}} W_{I}$. The permutation $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ if and only if $\sigma_{I}$ maps $\mathcal{L}\left(\mathrm{T}_{I}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{I}(W)\right)$ for any $I$ in $\mathcal{I}$.

Proof. The implication follows from Proposition 3.31. Conversely, suppose that $\sigma_{I}$ maps $\mathcal{L}\left(\mathrm{T}_{I}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{I}(W)\right)$ for any $I$ in $\mathcal{I}$. First, let us prove that $V$ and $W$ have the same number of elements. Let $I$ be a part of $\mathcal{I}$. Since $\sigma_{I}$ maps $\mathcal{L}\left(\mathrm{T}_{I}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{I}(W)\right)$, Proposition 3.21 states that $\mathrm{T}_{I}(V)$ and $\mathrm{T}_{I}(W)$ are isomorphic. Then $\mathrm{T}_{I}\left(V_{I}\right)$ and $\mathrm{T}_{I}\left(W_{I}\right)$ are isomorphic by Remark 3.41. It is not hard to see that the restriction of $\mathrm{T}_{I}$ to $V_{I}$ is one-to-one. Therefore, $\mathrm{T}_{I}\left(V_{I}\right)$ is isomorphic to $V_{I}$ and similarly, $\mathrm{T}_{I}\left(W_{I}\right)$ is isomorphic to $W_{I}$. Gathering together these results, we deduce that $V_{I}$ and $W_{I}$ are isomorphic for each part $I$ of $\mathcal{I}$. Consequently, $V=\oplus_{I \in \mathcal{I}} V_{I}$ and $W=\oplus_{I \in \mathcal{I}} W_{I}$ have the same dimension, and thus the same number of elements.

To prove that $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$, it is sufficient to show that the equality $\sigma(x+V)=\sigma(x)+W$ holds for any element $x$ of $\mathbb{F}_{2}^{n m}$ thanks to Lemma 3.14. Hence, let $x$ belong to $\mathbb{F}_{2}^{n m}$. The discussion above implies that $\sigma(x+V)$ and $\sigma(x)+W$ have the same cardinality. Thus, we just need to verify that $\sigma(x+V) \subseteq \sigma(x)+W$. Let $v$ be any element of $V$. By hypothesis and by Lemma 3.18, for each part $I$ of $\mathcal{I}$, there exists $t_{I}$ in $\mathrm{T}_{I}(W)$ such that

$$
\sigma_{I}\left(\mathrm{~T}_{I}(x)+\mathrm{T}_{I}(v)\right)=\sigma_{I}\left(\mathrm{~T}_{I}(x)\right)+t_{I} .
$$

Observe that for any index $0 \leq i<m$, denoting by [i] the unique part of $\mathcal{I}$ containing $i$, we have the following:

$$
\begin{aligned}
\sigma(x+v)_{i} & =\sigma_{[i]}\left(\mathrm{T}_{[i]}(x)+\mathrm{T}_{[i]}(v)\right)_{i}=\sigma_{[i]}\left(\mathrm{T}_{[i]}(x)\right)_{i}+\left(t_{[i]}\right)_{i} \\
& =\sigma(x)_{i}+\left(t_{[i]}\right)_{i} .
\end{aligned}
$$

Then, define $w=\left(w_{0}, \ldots, w_{m-1}\right)$ by $w_{i}=\left(t_{[i]}\right)_{i}$. This yields the equality

$$
\sigma(x+v)=\sigma(x)+w .
$$

It remains to explain why $w$ lies in $W$. By hypothesis, $W=\oplus_{I \in \mathcal{I}} W_{I}$. Because $t_{I}$ is in $\mathrm{T}_{I}(W)$, there exists $w_{I}^{\prime}$ in $W$ such that $\mathrm{T}_{I}\left(w_{I}^{\prime}\right)=t_{I}$. As $\mathrm{T}_{I}=\mathrm{T}_{I} \circ \mathrm{P}_{I}$, we have $t_{I}=\mathrm{T}_{I}\left(\mathrm{P}_{I}\left(w_{I}^{\prime}\right)\right)=\mathrm{T}_{I}\left(w_{I}\right)$ with $w_{I}=\mathrm{P}_{I}\left(w_{I}^{\prime}\right)$. Next, Lemma 3.40 states that $W_{I}=\mathrm{P}_{I}(W)$ for any part $I$ of $\mathcal{I}$ thus $w_{I}$ belongs to $W_{I}$. Finally, it is easy to see that $w=\sum_{I \in \mathcal{I}} w_{I}$, and hence $w$ belongs to $W$. Summarizing, this proves that $\sigma(x+V)$ is included in $\sigma(x)+W$, as desired.

## Chapter 3 - Partition-Based Backdoor Ciphers

The preceding proposition establishes that the converse of Implication (3.2) (page 88) holds whenever the partition $\mathcal{I}$ satisfies both $V=\bigoplus_{I \in \mathcal{I}} V_{I}$ and $W=\bigoplus_{I \in \mathcal{I}} W_{I}$. For such a partition, the problem of finding all the substitution layers $\sigma$ mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$ can equivalently be broken down into the independent sub-problems of finding all the $\sigma_{I}$ mapping $\mathcal{L}\left(\mathrm{T}_{I}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{I}(W)\right)$ for each part $I$ of $\mathcal{I}$.

### 3.3.3. Linked and Independent S-Boxes

Of course, there may be several partitions $\mathcal{I}$ such that $V=\oplus_{I \in \mathcal{I}} V_{I}$ and $W=\oplus_{I \in \mathcal{I}} W_{I}$, each yielding a different decomposition of the substitution layer. A few of these decompositions are certainly more interesting or easier to solve. The purpose of this section is to study such partitions. Let us begin with the following lemma.

Lemma 3.43. Suppose that $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. For every partition $\mathcal{I}$ of $\llbracket 0, m \llbracket, V=\oplus_{I \in \mathcal{I}} V_{I}$ if and only if $W=\oplus_{I \in \mathcal{I}} W_{I}$.

Proof. Let $\mathcal{I}$ be a partition of $\llbracket 0, m \llbracket$. Suppose that $V=\oplus_{I \in \mathcal{I}} V_{I}$. Firstly, let us prove that $W=\sum_{I \in \mathcal{I}} W_{I}$. Since the $W_{I}$ are subspaces of $W$, the inclusion $\sum_{I \in \mathcal{I}} W_{I} \subseteq W$ clearly holds. Now, let us prove the converse inclusion. Let $w$ be an element of $W$. Define $x=\sigma^{-1}\left(0_{n m}\right)=\left(S_{i}^{-1}\left(0_{n}\right)\right)_{0 \leq i<m}$. According to Lemma 3.18, we have

$$
\sigma(x+V)=\sigma(x)+W=\sigma\left(\sigma^{-1}\left(0_{n m}\right)\right)+W=W .
$$

Hence, there exists an element $v$ of $V$ satisfying the equality $\sigma(x+v)=w$. Then, Lemma 3.40 ensures that $v=\sum_{I \in \mathcal{I}} \mathrm{P}_{I}(v)$. For any $0 \leq i<m$, we have

$$
\sigma\left(x+\mathrm{P}_{I}(v)\right)_{i}=S_{i}\left(x_{i}+\mathrm{P}_{I}(v)_{i}\right)= \begin{cases}S_{i}\left(x_{i}+v_{i}\right) & \text { if } i \in I \\ S_{i}\left(x_{i}+0_{n}\right)=0_{n} & \text { if } i \in I^{c}\end{cases}
$$

Consequently, $\sigma\left(x+\mathrm{P}_{I}(v)\right)$ lies in $\mathrm{Wall}_{I}$ and $W$, so in $W_{I}$. Note that

$$
w=\sigma(x+v)=\sum_{I \in \mathcal{I}} \sigma\left(x+\mathrm{P}_{I}(v)\right)
$$

since $\mathcal{I}$ is a partition of $\llbracket 0, m \llbracket$. The inclusion $W \subseteq \sum_{I \in \mathcal{I}} W_{I}$ follows. Finally, the definition of the $W_{I}$ implies that $W=\oplus_{I \in \mathcal{I}} W_{I}$.

Conversely, suppose that $W=\oplus_{I \in \mathcal{I}} W_{I}$. Following the previous reasoning with $\sigma^{-1}$ instead of $\sigma$ gives the equality $V=\oplus_{I \in \mathcal{I}} V_{I}$, as desired.

The contrapositive of Lemma 3.43 is the following: if there exists a partition $\mathcal{I}$ such that $V=\oplus_{I \in \mathcal{I}} V_{I}$ and $W \neq \bigoplus_{I \in \mathcal{I}} W_{I}$ or such that $V \neq \bigoplus_{I \in \mathcal{I}} V_{I}$ and $W=\oplus_{I \in \mathcal{I}} W_{I}$, then there exists no substitution layer mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Because we intend to study the substitution layers mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$, Lemma 3.43 suggests to assume the following.

Assumption 3.44. For the remainder of this section, we assume that for any partition $\mathcal{I}$ of $\llbracket 0, m \llbracket$, it holds that

$$
V=\bigoplus_{I \in \mathcal{I}} V_{I} \Longleftrightarrow W=\bigoplus_{I \in \mathcal{I}} W_{I}
$$



Figure 3.12: The partitions $\mathcal{I}$ of $\{0,1,2,3\}$ such that $V=\oplus_{I \in \mathcal{I}} V_{I}$.

Proposition 3.42, together with the preceding assumption, suggests the following definition.

Definition 3.45 (Decomposition Partition). A decomposition partition (with respect to $V$ and $W)$ is a partition of $\llbracket 0, m \llbracket$ such that $V=\oplus_{I \in \mathcal{I}} V_{I}$.

Remark 3.46 (Partial Order on Partitions). Recall that if $\mathcal{I}$ and $\mathcal{J}$ are two partitions of $\llbracket 0, m \llbracket$, then the partition $\mathcal{I}$ is said to be finer than $\mathcal{J}$ if for any part $I$ in $\mathcal{I}$, there exists a part $J$ in $\mathcal{J}$ such that $I \subseteq J$.

Example 3.47. The purpose of this example is to find all the decomposition partitions with regards to $V$ and $W$. By virtue of Lemma 3.40, the subspace $V$ can be decomposed as $\bigoplus_{I \in \mathcal{I}} V_{I}$ if and only if $V_{I}$ is equal to $\mathrm{P}_{I}(V)$ for each part $I$ of $\mathcal{I}$. The eight framed subspaces in the middle of Figure 3.10 are exactly those which satisfy $V_{E}=\mathrm{P}_{E}(V)$. Hence, the decomposition partitions are the partitions whose parts are selected from the following:

$$
\varnothing,\{1\},\{2\},\{1,2\},\{0,3\},\{0,1,3\},\{0,2,3\},\{0,1,2,3\} .
$$

It is then easy to check that the decomposition partitions of $V$ are:

$$
\begin{gathered}
\{\{1\},\{2\},\{0,3\}\}, \quad\{\{1\},\{0,2,3\}\}, \quad\{\{2\},\{0,1,3\}\}, \\
\{\{0,3\},\{1,2\}\} \text { and }\{\{0,1,2,3\}\} .
\end{gathered}
$$

## Chapter 3 - Partition-Based Backdoor Ciphers

In Figure 3.12 , all the partitions of $\llbracket 0,4 \llbracket$ are ordered by the "finer-than" relation and the decomposition partitions are emphasized. What stands out is that the decomposition partition $\{\{1\},\{2\},\{0,3\}\}$ is finer than all other decomposition partitions.

The existence of this least decomposition partition in the example above is a very welcome and non-trivial property. This means that all the truncated substitution layers obtained using Proposition 3.42 are the smallest possible. Thus, such a partition should be preferred to any other decomposition partition. We will now prove that this least decomposition partition always exists.

Notation 3.48 (Partition Intersection). Let $\mathcal{I}$ and $\mathcal{J}$ be two partitions of $\llbracket 0, m \llbracket$. We denote by $\mathcal{I} \cap \mathcal{J}$ the set $\{I \cap J \mid(I, J) \in \mathcal{I} \times \mathcal{J}\} \backslash\{\varnothing\}$. Note that $\mathcal{I} \cap \mathcal{J}$ is a partition of $\llbracket 0, m \llbracket$ finer than $\mathcal{I}$ and $\mathcal{J}$.

Lemma 3.49. Let $\mathcal{I}$ and $\mathcal{J}$ be two partitions of $\llbracket 0, m \llbracket$ such that $V=\oplus_{I \in \mathcal{I}} V_{I}=$ $\oplus_{J \in \mathcal{J}} V_{J}$. Then, $V=\oplus_{K \in \mathcal{I} \cap \mathcal{J}} V_{K}$.

Proof. Let $K$ be a part of $\mathcal{I} \cap \mathcal{J}$. According to Lemma 3.40, we only have to prove that $\mathrm{P}_{K}(V)=V_{K}$. Clearly, $V_{K} \subseteq \mathrm{P}_{K}(V)$. Thus, it remains to show that $\mathrm{P}_{K}(V) \subseteq V_{K}$. Since or more precisely that $\mathrm{P}_{K}(V) \subseteq V_{K}$. By definition, there exists parts $I$ and $J$ of $\mathcal{I}$ and $\mathcal{J}$ such that $K=I \cap J$. Let $v$ be an element of $V$. Since $V=\oplus_{I^{\prime} \in \mathcal{I}} V_{I^{\prime}}$, Lemma 3.40 ensures that $\mathrm{P}_{I}(v)$ lies in $V_{I}$, hence in $V$. In the same way, using the relation $V=\oplus_{J^{\prime} \in \mathcal{J}} V_{J^{\prime}}$, we deduce that $\mathrm{P}_{J}\left(\mathrm{P}_{I}(v)\right)$ lies in $V_{J}$, so in $V$. Note that $\mathrm{P}_{J}\left(\mathrm{P}_{I}(v)\right)=\mathrm{P}_{I \cap J}(v)=\mathrm{P}_{K}(v)$. Therefore, $\mathrm{P}_{K}(v)$ belongs to $V \cap \mathrm{Wall}_{K}=V_{K}$.

Proposition 3.50. The set of the partitions $\mathcal{I}$ of $\llbracket 0, m \llbracket$ satisfying $V=\oplus_{I \in \mathcal{I}} V_{I}$ has a least element denoted $\mathcal{I}_{\text {ld }}$.

Proof. Let $\mathcal{P}$ denote the set of all the partitions $\mathcal{I}$ of $\llbracket 0, m \llbracket$ satisfying $V=\oplus_{I \in \mathcal{I}} V_{I}$. By virtue of Lemma 3.49, the set $\mathcal{P}$ is closed under the operation of intersection. Then, it is sufficient to define $\mathcal{I}_{l d}$ to be the intersection of all the elements of $\mathcal{P}$.

Consequently, the only decomposition partition that will be considered in the remainder of this chapter is the least decomposition partition $\mathcal{I}_{\mathrm{ld}}$. The following definition is inspired by Proposition 3.42 and Proposition 3.50.

Definition 3.51 (Linked and independent S-boxes). Suppose that $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Let $I$ be a part of $\mathcal{I}_{\text {ld }}$.

- If $I=\{i\}$, the S -box $S_{i}$ is said to be independent of the other S-boxes.

Moreover, if $V_{\{i\}}=\left\{0_{n m}\right\}$ or $V_{\{i\}}=$ Wall $_{\{i\}}$, the S-box $S_{i}$ is said to be inactive. Otherwise, $S_{i}$ is active.

- If $\# I \geq 2$, then the S-boxes whose indices lie in $I$ are said to be linked together.

Remark 3.52. Let $0 \leq i<m$ be an integer. We have already noted that the substitution layer $\sigma$ always preserves $\mathcal{L}\left(\left\{0_{n m}\right\}\right)$ and $\mathcal{L}\left(\right.$ Wall $\left._{\{i\}}\right)$. In addition, Proposition 3.42 ensures that $\sigma$ maps $\mathcal{L}\left(V_{\{i\}}\right)$ to $\mathcal{L}\left(W_{\{i\}}\right)$. Consequently, if $V_{\{i\}}=$ $\left\{0_{n m}\right\}$ or if $V_{\{i\}}=\operatorname{Wall}_{\{i\}}$, then $V_{\{i\}}=W_{\{i\}}$.

Suppose that the S-box $S_{i}$ is independent with regards to the subspaces $V$ and $W$. As established by Proposition 3.42 and Remark 3.41, if $S_{i}$ is replaced with another S-box $S_{i}^{\prime}$, then this new substitution layer still maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ provided that $S_{i}^{\prime} \operatorname{maps} \mathcal{L}\left(\mathrm{T}_{\{i\}}\left(V_{\{i\}}\right)\right)$ to $\mathcal{L}\left(\mathrm{T}_{\{i\}}\left(W_{\{i\}}\right)\right)$.

Suppose further that $S_{i}$ is active. By definition, $\left\{0_{n m}\right\} \nsubseteq V_{\{i\}} \mp$ Wall $_{\{i\}}$. Observe that the restriction of $\mathrm{T}_{\{i\}}$ to $\mathrm{Wall}_{\{i\}}$ is one-to-one, hence

$$
\left\{0_{n}\right\}=\mathrm{T}_{\{i\}}\left(\left\{0_{n m}\right\}\right) \nsubseteq \mathrm{T}_{\{i\}}\left(V_{\{i\}}\right) \nsubseteq \mathrm{T}_{\{i\}}\left(\operatorname{Wall}_{\{i\}}\right)=\mathbb{F}_{2}^{n} .
$$

Thus, $\mathrm{T}_{\{i\}}\left(V_{\{i\}}\right)$ is a non-trivial subspace of $\mathbb{F}_{2}^{n}$ and the requirement that $S_{i}^{\prime}$ maps $\mathcal{L}\left(\mathrm{T}_{\{i\}}\left(V_{\{i\}}\right)\right)$ to $\mathcal{L}\left(\mathrm{T}_{\{i\}}\left(W_{\{i\}}\right)\right)$ is also non-trivial. Therefore, an independent active S-box can be chosen independently of the other S-boxes but has to respect the structure of the subspaces $V$ and $W$.

Now suppose that $S_{i}$ is inactive. By definition, $V_{\{i\}}=\left\{0_{n m}\right\}$ or $V_{\{i\}}=\operatorname{Wall}_{\{i\}}$. Then the equality $V_{\{i\}}=W_{\{i\}}$ follows from Remark 3.52 and we have

$$
\mathrm{T}_{\{i\}}\left(V_{\{i\}}\right)=\mathrm{T}_{\{i\}}\left(W_{\{i\}}\right)=\left\{0_{n}\right\} \quad \text { or } \quad \mathrm{T}_{\{i\}}\left(V_{\{i\}}\right)=\mathrm{T}_{\{i\}}\left(W_{\{i\}}\right)=\mathbb{F}_{2}^{n} .
$$

In either case, the condition that $S_{i}^{\prime}$ maps $\mathcal{L}\left(\mathrm{T}_{\{i\}}\left(V_{\{i\}}\right)\right)$ to $\mathcal{L}\left(\mathrm{T}_{\{i\}}\left(W_{\{i\}}\right)\right)$ is trivial and any S-box fulfills it. As a consequence, an independent inactive S-box can be freely chosen. In other words, such an S-box has no impact on the fact that $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$.

Finally, suppose that some S-boxes are linked together. If only one of these S-boxes is replaced independently of the others, then the desired property of the substitution layer may not hold.
Example 3.53. As we have seen in Example 3.47 and Figure 3.12, the least decomposition partition with regards to the subspaces $V$ and $W$ is $\mathcal{I}_{\text {ld }}=\{\{1\},\{2\},\{0,3\}\}$. By Proposition 3.42, the substitution layer maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ if and only if the following equalities hold:

$$
\begin{array}{ll}
\sigma_{\{0,3\}}\left(\mathcal{L}\left(\mathrm{T}_{\{0,3\}}(V)\right)\right)=\mathcal{L}\left(\mathrm{T}_{\{0,3\}}(W)\right), & S_{1}\left(\mathcal{L}\left(\mathrm{~T}_{\{1\}}(V)\right)=\mathcal{L}\left(\mathrm{T}_{\{1\}}(W)\right),\right. \\
& S_{2}\left(\mathcal{L}\left(\mathrm{~T}_{\{2\}}(V)\right)=\mathcal{L}\left(\mathrm{T}_{\{2\}}(W)\right) .\right.
\end{array}
$$

Thus, the S-box $S_{1}$ is independent of the other S-boxes, the same applies to $S_{2}$ and the S-boxes $S_{0}$ and $S_{3}$ are linked together. As it was already noted in Figure 3.10, we have

$$
V_{\{1\}}=\{(00,00,00,00)\} \quad \text { and } \quad V_{\{2\}}=\operatorname{span}((00,00,1 \mathrm{~A}, 00),(00,00,07,00)) .
$$

Therefore, the S-box $S_{2}$ is active while $S_{1}$ is inactive.

### 3.3.4. The Forbidden Case

Throughout this section, we assume that the substitution layer $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. In order to prove the last main theorem of this chapter, we need to consider the following particular case.

## Chapter 3 - Partition-Based Backdoor Ciphers

Proposition 3.54. Let $\mathcal{I}$ be a decomposition partition. Let $I$ be a part of $\mathcal{I}$ such that $\# I \geq 2$ and let $E$ be a non-empty proper subset of $I$. Suppose that $V_{E}=V_{I \backslash E}=\left\{0_{n m}\right\}$ and $\mathrm{P}_{E}(V)=$ Wall $_{E}$. Then, for all $i$ in $E, S_{i}$ is an affine mapping.

If the subspace $V$ satisfies the assumption of the proposition above, then at least one of S-boxes has to be affine. Nowadays, an SPN whose substitution layer has an affine S-box cannot be taken seriously. Additionally, such a cipher is likely to be very weak to differential and linear cryptanalysis. This discussion explains the title of this section.

Example 3.55. As seen in Example 3.47, the least decomposition partition is $\mathcal{I}_{\text {ld }}=\{\{1\},\{2\},\{0,3\}\}$. Its only part of cardinality greater than or equal to 2 is $I=\{0,3\}$. The non-empty proper subsets if $I$ are the $E=\{0\}$ and $E=\{1\}$. According to Figure 3.10, we have $V_{\{0\}} \neq\left\{0_{20}\right\}$. Consequently, Proposition 3.54 does not apply to this example and this is good news because none of the S-boxes is affine. Otherwise, this would have disproved the contrapositive of Proposition 3.54.

Now let us introduced another example. Consider a substitution layer $\sigma^{\prime}$ made up two 3-bit S-boxes $S_{0}^{\prime}$ and $S_{1}^{\prime}$, hence its parameters are $m=2$ and $n=3$. Define the subspaces $V^{\prime}$ and $W^{\prime}$ of $\left(\mathbb{F}_{2}^{3}\right)^{2}$ to be

$$
V^{\prime}=W^{\prime}=\operatorname{span}((4,4),(2,2),(1,1))=\left\{(x, x) \mid x \in \mathbb{F}_{2}^{3}\right\}
$$

Finally, suppose that $\sigma^{\prime}$ maps $\mathcal{L}\left(V^{\prime}\right)$ to $\mathcal{L}\left(W^{\prime}\right)$. It is easily seen that

$$
\begin{array}{llll}
V_{\varnothing}^{\prime}=\{(0,0)\}, & V_{\{0\}}^{\prime}=\{(0,0)\}, & V_{\{1\}}^{\prime}=\{(0,0)\}, & V_{\{0,1\}}^{\prime}=V, \\
\mathrm{P}_{\varnothing}\left(V^{\prime}\right)=\operatorname{Wall}_{\varnothing}, & \mathrm{P}_{\{0\}}\left(V^{\prime}\right)=\operatorname{Wall}_{\{0\}}, & \mathrm{P}_{\{1\}}\left(V^{\prime}\right)=\operatorname{Wall}_{\{1\}}, & \mathrm{P}_{\{0,1\}}\left(V^{\prime}\right)=V .
\end{array}
$$

Thus, the least decomposition partition with regards to $V^{\prime}$ and $W^{\prime}$ is $\{\{0,1\}\}$. The S-boxes $S_{0}^{\prime}$ and $S_{1}^{\prime}$ are then linked together. Choosing $E=\{0\}$ in Proposition 3.54 ensures that $S_{0}^{\prime}$ must be affine. Similarly, we can prove that $S_{1}^{\prime}$ must also be affine by considering $E=\{1\}$. As a result, any substitution layer $\sigma^{\prime}$ mapping $\mathcal{L}\left(V^{\prime}\right)$ to $\mathcal{L}\left(W^{\prime}\right)$ is necessary affine. These subspaces are thus completely prohibited as the whole cipher is then affine.

The rest of this section is devoted to the proof of Proposition 3.54.

Lemma 3.56. Let $E$ be a subset of $\llbracket 0, m \llbracket$. Suppose that $V_{E}=V_{E^{c}}=\left\{0_{n m}\right\}$ and $\mathrm{P}_{E}(V)=$ Wall $_{E}$. Then $W_{E}=W_{E^{c}}=\left\{0_{n m}\right\}$ and $\mathrm{T}_{E}(V)=\mathrm{T}_{E}(W)=\left(\mathbb{F}_{2}^{n}\right)^{p}$ with $p=\# E$.

Proof. Recall that $\sigma$ maps $\mathcal{L}\left(V_{E}\right)$ to $\mathcal{L}\left(W_{E}\right)$. Then, Proposition 3.21 states that $V_{E}$ and $W_{E}$ are isomorphic, so $W_{E}=\left\{0_{n m}\right\}$. By a similar argument, we obtain the equality $W_{E^{c}}=\left\{0_{n m}\right\}$. Now, it is easy to see that $\mathrm{T}_{E}=\mathrm{T}_{E} \circ \mathrm{P}_{E}$. Hence, $\mathrm{T}_{E}(V)=\mathrm{T}_{E}\left(\mathrm{P}_{E}(V)\right)=\mathrm{T}_{E}\left(\mathrm{Wall}_{E}\right)=\left(\mathbb{F}_{2}^{n}\right)^{p}$ where $p$ denotes $\# E$. By Proposition 3.31, $\sigma_{E}$ maps $\mathcal{L}\left(\mathrm{T}_{E}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{E}(W)\right)$. It follows that $\mathrm{T}_{E}(V)$ and $\mathrm{T}_{E}(W)$ are isomorphic and $\mathrm{T}_{E}(W)$ is also equal to $\left(\mathbb{F}_{2}^{n}\right)^{p}$.

Lemma 3.57. Let $E$ be a subset of $\llbracket 0, m \llbracket$. Then $\# V=\# \mathrm{~T}_{E}(V) \times \# V_{E^{c}}$.

Proof. Let $p$ denote $\# E$. Consider the restriction of the linear mapping $\mathrm{T}_{E}$ to $V$. Its kernel is

$$
\operatorname{Ker}\left(\mathrm{T}_{E}\right)=\left\{v \in V \mid \mathrm{T}_{E}(v)=0_{n p}\right\}=\left\{v \in V \mid \forall i \in E, v_{i}=0_{n}\right\}=V_{E^{c}} .
$$

From the first isomorphism theorem, the quotient space $V / V_{E^{c}}$ is isomorphic to the image $\mathrm{T}_{E}(V)$. Particularly, the equality $\# V / \# V_{E^{c}}=\# \mathrm{~T}_{E}(V)$ holds.

Lemma 3.58. Let $E=\llbracket 0, p \llbracket$ with $0 \leq p<m$. Suppose that $V_{E}=V_{E^{c}}=\left\{0_{n m}\right\}$ and $\mathrm{T}_{E}(V)=\left(\mathbb{F}_{2}^{n}\right)^{p}$. There exist two isomorphisms $\varphi: \mathrm{T}_{E}(V) \rightarrow \mathrm{T}_{E^{c}}(V)$ and $\psi: \mathrm{T}_{E}(W) \rightarrow \mathrm{T}_{E^{c}}(W)$ such that

$$
V=\left\{[y \| \varphi(y)] \mid y \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\} \quad \text { and } \quad W=\left\{[z \| \psi(z)] \mid z \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\} .
$$

Proof. Lemma 3.57 ensures that $\# V=\# \mathrm{~T}_{E}(V) \times \# V_{E^{c}}$. By hypothesis, $V_{E^{c}}=\left\{0_{n m}\right\}$, so $\# V_{E^{c}}=1$. It follows that $\# V=\# \mathrm{~T}_{E}(V)$. Therefore, $V$ and $\mathrm{T}_{E}(V)$ have the same dimension $d$. Let $\mathcal{B}=\left(b^{[i]}\right)_{0 \leq i<d}$ be a basis of $\mathrm{T}_{E}(V)$. By definition, there exists a family $\left(c^{[i]}\right)_{0 \leq i<d}$ of vectors in $V$ such that $\mathrm{T}_{E}\left(c^{[i]}\right)=b^{[i]}$. That is, $c^{[i]}=\left[b^{[i]} \| \mathrm{T}_{E^{c}}\left(c^{[i]}\right)\right]$. Note that the vectors $c^{[0]}, \ldots, c^{[d-1]}$ are linearly independent as the $b^{[i]}$ are, and thus $\left(c^{[i]}\right)_{0 \leq i<d}$ is a basis of $V$. Define the linear mapping $\varphi: \mathrm{T}_{E}(V) \rightarrow \mathrm{T}_{E^{c}}(V)$ by the equalities $\varphi\left(b^{[i]}\right)=\mathrm{T}_{E^{c}}\left(c^{[i]}\right)$ for every $0 \leq i<d$. Let $v$ be an element of $V$. Since $\left(c^{[i]}\right)_{0 \leq i<d}$ is a basis of $V$, the vector $v$ can be written as $v=\sum_{i=0}^{d-1} \lambda_{i} c^{[i]}$ where the $\lambda_{i}$ are elements of $\mathbb{F}_{2}$. Next,

$$
\begin{aligned}
v & =\sum_{i=0}^{d-1} \lambda_{i} c^{[i]}=\sum_{i=0}^{d-1} \lambda_{i}\left[b^{[i]} \| \mathrm{T}_{E^{c}}\left(c^{[i]}\right)\right]=\sum_{i=0}^{d-1} \lambda_{i}\left[b^{[i]} \| \varphi\left(b^{[i]}\right)\right] \\
& =\left[\sum_{i=0}^{d-1} \lambda_{i} b^{[i]} \| \sum_{i=0}^{d-1} \lambda_{i} \varphi\left(b^{[i]}\right)\right]=\left[\sum_{i=0}^{d-1} \lambda_{i} b^{[i]} \| \varphi\left(\sum_{i=0}^{d-1} \lambda_{i} b^{[i]}\right)\right]=[y \| \varphi(y)]
\end{aligned}
$$

where $y$ denotes the element $\sum_{i=0}^{d-1} \lambda_{i} b^{[i]}$ of $\mathrm{T}_{E}(V)$. Consequently, every element of $V$ can be written in the desired form. As the converse inclusion is clear from the definition of $\varphi$, the equality $V=\left\{[y \| \varphi(y)] \mid y \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\}$ follows. Hence, the mapping $\varphi$ is onto. Applying Lemma 3.57 with the subset $E^{c}$ gives $\# V=\# \mathrm{~T}_{E^{c}}(V) \times \# V_{E}=$ $\# \mathrm{~T}_{E^{c}}(V)$, and thus $\mathrm{T}_{E^{c}}(V)$ is also a $d$-dimensional subspace. Therefore, $\varphi$ is an isomorphism. Because of Lemma 3.56, our assumptions about $V$ also hold for $W$. Thus, the same argument yields an isomorphism $\psi: \mathrm{T}_{E}(W) \rightarrow \mathrm{T}_{E^{c}}(W)$ satisfying $W=\left\{[z \| \psi(z)] \mid z \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\}$.

Lemma 3.59. Let $p$ be a non-negative integer and let $f:\left(\mathbb{F}_{2}^{n}\right)^{p} \rightarrow\left(\mathbb{F}_{2}^{n}\right)^{p}$. Suppose that there exists a mapping $g:\left(\mathbb{F}_{2}^{n}\right)^{p} \rightarrow\left(\mathbb{F}_{2}^{n}\right)^{p}$ satisfying $f(x+y)=f(x)+g(y)$ for all $x$ and $y$ in $\left(\mathbb{F}_{2}^{n}\right)^{p}$. Then $f$ is an affine mapping.

Proof. Let $y$ be an element of $\left(\mathbb{F}_{2}^{n}\right)^{p}$. Choosing $x=0_{n p}$ yields $f\left(0_{n p}+y\right)=f\left(0_{n p}\right)+g(y)$, and thus $g(y)=f(y)+f\left(0_{n p}\right)$. Therefore, the equalities

$$
\begin{aligned}
f(x+y)+f\left(0_{n p}\right) & =f(x)+g(y)+f\left(0_{n p}\right)=f(x)+\left(f(y)+f\left(0_{n p}\right)\right)+f\left(0_{n p}\right) \\
& =\left(f(x)+f\left(0_{n p}\right)\right)+\left(f(y)+f\left(0_{n p}\right)\right)
\end{aligned}
$$

## Chapter 3 - Partition-Based Backdoor Ciphers

hold for all $x$ and $y$ in $\left(\mathbb{F}_{2}^{n}\right)^{p}$. This proves that the mapping $x \mapsto f(x)+f\left(0_{n p}\right)$ is linear. The result follows.

Lemma 3.60. Let $I$ be a part of a decomposition partition and let $E$ be a subset of $I$. The following equalities hold:

$$
\mathrm{P}_{E}\left(\mathrm{~T}_{I}(V)\right)=\mathrm{T}_{I}\left(\mathrm{P}_{E}(V)\right) \quad \text { and } \quad\left(\mathrm{T}_{I}(V)\right)_{E}=\mathrm{T}_{I}\left(V_{E}\right) .
$$

Remark 3.61. The statement of the lemma above is an abuse of notation. The domain of the projection $\mathrm{P}_{E}$ on the left side of the first equality is $\left(\mathbb{F}_{2}^{n}\right)^{I}$ whereas the domain of $\mathrm{P}_{E}$ on the other side is $\left(\mathbb{F}_{2}^{n}\right)^{m}$. Similarly, $\left(\mathrm{T}_{I}(V)\right)_{E}$ denotes the set $\mathrm{T}_{I}(V) \cap \operatorname{Wall}_{E}^{I}$ where $\operatorname{Wall}_{E}^{I}=\left\{x \in\left(\mathbb{F}_{2}^{n}\right)^{I} \mid \forall i \in I \backslash E, x_{i}=0_{n}\right\}$ is the wall associated with $E$ in $\left(\mathbb{F}_{2}^{n}\right)^{I}$.

Proof. Let $x$ be an element of $\left(\mathbb{F}_{2}^{n}\right)^{m}$. We have

$$
\mathrm{T}_{I}\left(\mathrm{P}_{E}(x)\right)=\mathrm{T}_{I}\left(\left(\delta_{i \in E} \cdot x_{i}\right)_{i<m}\right)=\left(\delta_{i \in E} \cdot x_{i}\right)_{i \in I}=\mathrm{P}_{E}\left(\left(x_{i}\right)_{i \in I}\right)=\mathrm{P}_{E}\left(\mathrm{~T}_{I}(x)\right) .
$$

Thus, $\mathrm{T}_{I} \circ \mathrm{P}_{E}=\mathrm{P}_{E} \circ \mathrm{~T}_{I}$ and the first equality follows.
Observe that Wall $_{E} \subseteq$ Wall $_{I}$ because $E \subseteq I$. Thus, Wall $_{I} \cap \operatorname{Wall}_{E}=$ Wall $_{E}$. Since $I$ is a part of a decomposition partition, Lemma 3.40 implies that $\mathrm{P}_{I}(V)=V_{I}$. Hence, we have

$$
\begin{aligned}
V_{E} & =V \cap \operatorname{Wall}_{E}=V \cap\left(\operatorname{Wall}_{I} \cap \operatorname{Wall}_{E}\right)=\left(V \cap \operatorname{Wall}_{I}\right) \cap \operatorname{Wall}_{E}=V_{I} \cap \operatorname{Wall}_{E} \\
& =\mathrm{P}_{I}(V) \cap \operatorname{Wall}_{E} .
\end{aligned}
$$

Note that $\mathrm{P}_{I}(V)$ and $\mathrm{Wall}_{E}$ are two subsets of $\mathrm{Wall}_{I}$. In addition, the restriction of $\mathrm{T}_{I}$ to $\mathrm{Wall}_{I}$ is clearly one-to-one. Therefore,

$$
\mathrm{T}_{I}\left(V_{E}\right)=\mathrm{T}_{I}\left(\mathrm{P}_{I}(V) \cap \operatorname{Wall}_{E}\right)=\mathrm{T}_{I}\left(\mathrm{P}_{I}(V)\right) \cap \mathrm{T}_{I}\left(\operatorname{Wall}_{E}\right)=\mathrm{T}_{I}(V) \cap \operatorname{Wall}_{E}^{I}=\mathrm{T}_{I}(V)_{E},
$$

The result is proven.
We have now all the tools needed to prove Proposition 3.54. For convenience, we recall its statement.

Let $\mathcal{I}$ be a decomposition partition. Let $I$ be a part of $\mathcal{I}$ such that $\# I \geq 2$ and let $E$ be a non-empty proper subset of $I$. Suppose that $V_{E}=V_{I \backslash E}=\left\{0_{n m}\right\}$ and $\mathrm{P}_{E}(V)=$ Wall $_{E}$. Then, for all $i$ in $E, S_{i}$ is an affine mapping.

Proof (of Proposition 3.54). Denote $m^{\prime}$ the cardinality of $I$. Define $\sigma^{\prime}=\sigma_{I}$, $V^{\prime}=\mathrm{T}_{I}(V)$ and $W^{\prime}=\mathrm{T}_{I}(W)$. Proposition 3.31 establishes that $\sigma^{\prime}$ maps $\mathcal{L}\left(V^{\prime}\right)$ to $\mathcal{L}\left(W^{\prime}\right)$. Then, Lemma 3.60 states that

$$
V_{E}^{\prime}=\left(\mathrm{T}_{I}(V)\right)_{E}=\mathrm{T}_{I}\left(V_{E}\right)=\mathrm{T}_{I}\left(\left\{0_{n m}\right\}\right)=\left\{0_{n m^{\prime}}\right\} .
$$

Similarly, $V_{I \backslash E}^{\prime}=\left\{0_{n m^{\prime}}\right\}$ and $\mathrm{P}_{E}\left(V^{\prime}\right)=$ Wall $_{E}$. Consequently, we can assume without loss of generality that $\mathcal{I}=\{\llbracket 0, m \llbracket\}$ and $I=\llbracket 0, m \llbracket$.

Even if it means to change the order of the S-boxes and the bundles of the spaces $V$ and $W$, we can assume that $E=\llbracket 0, p \llbracket$ with $0<p<m$, and hence $E^{c}=\llbracket p, m \llbracket$.

Thus, every element $x$ of $\mathbb{F}_{2}^{n m}$ can be written as $\left[\mathrm{T}_{E}(x) \| \mathrm{T}_{E^{c}}(x)\right]$. Define $q=m-p$. Firstly, note that $\mathrm{T}_{E}(V)=\mathrm{T}_{E}(W)=\left(\mathbb{F}_{2}^{n}\right)^{p}$ by Lemma 3.56. According to Lemma 3.58, there exist two isomorphisms $\varphi: \mathrm{T}_{E}(V) \rightarrow \mathrm{T}_{E^{c}}(V)$ and $\psi: \mathrm{T}_{E}(W) \rightarrow \mathrm{T}_{E^{c}}(W)$ such that

$$
V=\left\{[y \| \varphi(y)] \mid y \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\} \quad \text { and } \quad W=\left\{[z \| \psi(z)] \mid z \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\} .
$$

Let $g$ be the permutation of $\left(\mathbb{F}_{2}^{n}\right)^{p}$ defined by the formula

$$
g(y)=\psi^{-1}\left(\sigma_{E^{c}}(\varphi(y))+\sigma_{E^{c}}\left(0_{n q}\right)\right) .
$$

Before going any further, we should explain why $g$ is well-defined. Let $y$ be an element of $\left(\mathbb{F}_{2}^{n}\right)^{p}=\mathrm{T}_{E}(V)$. First, $\varphi(y)$ belongs to $\mathrm{T}_{E^{c}}(V)$. By Proposition 3.31, $\sigma_{E^{c}}$ maps $\mathcal{L}\left(\mathrm{T}_{E^{c}}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{E^{c}}(W)\right)$. Then, the part $\mathrm{T}_{E^{c}}(V)$ is mapped to $\sigma_{E^{c}}\left(0_{n q}\right)+\mathrm{T}_{E^{c}}(W)$ according to Lemma 3.18. Therefore, $\sigma_{E^{c}}(\varphi(y))+\sigma_{E^{c}}\left(0_{n q}\right)$ lies in $\mathrm{T}_{E^{c}}(W)$, and thus $\psi^{-1}$ brings it back to $\mathrm{T}_{E}(W)=\left(\mathbb{F}_{2}^{n}\right)^{p}$.

Let $x$ be an element of $\left(\mathbb{F}_{2}^{n}\right)^{p}$. From Lemma 3.18, we have the following:

$$
\sigma\left(\left[x \| 0_{n q}\right]+V\right)=\sigma\left(\left[x \| 0_{n q}\right]\right)+W
$$

On one hand,

$$
\begin{aligned}
\sigma\left(\left[x \| 0_{n q}\right]+V\right) & =\sigma\left(\left\{\left[x \| 0_{n q}\right]+[y \| \varphi(y)] \mid y \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\}\right) \\
& =\sigma\left(\left\{[x+y \| \varphi(y)] \mid y \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\}\right) \\
& =\left\{\left[\sigma_{E}(x+y) \| \sigma_{E^{c}}(\varphi(y))\right] \mid y \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\} .
\end{aligned}
$$

On the other hand,

$$
\begin{aligned}
\sigma\left(\left[x \| 0_{n q}\right]\right)+W & =\left\{\sigma\left(\left[x \| 0_{n q}\right]\right)+[z \| \psi(z)] \mid z \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\} \\
& \left.=\left\{\left[\sigma_{E}(x) \| \sigma_{E^{c}}\left(0_{n q}\right)\right]\right)+[z \| \psi(z)] \mid z \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\} \\
& =\left\{\left[\sigma_{E}(x)+z \| \sigma_{E^{c}}\left(0_{n q}\right)+\psi(z)\right] \mid z \in\left(\mathbb{F}_{2}^{n}\right)^{p}\right\} .
\end{aligned}
$$

Let $y$ be an element of $\left(\mathbb{F}_{2}^{n}\right)^{p}$. Since $\left[\sigma_{E}(x+y) \| \sigma_{E^{c}}(\varphi(y))\right]$ belongs to the part $\sigma\left(\left[x \| 0_{n q}\right]\right)+W$, there exists $z$ in $\left(\mathbb{F}_{2}^{n}\right)^{p}$ satisfying the following two equations:

$$
\left\{\begin{align*}
\sigma_{E}(x+y) & =\sigma_{E}(x)+z  \tag{3.3}\\
\sigma_{E^{c}}(\varphi(y)) & =\sigma_{E^{c}}\left(0_{n q}\right)+\psi(z)
\end{align*}\right.
$$

The bottom equation can be restated as $z=g(y)$. Combining with the top equation, we see that

$$
\sigma_{E}(x+y)=\sigma_{E}(x)+g(y) .
$$

Since this equality holds for all $x$ and $y$ in $\left(\mathbb{F}_{2}^{n}\right)^{p}$, Lemma 3.59 states that the truncated substitution layer $\sigma_{E}$ is an affine mapping.

Now, it remains to prove that all the S-boxes involved in $\sigma_{E}$ are affine mappings. Let $i$ be an element of $E$. The mapping $I_{i}: \mathbb{F}_{2}^{n} \rightarrow\left(\mathbb{F}_{2}^{n}\right)^{m}, x \mapsto\left(\delta_{i, 0} x, \ldots, \delta_{i, m-1} x\right)$ is clearly linear (where $\delta_{i, j}=1$ if $i=j$ and 0 otherwise). Observe that $S_{i}=\sigma_{\{i\}}=\mathrm{T}_{\{i\}} \sigma_{E} I_{i}$. Therefore, the S-box $S_{i}$ is the composition of several affine (or linear) mappings, and hence, is itself an affine mapping.

## Chapter 3 - Partition-Based Backdoor Ciphers

### 3.3.5. Reduction to one S-Box

To prove our main result about the substitution layer, we need the following two preliminary lemmas.
Lemma 3.62. Let $I$ be an element of $\mathcal{I}_{\text {ld }}$. Let $E$ be a non-empty proper subset of $I$. Then $V_{E} \mp \mathrm{P}_{E}(V)$ and $\mathrm{P}_{E}(V) \neq\left\{0_{n m}\right\}$.
Proof. By construction, $V_{E}$ is a subset of $\mathrm{P}_{E}(V)$. Let us prove that $V_{E} \neq \mathrm{P}_{E}(V)$. By contradiction, suppose that $V_{E}=\mathrm{P}_{E}(V)$. Let $v$ be an element of $V$. By hypothesis, $\mathrm{P}_{E}(v)$ belongs to $V_{E}$. Especially, $\mathrm{P}_{E}(v)$ lies in $V$, so $v+\mathrm{P}_{E}(v)$ also lies in $V$. Since $v+\mathrm{P}_{E}(v)=\mathrm{P}_{E^{c}}(v)$, we deduce that $\mathrm{P}_{E^{c}}(v)$ belongs to $V_{E^{c}}$. Let $\mathcal{J}$ denotes the partition $\left\{E, E^{c}\right\}$. Lemma 3.40 states that $V=\oplus_{J \in \mathcal{J}} V_{J}$. Then, $V=\oplus_{K \in \mathcal{I}_{\mathrm{ld}} \cap \mathcal{J}} V_{K}$ follows from Lemma 3.49. Observe that the partition $\mathcal{I}_{\text {ld }} \cap \mathcal{J}$ is strictly finer than $\mathcal{I}_{\text {ld }}$ because $E$ is a proper subset of $I$. This is a contradiction, and therefore $V_{E} \mp \mathrm{P}_{E}(V)$.

By contradiction, suppose that $\mathrm{P}_{E}(V)=\left\{0_{n m}\right\}$. From the previous result, we obtain $\left\{0_{n m}\right\} \subseteq V_{E} \mp \mathrm{P}_{E}(V)=\left\{0_{n m}\right\}$, which is a contradiction. As a consequence, $\mathrm{P}_{E}(V) \neq\left\{0_{n m}\right\}$.

Lemma 3.63. Let $I$ be a part of $\mathcal{I}_{\text {ld }}$ and $E$ be a non-empty proper subset of $I$.

- If $V_{E}$ is a wall, then $V_{E}=\mathrm{Wall}_{\varnothing}=\left\{0_{n m}\right\}$.
- If $\mathrm{P}_{E}(V)$ is a wall, then $\mathrm{P}_{E}(V)=\operatorname{Wall}_{E}$.

Proof. By contradiction, suppose that $V_{E}$ is any wall different from $\left\{0_{n m}\right\}$. Hence, there exists a non-empty subset $F$ of $E$ such that $V_{E}=$ Wall $_{F}$. Therefore Wall ${ }_{F} \subseteq V$ and so $\operatorname{Wall}_{F}=\operatorname{Wall}_{F} \cap V=V_{F}$. Next, $\operatorname{Wall}_{F}=V_{F} \subseteq \mathrm{P}_{F}(V) \subseteq \operatorname{Wall}_{F}$, and thus $V_{F}=\mathrm{P}_{F}(V)$. Since $F$ is a non-empty proper subset of $I$, we have a contradiction with Lemma 3.62. Consequently, $V_{E}=\left\{0_{n m}\right\}$.

By contradiction, suppose that $\mathrm{P}_{E}(V)$ is any wall different from Wall ${ }_{E}$. There exists a proper subset $F$ of $E$ such that $\mathrm{P}_{E}(V)=$ Wall $_{F}$. Thus, for every $v$ in $V$ and every $i$ in $E \backslash F, \mathrm{P}_{E}(v)_{i}=0_{n}$. As a consequence, $\mathrm{P}_{E \backslash F}(V)=\left\{0_{n m}\right\}$. This is a contradiction with Lemma 3.62 because $E \backslash F$ is a non-empty proper subset of $I$. The result follows.

Now we have all the results needed, let us state and prove the main result of Section 3.3 which is depicted in Figure 3.13.

Theorem 3.64. Let $n \geq 2$ and $m$ be two positive integers. Let $S_{0}, \ldots, S_{m-1}$ be $n$-bit S-boxes. Define the permutation $\sigma$ of $\left(\mathbb{F}_{2}^{n}\right)^{m}$ which maps the element $\left(x_{i}\right)_{0 \leq i<m}$ to $\left(S_{i}\left(x_{i}\right)\right)_{0 \leq i<m}$. Let $V$ and $W$ be two subspaces of $\left(\mathbb{F}_{2}^{n}\right)^{m}$ such that $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Suppose that $V$ is not a wall. Then, at least one of the S -boxes maps a non-trivial linear partition to another one.

Proof. Let us prove this result by complete induction on the number $m$ of S-boxes. Suppose that $m=1$. In this case, $\sigma=S_{0}$. By hypothesis, $V$ is different from $\left\{0_{n}\right\}$ and $\mathbb{F}_{2}^{n}$. Hence, $\mathcal{L}(V)$ is a non-trivial partition and $S_{0}$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$.

Let $m \geq 2$ be an integer. Suppose that the result holds for any positive integer strictly less than $m$. Firstly, suppose that all the S-boxes are independent. In

Theorem 3.64


Figure 3.13: Diagrammatic representation of Theorem 3.64.
other words, $\mathcal{I}_{\text {ld }}=\{\{i\} \mid i \in \llbracket 0, m \llbracket\}$. If each S -box is inactive, then $V$ is a wall, a contradiction with our hypothesis. Thus, there exists at least one active S-box $S_{i}$. In this case, $\left\{0_{n m}\right\} \mp V_{\{i\}} \mp$ Wall $_{\{i\}}$. According to Lemma 3.40, the equality $\mathrm{P}_{\{i\}}(V)=V_{\{i\}}$ holds. Then, $\mathrm{T}_{\{i\}}\left(V_{\{i\}}\right)=\mathrm{T}_{\{i\}}\left(\mathrm{P}_{\{i\}}(V)\right)=\mathrm{T}_{\{i\}}(V)$ is a non-trivial subspace of $\mathbb{F}_{2}^{n}$, so $\mathcal{L}\left(\mathrm{T}_{\{i\}}(V)\right)$ is also non-trivial. Finally, Proposition 3.31 states that $S_{i}$ maps $\mathcal{L}\left(\mathrm{T}_{\{i\}}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{\{i\}}(W)\right)$, and thus the result holds in this case.

Now, suppose that some S-boxes are linked together. Then, there exists an element $I$ of $\mathcal{I}_{\text {ld }}$ such that $\# I \geq 2$. Next, at least one of the following three cases holds.

1. Suppose that there exists a non-empty proper subset $E$ of $I$ such that $\mathrm{P}_{E}(V)$ is not a wall. Let $p$ denote the cardinality of $E$. Recall that $\mathrm{T}_{E}\left(\mathrm{P}_{E}(V)\right)=\mathrm{T}_{E}(V)$. It follows that $\mathrm{T}_{E}(V)$ is not a wall of $\left(\mathbb{F}_{2}^{n}\right)^{p}$. According to Proposition 3.31, $\sigma_{E}$ maps $\mathcal{L}\left(\mathrm{T}_{E}(V)\right)$ to $\mathcal{L}\left(\mathrm{T}_{E}(W)\right)$. Note that $E$ is a non-empty proper subset of $I$, so of $\llbracket 0, m \llbracket$. Hence $p<m$, so the induction hypothesis ensures that at least one of the S-boxes of $\sigma_{E}$ maps a non-trivial partition to another one.
2. Suppose that there exists a non-empty proper subset $E$ of $I$ such that $V_{E}$ is not a wall. Recall that $\sigma$ maps $\mathcal{L}\left(V_{E}\right)$ to $\mathcal{L}\left(W_{E}\right)$. Proposition 3.31 ensures that $\sigma_{E}$ maps $\mathcal{L}\left(\mathrm{T}_{E}\left(V_{E}\right)\right)$ to $\mathcal{L}\left(\mathrm{T}_{E}\left(W_{E}\right)\right)$. It is easily seen that $\mathrm{T}_{E}\left(V_{E}\right)$ is not a wall. As before, the result is a consequence of the induction hypothesis.
3. Suppose that there exists a non-empty proper subset $E$ of $I$ such that $\mathrm{P}_{E}(V)$, $V_{E}$ and $V_{I \backslash E}$ are all walls. Then, Lemma 3.63 implies that $\mathrm{P}_{E}(V)=\mathrm{Wall}_{E}$ and $V_{E}=V_{I \backslash E}=\left\{0_{n m}\right\}$. According to Proposition 3.54, the S-boxes whose indices belong to $E$ are affine mappings. Combining Proposition 3.25 and 3.23 , we see that these S-boxes map any non-trivial linear partition to another one.

In any case, the result holds for this integer $m$. The result follows by induction.
Example 3.65. It is worthwhile to note that the proof of Theorem 3.64 is constructive. Therefore, it gives a method to find necessary conditions on the S-boxes for the substitution layer to map $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Let us apply this method to our main example.

The first step is equivalent to what had been done in Examples 3.47 and 3.53. Consider the least decomposition partition $\mathcal{I}_{\text {ld }}=\{\{1\},\{2\},\{0,3\}\}$ and deduce that:

## Chapter 3 - Partition-Based Backdoor Ciphers

- $S_{1}$ is inactive;
- $S_{2}$ is active and maps $\mathcal{L}(\operatorname{span}(07,1 \mathrm{~A}))$ to $\mathcal{L}(\operatorname{span}(0 \mathrm{E}, 12))$ (see Figure 3.3);
- $S_{0}$ and $S_{3}$ are linked together.

Now, consider the part $I=\{0,3\}$ of $\mathcal{I}_{\text {ld }}$. Thus, the non-empty proper subsets of $I$ are $\{0\}$ and $\{3\}$. The first case requires to compute the following projections:

$$
\mathrm{P}_{\{0\}}(V)=\operatorname{Wall}_{\{0\}} \quad \text { and } \quad \mathrm{P}_{\{3\}}(V)=\operatorname{span}((00,00,00,0 \mathrm{~B}),(00,00,00,1 \mathrm{C})) .
$$

Thus, $\mathrm{P}_{\{3\}}(V)$ is not a wall. As in Example 3.33 and Figure 3.9, we see that $S_{3}$ maps $\mathcal{L}(0 \mathrm{~B}, 1 \mathrm{C})$ to $\mathcal{L}(08,15)$ by truncating $\sigma$ and the subspaces $\mathrm{P}_{\{3\}}(V), \mathrm{P}_{\{3\}}(W)$ to $\{3\}$. Now, we need to compute the following subspaces:

$$
V_{\{0\}}=\operatorname{span}((03,00,00,00),(0 \mathrm{D}, 00,00,00),(15,00,00,00)) \quad \text { and } \quad V_{\{3\}}=\operatorname{Wall}_{\varnothing} .
$$

Since $V_{\{0\}}$ is not a wall, the second case applies. Then, truncate the substitution layer $\sigma$ and the subspaces $V_{\{0\}}$ and $W_{\{0\}}$ to prove that $S_{0}$ maps $\mathcal{L}(03,0 \mathrm{D}, 15)$ to $\mathcal{L}(01,0 \mathrm{E}, 14)$. This property was stressed in Example 3.37 and Figure 3.10. Finally, recall that the third case does not apply to these subspaces, as observed in Example 3.55 .

The preceding example covers only the first and the second cases in the treatment of linked S-boxes given by the proof of Theorem 3.64. To illustrate the third case, we introduced the following example.

Example 3.66. Let $n=m=3$. Thus, the substitution layer $\sigma$ is made up of three 3-bit S-boxes denoted by $S_{0}, S_{1}$ and $S_{2}$. Define the subspaces $V$ and $W$ of $\left(\mathbb{F}_{2}^{3}\right)^{3}$ to be

$$
V=W=\left\{(x, y, x+y) \mid x, y \in \mathbb{F}_{2}^{3}\right\}
$$

and assume that the substitution layer $\sigma$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. By definition, it holds that $\mathrm{P}_{\varnothing}(V)=\{(0,0,0)\}$ and $\mathrm{P}_{\{0,1,2\}}(V)=V$. Then, for each non-empty proper subset $E$ of $\{0,1,2\}$, it is easily seen that $\mathrm{P}_{E}(V)=$ Wall $_{E}$. For instance,

$$
\mathrm{P}_{\{0,1\}}(V)=\left\{(x, y, 0) \mid x, y \in \mathbb{F}_{2}^{3}\right\}=\operatorname{Wall}_{\{0,1\}} .
$$

We know that $V_{\varnothing}=\{(0,0,0)\}$ and $V_{\{0,1,2\}}(V)=V$. The other subspaces $V_{E}$ are the following:

$$
\begin{array}{lll}
V_{\{0\}}=\{(0,0,0)\}, & V_{\{1\}}=\{(0,0,0)\}, & V_{\{2\}}=\{(0,0,0)\}, \\
V_{\{0,1\}}=\left\{(x, x, 0) \mid x \in \mathbb{F}_{2}^{3}\right\}, & V_{\{0,2\}}=\left\{(x, 0, x) \mid x \in \mathbb{F}_{2}^{3}\right\}, & V_{\{1,2\}}=\left\{(0, x, x) \mid x \in \mathbb{F}_{2}^{3}\right\} .
\end{array}
$$

Thus, the equality $\mathrm{P}_{E}(V)=V_{E}$ holds only for $E=\varnothing$ and $E=\{0,1,2\}$. Consequently, the least decomposition partition is $\mathcal{I}_{\text {ld }}=\{\{0,1,2\}\}$, and hence all the $S$-boxes are linked together.

From now on, we follow the method given in the proof of Theorem 3.64. As previously noted, for each non-empty proper subset $E$ of $\{0,1,2\}$, the projection $\mathrm{P}_{E}(V)$ is a wall. Therefore, the first case does not apply to this example. We move on to the second case. By induction, the substitution layer and the subspaces $V_{\{0,1\}}$ and
$W_{\{0,1\}}$ are truncated to $\{0,1\}$. Hence, we now consider the permutation $\sigma^{\prime}=\sigma_{\{0,1\}}$ which maps $\mathcal{L}\left(V^{\prime}\right)$ to $\mathcal{L}\left(W^{\prime}\right)$ where

$$
V^{\prime}=W^{\prime}=\mathrm{T}_{\{0,1\}}\left(V_{\{0,1\}}\right)=\left\{(x, x) \mid x \in \mathbb{F}_{2}^{3}\right\}
$$

Such a substitution layer has already been studied in Example 3.55. Recall that

$$
\begin{array}{llll}
V_{\varnothing}^{\prime}=\{(0,0)\}, & V_{\{0\}}^{\prime}=\{(0,0)\}, & V_{\{1\}}^{\prime}=\{(0,0)\}, & V_{\{0,1\}}^{\prime}=V, \\
\mathrm{P}_{\varnothing}\left(V^{\prime}\right)=\operatorname{Wall}_{\varnothing}, & \mathrm{P}_{\{0\}}\left(V^{\prime}\right)=\operatorname{Wall}_{\{0\}}, & \mathrm{P}_{\{1\}}\left(V^{\prime}\right)=\operatorname{Wall}_{\{1\}}, & \mathrm{P}_{\{0,1\}}\left(V^{\prime}\right)=V .
\end{array}
$$

Thus, the least decomposition partition with regards to $V^{\prime}$ and $W^{\prime}$ is $\{\{0,1\}\}$. Since $V_{\{0\}}^{\prime}, V_{\{1\}}^{\prime}, \mathrm{P}_{\{0\}}\left(V^{\prime}\right)$ and $\mathrm{P}_{\{1\}}\left(V^{\prime}\right)$ are all walls, the first and second cases do not apply. Choosing $E=\{0\}$ and $E=\{1\}$ in the third case proves that $S_{0}$ and $S_{1}$ are affine mappings. Come back to the full substitution layer. Similarly, it is straightforward to verify that $S_{2}$ must be affine by truncating $\sigma$ and the subspaces $V_{\{0,2\}}, W_{\{0,2\}}$ to $\{0,2\}$. To summarize, we have proven that any substitution layer mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$ is necessarily affine.

### 3.4. Conclusion

In this chapter, we have studied a generic SPN mapping a partition of the plaintexts to a partition of the ciphertexts, independently of the round keys used. Combining Theorem 3.26 and Corollary 3.27 , we proved that there exist two families $\left(V^{[i]}\right)_{0 \leq i \leq r}$ and $\left(W^{[i]}\right)_{0 \leq i<r}$ of subspaces such that the substitution layer $\sigma$ maps $\mathcal{L}\left(V^{[i]}\right)$ to $\mathcal{L}\left(W^{[i]}\right)$ for each $0 \leq i<r$. This result has been illustrated in Figure 3.6.

First, suppose that all the $V^{[i]}$ are walls. In such a case, the diffusion layer of the cipher is probably not playing its role (or the round number is very small). As it is generally the case, suppose that there is no diffusion layer in the last round of the SPN. Then, the input and the output partitions are both linear partitions associated with walls. This implies that some ciphertext bundles are independent of some plaintext bundles. Such a property must be avoided in any good cipher. To characterize a diffusion layer which does not have this weakness, Calderini introduced the following definition in [23].

Definition 3.67 (Strongly Proper $r$-Round Diffusion Layer). The diffusion layer $\pi$ is said to be strongly proper over rounds if for each proper wall $W$, there exists an integer $1 \leq i<r$ such that $\pi^{i}(W)$ is not a wall.

Assuming that the diffusion layer of the SPN is strongly proper over $r$ rounds, at least one of the $V^{[i]}$ is not a wall. This second case is far more interesting than the previous one. By virtue of Theorem 3.64, at least one of the S-boxes must map a non-trivial linear partition to another one, as illustrated in Figure 3.13.

Thus, we have proven in this chapter that any partition-based backdoor SPN with a strongly proper diffusion layer has at least one S-box mapping a non-trivial linear partition to another one. The following chapter aims at designing such an S-box with the best security against differential and linear cryptanalysis.

Chapter 3 - Partition-Based Backdoor Ciphers

## Analysis of a Backdoor S-Box

In the preceding chapter, we have considered a generic substitution-permutation network together with a partition-based backdoor holding independently of the key schedule. Assuming that its diffusion layer is strongly proper, we have proven that at least one S-box must map a linear partition to another one, thereby reducing the study of the whole cipher to the study of one single S-box.

As said in introduction, differential and linear cryptanalysis are considered as the most important attacks against block ciphers, and therefore any new cipher should be proven secure against these two attacks. Since the S-boxes are the only building-blocks of an SPN which are not affine, they must provide sufficient resistance to make the whole cipher secure. On the other hand, the diffusion layer aims at spreading the confusion provided by the substitution layer through the whole message. But even with a carefully designed diffusion layer, an SPN which has poor S-boxes is unlikely to achieve performance and security. To summarize, if we want our backdoor cipher to be secure against these attacks, then we must design an S-box mapping a linear partition to another one while providing good differential and linear properties. This is the purpose of this chapter.

Firstly, Section 4.1 explains how an S-box mapping a linear partition to another one can be associated with an imprimitive S-box which has the same properties with respect to differential and linear cryptanalysis. Then, we recall a fundamental decomposition result of imprimitive S-boxes. Secondly, Section 4.2 relates the linear and differential properties of an imprimitive S-box to the ones of its decomposition. Following these results, we derive an algorithm to design strong S-boxes mapping a linear partition to another one. Next, a toy partition-based backdoor cipher is given in Section 4.3. This example illustrates the results of the previous and this chapters. Lastly, we discuss ways to prevent partition-based backdoor ciphers in Section 4.4. The content of this chapter was published in the same papers as the previous chapter, that is in [9] and [12].

### 4.1. Structure of a Backdoor S-Box

Optimal differential and linear resistances of vectorial Boolean functions are generally studied by means of equivalence relations preserving their properties. Following

## Chapter 4 - Analysis of a Backdoor S-Box

the terminology introduced in [20], the three widely used equivalence relations are affine-equivalence, EA-equivalence (Extended Affine) and CCZ-equivalence (Carlet-Charpin-Zinoviev [34, Proposition 3]), sorted here from the least to the most general. In our treatment of backdoor S-boxes we will use the simplest, namely the affineequivalence.

Recall that two permutations $S_{1}$ and $S_{2}$ of $\mathbb{F}_{2}^{n}$ are said to be affine-equivalent if there exist two linear mappings $L_{1}, L_{2}$ of $\mathbb{F}_{2}^{n}$ and two elements $v_{1}, v_{2}$ of $\mathbb{F}_{2}^{n}$ such that

$$
\begin{equation*}
\forall x \in \mathbb{F}_{2}^{n}, \quad S_{2}(x)=L_{2}\left(S_{1}\left(L_{1}(x)+v_{1}\right)\right)+v_{2} . \tag{4.1}
\end{equation*}
$$

It is well known that affine-equivalent $S$-boxes have the same security against differential and linear cryptanalysis [80, Proposition 1]. Indeed, assuming that $S_{1}$ and $S_{2}$ are affine-equivalent, it is straightforward to prove that for all $a, b$ in $\mathbb{F}_{2}^{n}$, we have

$$
\begin{align*}
\operatorname{DP}_{S_{2}}(a, b) & =\operatorname{DP}_{S_{1}}\left(L_{1}(a), L_{2}^{-1}(b)\right),  \tag{4.2}\\
\operatorname{LP}_{S_{2}}(a, b) & =\operatorname{LP}_{S_{1}}\left(\left(L_{1}^{-1}\right)^{\top}(a), L_{2}^{\top}(b)\right), \tag{4.3}
\end{align*}
$$

see for instance [27, Proposition 2.16]. The first relation means that their differential probability matrices are equal up to row and column permutations. The second is its analogous for linear potentials. More precisely, their correlation matrices are linked by

$$
\begin{equation*}
\mathrm{C}_{S_{2}}(a, b)=(-1)^{\left\langle a, L_{1}^{-1}\left(v_{1}\right)\right\rangle+\left\langle b, v_{2}\right\rangle} \mathrm{C}_{S_{1}}\left(\left(L_{1}^{-1}\right)^{\top}(a), L_{2}^{\top}(b)\right) . \tag{4.4}
\end{equation*}
$$

Thus, they are equal up to row and column permutations and up to the signs of their coefficients.

Coming back to partition-based backdoor S-boxes, let $V$ and $W$ be two subspaces of $\mathbb{F}_{2}^{n}$ and suppose that $S^{\prime}$ is an $n$-bit S-Box mapping the partition $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Then there exists an automorphism $L$ of $\mathbb{F}_{2}^{n}$ mapping the subspace $V$ to $W$, as ensured by Proposition 3.21. Naturally its inverse $L^{-1}$ maps $W$ to $V$ and Proposition 3.25 states that $L^{-1}$ maps the partition $\mathcal{L}(W)$ to $\mathcal{L}(V)$. Finally, the S-box $S$ defined to be $L^{-1} \circ S^{\prime}$ is by construction affine-equivalent to $S^{\prime}$ and preserves the partition $\mathcal{L}(V)$. This discussion establishes the following Proposition.

Proposition 4.1. Let $V$ and $W$ be two subspaces of $\mathbb{F}_{2}^{n}$ and let $S^{\prime}$ be an $n$-bit S-box mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$. There exists an affine-equivalent S-box $S$ to $S^{\prime}$ preserving $\mathcal{L}(V)$.

Remark 4.2. Conversely, suppose that $S$ preserves the partition $\mathcal{L}(V)$. Let $W$ be any subspace isomorphic to $V$ and denote by $L$ an isomorphism from $V$ to $W$. By Proposition 3.25, the composite $L \circ S$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ and is obviously affine-equivalent to $S$.

Example 4.3. Let us consider the 5-bit S-box $S^{\prime}$ given in Figure 4.1. This S-box has already been met in Examples 3.17 and 3.28 (denoted by $f$ and $S_{2}$ respectively). Thus, we know that $S^{\prime}$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ where

$$
V=\operatorname{span}(07,1 \mathrm{~A}) \quad \text { and } \quad W=\operatorname{span}(0 \mathrm{E}, 12) .
$$

|  |  | . 0 | . 1 | . 2 | . 3 | . 4 | . 5 | . 6 | . 7 | . 8 | . 9 | . A | . B | . C | . D | . E | F |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $S^{\prime}(x)$ | 0. | 1E | 08 | 04 | 13 | OF | 18 | 14 | 10 | 19 | 15 | OE | OD | 03 | 1C | 07 | 17 |
|  | 1. | 12 | 11 | OB | 1B | 09 | 05 | 1F | 00 | OA | 01 | 02 | 1A | 06 | OC | 1D | 16 |
| $L^{-1}(x)$ | 0 | 00 | 01 | 02 | 03 | 08 | 09 | 0A | OB | OD | OC | OF | OE | 05 | 04 | 07 | 06 |
|  | 1. | 18 | 19 | 1 A | 1B | 10 | 11 | 12 | 13 | 15 | 14 | 17 | 16 | 1D | 1C | 1F | 1E |
| $S(x)$ | 0 | 1F | OD | 08 | 1B | 06 | 15 | 10 | 18 | 14 | 11 | 07 | 04 | 03 | 1D | OB | 13 |
|  | 1 | 1A | 19 | OE | 16 | OC | 09 | 1E | 00 | OF | 01 | 02 | 17 | OA | 05 | 1C | 12 |

Figure 4.1: Construction of the S-Box $S$ used throughout Chapter 4.


Figure 4.2: The permutation $S$ preserving $\mathcal{L}(V)$ where $V=\operatorname{span}(07,1 \mathrm{~A})$.
Referring back to Example 3.22, we end up with an automorphism $L$ of $\mathbb{F}_{2}^{5}$ satisfying $L(V)=W$. Its inverse $L^{-1}$ and the composite $S=L^{-1} S^{\prime}$ are given in Figure 4.1. For instance, $S(07)=L^{-1}\left(S^{\prime}(07)\right)=L^{-1}(10)=18$.

By construction, this new permutation $S$ is equivalent to $S^{\prime}$ and preserves the linear partition $\mathcal{L}(V)$, as can be seen in Figure 4.2. The similarity between Figures 3.3 and 4.2 is striking, thereby clarifying the choices we have made when constructing the automorphism $L$ in Example 3.22. This S-box $S$ will be studied throughout this chapter.

As a consequence of Proposition 4.1, it can be assumed without loss of generality that the subspaces $V$ and $W$ are equal when studying the linear and differential properties of an S-box mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Therefore, we consider the following in the remainder of this section:

- let $V$ be a $d$-dimensional non-trivial subspace of $\mathbb{F}_{2}^{n}$,
- let $U$ be a complement space of $V$,
- let $S$ be an $n$-bit $S$-box preserving $\mathcal{L}(V)$.

Since $U$ is a complement subspace of $V$, the space $\mathbb{F}_{2}^{n}$ is equal to the direct sum $U \oplus V$. In other words, every element $x$ of $\mathbb{F}_{2}^{n}$ can be uniquely written as the sum $x=u+v$ where $u$ and $v$ belong to $U$ and $V$ respectively. Let $[u]$ denote the coset of $V$ with respect to $u$. Thus, $[u]=u+V$ is the unique part of $\mathcal{L}(V)$ containing $u$ and we have

$$
\mathcal{L}(V)=\{[u] \mid u \in U\} .
$$

Since $V$ is $d$-dimensional, the complement space $U$ is $(n-d)$-dimensional. In addition, we have the inequalities

$$
1 \leq d \leq n-1 \quad \text { and } \quad 1 \leq n-d \leq n-1
$$

## Chapter 4 - Analysis of a Backdoor S-Box

because $V$ is assumed to be a non-trivial subspace of $\mathbb{F}_{2}^{n}$.
The following theorem describes the structure of permutations preserving a linear partition. A similar result has been introduced by Harpes in his thesis [50, Theorem 5.6]. However, our statement will be more appropriate for the next results of this chapter.

Theorem 4.4 (Decomposition of an Imprimitive S-Box). Let $S$ be an $n$-bit S-box preserving $\mathcal{L}(V)$. There exist a unique permutation $\rho$ of $U$ and a unique family of permutations $\left(\tau_{u}\right)_{u \in U}$ of $V$ such that, for all $x=u+v$ in $\mathbb{F}_{2}^{n}$,

$$
S(u+v)=\rho(u)+\tau_{u}(v) .
$$

Conversely, if $\rho$ is a permutation of $U$ and if $\left(\tau_{u}\right)_{u \in U}$ is a family of permutations of $V$, then the mapping $S^{\prime}$ defined by the rule $S^{\prime}(u+v)=\rho(u)+\tau_{u}(v)$ preserves $\mathcal{L}(V)$.

As will be seen in Section 4.1.3, this theorem is a corollary of Krasner-Kaloujnine embedding theorem [65] (see Theorem 4.13). But for convenience, we give below a direct proof.

Proof. By hypothesis, $S$ preserves $\mathcal{L}(V)$. Thus, $S$ induces a permutation $\rho$ of $U$ defined as follows. Let $u$ be an element of $U$. Hence, there exists a unique $u^{\prime}$ in $U$ such as $S([u])=\left[u^{\prime}\right]$. Define then $\rho(u)=u^{\prime}$. For each element $u$ of $U$, define the permutation $\tau_{u}$ of $V$ which maps $v$ to $S(u+v)+\rho(u)$. By construction, for any $u$ in $U$ and any $v$ in $V$ we have

$$
\tau_{u}(v)=S(u+v)+\rho(u) \quad \text { and hence } \quad S(u+v)=\rho(u)+\tau_{u}(v) .
$$

The existence of the permutations $\rho$ and $\tau_{u}$ is proven. Now, let us show their uniqueness. Suppose that there exist a permutation $\tilde{\rho}$ of $U$ and a family of permutations $\left(\tilde{\tau}_{u}\right)_{u \in U}$ of $V$ satisfying the result. Let $(u, v)$ be an element of $U \times V$. By hypothesis, we have the relation

$$
\rho(u)+\tau_{u}(v)=\tilde{\rho}(u)+\tilde{\tau}_{u}(v) .
$$

Because the sum of $U$ and $V$ is direct, it follows that $\rho(u)=\tilde{\rho}(u)$ and $\tau_{u}(v)=\tilde{\tau}_{u}(v)$. The uniqueness of $\rho$ and the $\tau_{u}$ follows.

Conversely, let $\rho$ be a permutation of $U$ and $\left(\tau_{u}\right)_{u \in U}$ be a family of permutations of $V$. Denote by $S^{\prime}$ the mapping from $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{n}$ defined by the rule $S^{\prime}(u+v)=\rho(u)+\tau_{u}(v)$. Because $\rho$ and the $\tau_{u}$ are permutations of $U$ and $V$ respectively the mapping $S^{\prime}$ is a permutation of $U \oplus V=\mathbb{F}_{2}^{n}$. For every element $u$ of $U$, it holds that

$$
\begin{aligned}
S^{\prime}([u]) & =\left\{S^{\prime}(u+v) \mid v \in V\right\}=\left\{\rho(u)+\tau_{u}(v) \mid v \in V\right\} \\
& =\rho(u)+\left\{\tau_{u}(v) \mid v \in V\right\}=\rho(u)+V=[\rho(u)] .
\end{aligned}
$$

Hence, $S^{\prime}$ preserves the linear partition $\mathcal{L}(V)$, as desired.
This theorem is of great significance as it yields a general construction for imprimitive S-boxes using permutations with smaller domains. Intuitively, this result can be explained as follows. We already know that the linear partition $\mathcal{L}(V)$ consists
of cosets of $V$. By permuting the elements of each coset [ $u$ ], the whole partition is left unchanged. The way we permute the elements of [ $u$ ] is represented by the permutation $\tau_{u}$ of $V$, namely $u+v$ is mapped to $u+\tau_{u}(v)$. Therefore, we need a family $\left(\tau_{u}\right)_{u \in U}$ to represent all these local permutations. Up to this point, each coset is mapped to itself, so it remains to explain how the cosets are permuted. This is the role of the permutation $\rho$ of $U$. Thus the coset [ $u$ ] is mapped as a whole to $[\rho(u)]$, that is to say, each element $u+\tau_{u}(v)$ is mapped to $\rho(u)+\tau_{u}(v)$. To summarize, the family $\left(\tau_{u}\right)_{u \in U}$ describes how the elements are moved inside each part and the permutation $\rho$ tells us how $S$ permutes the parts of the partition $\mathcal{L}(V)$.
Example 4.5. Again, we consider the S-box $S$ introduced in Example 4.3. Define the following complement subspace of $V$ :

$$
U=\operatorname{span}(01,02,08)=\{00,01,02,03,08,09,0 \mathrm{~A}, 0 \mathrm{~B}\} .
$$

Figure 4.2 shows that $S$ induces a permutation $\rho$ of $U$. For instance, $\rho(01)=0 \mathrm{~A}$ because $S$ maps the coset [01] to [0A]. Next, for each $u$ in $U$, define the permutation $\tau_{u}$ of $V$ by the rule $\tau_{u}(v)=S(u+v)+\rho(u)$. For instance,

$$
\tau_{01}(07)=S(01+07)+\rho(01)=S(06)+\rho(01)=10+0 \mathrm{~A}=1 \mathrm{~A} .
$$

This decomposition of $S$ is illustrated in Figure 4.3. For example, the image of 06 under $S$ is computed as follows. First, 06 is uniquely written as the sum $u+v=01+07$ of an element $u$ in $U$ with an element $v$ of $V$. Hence, 06 lies in the coset

$$
[01]=01+V=01+\{00,07,1 \mathrm{~A}, 1 \mathrm{D}\}=\{01,06,1 \mathrm{~B}, 1 \mathrm{C}\} .
$$

The first step consists in moving 06 inside the coset [01], or equivalently modifying its component in $V$. Thus, 06 is mapped to $01+\tau_{01}(07)=01+1 \mathrm{~A}=1 \mathrm{~B}$. The second step permutes the coset representatives in $U$, and hence leaves the elements of same coset in the same relative positions. The element $1 \mathrm{~B}=01+1 \mathrm{~A}$ is then mapped to $\rho(01)+1 \mathrm{~A}=0 \mathrm{~A}+1 \mathrm{~A}=10$. Therefore, the S-box $S$ maps 06 to 10 .

The next three subsections aim at explaining how Theorem 4.4 can be seen as a corollary of Krasner-Kaloujnine embedding theorem. Since this result has already been proven, the reader can jump directly to Section 4.2 for a first reading. Nevertheless, this connection highlights the group structure behind the decomposition of an S-box preserving a linear partition, bringing us back to imprimitive groups.

### 4.1.1. Wreath Product

As direct products for finite-dimensional vector spaces, wreath products naturally arise when studying imprimitive permutation groups. The result justifying this analogy is known as Krasner-Kaloujnine embedding theorem. Informally, it establishes that every imprimitive permutation group can be embedded into a wreath product, namely seen as a subgroup of a wreath product up to isomorphism. Roughly speaking, this result implies that wreath products are the biggest imprimitive groups.

In this section, we recall the definition of wreath products. However, it turns out that there are several ways to define wreath products. Several groups are involved in

Chapter 4 - Analysis of a Backdoor S-Box


Figure 4.3: The permutation $S$ preserving $\mathcal{L}(V)$ where $V=\operatorname{span}(07,1 \mathrm{~A})$.
this structure and each of them can act on the right or on the left. The following choices are made in order to derive Theorem 4.4 from Krasner-Kaloujnine embedding theorem. Because some of them are very unusual, all the results will be proven. To see other classic representations of wreath products, readers may refer to [42, 26, 6, 55]. Wreath products are based on the so-called semidirect products recalled below.

Definition 4.6 (Outer Semidirect Product). Let $N$ and $H$ be two groups and let $\phi$ be a homomorphism from $H$ to $\operatorname{Aut}(N)$. To simplify the reading, let $\star$ denote the group law of $N$ and let $\phi_{h}$ denote the automorphism of $N$ associated with an element $h$ of $H$. The semidirect product of $H$ and $N$, denoted by $H \ltimes_{\phi} N$, is the group formed by the Cartesian product $H \times N$ together with the following binary operation

$$
\left(h_{1}, n_{1}\right) \otimes\left(h_{2}, n_{2}\right)=\left(h_{1} h_{2}, \phi_{h_{2}^{-1}}\left(n_{1}\right) \star n_{2}\right) .
$$

Remark 4.7. As explained in Definition 3.1, an action of a group $G$ on $X$ can be defined to be a homomorphism from $G$ to $\operatorname{Sym}(X)$. The homomorphism $\phi$ is then an action of $H$ on $N$ whose image is included in the subgroup $\operatorname{Aut}(N)$ of $\operatorname{Sym}(N)$. In this case, the group $H$ is said to act by automorphisms on $N$. Finally, it should be noted that when this action is trivial (namely $\phi_{h}=\operatorname{Id}_{N}$ for every $h$ in $H$ ), the semidirect product of $H$ and $N$ is just their direct product.
Proof. First, let us prove that $\left(e_{H}, e_{N}\right)$ is the identity element of $H \ltimes_{\phi} N$. Let $(h, n)$ be an element of $H \times N$. It holds that

$$
\begin{aligned}
& (h, n) \otimes\left(e_{H}, e_{N}\right)=\left(h e_{H}, \phi_{e_{H}^{-1}}(n) \star e_{N}\right)=\left(h, \phi_{e_{H}}(n)\right)=(h, \operatorname{Id}(n))=(h, n), \\
& \left(e_{H}, e_{N}\right) \otimes(h, n)=\left(e_{H} h, \phi_{h^{-1}}\left(e_{N}\right) \star n\right)=\left(h, e_{N} \star n\right)=(h, n) .
\end{aligned}
$$

Thus, $\left(e_{H}, e_{N}\right)$ is the identity element. Now, let us prove that $\left(h^{-1}, \phi_{h}\left(n^{-1}\right)\right)$ is the inverse of $(h, n)$.

$$
\begin{aligned}
(h, n) \otimes\left(h^{-1}, \phi_{h}\left(n^{-1}\right)\right) & =\left(h h^{-1}, \phi_{h}(n) \star \phi_{h}\left(n^{-1}\right)\right)=\left(e_{H}, \phi_{h}\left(n \star n^{-1}\right)\right) \\
& =\left(e_{H}, \phi_{h}\left(e_{N}\right)\right)=\left(e_{H}, e_{N}\right), \\
\left(h^{-1}, \phi_{h}\left(n^{-1}\right)\right) \otimes(h, n) & =\left(h^{-1} h, \phi_{h^{-1}}\left(\phi_{h}\left(n^{-1}\right)\right) \star n\right)=\left(e_{H}, \phi_{h^{-1} h}\left(n^{-1}\right) \star n\right) \\
& =\left(e_{H}, \phi_{e_{H}}\left(n^{-1}\right) \star n\right)=\left(e_{H}, n^{-1} \star n\right)=\left(e_{H}, e_{N}\right) .
\end{aligned}
$$

Finally, it remains to prove that $\otimes$ is associative. Let $\left(h_{1}, n_{1}\right),\left(h_{2}, n_{2}\right)$ and $\left(h_{3}, n_{3}\right)$ be three elements of $H \times N$. We have

$$
\begin{aligned}
\left(h_{1}, n_{1}\right) \otimes\left[\left(h_{2}, n_{2}\right) \otimes\left(h_{3}, n_{3}\right)\right] & =\left(h_{1}, n_{1}\right) \otimes\left(h_{2} h_{3}, \phi_{h_{3}^{-1}}\left(n_{2}\right) \star n_{3}\right) \\
& =\left(h_{1} h_{2} h_{3}, \phi_{\left(h_{2} h_{3}\right)^{-1}}\left(n_{1}\right) \star \phi_{h_{3}^{-1}}\left(n_{2}\right) \star n_{3}\right), \\
{\left[\left(h_{1}, n_{1}\right) \otimes\left(h_{2}, n_{2}\right)\right] \otimes\left(h_{3}, n_{3}\right) } & =\left(h_{1} h_{2}, \phi_{h_{2}^{-1}}\left(n_{1}\right) \star n_{2}\right) \otimes\left(h_{3}, n_{3}\right) \\
& =\left(h_{1} h_{2} h_{3}, \phi_{h_{3}^{-1}}\left(\phi_{h_{2}^{-1}}\left(n_{1}\right) \star n_{2}\right) \star n_{3}\right) .
\end{aligned}
$$

Observe that

$$
\begin{aligned}
\phi_{h_{3}^{-1}}\left(\phi_{h_{2}^{-1}}\left(n_{1}\right) \star n_{2}\right) & =\phi_{h_{3}^{-1}}\left(\phi_{h_{2}^{-1}}\left(n_{1}\right)\right) \star \phi_{h_{3}^{-1}}\left(n_{2}\right)=\phi_{h_{3}^{-1} h_{2}^{-1}}\left(n_{1}\right) \star \phi_{h_{3}^{-1}}\left(n_{2}\right) \\
& =\phi_{\left(h_{2} h_{3}\right)^{-1}}\left(n_{1}\right) \star \phi_{h_{3}^{-1}}\left(n_{2}\right) .
\end{aligned}
$$

## Chapter 4 - Analysis of a Backdoor S-Box

Consequently, the associativity of the binary operation $\otimes$ follows and the desired result is proven.

Proposition 4.8. Let $A$ be a group and let $B$ be a group acting on a set $I$. Define $\phi: B \rightarrow \mathfrak{S}\left(A^{I}\right)$ which maps an element $b$ of $B$ to the permutation

$$
\begin{aligned}
\phi_{b}: A^{I} & \longrightarrow A^{I} \\
\left(a_{i}\right)_{i \in I} & \longmapsto\left(a_{b^{-1} \cdot}\right)_{i \in I} .
\end{aligned}
$$

Then, $\phi$ is a homomorphism whose image is included in $\operatorname{Aut}\left(A^{I}\right)$.
Remark 4.9. Using the vocabulary introduced in Remark 4.7, the group $B$ acts on the direct product $A^{I}$ by automorphisms. This action is quite simple as $B$ only permutes the components of the elements of $A^{I}$ in the natural way. Let $\left(a_{i}\right)_{i \in I}$ be an element of $A^{I}$ and let $\left(a_{i}^{\prime}\right)_{i \in I}=\phi_{b}\left(\left(a_{i}\right)_{i \in I}\right)$ denote its image under the action of a given $b$ in $B$. The component $a_{i}$ is moved to the index $b \cdot i$, and hence $a_{i}=a_{b \cdot i}^{\prime}$ leading to the equality $\left(a_{i}\right)_{i \in I}=\left(a_{b \cdot i}^{\prime}\right)_{i \in I}$. Equivalently, $\left(a_{b^{-1 \cdot i}}\right)_{i \in I}=\left(a_{i}^{\prime}\right)_{i \in I}$, whence $\phi_{b}\left(\left(a_{i}\right)_{i \in I}\right)=\left(a_{b^{-1} \cdot i}\right)_{i \in I}$. This discussion explains the definition of the action $\phi$.
Proof. First, let us prove that $\phi$ is well-defined. Let $b$ be an element of $B$. We need to prove that $\phi_{b}$ is a permutation of $A^{I}$. Let $\left(a_{i}\right)_{i \in I}$ be an element of $A^{I}$. We have

$$
\phi_{b^{-1}} \circ \phi_{b}\left(\left(a_{i}\right)_{i \in I}\right)=\phi_{b^{-1}}\left(\left(a_{b^{-1} \cdot i}\right)_{i \in I}\right)=\left(a_{b^{-1} \cdot(b \cdot i)}\right)_{i \in I}=\left(a_{b^{-1} b \cdot i}\right)_{i \in I}=\left(a_{e_{B} \cdot i}\right)_{i \in I}=\left(a_{i}\right)_{i \in I} .
$$

Similarly, $\phi_{b} \circ \phi_{b^{-1}}=\operatorname{Id}_{A^{I}}$. As a consequence, $\phi_{b}$ is a permutation of $A^{I}$ and $\phi$ is well-defined. Now, let us prove that $\phi$ is a group homomorphism. Let $b_{1}, b_{2}$ be two elements of $B$ and let $\left(a_{i}\right)_{i \in I}$ be an element of $A^{I}$. Next,

$$
\phi_{b_{1}} \circ \phi_{b_{2}}\left(\left(a_{i}\right)_{i \in I}\right)=\phi_{b_{1}}\left(\left(a_{b_{2}^{-1} \cdot i}\right)_{i \in I}\right)=\left(a_{b_{2}^{-1} b_{1}^{-1} \cdot i}\right)_{i \in I}=\left(a_{\left(b_{1} b_{2}\right)^{-1 \cdot i}}\right)_{i \in I}=\phi_{b_{1} b_{2}}\left(\left(a_{i}\right)_{i \in I}\right) .
$$

It follows that $\phi_{b_{1}} \circ \phi_{b_{2}}=\phi_{b_{1} b_{2}}$ proving that $\phi$ is a homomorphism. Let $b$ be an element of $B$. To prove that the image of $\phi$ is included in $\operatorname{Aut}\left(A^{I}\right)$, it suffices to show that $\phi_{b}$ is a homomorphism. For all $\left(a_{i}\right)_{i \in I}$ and $\left(a_{i}^{\prime}\right)_{i \in I}$ in $A^{I}$, it holds that

$$
\begin{aligned}
\phi_{b}\left(\left(a_{i}\right)_{i \in I} \times\left(a_{i}^{\prime}\right)_{i \in I}\right) & =\phi_{b}\left(\left(a_{i} a_{i}^{\prime}\right)_{i \in I}\right)=\left(a_{b^{-1 . i}} a_{b^{-1 \cdot i}}^{\prime}\right)_{i \in I}=\left(a_{b^{-1 \cdot i}}\right)_{i \in I} \times\left(a_{b^{-1 \cdot i}}^{\prime}\right)_{i \in I} \\
& =\phi_{b}\left(\left(a_{i}\right)_{i \in I}\right) \times \phi_{b}\left(\left(a_{i}^{\prime}\right)_{i \in I}\right) .
\end{aligned}
$$

This concludes the proof of our proposition.
Given two groups $A$ and $B$ acting respectively on $X$ and $I$, their wreath product $A \_B$ naturally acts on the product $I \times X$. Intuitively, the set $I \times X$ may be thought as a collection of $\# I$ copies of the set $X$. Similarly, the wreath product $A_{2} B$ contains $\# I$ copies of the group $A$, each acting on its associated copy of $X$. Then, $B$ acts on $I \times X$ by permuting the copies of $X$. The resulting action of $A$ 乙 $B$ on $I \times X$ is thus imprimitive since it preserves these copies.

Definition 4.10 (Wreath Product). Let $A$ be a group and let $B$ be a group acting on a set $I$. The wreath product of $A$ and $B$ denoted by $A z B$, is defined to be the semidirect product $B \ltimes_{\phi} A^{I}$ where $\phi$ is given in Proposition 4.8. Explicitly, the group law of $A$ 々 $B$ is given for all $\left(b,\left(a_{i}\right)_{i \in I}\right)$ and $\left(b^{\prime},\left(a_{i}^{\prime}\right)_{i \in I}\right)$ in $B \times A^{I}$ by

$$
\left(b,\left(a_{i}\right)_{i \in I}\right) \otimes\left(b^{\prime},\left(a_{i}^{\prime}\right)_{i \in I}\right)=\left(b b^{\prime}, \phi_{b^{\prime-1}}\left(\left(a_{i}\right)_{i \in I}\right) \times\left(a_{i}^{\prime}\right)_{i \in I}\right)=\left(b b^{\prime},\left(a_{b^{\prime} \cdot i} a_{i}^{\prime}\right)_{i \in I}\right) .
$$

Proposition 4.11 (Imprimitive Action of $A_{2} B$ ). Let $A$ and $B$ be two groups and suppose that $A$ acts on $X$ and that $B$ acts on $I$. Then, the wreath product $A$ 乙 $B$ acts on $I \times X$ by

$$
\left(b,\left(a_{i}\right)_{i \in I}\right) \cdot(j, x)=\left(b \cdot j, a_{j} \cdot x\right)
$$

for all $\left(b,\left(a_{i}\right)_{i \in I}\right)$ in $B \times A^{I}$ and $(j, x)$ in $I \times X$. Furthermore, let $X_{i}$ denote the set $\{i\} \times X$ for each $i$ in $I$. Then, $A$ 々 $B$ preserves the partition $\left\{X_{i} \mid i \in I\right\}$.

Remark 4.12. In other words, $\mathcal{B}=\left\{X_{i} \mid i \in I\right\}$ is an $(A \imath B)$-invariant partition of $I \times X$. Since this partition is non-trivial (whenever $\# I, \# X \geq 2$ ), the wreath product $A$ \& $B$ acts imprimitively on $I \times X$.

Proof. Let $(j, x)$ be an element of $I \times X$. Observe that

$$
\left(e_{B},\left(e_{A}\right)_{i \in I}\right) \cdot(j, x)=\left(e_{B} \cdot j, e_{A} \cdot x\right)=(j, x) .
$$

Thus, the element $(j, x)$ is fixed under the action of the identity element of $A$ \& $B$. Now, let $\left(b,\left(a_{i}\right)_{i \in I}\right)$ and $\left(b^{\prime},\left(a_{i}^{\prime}\right)_{i \in I}\right)$ be two elements of $A z B$. On the one hand,

$$
\left(b,\left(a_{i}\right)_{i \in I}\right) \cdot\left[\left(b^{\prime},\left(a_{i}^{\prime}\right)_{i \in I}\right) \cdot(j, x)\right]=\left(b,\left(a_{i}\right)_{i \in I}\right) \cdot\left(b^{\prime} \cdot j, a_{j}^{\prime} \cdot x\right)=\left(b b^{\prime} \cdot j, a_{b^{\prime} \cdot j}^{\prime} a_{j}^{\prime} \cdot x\right) .
$$

On the other hand,

$$
\left[\left(b,\left(a_{i}\right)_{i \in I}\right) \cdot\left(b^{\prime},\left(a_{i}^{\prime}\right)_{i \in I}\right)\right] \cdot(j, x)=\left(b b^{\prime},\left(a_{b^{\prime} \cdot i} a_{i}^{\prime}\right)_{i \in I}\right) \cdot(j, x)=\left(b b^{\prime} \cdot j, a_{b^{\prime} \cdot j} a_{j}^{\prime} \cdot x\right)
$$

Therefore, $A$ ¿ $B$ acts on $I \times X$.
It remains to prove that this action preserves the partition $\left\{X_{i} \mid i \in I\right\}$. Let $g=\left(b,\left(a_{i}\right)_{i \in I}\right)$ be an element of $A \_B$ and let $j$ be an element of $I$. We will prove that $g \cdot X_{j}=X_{b \cdot j}$. Let $g \cdot(j, x)$ be an element of $g \cdot X_{j}$. Then $g \cdot(j, x)=\left(b \cdot j, a_{j} \cdot x\right)$ belongs to $X_{b \cdot j}$. Thus, $g \cdot X_{j}$ is included in $X_{b \cdot j}$. Now, let $(b \cdot j, x)$ be an element of $X_{b \cdot j}$. Then $\left(j, a_{j}^{-1} \cdot x\right)$ belongs to $X_{j}$ and

$$
g \cdot\left(j, a_{j}^{-1} \cdot x\right)=\left(b \cdot j, a_{j} a_{j}^{-1} \cdot x\right)=(b \cdot j, x) .
$$

Thus, $(b \cdot j, x)$ lies in $g \cdot X_{j}$. Therefore, $g \cdot X_{j}=X_{b \cdot j}$. The desired result follows from Lemma 3.14.

### 4.1.2. Krasner-Kaloujnine Embedding Theorem

It is now time to state Krasner-Kaloujnine embedding theorem which relates every imprimitive group action to the imprimitive action of a wreath product.

## Chapter 4 - Analysis of a Backdoor S-Box

Theorem 4.13 (Krasner, Kaloujnine 65). Let $G$ be an imprimitive permutation group on a set $E$ and let $\mathcal{P}$ be a $G$-invariant partition of $E$. Let $R$ be a system of distinct representatives of $\mathcal{P}$. For each $r$ in $R$, let $[r]$ denote the unique part of $\mathcal{P}$ containing $r$. Let $r_{0}$ be an element of $R$.

- Let $A$ be the permutation group on $\left[r_{0}\right.$ ] induced by the action of the set-wise stabilizer of $\left[r_{0}\right]$ in $G$.
- Let $B$ be the permutation group on $R$ induced by $G$.

Then $E$ may be identified with $R \times\left[r_{0}\right]$ in a such way that $G$ on $E$ is permutation isomorphic to a subgroup of $A \_B$ acting imprimitively on $R \times\left[r_{0}\right]$.

Proof. For each $r$ in $R$, choose an element $t_{r}$ of $G$ satisfying $t_{r}\left(\left[r_{0}\right]\right)=[r]$. Such elements exist by virtue of Lemma 3.5. Let $\lambda$ be the mapping from $E$ to $R \times\left[r_{0}\right]$ which maps $x$ to $\left(r, t_{r}^{-1}(x)\right)$ where $r$ is the unique element of $R$ such that $x \in[r]$. Finally, let $\varphi$ denote the mapping from $G$ to $A$ 乙 $B$ defined by the formula

$$
\varphi(g)=\left(\bar{g},\left(t_{\bar{g}(r)}^{-1} \circ g \circ t_{r}\right)_{r \in R}\right)
$$

where $\bar{g}: R \rightarrow R$ maps $r$ to the representative of $[g(r)]$ in $R$. We will prove that $(\varphi, \lambda)$ is a permutation isomorphism from $G$ on $E$ to $\varphi(G)$ on $R \times\left[r_{0}\right]$.

Let us begin by showing that $\lambda$ is a bijection. Since $\# E=\# \mathcal{P} \times \# P_{0}$, it is sufficient to prove that $\lambda$ is one-to-one. Let $x$ and $x^{\prime}$ be two elements of $E$ such that $\lambda(x)=\lambda\left(x^{\prime}\right)$. Denote $r$ and $r^{\prime}$ the elements of $R$ satisfying $x \in[r]$ and $x^{\prime} \in\left[r^{\prime}\right]$. Hence, the equality $\lambda(x)=\lambda\left(x^{\prime}\right)$ becomes $\left(r, t_{r}^{-1}(x)\right)=\left(r^{\prime}, t_{r^{\prime}}^{-1}(x)\right)$. This implies that $t_{r}^{-1}(x)=t_{r}^{-1}\left(x^{\prime}\right)$ and finally that $x=x^{\prime}$ as $t_{r}^{-1}$ is a permutation of $E$.

Now, we will prove that $\varphi$ is a one-to-one homomorphism. Let $g_{1}$ and $g_{2}$ be two elements of $G$. It holds that

$$
\begin{aligned}
\varphi\left(g_{1}\right) \otimes \varphi\left(g_{2}\right) & =\left(\overline{g_{1}},\left(t_{\overline{g_{1}}(r)}^{-1} g_{1} t_{r}\right)_{r \in R}\right) \oplus\left(\overline{g_{2}},\left(t_{\overline{g_{2}}(r)}^{-1} g_{2} t_{r}\right)_{r \in R}\right) \\
& =\left(\overline{g_{1}} \overline{g_{2}},\left(t_{\overline{\bar{q}_{1}}\left(\overline{g_{2}}(r)\right)}^{-1} g_{1} t_{\overline{g_{2}(r)}} t_{\overline{g_{2}}(r)}^{-1} g_{2} t_{r}\right)_{r \in R}\right) \\
& =\left(\overline{g_{1} g_{2}},\left(t_{\overline{g_{1} g_{2}}(r)}^{-1} g_{1} g_{2} t_{r}\right)_{r \in R}\right)=\varphi\left(g_{1} g_{2}\right) .
\end{aligned}
$$

Therefore, $\varphi$ is a homomorphism. We still have to prove that $\varphi$ is one-to-one. Assume that $\varphi\left(g_{1}\right)=\varphi\left(g_{2}\right)$. This hypothesis can be restated as follows

$$
\begin{equation*}
\left(\overline{g_{1}},\left(t_{\bar{g}_{1}(r)}^{-1} g_{1} t_{r}\right)_{r \in R}\right)=\left(\overline{g_{2}},\left(t_{\bar{g}_{2}(r)}^{-1} g_{2} t_{r}\right)_{r \in R}\right) \tag{4.5}
\end{equation*}
$$

Let $x$ be an element of $E$ and let $r$ be its representative in $R$. Then, $x_{0}=t_{r}^{-1}(x)$ belongs to $\left[r_{0}\right]$. By assumption,

$$
\left(t_{\overline{\bar{q}_{1}}(r)}\right)^{-1} g_{1} t_{r}\left(x_{0}\right)=\left(t_{\overline{g_{2}}(r)}\right)^{-1} g_{2} t_{r}\left(x_{0}\right) .
$$

Simplifying, we obtain $\left(t_{\overline{g_{1}(r)}}\right)^{-1} g_{1}(x)=\left(t_{\overline{g_{2}}(r)}\right)^{-1} g_{2}(x)$. Equation 4.5 implies that $\overline{g_{1}}=\overline{g_{2}}$. Thus, $\overline{g_{1}}(r)=\overline{g_{2}}(r)$ and $\left(t_{\overline{g_{1}}(r)}\right)^{-1}=\left(t_{\overline{g_{2}}(r)}\right)^{-1}$. Consequently, $g_{1}(x)=g_{2}(x)$. As this equality holds for all $x$ in $E$, is follows that $g_{1}$ and $g_{2}$ are equal, proving that $\varphi$ is one-to-one.

Let $x$ be an element of $E$ and let $g$ be an element of $G$. It remains to prove that $\lambda(g(x))=\varphi(g) \cdot \lambda(x)$. Let $r$ be the representative of $x$ in $R$. Then,

$$
\begin{aligned}
\varphi(g) \cdot \lambda(x) & =\left(\bar{g},\left(t_{\bar{g}(r)}^{-1} g t_{r}\right)_{r \in R}\right) \cdot\left(r, t_{r}^{-1}(x)\right)=\left(\bar{g}(r), t_{\bar{g}(r)}^{-1} g t_{r}\left(t_{r}^{-1}(x)\right)\right) \\
& =\left(\bar{g}(r), t_{\bar{g}(r)}^{-1} g(x)\right)=\lambda(g(x))
\end{aligned}
$$

The result is proven.
Theorem 4.4 establishes that any imprimitive permutation group can be embedded into a wreath product. In the following, we use the same notation as in Theorem 4.4. Observe that $A$ is a subgroup of $\operatorname{Sym}\left(\left[r_{0}\right]\right)$ and that $B$ is a subgroup of $\operatorname{Sym}(R)$. Therefore, the group $G$ can be identified with a subgroup of the wreath product $W=\operatorname{Sym}\left(\left[r_{0}\right]\right) \_\operatorname{Sym}(R)$. More formally, $G$ is a subgroup of the (isomorphic) image of $W$ under $\varphi^{-1}$.

Conversely, Proposition 4.11 ensures that the action of $W$ on $R \times\left[r_{0}\right]$ is imprimitive and preserves the partition

$$
\mathcal{Q}=\left\{\{r\} \times\left[r_{0}\right] \mid r \in R\right\} .
$$

Hence $\varphi^{-1}(W)$ preserves the partition $\lambda^{-1}(\mathcal{Q})=\mathcal{P}$. Combining these two results, we see that $\varphi^{-1}(W)$ is the biggest permutation group on $E$ preserving the partition $\mathcal{P}$.

By assumption, $\mathcal{P}$ is a $G$-invariant partition of $E$. Let $p$ denote the cardinality of $R$ and let $q$ denote the cardinality of $\left[r_{0}\right]$. In other words, $\mathcal{P}$ consists of $p$ parts, each of cardinality $q$ by virtue of Corollary 3.7. The discussion above proves that the number of permutations of $E$ preserving $\mathcal{P}$ is equal to the order of $\operatorname{Sym}\left(\left[r_{0}\right]\right) 2 \operatorname{Sym}(R)$, given by

$$
\begin{equation*}
\#\left(\operatorname{Sym}(R) \times \operatorname{Sym}\left(\left[r_{0}\right]\right)^{R}\right)=(p!) \times(q!)^{p} . \tag{4.6}
\end{equation*}
$$

### 4.1.3. Application of the Embedding Theorem

Recall that $V$ is a $d$-dimensional subspace of $\mathbb{F}_{2}^{n}$ and $S$ is an $n$-bit S-box preserving $\mathcal{L}(V)$. Since $U$ is a complement space of $V$, the partition $\mathcal{L}(V)$ is equal to $\{[u] \mid u \in$ $U\}$. Thus, $U$ is a system of distinct representatives of $\mathcal{L}(V)$.

Let $G$ denote the subgroup of $\operatorname{Sym}\left(\mathbb{F}_{2}^{n}\right)$ generated by $S$ and the key additions $\left\{\alpha_{x} \mid x \in \mathbb{F}_{2}^{n}\right\}$. By assumption, $S$ preserves $\mathcal{L}(V)$ and by Proposition 3.23, each key addition preserves $\mathcal{L}(V)$. Hence, the linear partition $\mathcal{L}(V)$ is $G$-invariant. Note that for each $x$ and $y$ in $\mathbb{F}_{2}^{n}$, the equality $\alpha_{x+y}(x)=y$ holds. Consequently, the group $G$ is transitive and imprimitive because $\mathcal{L}(V)$ is assumed to be non-trivial.

Following the proof of Theorem 4.13, let $t_{u}$ denote the key addition $\alpha_{u}$ for each $u$ in $U$. It is easily seen that $t_{u}([0])=t_{u}(V)=u+V=[u]$ so this definition meets the requirements of the proof. Moreover, we know that $\alpha_{u}$ is an involution, hence $\left(\alpha_{u}\right)^{-1}=\alpha_{u}$. Define the following mappings:

$$
\begin{aligned}
\lambda: \mathbb{F}_{2}^{n} & \longrightarrow U \times V & \varphi: G & \longrightarrow \operatorname{Sym}(U) \times \operatorname{Sym}(V)^{U} \\
x & \longmapsto\left(u_{x}, t_{u_{x}}(x)\right), & g & \longmapsto\left(\bar{g},\left(t_{\bar{g}(u)}^{-1} g t_{u}\right)_{u \in U}\right),
\end{aligned}
$$

## Chapter 4 - Analysis of a Backdoor S-Box

where $u_{x}$ denotes the representative in $U$ of $[x]$. Let $x=u+v$ be an element of $\mathbb{F}_{2}^{n}$ and let $g$ be an element of $G$. Then,

$$
\begin{aligned}
& \lambda(x)=\left(u, \alpha_{u}(x)\right)=(u, u+u+v)=(u, v), \\
& \varphi(g)=\left(\bar{g},\left(t_{\bar{g}(u)}^{-1} g t_{u}\right)_{u \in U}\right)=\left(\bar{g},\left(\alpha_{\bar{g}(u)} g \alpha_{u}\right)_{u \in U}\right) .
\end{aligned}
$$

Since $(\lambda, \varphi)$ is a permutation isomorphism from $G$ on $\mathbb{F}_{2}^{n}$ to $\operatorname{Sym}(V)$ ? $\operatorname{Sym}(U)$ on $U \times V$, the equality $\lambda(g(x))=\varphi(g) \cdot \lambda(x)$ holds. Note that

$$
\begin{aligned}
\varphi(g) \cdot \lambda(x) & =\left(\bar{g},\left(\alpha_{\bar{g}(u)} g \alpha_{u}\right)_{u \in U}\right) \cdot(u, v)=\left(\bar{g}(u), \alpha_{\bar{g}(u)} g \alpha_{u}(v)\right) \\
& =(\bar{g}(u), \bar{g}(u)+g(u+v)) .
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
g(u+v) & =\lambda^{-1}(\varphi(g) \cdot \lambda(x))=\lambda^{-1}(\bar{g}(u), \bar{g}(u)+g(u+v)) \\
& =\bar{g}(u)+(\bar{g}(u)+g(u+v)) .
\end{aligned}
$$

Let $\rho$ denote the permutation $\bar{S}$ of $U$ and for each $u$ in $U$, let $\tau_{u}$ denote the permutation of $V$ defined by the rule $\tau_{u}(v)=\rho(u)+S(u+v)$. Then, apply the preceding equality with $g=S$ to obtain

$$
S(u+v)=\rho(u)+\tau_{u}(v) .
$$

This proves that the decomposition of $S$ given by Theorem 4.4 can be obtained using Krasner-Kaloujnine embedding theorem.

Even though it might seem harder to derive Theorem 4.4 from Theorem 4.13 rather than to prove it directly, this new perspective emphasizes the group structure associated with the decomposition of imprimitive S-boxes. For instance, suppose that $S^{\prime}$ is another $n$-bit S-box preserving $\mathcal{P}$. Denote by $\varphi\left(S^{\prime}\right)=\left(\rho^{\prime},\left(\tau_{u}^{\prime}\right)_{u \in U}\right)$ the decomposition of $S^{\prime}$. As $\varphi$ is a homomorphism, $\varphi\left(S S^{\prime}\right)=\varphi(S) \otimes \varphi\left(S^{\prime}\right)$. Then, the decomposition of $S S^{\prime}$ is given for any $x=u+v$ in $\mathbb{F}_{2}^{n}$ by

$$
S S^{\prime}(u+v)=\rho \rho^{\prime}(u)+\tau_{\rho^{\prime}(u)} \tau_{u}^{\prime}(v) .
$$

In addition, the decomposition of $S^{-1}$ is given by the formula

$$
S^{-1}(u+v)=\rho^{-1}(u)+\tau_{\rho(u)}^{-1} .
$$

Finally, Equation (4.6) asserts that the number of S-boxes preserving $\mathcal{L}(V)$ is given by

$$
\left(2^{n-d}!\right) \times\left(2^{d}!\right)^{2^{n-d}}
$$

### 4.2. Differential and linear analyses

First, let us recall some basic facts about the differential and linear properties of S-boxes detailed in Chapter 1. Consider an $n$-bit S-box $S$ and two elements $a, b$ of
$\mathbb{F}_{2}^{n}$. The probability of the differential $(a, b)$ and the correlation of the approximation $(a, b)$ with respect to $S$ are defined to be

$$
\begin{aligned}
\operatorname{DP}_{S}(a, b) & =2^{-n} \times \#\left\{x \in \mathbb{F}_{2}^{n} \mid S(x)+S(x+a)=b\right\}, \\
\mathrm{C}_{S}(a, b) & =2^{-(n-1)} \times \#\left\{x \in \mathbb{F}_{2}^{n} \mid\langle a, x\rangle=\langle b, S(x)\rangle\right\}-1 .
\end{aligned}
$$

The linear potential of the approximation $(a, b)$ of $S$ is then the square of its correlation, that is $\operatorname{LP}_{S}(a, b)=\mathrm{C}_{S}(a, b)^{2}$. The maximum differential probability $\mathrm{DP}_{S}^{\max }$, the maximum absolute correlation $\mathrm{C}_{S}^{\max }$ and the maximum linear potential $\mathrm{LP}_{S}^{\max }$ of $S$ are defined to be

$$
\begin{aligned}
\operatorname{DP}_{S}^{\max } & =\max \left\{\operatorname{DP}(a, b) \mid a \in\left(\mathbb{F}_{2}^{n}\right)^{*}, b \in \mathbb{F}_{2}^{n}\right\}, \\
\mathrm{C}_{S}^{\max } & =\max \left\{|\mathrm{C}(a, b)| \mid a \in \mathbb{F}_{2}^{n}, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}, \\
\mathrm{LP}_{S}^{\max } & =\max \left\{\operatorname{LP}(a, b) \mid a \in \mathbb{F}_{2}^{n}, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}=\left(\mathrm{C}_{S}^{\max }\right)^{2} .
\end{aligned}
$$

Moreover, in Chapter 1 Section 1.5.1, we have observed that $\operatorname{DP}_{S}(a, b)$ is a multiple of $2^{-(n-1)}$ and that $\mathrm{DP}_{S}^{\max } \geq 2^{-(n-1)}$. According to the Sidelnikov-Chabaud-Vaudenay bound (see Equations (1.13) and (1.14)), we have

$$
\begin{equation*}
\mathrm{C}_{S}^{\max } \geq 2^{-\frac{n-1}{2}}, \quad \mathrm{LP}_{S}^{\max } \geq 2^{-(n-1)} \tag{4.7}
\end{equation*}
$$

Now, assume that $S$ preserves the partition $\mathcal{L}(V)$. In the previous section, we have proven that $S$ can be constructed using permutations with smaller domains. More precisely, Theorem 4.4 establishes the existence of a permutation $\rho$ of $U$ and permutations $\left(\tau_{u}\right)_{u \in U}$ of $V$ such that the relation

$$
S(u+v)=\rho(u)+\tau_{u}(v)
$$

holds for every $x=u+v$ in $\mathbb{F}_{2}^{n}$. This decomposition is fixed in the remainder of this section. In view of this result, it is natural to wonder if the differential probabilities and linear potentials of $S$ are related to the ones of the permutations in its decomposition. The first problem is that these notions are defined for vectorial Boolean function whereas the domains of $\rho$ and the $\tau_{u}$ are proper subspaces of $\mathbb{F}_{2}^{n}$. To solve this problem, we identify $U$ with $\mathbb{F}_{2}^{n-d}$ and $V$ with $\mathbb{F}_{2}^{d}$ using two isomorphisms, and then consider the permutations induced by $\rho$ and the $\tau_{u}$ on these sets.

Notation 4.14. Let $\mathcal{B}_{\mathcal{U}}=\left(u_{i}\right)_{i<n-d}$ and $\mathcal{B}_{\mathcal{V}}=\left(v_{i}\right)_{i<n-d}$ be two bases of $U$ and $V$ respectively. Define the following mappings:

$$
\begin{aligned}
L_{U}: \mathbb{F}_{2}^{n-d} & \longrightarrow U & L_{V}: \mathbb{F}_{2}^{d} & \longrightarrow V \\
\left(x_{n-d-1}, \ldots, x_{0}\right) & \longmapsto \sum_{i=0}^{n-d-1} x_{i} u_{i}, & \left(y_{d-1}, \ldots, y_{0}\right) & \longmapsto \sum_{i=0}^{d-1} y_{i} v_{i} .
\end{aligned}
$$

It is easily seen that $L_{U}$ and $L_{V}$ are both isomorphisms of vector spaces. Define $\bar{\rho}$ to be the permutation $L_{U}^{-1} \circ \rho \circ L_{U}$ induced by $\rho$ on $\mathbb{F}_{2}^{n-d}$. Similarly, for each $u$ in $U$, denote by $\bar{\tau}_{u}$ the permutation $L_{V}^{-1} \circ \tau_{u} \circ L_{V}$ induced by $\tau_{u}$ on $\mathbb{F}_{2}^{d}$.

The following lemma explains how a permutation $\mu$ of an $m$-dimensional subspace $W$ of $\mathbb{F}_{2}^{n}$ is linked to the differential probabilities and correlations of its induced permutation $\bar{\mu}$ on $\mathbb{F}_{2}^{m}$.

## Chapter 4 - Analysis of a Backdoor S-Box

Lemma 4.15. Let $W$ be an $m$-dimensional subspace of $\mathbb{F}_{2}^{n}$ and let $L$ be an isomorphism from $\mathbb{F}_{2}^{m}$ to $W$. Consider a permutation $\mu$ of $W$ and denote by $\bar{\mu}$ its induced permutation $L^{-1} \circ \mu \circ L$ on $\mathbb{F}_{2}^{m}$. Let $a$ and $b$ be elements of $W$ and denote $a^{\prime}=L^{-1}(a), b^{\prime}=L^{-1}(b), a^{t}=L^{\top}(a)$ and $b^{t}=L^{\top}(b)$. Then,

$$
\begin{aligned}
2^{m} \times \mathrm{DP}_{\bar{\mu}}\left(a^{\prime}, b^{\prime}\right) & =\#\{w \in W \mid \mu(w)+\mu(w+a)=b\}, \\
2^{m-1} \times\left(\mathrm{C}_{\bar{\mu}}\left(a^{t}, b^{t}\right)+1\right) & =\#\{w \in W \mid\langle a, w\rangle=\langle b, \mu(w)\rangle\}
\end{aligned}
$$

Proof. We begin with the correlation matrix of the permutation $\bar{\mu}$ induced by $\mu$ on $\mathbb{F}_{2}^{m}$. It is easily seen that

$$
\begin{aligned}
2^{m-1} \times\left(\mathrm{C}_{\bar{\mu}}\left(a^{t}, b^{t}\right)+1\right) & =\#\left\{x \in \mathbb{F}_{2}^{m} \mid\left\langle a^{t}, x\right\rangle=\left\langle b^{t}, \bar{\mu}(x)\right\rangle\right\} \\
& =\#\left\{x \in \mathbb{F}_{2}^{m} \mid\left\langle L^{\top}(a), x\right\rangle=\left\langle L^{\top}(b), L^{-1} \mu L(x)\right\rangle\right\} \\
& =\#\left\{x \in \mathbb{F}_{2}^{m} \mid\langle a, L(x)\rangle=\langle b, \mu(L(x))\rangle\right\}
\end{aligned}
$$

Denote by $E$ the set on the right side of the previous equation. As $L$ is bijective, the set $E$ and its image $L(E)$ have the same cardinality. Thus, replacing $E$ by $L(E)$ yields

$$
2^{m-1} \times\left(\mathrm{C}_{\bar{\mu}}\left(a^{t}, b^{t}\right)+1\right)=\#\{w \in W \mid\langle a, w\rangle=\langle b, \mu(w)\rangle\} .
$$

Next, it remains to prove the statement about the differential probability of $\bar{\mu}$. By definition,

$$
\begin{aligned}
2^{m} \times \mathrm{DP}_{\bar{\mu}}\left(a^{\prime}, b^{\prime}\right) & =\#\left\{x \in \mathbb{F}_{2}^{m} \mid \bar{\mu}(x)+\bar{\mu}\left(x+a^{\prime}\right)=b^{\prime}\right\} \\
& =\#\left\{x \in \mathbb{F}_{2}^{m} \mid L^{-1} \mu L(x)+L^{-1} \mu L\left(x+L^{-1}(a)\right)=L^{-1}(b)\right\}
\end{aligned}
$$

Because $L$ is bijective, $L(x)=L(y)$ if and only if $x=y$. Therefore,

$$
\begin{aligned}
2^{m} \times \mathrm{DP}_{\bar{\mu}}\left(a^{\prime}, b^{\prime}\right) & =\#\left\{x \in \mathbb{F}_{2}^{m} \mid L\left(L^{-1} \mu L(x)+L^{-1} \mu L\left(x+L^{-1}(a)\right)\right)=L L^{-1}(b)\right\} \\
& =\#\left\{x \in \mathbb{F}_{2}^{m} \mid \mu(L(x))+\mu(L(x)+a)=b\right\}
\end{aligned}
$$

Again, considering the image of the last set under $L$, we obtain

$$
2^{m} \times \operatorname{DP}_{\bar{\mu}}\left(a^{\prime}, b^{\prime}\right)=\#\{w \in W \mid \mu(w)+\mu(w+a)=b\}
$$

as was to be shown.
Example 4.16. Consider the bases $\mathcal{B}_{U}=(01,02,08)$ and $\mathcal{B}_{V}=(07,1 \mathrm{~A})$ of the subspaces $U$ and $V$. Next, we define the isomorphisms $L_{U}: \mathbb{F}_{2}^{3} \rightarrow U$ and $L_{V}: \mathbb{F}_{2}^{2} \rightarrow V$ following the construction given in Notation 4.14. For instance,

$$
L_{U}(6)=L_{U}(110)=1 u_{2}+1 u_{1}+0 u_{0}=08+02=0 \mathrm{~A} .
$$

Explicitly, these isomorphisms are given in Figure 4.4. We can now compute the permutation $\bar{\rho}$ of $\mathbb{F}_{2}^{3}$ and the permutations $\bar{\tau}_{u}$ of $\mathbb{F}_{2}^{2}$. For example,

$$
\bar{\rho}(1)=\left(L_{U}^{-1} \circ \rho \circ L_{U}\right)(1)=L_{U}^{-1}(\rho(01))=L_{U}^{-1}(0 \mathrm{~A})=6 .
$$

The permutation $\bar{\rho}$ and the family $\left(\bar{\tau}_{u}\right)_{u \in U}$ are illustrated in Figure 4.5, which should be compared to the original decomposition of $S$ represented in Figure 4.3.

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 00 | 01 | 02 | 03 | 08 | 09 | 0 A | 0 B |


| $x$ | 0 | 1 | 2 | 3 |
| :---: | :---: | :---: | :---: | :---: |
|  <br> $L_{V}(x)$ | 00 | 07 | 1 A | 1 D |

Figure 4.4: The linear transformations $L_{U}$ and $L_{V}$.


Figure 4.5: The family of permutations $\left(\bar{\tau}_{u}\right)_{u \in U}$ and the permutation $\bar{\rho}$.

### 4.2.1. Correlation Matrices and Linear Potentials

Until now, we have divided our imprimitive S-box $S$ into several smaller permutations and then transformed these permutations in order to reveal their differential and linear properties. We begin by investigating the correlation matrix of $S$. Our first result links some of its coefficients with the ones of the correlation matrix of $\bar{\rho}$. Even if the following theorem involves only few coefficients of $\mathrm{C}_{S}$, it has a significant practical impact because these coefficients happen to be the greatest in general, and hence determine the resistance of $S$ against linear cryptanalysis.

Theorem 4.17. Let $a$ and $b$ be two elements of $V^{\perp}$ and denote by $a^{t}$ and $b^{t}$ their respective images under $L_{U}^{\top}$. Then,

$$
\mathrm{C}_{S}(a, b)=\mathrm{C}_{\bar{\rho}}\left(a^{t}, b^{t}\right) \quad \text { and hence } \quad \operatorname{LP}_{S}(a, b)=\operatorname{LP}_{\bar{\rho}}\left(a^{t}, b^{t}\right) .
$$

Proof. Let $x=u+v$ be an element of $\mathbb{F}_{2}^{n}$. According to Theorem 4.4, the decomposition of $S(u+v)$ is $\rho(u)+\tau_{u}(v)$. Consequently,

$$
\langle a, u+v\rangle=\langle b, S(u+v)\rangle \Longleftrightarrow\langle a, u\rangle+\langle a, v\rangle=\langle b, \rho(u)\rangle+\left\langle b, \tau_{u}(v)\right\rangle
$$

as the dot product is bilinear. Recall that $a$ and $b$ belong to $V^{\perp}$ by assumption, so $\langle a, v\rangle$ and $\left\langle b, \tau_{u}(v)\right\rangle$ are both equal to 0 . This discussion proves that

$$
\left\{u+v \in \mathbb{F}_{2}^{n} \mid\langle a, u+v\rangle=\langle b, S(u+v)\rangle\right\}=\left\{u+v \in \mathbb{F}_{2}^{n} \mid\langle a, u\rangle=\langle b, \rho(u)\rangle\right\} .
$$

## Chapter 4 - Analysis of a Backdoor S-Box

Finally, combining Lemma 4.15 and the previous equation, we obtain

$$
\begin{aligned}
2^{n-1}\left(\mathrm{C}_{S}(a, b)+1\right) & =\#\left\{u+v \in \mathbb{F}_{2}^{n} \mid\langle a, u\rangle=\langle b, \rho(u)\rangle\right\} \\
& =\# V \times \#\{u \in U \mid\langle a, u\rangle=\langle b, \rho(u)\rangle\} \\
& =2^{d} \times 2^{n-d-1}\left(\mathrm{C}_{\bar{\rho}}\left(a^{t}, b^{t}\right)+1\right),
\end{aligned}
$$

which simplifies to give $\mathrm{C}_{S}(a, b)=\mathrm{C}_{\bar{\rho}}\left(a^{t}, b^{t}\right)$, as desired.
Remark 4.18. Consider the transpose $L_{U}^{\top}$ of $L_{U}$ seen as a mapping from $\mathbb{F}_{2}^{n-d}$ to $\mathbb{F}_{2}^{n}$ instead of $U$. Thus, $L_{U}^{\top}$ is a mapping from $\mathbb{F}_{2}^{n}$ to $\mathbb{F}_{2}^{n-d}$ which cannot be injective since $d>1$. According to Proposition 1.2, its kernel can be calculated as follows

$$
\operatorname{Ker}\left(L_{U}^{\top}\right)=\left(\operatorname{Im} L_{U}\right)^{\perp}=U^{\perp}
$$

Then, observe that $U^{\perp} \cap V^{\perp}=(U+V)^{\perp}=\left(\mathbb{F}_{2}^{n}\right)^{\perp}=\{0\}$. Consequently, the restriction of $L_{U}^{\top}$ to the orthogonal space of $V$ in $\mathbb{F}_{2}^{n}$ is injective and hence bijective because of the rank-nullity theorem. This discussion proves that the pairs $\left(a^{t}, b^{t}\right)$ as defined in Theorem 4.17 are all distinct. Therefore, $\mathrm{C}_{\bar{\rho}}$ is a submatrix of $\mathrm{C}_{S}$.

Corollary 4.19. The maximum linear potential of $S$ is lower bounded by $2^{-(n-d-1)}$.
Proof. As noted in Equation (4.7), there exist two elements $a^{t}$ and $b^{t}$ of $\mathbb{F}_{2}^{n-d}$ both non-zero such that

$$
\left|\mathrm{C}_{\bar{\rho}}\left(a^{t}, b^{t}\right)\right|=\mathrm{C}_{\bar{\rho}}^{\max } \geq 2^{-\frac{n-d-1}{2}} .
$$

Let $a$ and $b$ denote the images of $a^{t}$ and $b^{t}$ under $\left(L_{U}^{\top}\right)^{-1}$. Then, Theorem 4.17 implies that

$$
\left|\mathrm{C}_{S}(a, b)\right|=\left|\mathrm{C}_{\bar{\rho}}\left(a^{t}, b^{t}\right)\right| \geq 2^{-\frac{n-d-1}{2}} .
$$

Multiplying both sides of this inequality by themselves yields $\operatorname{LP}_{S}(a, b) \geq 2^{-(n-d-1)}$. Finally, observe that $a$ and $b$ are non-zero and the result is proven.
Remark 4.20. As explained in Section 1.5.1.c, the maximum absolute correlation of any 4 -bit S-box is lower bounded by $2^{\frac{4+2}{2}} \times 2^{-4}=2^{-1}$. Therefore, if $n-d=4$ the previous reasoning yields the lower bound $\mathrm{LP}_{S}^{\max } \geq 2^{-2}$, strengthening Corollary 4.19. Similarly, we know that every 2 -bit S-box is affine, so has maximum absolute correlation equals to 1 . Thus, the maximum linear potential of $S$ is also equal to 1 when $n-d=2$.

Example 4.21. First of all, we should explicit the transpose of $L_{U}$. Recall that we have defined $L_{U}$ to be the linear mapping from $\mathbb{F}_{2}^{3}$ to $\mathbb{F}_{2}^{5}$ satisfying $L_{U}(1)=01$, $L_{U}(2)=02$ and $L_{U}(4)=08$. Therefore, for any $x$ in $\mathbb{F}_{2}^{3}$, we have

$$
L_{U}(x)=\left(x_{2}, x_{1}, x_{0}\right) \times\left(\begin{array}{lllll}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{array}\right)=x \times A_{U}
$$

By definition, its transpose is the mapping $L_{U}^{\top}$ from $\mathbb{F}_{2}^{5}$ to $\mathbb{F}_{2}^{3}$ defined by the rule

$$
L_{U}^{\top}(x)=\left(x_{4}, \ldots, x_{0}\right) \times A_{U}^{\top}=\left(x_{3}, x_{1}, x_{0}\right) .
$$

Recall that $V$ was defined to be the subspace of $\mathbb{F}_{2}^{5}$ spanned by $\{07,1 \mathrm{~A}\}$. It is easily checked that the vectors in $\{05,0 \mathrm{~B}, 13\}$ are linearly independent and orthogonal to each element of the previous basis of $V$. Thus, the family $(05,0 B, 13)$ is a basis of $V^{\perp}$ because this subspace is 3 -dimensional. The restriction of $L_{U}^{\top}$ to $V^{\perp}$ is explicitly given by

$$
\begin{array}{llll}
L_{U}^{\top}(00)=0, & L_{U}^{\top}(0 \mathrm{~B})=7, & L_{U}^{\top}(13)=3, & L_{U}^{\top}(18)=4 \\
L_{U}^{\top}(05)=1, & L_{U}^{\top}(0 \mathrm{E})=6, & L_{U}^{\top}(16)=2, & L_{U}^{\top}(1 \mathrm{D})=5 .
\end{array}
$$

As noted above, this restriction is a bijection. We will now reorder the rows and columns of the correlation matrix of $S$ to highlight that $\mathrm{C}_{\bar{\rho}}$ is one of its submatrices. Following Theorem 4.17, the firsts row and column indices should be

$$
\underbrace{\left(L_{U}^{\top}\right)^{-1}(0)}_{00}, \underbrace{\left(L_{U}^{\top}\right)^{-1}(1)}_{05}, \ldots, \underbrace{\left(L_{U}^{\top}\right)^{-1}(6)}_{0 \mathrm{E}}, \quad \underbrace{\left(L_{U}^{\top}\right)^{-1}(7)}_{\mathrm{OB}}
$$

The correlation matrix of $S$ is illustrated in Figure 4.6 in its original then reordered forms. Next, Figure 4.7 shows that the top left $8 \times 8$ submatrix of the reordered form of $\mathrm{C}_{S}$ is exactly the correlation matrix of $\bar{\rho}$. It goes without saying that the coefficients affected by Theorem 4.17 stress the structure of such a correlation matrix. Moreover we see that they determine the absolute maximal correlation of $S$, as it is generally the case. Finally, it is worth noting that

$$
\operatorname{LP}_{S}^{\max }=\left(\frac{16}{32}\right)^{2}=2^{-2}
$$

and thus $S$ meets the bound of Corollary 4.19 with equality.

### 4.2.2. Differential Probabilities

Along a similar line, we will investigate the differential probabilities of $S$ and their links with the decomposition of $S$. But before stating our main results, we need two preliminary lemmas.

Lemma 4.22. Let $a=u_{a}+v_{a}$ and $b=u_{b}+v_{b}$ be two elements of $\mathbb{F}_{2}^{n}$. Denote by $\mathcal{U}$ the set $\left\{u \in U \mid \rho(u)+\rho\left(u+u_{a}\right)=u_{b}\right\}$. Then,

$$
2^{n} \times \mathrm{DP}_{S}(a, b)=\sum_{u \in \mathcal{U}} \#\left\{v \in V \mid \tau_{u}(v)+\tau_{u+u_{a}}\left(v+v_{a}\right)=v_{b}\right\}
$$

Proof. Let $x$ be any element of $\mathbb{F}_{2}^{n}$. Consider the following equation

$$
\begin{equation*}
S(x)+S(x+a)=b \tag{4.8}
\end{equation*}
$$

Write $x$ as the sum $u+v$. According to Theorem 4.4, Equation (4.8) is equivalent to

$$
\begin{equation*}
\rho(u)+\tau_{u}(v)+\rho\left(u+u_{a}\right)+\tau_{u+u_{a}}\left(v+v_{a}\right)=u_{b}+v_{b} . \tag{4.9}
\end{equation*}
$$

## Chapter 4 - Analysis of a Backdoor S-Box



Figure 4.6: The reordered correlation matrix of $S$ (multiplied by $2^{5}$ ).

| $2^{5} \times \mathrm{C}_{S}(a, b)$ |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 00 | 05 | 16 | 13 | 18 | 1 D | OE | OB |
| 00 | 32 | $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ |
| 05 | $\cdot$ | 16 | 16 | $\cdot$ | $\cdot$ | 16 | -16 | $\cdot$ |
| 16 | $\cdot$ | $\cdot$ | -16 | -16 | -16 | 16 | $\cdot$ | $\cdot$ |
| 13 | $\cdot$ | -16 | $\cdot$ | -16 | 16 | $\cdot$ | -16 | $\cdot$ |
| 18 | $\cdot$ | 16 | $\cdot$ | -16 | $\cdot$ | -16 | $\cdot$ | -16 |
| 1D | $\cdot$ | $\cdot$ | -16 | 16 | $\cdot$ | $\cdot$ | -16 | -16 |
| OE | $\cdot$ | 16 | -16 | $\cdot$ | 16 | $\cdot$ | $\cdot$ | 16 |
| OB | $\cdot$ | $\cdot$ | $\cdot$ | $\cdot$ | 16 | 16 | 16 | -16 |

\[

\]

Figure 4.7: The $8 \times 8$ top left submatrix of the reordered correlation matrix of $S$ and the correlation matrix of $\bar{\rho}$.

Observe that $\rho(u)+\rho\left(u+u_{a}\right)$ lies in $U$ and $\tau_{u}(v)+\tau_{u+u_{a}}\left(v+v_{a}\right)$ lies in $V$. Since $\mathbb{F}_{2}^{n}$ is the direct sum of $U$ and $V$, Equation (4.9) holds if and only if the following two equations hold:

$$
\begin{align*}
\rho(u)+\rho\left(u+u_{a}\right) & =u_{b} \quad \text { and }  \tag{4.10}\\
\tau_{u}(v)+\tau_{u+u_{a}}\left(v+v_{a}\right) & =v_{b} \tag{4.11}
\end{align*}
$$

By definition, the statement " $u \in \mathcal{U}$ " is equivalent to Equation (4.10). Then, denoting by $P(u, v)$ the assertion "Equation (4.11) holds", we have

$$
\begin{aligned}
2^{n} \times \mathrm{DP}_{S}(a, b) & =\#\left\{x \in \mathbb{F}_{2}^{n} \mid(4.8) \text { holds }\right\} \\
& =\#\{(u, v) \in U \times V \mid u \in \mathcal{U} \text { and } P(u, v)\}=\sum_{u \in \mathcal{U}} \#\{v \in V \mid P(u, v)\}
\end{aligned}
$$

The result is proven.
Lemma 4.23. Let $\lambda, \mu$ be two permutations of $V$. For each $v_{a}, v_{b}$ in $V$, denote by $D\left(v_{a}, v_{b}\right)$ the set $\left\{v \in V \mid \mu(v)+\lambda\left(v+v_{a}\right)=v_{b}\right\}$. Let $v_{a}, v_{b}$ be elements of $V$. Then,

$$
\sum_{\tilde{v}_{b} \in V} \# D\left(v_{a}, \tilde{v}_{b}\right)=\sum_{\tilde{v}_{a} \in V} \# D\left(\tilde{v}_{a}, v_{b}\right)=\# V .
$$

Proof. Firstly, we contend that $\bigcup_{\tilde{v}_{b} \in V} D\left(v_{a}, \tilde{v}_{b}\right)$ is equal to $V$. Indeed, $V$ is included in $\bigcup_{\tilde{v}_{b} \in V} D\left(v_{a}, \tilde{v}_{b}\right)$ since any element $v$ belongs to $D\left(v_{a}, \mu(v)+\lambda\left(v+v_{a}\right)\right)$ and the converse inclusion clearly holds. It goes without saying that the sets $D\left(v_{a}, \tilde{v}_{b}\right)$ are pairwise disjoint. Thus,

$$
\# V=\# \bigcup_{\tilde{v}_{b} \in V} D\left(v_{a}, \tilde{v}_{b}\right)=\sum_{\tilde{v}_{b} \in V} \# D\left(v_{a}, \tilde{v}_{b}\right)
$$

Next, we claim that $\bigcup_{\tilde{v}_{a} \in V} D\left(\tilde{v}_{a}, v_{b}\right)$ is equal to $V$. As previously, we only need to prove that $V$ is included in $\bigcup_{\tilde{v}_{a} \in V} D\left(\tilde{v}_{a}, v_{b}\right)$. Let $v$ in $V$. Since $\lambda$ is onto, there exists an element $x$ of $V$ such that $\lambda(x)=\mu(v)+v_{b}$. Then, $v$ lies in $D\left(x+v, v_{b}\right)$, proving our claim. Moreover, the sets $D\left(\tilde{v}_{a}, v_{b}\right)$ are pairwise disjoint because $\lambda$ is one-to-one, implying that $\# V=\sum_{\tilde{v}_{a} \in V} \# D\left(\tilde{v}_{a}, v_{b}\right)$ as desired.

## Chapter 4 - Analysis of a Backdoor S-Box

Now is the time to introduce our first theorem about the differential probabilities of $S$. Unlike Theorem 4.17, the next result involves all the coefficients of the matrix $\mathrm{DP}_{S}$, thereby underlining its global structure.

Theorem 4.24. Let $a=u_{a}+v_{a}$ and $b=u_{b}+v_{b}$ be elements of $\mathbb{F}_{2}^{n}$ and denote by $u_{a}^{\prime}$ and $u_{b}^{\prime}$ their images under $L_{U}^{-1}$. It holds that

$$
\sum_{i \in\left[u_{a}\right]} \mathrm{DP}_{S}(i, b)=\sum_{j \in\left[u_{b}\right]} \mathrm{DP}_{S}(a, j)=\operatorname{DP}_{\bar{\rho}}\left(u_{a}^{\prime}, u_{b}^{\prime}\right) .
$$

Especially, $\mathrm{DP}_{S}(a, b) \leq \mathrm{DP}_{\bar{\rho}}\left(u_{a}^{\prime}, u_{b}^{\prime}\right)$ and thus $\mathrm{DP}_{S}^{\max } \leq \mathrm{DP}_{\bar{\rho}}^{\max }$.
Proof. Denote by $\mathcal{U}$ the set $\left\{u \in U \mid \rho(u)+\rho\left(u+u_{a}\right)=u_{b}\right\}$. According to Lemma 4.22, we have

$$
\begin{aligned}
2^{n} \times \sum_{i \in\left[u_{a}\right]} \mathrm{DP}_{S}(i, b) & =2^{n} \times \sum_{\tilde{v}_{a} \in V} \operatorname{DP}_{S}\left(u_{a}+\tilde{v}_{a}, b\right) \\
& =\sum_{\tilde{v}_{a} \in V}\left(\sum_{u \in \mathcal{U}} \#\left\{v \in V \mid \tau_{u}(v)+\tau_{u+u_{a}}\left(v+\tilde{v}_{a}\right)=v_{b}\right\}\right) .
\end{aligned}
$$

Reversing the order of summation, we get

$$
2^{n} \times \sum_{i \in\left[u_{a}\right]} \operatorname{DP}_{S}(i, b)=\sum_{u \in \mathcal{U}}\left(\sum_{\tilde{v}_{a} \in V} \#\left\{v \in V \mid \tau_{u}(v)+\tau_{u+u_{a}}\left(v+\tilde{v}_{a}\right)=v_{b}\right\}\right) .
$$

In the same way, it can be proven that

$$
2^{n} \times \sum_{j \in\left[u_{b}\right]} \operatorname{DP}_{S}(a, j)=\sum_{u \in \mathcal{U}}\left(\sum_{\tilde{v}_{b} \in V} \#\left\{v \in V \mid \tau_{u}(v)+\tau_{u+u_{a}}\left(v+v_{a}\right)=\tilde{v}_{b}\right\}\right) .
$$

By virtue of Lemma 4.23, we have

$$
2^{n} \times \sum_{i \in\left[u_{a}\right]} \operatorname{DP}_{S}(i, b)=2^{n} \times \sum_{j \in\left[u_{b}\right]} \operatorname{DP}_{S}(a, j)=\sum_{u \in \mathcal{U}} \# V=\# \mathcal{U} \times 2^{d} .
$$

Finally, Lemma 4.15 ensures that $\# \mathcal{U}=2^{n-d} \times \operatorname{DP}_{\bar{\rho}}\left(u_{a}^{\prime}, u_{b}^{\prime}\right)$. The result follows.
The next result is the analog of Theorem 4.17 for the differential probabilities. In a similar way, it considers few coefficients of $\mathrm{DP}_{S}$ but these coefficients are generally the greatest. Therefore, this result will be used to derive a lower bound on the resistance of $S$ against differential cryptanalysis.

Theorem 4.25. Let $v_{a}$ and $v_{b}$ be two elements of $V$ and denote by $v_{a}^{\prime}$ and $v_{b}^{\prime}$ their respective images under $L_{V}^{-1}$. Then

$$
\mathrm{DP}_{S}\left(v_{a}, v_{b}\right)=\frac{1}{2^{n-d}} \sum_{u \in U} \operatorname{DP}_{\bar{\tau}_{u}}\left(v_{a}^{\prime}, v_{b}^{\prime}\right) .
$$

Particularly, the family $\left(\mathrm{DP}_{S}\left(v_{a}, v_{b}\right)\right)_{v_{a}, v_{b} \in V}$ is uniquely determined by $\left(\mathrm{DP}_{\bar{\tau}_{u}}\right)_{u \in U}$.

Proof. Applying Lemma 4.22 with $a=0+v_{a}$ and $b=0+v_{b}$ yields

$$
2^{n} \times \mathrm{DP}_{S}\left(v_{a}, v_{b}\right)=\sum_{u \in U} \#\left\{v \in V \mid \tau_{u}(v)+\tau_{u}\left(v+v_{a}\right)=v_{b}\right\},
$$

since $\mathcal{U}=\{u \in U \mid \rho(u)+\rho(u+0)=0\}=U$. Then, Lemma 4.15 ensures that

$$
\sum_{u \in U} \#\left\{v \in V \mid \tau_{u}(v)+\tau_{u}\left(v+v_{a}\right)=v_{b}\right\}=\sum_{u \in U} 2^{d} \times \mathrm{DP}_{\bar{\tau}_{u}}\left(v_{a}^{\prime}, v_{b}^{\prime}\right)
$$

Simplifying, we obtain the desired result.
Corollary 4.26. The maximum differential probability of $S$ is lower bounded by the smallest multiple of $2^{-(n-1)}$ being directly greater than or equal to $\frac{1}{2^{d}-1}$.

Proof. Let $v_{a}$ be a nonzero element of $V$. Applying Theorem 4.24 with $a=0+v_{a}$ and $b=0+0$ yields

$$
\sum_{j \in[0]} \mathrm{DP}_{S}\left(v_{a}, j\right)=\mathrm{DP}_{\bar{\rho}}(0,0)=1
$$

Since $[0]=V$, we have $\sum_{v \in V} \mathrm{DP}_{S}\left(v_{a}, v\right)=1$. Moreover, we know that $\mathrm{DP}_{S}\left(v_{a}, 0\right)=0$ because $v_{a}$ is nonzero and $S$ is a permutation. Thus, there are at most $2^{d}-1$ elements $v$ in $V$ such that $\mathrm{DP}_{S}\left(v_{a}, v\right)$ is nonzero. In order to minimize $\mathrm{DP}_{S}^{\max }$, we would ideally require that $\operatorname{DP}_{S}\left(v_{a}, v\right)=\frac{1}{2^{d}-1}$ for each nonzero element $v$ of $V$. The result follows since any coefficient $\mathrm{DP}_{S}\left(v_{a}, v\right)$ must be a multiple of $2^{-(n-1)}$.

Example 4.27. As was the case for Example 4.21, we will reorder the matrix $\mathrm{DP}_{S}$ to illustrate Theorems 4.24 and 4.25. Recall that the subspaces $U$ and $V$ can be expressed as

$$
\begin{aligned}
U & =\left\{L_{U}(x) \mid x \in \mathbb{F}_{2}^{3}\right\} \\
V & =\{00,01,02,03,08,09,0 \mathrm{~A}, 0 \mathrm{~B}\}, \\
V & =\left\{L_{V}(x) \mid x \in \mathbb{F}_{2}^{2}\right\}=\{00,07,1 \mathrm{~A}, 1 \mathrm{D}\} .
\end{aligned}
$$

Then, Theorem 4.24 suggests to consider the rows and columns of $\mathrm{DP}_{S}$ coset by coset. In other words, the row and column indices may be reordered as follows:

$$
\begin{array}{cccc}
L_{U}(0)+L_{V}(0), & L_{U}(0)+L_{V}(1), & L_{U}(0)+L_{V}(2), & L_{U}(0)+L_{V}(3), \\
\ldots & \ldots & \ldots & \ldots \\
L_{U}(7)+L_{V}(0), & L_{U}(7)+L_{V}(1), & L_{U}(7)+L_{V}(2), & L_{U}(7)+L_{V}(3) .
\end{array}
$$

The natural and reordered forms of the matrix $\mathrm{DP}_{S}$ are represented in Figure 4.8. Thanks to this representation, it is now obvious that this matrix is highly structured. But to understand it, we give the differential probabilities matrices of $\bar{\rho}$ and $\left(\bar{\tau}_{u}\right)_{u \in U}$ in Figure 4.9. It is easily seen how $\bar{\rho}$ globally shapes the matrix $\mathrm{DP}_{S}$. According to Theorem 4.24, if we fix a row and add all the coefficients whose column indices lie in the same coset, then we obtain a coefficient of $\mathrm{DP}_{\bar{\rho}}$. For instance, consider the row $06=01+07$ and the coset [02]. Then

$$
\begin{aligned}
\sum_{j \in[02]} \mathrm{DP}_{S}(06, j) & =\mathrm{DP}_{S}(06,02)+\mathrm{DP}_{S}(06,05)+\mathrm{DP}_{S}(06,18)+\mathrm{DP}_{S}(06,1 \mathrm{~F}) \\
& =\frac{4}{32}+\quad 0+0+\frac{4}{32} \\
& =\frac{1}{4}=\mathrm{DP}_{\bar{\rho}}\left(L_{U}^{-1}(01), L_{U}^{-1}(02)\right)=\mathrm{DP}_{\bar{\rho}}(1,2)
\end{aligned}
$$

## Chapter 4 - Analysis of a Backdoor S-Box



Figure 4.8: The reordered differential probabilities matrix of $S$ (multiplied by $2^{5}$ ).


Figure 4.9: The differential probabilities matrices of $\bar{\rho}$ and $\left(\bar{\tau}_{u}\right)_{u \in U}$.

Moreover, a similar result holds when we fix a column. Next, Theorem 4.25 ensures that the submatrix $\left(\mathrm{DP}_{S}\left(v_{a}, v_{b}\right)\right)_{v_{a}, v_{b} \in V}$ is the average of the matrices $\mathrm{DP}_{\bar{\tau}_{u}}$. For instance,

$$
\begin{aligned}
\mathrm{DP}_{S}(07,1 \mathrm{D}) & =\frac{1}{8} \times\left(\sum_{u \in U} \mathrm{DP}_{\bar{\tau}_{u}}\left(L_{V}^{-1}(07), L_{V}^{-1}(1 \mathrm{D})\right)\right)=\frac{1}{8} \times\left(\sum_{u \in U} \mathrm{DP}_{\bar{\tau}_{u}}(1,3)\right) \\
& =\frac{1}{8} \times(0+1+1+1+0+0+0+0)=\frac{3}{8}=\frac{12}{32}
\end{aligned}
$$

To conclude, let us take a look at the bound given in Corollary 4.26. The maximal differential probability of $S$ is lower bounded by the smallest multiple of $2^{-(5-1)}=\frac{2}{32}$ greater than

$$
\frac{1}{2^{2}-1}=\frac{10+\frac{2}{3}}{32} \text { hence } \frac{12}{32} .
$$

Since $\mathrm{DP}_{S}^{\max }=\frac{12}{32}$ this bound is tight for $(n, d)=(5,2)$.

### 4.2.3. Designing a Backdoor S-Box

Relying on the results obtained so far, we will derive a construction for almost optimal partition-based backdoor S-boxes. For this purpose, let us summarize what we have learned from the three theorems of this section.

- According to Theorems 4.17 and 4.24 the maximum linear potential and differential probability of the permutation $\bar{\rho}$ should be as low as possible.
- In addition, Theorem 4.25 ensures that the sum of the matrices $\mathrm{DP}_{\bar{\tau}_{u}}$ should have the smallest possible coefficients.
All the bounds given by Corollaries 4.19, 4.26 and Remark 4.20 for each $2 \leq n \leq 10$ and $1 \leq d<n$ are gathered in Figure 4.10.

Remark 4.28. By an ( $n, d$ )-PBB S-box, we mean an $n$-bit partition-based backdoor S-box mapping the linear partition associated with a $d$-dimensional subspace to another linear partition. As can be seen in Figure 4.10, if $d$ is close to 0, any

## Chapter 4 - Analysis of a Backdoor S-Box



Figure 4.10: Lower bounds on maximum differential probability and linear potential of an S-box $S$ mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$ where $V$ and $W$ are both $d$-dimensional subspaces of $\mathbb{F}_{2}^{n}$.
$(n, d)$-PBB S-box is weak against differential cryptanalysis. Inversely, is $d$ is close to $n$, then any $(n, d)$-PBB S-box is weak against linear cryptanalysis. Therefore, an ( $n, d$ )-PBB S-box which resists differential and linear cryptanalysis must be such that $d \approx \frac{n}{2}$.

Let $n$ be a positive integer. Choose two proper $d$-dimensional subspaces $V$ and $W$ of $\mathbb{F}_{2}^{n}$ and an isomorphism $L$ from $V$ to $W$. We now detail how to design a "good" S-box mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$. First, choose a complement subspace $U$ of $V$ in $\mathbb{F}_{2}^{n}$ and define the isomorphisms $L_{U}$ and $L_{V}$. Then, proceed as follows.

1. Construct a permutation $\bar{\rho}$ of $\mathbb{F}_{2}^{n-d}$ which is (almost) optimal with respect to differential and linear cryptanalysis.
2. Construct a family of permutations $\left(\bar{\tau}_{u}\right)_{u \in U}$ of $\mathbb{F}_{2}^{d}$ such that the sum (denoted by SDP) of their differential probability matrices satisfies

$$
\frac{1}{2^{n-d}} \times \max _{a, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}} \operatorname{SDP}(a, b) \text { is close to the bound of Corollary } 4.26
$$

3. Define the permutation $S$ of $\mathbb{F}_{2}^{n}$ by the formula

$$
S(u+v)=\left(L_{U} \circ \bar{\rho} \circ L_{U}^{-1}\right)(u)+\left(L_{V} \circ \bar{\tau}_{u} \circ L_{V}^{-1}\right)(v) .
$$

4. If $\mathrm{DP}_{S}^{\max }$ and $\mathrm{LP}_{S}^{\max }$ are close to the bounds of Figure 4.10, then $L \circ S$ is a good S-box mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Otherwise, return to Step 1.

The reader may refer to Section 1.5.1.c which enumerates several families of permutations with optimal (or almost optimal) resistance against differential and linear cryptanalysis. Once we have such a permutation, other permutations which have the same differential and linear properties can be obtained using the affineequivalence (see Equation (4.1)), the EA-equivalence or the CCZ-equivalence [34] (see [20]). When $d$ is greater than 4, we suggest to search for the family of permutations $\left(\bar{\tau}_{u}\right)_{u \in U}$ among the permutations with good differential properties. In practice, we obtain partition-based backdoor S-boxes close to the bounds of Figure 4.10 after a small number of iterations.

### 4.3. A Toy Partition-Based Backdoor Cipher

Before concluding in the next section, we introduce a toy partition-based backdoor cipher called TBC (standing for Toy Backdoor Cipher) to illustrate this and the previous chapters.

### 4.3.1. Specification of TBC

TBC is a substitution-permutation network processing a 36 -bit block of plaintext using a 36 -bit cipher key. The round function of TBC is quite simple and is largely inspired from the lightweight cipher Present [17] and its small-scale variants SmallPresent [69]. Just as in all substitution permutation networks, the round function

## Chapter 4 - Analysis of a Backdoor S-Box



Figure 4.11: The 6-bit S-box $S$ (left) and the 12-bit diffusion $D$ (right) of TBC.


Figure 4.12: The round function $F_{k^{[i]}}$ of TBC.
consists of a round-key addition, a substitution layer and a diffusion layer. The substitution layer uses one 6-bit S-box which is applied six times in parallel across the 36 bits of the block. This S-box is denoted by $S$ and is defined in Figure 4.11. Then the diffusion layer is a bit permutation (see Definition 1.12) given by the formula

$$
\phi(i)=6 \times(i \bmod 6)+\left\lfloor\frac{i}{6}\right\rfloor .
$$

A diagrammatic representation of the round function is provided in Figure 4.12. The encryption process consists of 21 iterative applications of this round function, then ends with a key addition. Therefore, the last round is equal to the other rounds and the encryption requires 22 round keys.

The TBC key schedule is inspired by the AES-128 key schedule. The cipher key $K$ is also the first round key $k^{[0]}$ and each round key $k^{[i]}$ is computed by applying a function $G_{i}$ to the preceding round key $k^{[i-1]}$. This function uses a 12-bit linear permutation $D$ illustrated in Figure 4.11. Explicitly, the linear diffusion $D$ is defined for each $x$ in $\mathbb{F}_{2}^{12}$ by the rule

$$
\begin{aligned}
& D\left(x_{0}, \ldots, x_{11}\right)=\left(x_{2}+x_{3}+x_{10}+x_{11}, x_{10}+x_{11},\right. \\
& x_{4}+x_{5}+x_{8}+x_{9}, x_{8}+x_{9} \text {, } \\
& x_{0}+x_{1}+x_{6}+x_{7}, x_{6}+x_{7} \text {, } \\
& x_{5}+x_{11} \quad, x_{11} \quad, \\
& x_{3}+x_{7} \quad, x_{7} \quad, \\
& x_{1}+x_{9} \quad, x_{9} \quad .
\end{aligned}
$$



Figure 4.13: The round function $G_{i}$ of TBC key schedule.
For instance, $D$ maps ( $30 \| 07$ ) to ( $0 C \| 31$ ). Now, let us explain how the round function $G_{i}$ of the key schedule derives the round key $k^{[i+1]}$ from $k^{[i]}$. First, the diffusion $D$ is applied three times in parallel to $k^{[i]}$ to obtain a 36 -bit block denoted by $x$, that is to say

$$
D\left(k_{0}^{[i]} \| k_{1}^{[i]}\right)=\left(x_{0} \| x_{1}\right), \quad D\left(k_{2}^{[i]} \| k_{3}^{[i]}\right)=\left(x_{2} \| x_{3}\right), \quad D\left(k_{4}^{[i]} \| k_{5}^{[i]}\right)=\left(x_{4} \| x_{5}\right) .
$$

Then, compute $\left(y_{4} \| y_{5}\right)=\left(S\left(x_{4}+r_{i}\right) \| S\left(x_{5}\right)\right)$. Here $x_{4}+r_{i}$ denotes the addition of the round constant $r_{i}$ which is performed in $\mathbb{F}_{2}^{6}$, so is just a bitwise exclusive or (Xor) between $x_{6}$ and $r_{i}$. The round constant $r_{i}$ is equal to the integer $i+1$ expressed in binary. For instance $r_{0}=01$ and $r_{9}=0 \mathrm{~A}$. Finally, the next round key $k^{[i+1]}$ is computed as follows:

$$
\begin{aligned}
& \left(k_{0}{ }^{[i+1]} \| k_{1}{ }^{[i+1]}\right)=\left(x_{0} \| x_{1}\right)+\left(y_{4} \| y_{5}\right), \\
& \left(k_{2}{ }^{[i+1]} \| k_{3}{ }^{[i+1]}\right)=\left(x_{2} \| x_{3}\right)+\left(k_{0}{ }^{[i+1]} \| k_{1}^{[i+1]}\right), \\
& \left(k_{4}{ }^{[i+1]} \| k_{5}{ }^{[i+1]}\right)=\left(x_{4} \| x_{5}\right)+\left(k_{2}{ }^{[i+1]} \| k_{3}{ }^{[i+1]}\right) .
\end{aligned}
$$

An illustration of the round function of TBC key schedule is given in Figure 4.13.

### 4.3.2. Differential and Linear Cryptanalysis

It is easily checked with a computer that the S-box $S$ has maximum linear potential equal to $2^{-2}$ and maximum differential probability equal to $\frac{14}{64}=1.75 \times 2^{-3}$. Since any linear or differential trail has at least one active S-box per round, we can upper bound the potential of an optimal 20 -round linear trail by $\left(2^{-2}\right)^{20}=2^{-40}$ and the probability of an optimal 20 -round differential trail by $\left(1.75 \times 2^{-3}\right)^{20} \approx 1.11 \times 2^{-46}$.

Using the algorithm OptTrail presented in Chapter 2, we have proven that the potential of an optimal 19-round linear trail is really equal to $2^{-40}$ but the probability

## Chapter 4 - Analysis of a Backdoor S-Box

of an optimal 19-round differential trial is equal to $1.76 \times 2^{-49}$. Therefore, a linear cryptanalysis would require $c \times 2^{40}$ known plaintext/ciphertext pairs and a differential cryptanalysis $c \times 2^{49}$ chosen plaintext/ciphertext pairs with $c \geq 5$. Since there are only $2^{36}$ different plaintext blocks, this cipher is practically secure against differential and linear cryptanalysis.

Observe that we have used here the heuristic measure [57, so we have never considered the probability of an optimal 19-round differential. As will be seen in Section 4.3.4, TBC is actually weak with respect to differential cryptanalysis.

### 4.3.3. The Backdoor

As claimed in introduction, TBC is a partition-based backdoor cipher. Thus, the encryption function maps a partition of the plaintext space to a partition of the ciphertext space, no matter the cipher key used. More precisely, this property still holds with independent round keys, and hence the theoretical framework of Chapter 3 applies.

Since the diffusion layer of TBC is strongly proper over 1 round, we know that the S-box $S$ maps a non-trivial linear partition $\mathcal{L}(V)$ to another partition $\mathcal{L}(W)$. Actually, $S$ preserves the partition $\mathcal{L}(V)$ where $V$ is the subspace of $\mathbb{F}_{2}^{6}$ defined to be

$$
V=\operatorname{span}(20,08,02)=\left\{\left(x_{5}, 0, x_{3}, 0, x_{1}, 0\right) \mid x_{5}, x_{3}, x_{1} \in \mathbb{F}_{2}\right\} .
$$

Probably the simplest complement subspace $U$ of $V$ in $\mathbb{F}_{2}^{6}$ is

$$
U=\operatorname{span}(10,04,01)=\left\{\left(0, x_{4}, 0, x_{2}, 0, x_{0}\right) \mid x_{4}, x_{2}, x_{0} \in \mathbb{F}_{2}\right\} .
$$

Therefore, $\mathcal{L}(V)$ is equal to $\{u+V \mid u \in U\}$. Knowing that $S$ preserves $\mathcal{L}(V)$, it is easily seen that the substitution layer preserves any linear partition of the form

$$
\mathcal{L}\left(\prod_{i=0}^{5} E_{i}\right) \quad \text { where for each } i, E_{i}=\left\{0_{6}\right\} \text { or } E_{i}=V \text { or } E_{i}=\mathbb{F}_{2}^{6} .
$$

Denote by $\pi$ the diffusion layer of TBC. If $\pi$ maps the subspace $E=\prod_{i=0}^{5} E_{i}$ to $E^{\prime}=\prod_{i=0}^{5} E_{i}^{\prime}$, then one (and only one) of the following cases holds

- $E=E^{\prime}=\left(V \times\left\{0_{6}\right\}\right)^{3}$,
- $E=V^{6}$ and $E^{\prime}=\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}$,
- $E=\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}$ and $E^{\prime}=V^{6}$,
- $E=E^{\prime}=\left(\mathbb{F}_{2}^{6} \times V\right)^{3}$.

All these cases are illustrated in Figure 4.14. Next, we can easily derive the next theorem from Proposition 3.23 and 3.25 .

Theorem 4.29 (TBC Round Function). The round function $F$ of TBC preserves at the same time the linear partitions $\mathcal{L}\left(\left(V \times\left\{0_{6}\right\}\right)^{3}\right)$ and $\mathcal{L}\left(\left(\mathbb{F}_{2}^{6} \times V\right)^{3}\right)$. Moreover, it maps $\mathcal{L}\left(\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}\right)$ to $\mathcal{L}\left(V^{6}\right)$ and vice versa. Since the encryption function is a composition of 21 round functions with a final round key addition, the same result holds for the whole encryption process.


Figure 4.14: Spaces used by the linear mappings of TBC.

## Chapter 4 - Analysis of a Backdoor S-Box

### 4.3.3.a. Basic and Multiple Partitions Attacks

In Chapter 3 Section 3.1.3, we have presented several ways to exploit such a backdoor following Paterson's work [88]. Denoting by $G$ the group generated by the round functions, Theorem 4.29 ensures that $\mathcal{L}\left(\left(V \times\left\{0_{6}\right\}\right)^{3}\right)$ and $\mathcal{L}\left(\left(\mathbb{F}_{2}^{6} \times V\right)^{3}\right)$ are two $G$-invariant partitions. Consider for instance the partition $\mathcal{B}=\mathcal{L}\left(\left(V \times\left\{0_{6}\right\}\right)^{3}\right)$. First, we need an efficient description of $\mathcal{B}$, namely we require that

- it must be easy to give one representative message for each part of $\mathcal{B}$,
- given a message $x$, it must be easy to enumerate all the messages lying in the same part of $\mathcal{B}$ as $x$.
Because $U$ is a complement subspace of $V$, the subspace $\left(U \times \mathbb{F}_{2}^{6}\right)^{3}$ is a complement of $\left(V \times\left\{0_{6}\right\}\right)^{3}$ in $\left(\mathbb{F}_{2}^{6}\right)^{6}$. Hence, we have

$$
\mathcal{L}\left(\left(V \times\left\{0_{6}\right\}\right)^{3}\right)=\left\{u+\left(V \times\left\{0_{6}\right\}\right)^{3} \mid u \in\left(U \times \mathbb{F}_{2}^{6}\right)^{3}\right\} .
$$

Thus, each message in $\left(\mathbb{F}_{2}^{6}\right)^{6}$ can be written as

$$
\begin{array}{r}
\left(\left(v_{00}, u_{01}, v_{02}, u_{03}, v_{04}, u_{05}\right),\left(u_{10}, u_{11}, u_{12}, u_{13}, u_{14}, u_{15}\right),\left(v_{20}, u_{21}, v_{22}, u_{23}, v_{24}, u_{25}\right)\right. \\
\left.\quad\left(u_{30}, u_{31}, u_{32}, u_{33}, u_{34}, u_{35}\right),\left(v_{40}, u_{41}, v_{42}, u_{43}, v_{44}, u_{45}\right),\left(u_{50}, u_{51}, u_{52}, u_{53}, u_{54}, u_{55}\right)\right) .
\end{array}
$$

The bits $u_{i}$ give the coset representative of the message and bits $v_{i}$ represent its index within this coset.

We can now present a basic cryptanalysis. Let $K$ be an unknown cipher key and denote by $E_{K}$ the encryption function of TBC associated with $K$. For each $u$ in $\left(U \times \mathbb{F}_{2}^{6}\right)^{3}$, require its encryption $c=E_{K}(u)$ and denote by $c_{u}$ its coset representative in $\left(U \times \mathbb{F}_{2}^{6}\right)^{3}$. Thus, we have to store $2^{27}$ pairs $\left(u, c_{u}\right)$. Next, assume that we are given an unknown ciphertext $c$. We can then compute its coset representative $c_{u}$ and obtain a representative of the corresponding plaintext. In other words, the plaintext lies in the set $c_{u}+\left(V \times\left\{0_{6}\right\}\right)^{3}$.

To summarize, this cryptanalysis requires $2^{27}$ chosen plaintexts. Then, we recover $2^{9}$ plaintext candidates for each unknown ciphertext, compromising seriously the security of TBC. Inversely, the same cryptanalysis based on the partition $\mathcal{L}\left(\left(\mathbb{F}_{2}^{6} \times V\right)^{3}\right)$ requires only $2^{9}$ chosen plaintexts but yields 27 bits of uncertainty on each plaintext.

Finally, it is a simple matter to verify that this cryptanalysis can be generalized to any partition-based backdoor cipher. Knowing that the encryption function maps $\mathcal{L}\left(\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}\right)$ to $\mathcal{L}\left(V^{6}\right)$, we can attack the cipher with $2^{18}$ chosen plaintexts. Then we can recover 18 bits of the plaintext corresponding to an unknown ciphertext. Since the encryption process also maps $\mathcal{L}\left(V^{6}\right)$ to $\mathcal{L}\left(\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}\right)$, we deduce another cryptanalysis with the same parameters. Nonetheless, these two attacks can be combined as described in Section 3.1.3. The resulting cryptanalysis needs $2 \times 2^{18}$ chosen plaintexts but can then recover 27 bits of any plaintext.

### 4.3.3.b. Key Schedule Dependent Attack

Even if this last cryptanalysis gives a clear advantage to any attacker aware of the backdoor, we can do much better using a key schedule dependent attack. As can
be seen in Figure 4.14, the diffusion $D$ preserves the partitions $\mathcal{L}\left(V \times\left\{0_{6}\right\}\right)$ and $\mathcal{L}\left(\mathbb{F}_{2}^{6} \times V\right)$, maps $\mathcal{L}\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)$ to $\mathcal{L}\left(V^{2}\right)$ and maps $\mathcal{L}\left(V^{2}\right)$ to $\mathcal{L}\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)$. Referring now to Figure 4.13, it is straightforward to check that Theorem 4.29 still holds if we consider the round function of the key schedule.

Corollary 4.30 (TBC Key Schedule). Each round $G_{i}$ of TBC key schedule preserves $\mathcal{L}\left(\left(V \times\left\{0_{6}\right\}\right)^{3}\right)$ and $\mathcal{L}\left(\left(\mathbb{F}_{2}^{6} \times V\right)^{3}\right)$. In addition, it maps $\mathcal{L}\left(\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}\right)$ to $\mathcal{L}\left(V^{6}\right)$ and inversely.

Assume that $A$ and $B$ are two subspaces of $\mathbb{F}_{2}^{36}$ such that for each round key $k$ the round function $F_{k}$ maps $\mathcal{L}(A)$ to $\mathcal{L}(B)$. Consider two round keys $k$ and $k^{\prime}$ lying in the same coset of $A$. Since the linear partition $\mathcal{L}(A)$ is equal to the quotient space $\mathbb{F}_{2}^{36} / A$ and since the cosets $k+A$ and $k^{\prime}+A$ are equal, the key additions $\alpha_{k}$ and $\alpha_{k^{\prime}}$ induce the same permutation of $\mathcal{L}(A)$. As a consequence, for each message $x$ in $\mathbb{F}_{2}^{36}$, it holds that

$$
F_{k}(x+A)=F_{k^{\prime}}(x+A) \quad \text { or equivalently } \quad F_{k}(x)+B=F_{k^{\prime}}(x)+B .
$$

Combining this observation with Corollary 4.30, we deduce the following theorem.
Theorem 4.31 (Key Schedule Dependent Attack). Denote by $(\mathcal{L}(A), \mathcal{L}(B))$ an input/output partition pair given by Theorem 4.29. If two cipher keys $K$ and $K^{\prime}$ lie in the same coset of $A$, then for each message $x$ in $\mathbb{F}_{2}^{36}$, we have

$$
E_{K}(x)+B=E_{K^{\prime}}(x)+B .
$$

Let us now detail an efficient key schedule dependent cryptanalysis of TBC. Let $K$ be the unknown cipher key. Then obtain a few plaintext/ciphertext pairs $\left(p_{i}, c_{i}\right)$. According to our experiments, only two or three pairs are sufficient. For simplicity of explanation, denote the cipher key $K$ by

$$
\begin{aligned}
& \left(\left(v_{00}, u_{01}, v_{02}, u_{03}, v_{04}, u_{05}\right),\left(v_{10}, u_{11}, v_{12}, u_{13}, v_{14}, u_{15}\right),\left(v_{20}, u_{21}, v_{22}, u_{23}, v_{24}, u_{25}\right),\right. \\
& \left.\quad\left(v_{30}, u_{31}, v_{32}, u_{33}, v_{34}, u_{35}\right),\left(v_{40}, u_{41}, v_{42}, u_{43}, v_{44}, u_{45}\right),\left(v_{50}, u_{51}, v_{52}, u_{53}, v_{54}, u_{55}\right)\right) .
\end{aligned}
$$

The first step considers the subspaces $A=B=\left(\mathbb{F}_{2}^{6} \times V\right)^{3}$. According to Theorem 4.31, if a cipher key $K^{\prime}$ lies in the same coset of $A$ as $K$, then for each index $i, E_{K^{\prime}}\left(p_{i}\right)$ and $c_{i}$ lie in the same coset of $B$. This property can be used in the following key recovery attack.

1. For each representative $K^{\prime}$ in $\left(\left\{0_{6}\right\} \times U\right)^{3}$, test whether $E_{K^{\prime}}\left(p_{i}\right)$ and $c_{i}$ lie in the same coset of $\left(\mathbb{F}_{2}^{6} \times V\right)^{3}$ for each index $i$.

Among the $2^{9}$ representatives tested, it should remain only one or two candidates. Thus, we can assume that we now know the bits $u_{i j}$ for all $i, j$ in $\{1,3,5\}$. For the second step, consider the subspaces $A=V^{6}$ and $B=\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}$.
2. For each candidate representative found in step 1 ,

Denote by $\left(u_{i j}\right)_{i, j \in\{1,3,5\}}$ the bits found previously.

## Chapter 4 - Analysis of a Backdoor S-Box

For each representative $K^{\prime}$ in $U^{6}$ such that $u_{i j}^{\prime}=u_{i j}$ for all $i, j$ in $\{1,3,5\}$, test whether $E_{K^{\prime}}\left(p_{i}\right)$ and $c_{i}$ lie in the same coset of $\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}$ for each index $i$.

After this step, we can assume that we know the bits $u_{i j}$ for all $0 \leq i<6$ and $j$ in $\{1,3,5\}$. For the third step, consider the subspaces $A=B=\left(V \times\left\{0_{6}\right\}\right)^{3}$.
3. For each candidate representative found in step 2 ,

Denote by $\left(u_{i j}\right)_{0 \leq i<6, j \in\{1,3,5\}}$ the bits found previously.
For each representative $K^{\prime}$ in $\left(U \times \mathbb{F}_{2}^{6}\right)^{3}$ such that $u_{i j}^{\prime}=u_{i j}$ for all $i, j$, test whether $E_{K^{\prime}}\left(p_{i}\right)$ and $c_{i}$ lie in the same coset of $\left(V \times\left\{0_{6}\right\}\right)^{3}$ for each index $i$.

Now, we know all the cipher key bits except $\left(v_{i j}\right)_{i, j \in\{0,2,4\}}$. These nine remaining bits are found with an exhaustive search.
4. For each candidate representative found in step 3,

Denote by $\left(u_{i j}\right)_{i j}$ and $\left(v_{i j}\right)_{i, j \in\{0,2,4\}}$ the bits found previously.
For each cipher $K^{\prime}$ such that $u_{i j}^{\prime}=u_{i j}$ and $v_{i j}^{\prime}=v_{i j}$, test whether $E_{K^{\prime}}\left(p_{i}\right)=$ $c_{i}$ holds for each index $i$.
A candidate cipher key in step 4 is almost always equal to the true cipher key $K$.
Using two pairs $\left(p_{i}, c_{i}\right)$, each step requires at most $2 \times 2^{9}$ encryptions. Assuming that there is only one candidate after each step, this cryptanalysis computes $4 \times 2^{10}=$ $2^{12}$ encryptions to recover the cipher key. We found experimentally that on average, this attack performs almost $2^{10}$ encryptions.

### 4.3.4. The Flaws of This Cipher

The main flaw of TBC is that the S-boxes are incomplete, namely there are some output bits independent of some input bits. Unfortunately, the whole encryption function inherits this bad property. For instance, for any message $x$ in $\left(\mathbb{F}_{2}^{6}\right)^{6}$ we have

$$
E_{K}\left(x+\left(\mathbb{F}_{2}^{6} \times\left\{0_{6}\right\}\right)^{3}\right)=E_{K}\left(\left\{\left(y_{0}, x_{1}, y_{2}, x_{3}, y_{4}, x_{5}\right) \mid y_{0}, y_{2}, y_{4} \in \mathbb{F}_{2}^{6}\right\}\right)=E_{K}(x)+V^{6} .
$$

As a consequence, every output bits which has odd index is independent of the bundles 1,3 , and 5 . This proves that TBC cannot seem to be secure, even when we are not aware of the backdoor.

The second flaw of TBC relies on an attack introduced by Knudsen in 60], called truncated differential cryptanalysis. An $n$-bit truncated difference pattern $a$ is an element of $\{0,1, \star\}^{n}$. By the set of the difference patterns associated with $a$, we mean

$$
\{a\}=\left\{\left(x_{0}, \ldots, x_{n-1}\right) \in \mathbb{F}_{2}^{n} \mid \forall i<n,\left(a_{i} \in \mathbb{F}_{2} \Rightarrow x_{i}=a_{i}\right)\right\} .
$$

For instance, the set associated with the truncated pattern $(1 \star 01 \star)$ is

$$
\{1 \star 01 \star\}=\{10010,10011,11010,11011\} .
$$

Alternatively, a truncated difference pattern can be seen as a collection of difference patterns. Then an $r$-round truncated differential is a pair $(a, b)$ of truncated patterns
which predicts that if two plaintexts have a difference lying in $\{a\}$, then their corresponding ciphertexts have a difference lying in $\{b\}$ with some probability. As explained in [64, pp. 156], the term truncated draws attention to the fact that only some bits of the output difference are predicted.

Caranti et al. established a link between imprimitive ciphers and truncated differential cryptanalysis in [31, Corollary 4.1]. Their result can be easily generalized to partition-based backdoor ciphers with independent round keys.

Proposition 4.32. Let $E$ be a partition-based backdoor cipher mapping $\mathcal{L}(V)$ to $\mathcal{L}(W)$. If the difference of two plaintexts lies in $V$, then the difference of their ciphertexts lies in $W$.

Proof. Consider two plaintexts $p$ and $p^{\prime}$ such that $p+p^{\prime}$ is in $V$. Then, there exists $v$ in $V$ such that $p=p^{\prime}+v$ and hence $p$ and $p^{\prime}$ lis in the same coset of $V$. Since $E_{K}$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W), E_{K}(p)$ belongs to the same coset of $W$ as $E_{K}\left(p^{\prime}\right)$. The result follows.

Now, observe that the subspace $V$ used in the backdoor of TBC can be written as $V=\{\star 0 \star 0 \star 0\}$. Combining this observation with Proposition 4.32, it is easily seen that each input/output partitions pairs of Theorem 4.29 yields a truncated differential with probability 1 . However, we can argue that finding such a truncated differential is equivalent to recover the backdoor.

This link with truncated differential cryptanalysis also affects the resistance of TBC with respect to classical differential cryptanalysis. Indeed, we have just seen that the truncated differential $(a, b)$ where

$$
a=b=(0 \star 0 \star 0 \star, 000000,0 \star 0 \star 0 \star, 000000,0 \star 0 \star 0 \star, 000000)
$$

holds with probability ones over any number of rounds since the round function preserves the partition $\mathcal{L}\left(\left(V \times 0_{6}\right)^{3}\right)$. Consequently, the (classical) differential ( $a, b$ ) with

$$
a=b=(20,00,00,00,00,00)
$$

also holds with high probability. Our experiments showed that this probability is close to $2^{-9}$. Therefore, TBC is vulnerable to differential cryptanalysis, even if it seemed secure using the heuristic measure.

### 4.4. Preventing Partition-Based Backdoors

To conclude this theoretical treatment of partition-based backdoor ciphers, we will now present two criteria to prove that an SPN does not have such a backdoor. In the previous chapter, we have considered a generic SPN which maps a partition of the plaintext to a partition of the ciphertexts independently of the round keys used. We have then proven that when its diffusion layer is strongly proper, at least one of its S-boxes must map a linear partition to another one. In this chapter, the differential and linear properties of such S-boxes have been studied. We then
derive lower bounds on their resistance to these attacks in Corollaries 4.19, 4.26 and Remark 4.20. Therefore, if all the S-boxes of an SPN have a better resistance than what is possible to achieve using backdoor S-boxes, then the cipher does not have a partition-based backdoor. This proves the following theorem.

Theorem 4.33. Consider an $n m$-bit substitution permutation network with $m$ S-boxes over $\mathbb{F}_{2}^{n}$. Assume that its diffusion layer is strongly proper over $r$ rounds. If each S-box $S_{i}$ is such that for each $1 \leq d \leq n-1$, the values $\mathrm{LP}_{S_{i}}^{\max }$ and $\mathrm{DP}_{S_{i}}^{\max }$ are less than the bounds given in Figure 4.10, then the SPN does not have a partition-based backdoor holding with independent round keys.

Moreover, if the values $\mathrm{LP}_{S_{i}}^{\max }$ and $\mathrm{DP}_{S_{i}}^{\max }$ are significantly less than the bounds in Figure 4.10, then the SPN is unlikely to be a probabilistic partition-based backdoor cipher. For instance, this criterion can be used to prove that the AES [39] is not a (probabilistic) partition-based backdoor cipher. As explained in [23], its diffusion layer is strongly proper over 2 rounds. In addition, the maximum linear potential and differential probability of the AES S-box are far below the lower bounds given in Figure 4.10, no matter what the dimension $d$ of the subspace $V$ is. As a consequence, this S-box does not map any linear partition to another one.

The results of this chapter can also be used to recover a partition-based backdoor. Consider an S-box $S$ mapping a linear partition $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Paying particular attention to the correlation and differential probability matrices of $S$, it should not be difficult to recover the subspaces $V$ and $W$. Indeed, Theorems 4.17 and 4.25 suggest to consider the greatest coefficients of these matrices to recover the subspaces $V^{\perp}$ and $V$ respectively, provided that $V$ is equal to $W$. However, using Proposition 4.1 and Equations (4.2) and (4.4) it is straightforward to generalize these theorems to S -boxes mapping a linear partition to another one.

The second criteria is due to Calderini and was introduced recently in [23]. In this paper, the author considers translation-based cipher, a family of ciphers introduced in [30] which generalizes our definition of SPN. Intuitively, a translation-based cipher is a substitution-permutation network in which the substitution and diffusion layers can be round-dependent. Moreover, the key-schedule must be surjective for at least one round, which is normally the case. We restate below Calderini's criteria for substitution-permutation networks.

Definition 4.34 (Strongly d-Anti-Invariant S-Box [30]). Let $f: \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ be a mapping satisfying $f\left(0_{n}\right)=0_{n}$ and let $1 \leq d<n$. The mapping $f$ is said to be strongly $d$-anti-invariant if any proper subspace $V$ of $\mathbb{F}_{2}^{n}$ whose image $f(V)$ is also a subspace of $\mathbb{F}_{2}^{n}$ has dimension strictly less than $n-d$.
An S-box $S$ is said to be strongly $d$-anti-invariant if its equivalent S-box $S^{\prime}$ defined by the formula $S^{\prime}(x)=S(x)+S(0)$ is strongly $d$-anti-invariant.

Remark 4.35. If $S$ is strongly $d$-anti-invariant, then $S$ is also $i$-anti-invariant for each $1 \leq i \leq d$. As proven in [4], $S$ is strongly 1-anti-invariant if and only if $\mathrm{LP}_{S}^{\max }<1$.

Proposition 4.36. Assume that for each S-box $S_{i}$, there exists an integer $d_{i}<n$ such that the following two conditions hold:

- $2^{n} \times \mathrm{DP}_{S_{i}}^{\max } \leq 2^{d r_{i}}$,
- $S_{i}$ is strongly $\left(d_{i}-1\right)$-anti-invariant.

The permutation $\sigma$ maps a linear partition $\mathcal{L}(V)$ to another linear partition $\mathcal{L}(W)$ if and only if both $V$ and $W$ are walls.

Theorem 4.37. Suppose that the substitution layer satisfies the two conditions of Proposition 4.36 and that the diffusion layer is strongly proper over $r$ rounds. Then, the SPN is not a partition-based backdoor cipher.

This result is complementary to our criteria since it gives other conditions. However, we will see in the next chapter that it gives no information about probabilistic partition-based backdoor ciphers.

Chapter 4 - Analysis of a Backdoor S-Box


## Backdoored Encryption Algorithm 1

BEA-1 (standing for Backdoored Encryption Algorithm) is a real-size probabilistic partition-based backdoor ciphers whose design relies on the theory developed in Chapters 3 and 4 . This cipher is largely inspired by the AES, the current standard of block ciphers, and is proven to be practically secure against linear and differential cryptanalysis. Nonetheless, the backdoor enables recovery of the full 120-bit cipher key in just a few seconds on a laptop computer using only $2^{16}$ chosen plaintext blocks. The success probability of this cryptanalysis was experimentally verified to be greater that $95 \%$.

This chapter is organized as follows. First, the specification of the cipher BEA-1 and its security analysis against linear and differential cryptanalysis are given in Section 5.1. Next, Section 5.2 explores the hidden property of the algorithm and its design. Secondly, the main idea of the cryptanalysis is illustrated and formalized in Section 5.3. The full cryptanalysis of BEA-1 is then detailed in Section 5.4. To conclude, we compare our attack to Harpes' partitioning cryptanalysis and expose some advantages of probabilistic partition-based backdoors. Our cipher BEA-1 was introduced as a challenge in [10]. Its cryptanalysis was then outlined in [11] and described in [12].

### 5.1. Presentation of BEA-1

The cipher BEA-1 is directly inspired by Rijndael [39, the block cipher designed by Joan Daemen and Vincent Rijmen, now known as the AES [85]. Our algorithm encrypts 80-bit plaintext blocks using a 120-bit cipher key. Unlike the AES, the internal state is not seen as a matrix of bytes but as an array of 10 -bit bundles. Therefore, the message and key spaces are respectively $\left(\mathbb{F}_{2}^{10}\right)^{8}$ and $\left(\mathbb{F}_{2}^{10}\right)^{12}$.

### 5.1.1. Specification of the Encryption Process

The encryption consists in applying eleven times a simple keyed operation called round function to the data block. A different 80 -bit round key is used for each iteration of the round function. Since the last round is slightly different and uses

## Chapter 5 - Backdoored Encryption Algorithm 1

two round keys, the encryption requires twelve 80 -bit round keys. These round keys are derived from the 120-bit cipher key using a key schedule.

Like any other Substitution-Permutation Network, the round function is made up of three stages: a key addition, a substitution layer and a diffusion layer.

- The key addition is just a bitwise "exclusive or" (XOR) between the data block and the round key.
- The substitution layer consists in the parallel evaluation of four different 10 -bit S-boxes and is the only part of the cipher which is not affine. These S-boxes are referred to as $S_{0}, S_{1}, S_{2}, S_{3}$ and are defined in Figures A.5, A.7, A. 9 and A. 11 given in Appendix. They should not be confused with the secret S-boxes $\mathbf{S}_{0}, \mathbf{S}_{1}, \mathbf{S}_{2}$ and $\mathbf{S}_{3}$, only used in the design and the cryptanalysis of BEA-1.
- Following the design principles of the AES, the diffusion layer comes in two parts: the ShiftRows and the MixColumns operations. The first part is a bundle permutation. The second evaluates in parallel the linear transformation $M:\left(\mathbb{F}_{2}^{10}\right)^{4} \rightarrow\left(\mathbb{F}_{2}^{10}\right)^{4}$ processing four 10 -bit bundles. Because of its linearity, $M$ is only defined over the standard basis of $\left(\mathbb{F}_{2}^{10}\right)^{4}$ in Figure A. 3 in Appendix. For convenience, its inverse $M^{-1}$ is also in the same figure.
The pseudo-code for the key schedule is given in Figure 5.1 together with an illustration providing an overview of its structure. This representation also emphasizes the similarities between the key schedules of BEA-1 and Rijndael. In the same way, Figure 5.2 describes the encryption process of BEA-1.

Remark 5.1. The decryption is straightforward from the encryption since all the transformations are bijective. Thus, to decrypt, we just have to apply the inverse operations in the reverse order. It should be stressed that the key addition and the ShiftRows are involutions, therefore the same operations are used in the decryption process. Finally, note that the inverse S-boxes are not given here but can be computed by using the equation $S_{i}^{-1}(S(x))=x$ holding for each $x$ in $\mathbb{F}_{2}^{10}$.

### 5.1.2. Differential and Linear Cryptanalysis

The differential and linear branch numbers of the linear transformation were recalled in Section 1.5.2. With an exhaustive search, it can be checked that the branch numbers of $M$ are both equal to five, which is the maximum. According to Theorem 1.52 , any 2 -round trail actives at least five S -boxes. Thus, a 10 -round trail actives at least 25 S-boxes.

It is not hard to verify with a computer that every S -box has a maximum differential probability less than $\frac{40}{2^{10}}=1.25 \times 2^{-5}$ and a maximum linear potential equal to $2^{-4}$. Therefore, the differential probability and linear potential of any 10 -round trail are upper-bounded by $\left(1.25 \times 2^{-5}\right)^{25} \approx 1.03 \times 2^{-117}$ and $\left(2^{-4}\right)^{25}=2^{-100}$ respectively. Consequently, a differential cryptanalysis of the 10 -round version of our cipher would require at least $2^{117}$ chosen plaintext/ciphertext pairs and a linear cryptanalysis would require $2^{100}$ known plaintext/ciphertext pairs.

Even if this is a rough approximation since it does not take into account the inter-column diffusion provided by the ShiftRows operation, it suffices to prove the

```
Algorithm 5 - ExpandKey
Input. The 120 -bit cipher key \(K=\left(K_{0}, \ldots, K_{11}\right) \in\left(\mathbb{F}_{2}^{10}\right)^{12}\).
Output. The twelve 80-bit round keys \(k^{[0]}, \ldots, k^{[11]} \in\left(\mathbb{F}_{2}^{10}\right)^{8}\).
\({ }_{1}\left(k_{0}, \ldots, k_{11}\right) \leftarrow\left(K_{0}, \ldots, K_{11}\right)\)
2 For i from 0 to 6 do
    \(x \leftarrow M\left(k_{12 i+8}, \ldots, k_{12 i+11}\right)\)
    \(x \leftarrow\left(S_{j}\left(x_{j}\right)\right)_{j<4}\)
    \(x \leftarrow\left(x_{0} \oplus\left(3^{i} \bmod 2^{10}\right), x_{1}, x_{2}, x_{3}\right)\)
    \(\left(k_{12 i+12}, \ldots, k_{12 i+15}\right) \leftarrow\left(k_{12 i+0}, \ldots, k_{12 i+3}\right) \oplus x\)
    \(\left(k_{12 i+16}, \ldots, k_{12 i+19}\right) \leftarrow\left(k_{12 i+4}, \ldots, k_{12 i+7}\right) \oplus\left(k_{12 i+12}, \ldots, k_{12 i+15}\right)\)
    \(\left(k_{12 i+20}, \ldots, k_{12 i+23}\right) \leftarrow\left(k_{12 i+8}, \ldots, k_{12 i+11}\right) \oplus\left(k_{12 i+16}, \ldots, k_{12 i+19}\right)\)
For r from 0 to 11 do
    \(k^{[r]} \leftarrow\left(k_{8 r+i}\right)_{i<8}\)
Return \(k^{[0]}, \ldots, k^{[11]}\)
```



Figure 5.1: The key schedule of BEA-1.

## Chapter 5 - Backdoored Encryption Algorithm 1

## Algorithm 6 - Encrypt

Input. The 120 -bit master key $K \in\left(\mathbb{F}_{2}^{10}\right)^{12}$ and the 80 -bit plaintext block $p \in\left(\mathbb{F}_{2}^{10}\right)^{8}$. Output. The 80-bit ciphertext block $c \in\left(\mathbb{F}_{2}^{10}\right)^{8}$.

```
\(1 \quad k^{[0]}, \ldots, k^{[11]} \leftarrow \operatorname{ExpandKey}(K)\)
\(2 x \leftarrow p\)
3 For r from 0 to 9 do
\({ }^{4} \quad x \leftarrow x \oplus k^{[r]} \quad\) AddRoundKey
\(5 \quad x \leftarrow\left(S_{i \bmod 4}\left(x_{i}\right)\right)_{i<8}\)
    \(x \leftarrow\left(x_{0}, x_{5}, x_{2}, x_{7}, x_{4}, x_{1}, x_{6}, x_{3}\right)\)
    SubBundles
    ShiftRows
\({ }^{7} \quad\llcorner\leftarrow(M \| M)(x)\)
    MixColumns
\(8 \quad x \leftarrow x \oplus k^{[10]}\)
AddRoundKey
\({ }^{9} x \leftarrow\left(S_{i \bmod 4}\left(x_{i}\right)\right)_{i<8}\)
    SubBundles
\({ }_{10} x \leftarrow\left(x_{0}, x_{5}, x_{2}, x_{7}, x_{4}, x_{1}, x_{6}, x_{3}\right)\)
\(11 x \leftarrow x \oplus k^{[11]}\)
    ShiftRows
AddRoundKey
12 Return \(x\)
```



Figure 5.2: The round function of BEA-1.
cipher's practical resistance against classical differential and linear cryptanalysis. In fact, there are only $2^{80}$ different plaintext/ciphertext pairs for a fixed cipher key.

### 5.2. Design of the Backdoor

The presentation of secret structure of BEA-1 comes in two parts. First, Section 5.2.1 explains the nature of this backdoor and provides all the results needed to address the cryptanalysis. Then, the design of BEA-1's building-blocks is given in Sections 5.2.2 and 5.2.3. The reader who just wants to understand how the backdoor works can skip these two sections. Indeed, they are more technical and are also independent of the remainder of this chapter.

### 5.2.1. The Linear Partitions Throughout the Encryption

As said in introduction, the backdoor of BEA-1 relies on the theoretical framework developed in Chapters 3 and 4. Thus, it should not be surprising that linear partitions must play a key role in it. For this purpose, let us introduce the following 5-dimensional subspaces of $\mathbb{F}_{2}^{10}$

$$
\begin{array}{ll}
V_{0}=\operatorname{span}(266,343,3 \mathrm{ED}, 354,17 \mathrm{~F}), & W_{0}=\operatorname{span}(16 \mathrm{~A}, 11 \mathrm{~B}, 306,05 \mathrm{E}, 0 \mathrm{~B} 8), \\
V_{1}=\operatorname{span}(398,229,34 \mathrm{C}, 251,37 \mathrm{~B}), & W_{1}=\operatorname{span}(04 \mathrm{~B}, 3 \mathrm{~B} 7,0 \mathrm{D} 5,027,2 \mathrm{C} 8), \\
V_{2}=\operatorname{span}(0 \mathrm{BA}, 155,307,37 \mathrm{E}, 318), & W_{2}=\operatorname{span}(1 \mathrm{~A} 9,095,107,36 \mathrm{~F}, 2 \mathrm{~A} 3), \\
V_{3}=\operatorname{span}(1 \mathrm{D} 1,21 \mathrm{E}, 134,0 \mathrm{DC}, 15 \mathrm{~A}), & W_{3}=\operatorname{span}(0 \mathrm{~F} 0,2 \mathrm{FE}, 191,332,1 \mathrm{~A} 6) .
\end{array}
$$

Denote by $V$ and $W$ the 40-dimensional subspaces $\prod_{i=0}^{7} V_{i \bmod 4}$ and $\prod_{i=0}^{7} W_{i \bmod 4}$ of message space $\left(\mathbb{F}_{2}^{10}\right)^{8}$. Therefore, the linear partitions $\mathcal{L}(V)$ and $\mathcal{L}(W)$ are both made up with $2^{40}$ cosets, each containing $2^{40}$ elements.

The S-boxes $S_{0}, S_{1}, S_{2}$ and $S_{3}$ given in the specification of BEA-1 are actually derived from the secret S-boxes $\mathbf{S}_{0}, \mathbf{S}_{1}, \mathbf{S}_{2}$ and $\mathbf{S}_{3}$ given in Figures A.4, A.6, A. 8 and A. 10 in Appendix. The relation between the secret $S$-boxes $\mathbf{S}_{i}$ and their modified versions $S_{i}$ will be detailed later in Section 5.2.2. In the first place, let us state the following theorem relating BEA-1 to the theory of partition-based backdoor ciphers.

Theorem 5.2. Consider the encryption function of BEA-1 where the modified S-boxes $S_{0}, S_{1}, S_{2}$ and $S_{3}$ are replaced with their secret counterparts $\mathbf{S}_{0}, \mathbf{S}_{1}, \mathbf{S}_{2}$ and $\mathrm{S}_{3}$. Then, the round function preserves the linear partition $\mathcal{L}(V)$ of $\left(\mathbb{F}_{2}^{10}\right)^{8}$ and the last round maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$, no matter the round keys used. As a consequence, the full encryption maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$.

More precisely, Figure 5.3 depicts the evolution of the linear partition $\mathcal{L}(V)$ throughout each primitive of the secret encryption process. For instance, we can see that the S -box $\mathbf{S}_{i}$ maps the linear partition $\mathcal{L}\left(V_{i}\right)$ to $\mathcal{L}\left(W_{i}\right)$ and hence the substitution layer maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Similarly, the diffusion layer comes back to the original partition since it maps $\mathcal{L}(W)$ to $\mathcal{L}(V)$.

## Chapter 5 - Backdoored Encryption Algorithm 1



Figure 5.3: The linear partitions throughout the round function.

Remark 5.3. Theorem 5.2, as well as Theorem 5.4 stated hereinafter, will be proven in Sections 5.2.2 and 5.2.3. Indeed, they establish the main properties of the backdoor and are hence closely related to the design of the cipher's primitives.

Thanks to Theorem 5.2, we can now explain our choices for the $V_{i}$ and $W_{i}$. Each of these subspaces of $\mathbb{F}_{2}^{10}$ is a 5 -dimensional linear code whose minimal distance is equal to 4 . This property ensures that the Hamming distance of any two different elements lying in the same coset is at least equal to 4 . The subspaces $V$ and $W$ of $\mathbb{F}_{2}^{80}$ inherit this property. Thus, if $p$ is a plaintext, then any other plaintext $p^{\prime}$ lying in the same coset of $V$ differs from $p$ in at least four bits. Considering the secret encryption function, Theorem 5.2 establishes that their ciphertexts $c$ and $c^{\prime}$ belong to the same coset of $W$. Thus, $c$ and $c^{\prime}$ have at least four different bits. As it will become clear in the next two sections, the subspaces $V_{i}$ and $W_{i}$ could have been freely chosen among the 5 -dimensional subspaces of $\mathbb{F}_{2}^{10}$. We surmised that using linear codes with high minimal distance should reduce the likelihood of observing the backdoor by accident, hence our choice for the $V_{i}$ and $W_{i}$.

Having explained the main property of the secret encryption function, now is the time to introduce the following theorem establishing a link between the secret cipher and BEA-1.

Theorem 5.4. Let $\mathbf{F}$ and $\mathbf{E}$ denote the round function and the encryption function of BEA-1 using the secret S-boxes. Let $p=p^{[0]}$ be any plaintext. Define the following elements with respect to the round keys $k^{[0]}, \ldots, k^{[10]}$ :

$$
p^{[i+1]}=F_{k}[i]\left(p^{[i]}\right) \quad \text { and } \quad \mathbf{p}^{[i+1]}=\mathbf{F}_{k}\left({ }^{[i]}\left(p^{[i]}\right) \quad \text { for } 0 \leq i<11 .\right.
$$

Assume that the round keys $k^{[0]}, \ldots, k^{[10]}$ are independent and uniformly distributed. The probability that all the equations $p^{[i]}=\mathbf{p}^{[i]}$ hold for each $1 \leq i \leq 11$ is given by

$$
\left(\left(\frac{944}{1024}\right)^{6} \times\left(\frac{925}{1024}\right)^{2}\right)^{11} \approx 2^{-11} .
$$

Therefore, the probability that $p$ is encrypted equally with $E$ and $\mathbf{E}$ can be approximated by $2^{-11}$.

Remark 5.5. The fact that the MixColumns operation is replaced with a key addition in the last round of BEA-1 does not matter in Theorem 5.4. For the sake of simplicity, we then ignore this detail. This explains why the last round key $k^{[11]}$ does not appear in the statement of this result.

Needless to say, the hypothesis that the round keys are independent and uniformly distributed is mathematically wrong in any practical cryptanalysis. Indeed, the twelve 80 -bit round keys are all extracted from one 120-bit cipher key. However, the cipher key needs to have (at least) 960 bits to provide independence and uniform distribution to its round keys. Such a cipher key must be related to the concept of long-key cipher, see Definition 1.8. Nonetheless, if the cipher key is uniformly distributed, the same applies for each round key.

In our cryptanalysis of BEA-1, we are given plaintexts with their ciphertexts encrypted under a fixed cipher key. Even if we forget about the independence of the round keys, each plaintext must be encrypted with a random cipher key to make use of Theorem 5.4.

Fortunately, our experiments suggest that the proportion of the plaintexts encrypted equally with $E_{K}$ and $\mathbf{E}_{K}$ is approximately $2^{-11}$, even when the round keys are derived from a fixed cipher key $K$. To put it another way, if $\mathcal{P}$ is a subset of the plaintext space $\left(\mathbb{F}_{2}^{10}\right)^{8}$, it seems reasonable to assume that

$$
\begin{equation*}
\#\left\{p \in \mathcal{P} \mid E_{K}(p)=\mathbf{E}_{K}(p)\right\} \approx \frac{\# \mathcal{P}}{2^{11}} \tag{5.1}
\end{equation*}
$$

Now, suppose that $\mathcal{P}$ is included in a coset of $V$ denoted by $x+V$. As the secret encryption function $\mathbf{E}_{K}$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$ (see Theorem 5.2), we know that the image of $\mathcal{P}$ under $\mathbf{E}_{K}$ is included in a coset of $W$. More precisely, Lemma 3.18 establishes that $\mathbf{E}_{K}(\mathcal{P})$ is included in $y+W$ where $y=\mathbf{E}_{K}(x)$. Hence,

$$
\begin{equation*}
\left\{p \in \mathcal{P} \mid E_{K}(p)=\mathbf{E}_{K}(p)\right\} \subseteq\left\{p \in \mathcal{P} \mid E_{K}(p) \in(y+W)\right\} \tag{5.2}
\end{equation*}
$$

Combining (5.1) with (5.2), we conclude that approximately $\# \mathcal{P} \times 2^{-11}$ ciphertexts in $\mathcal{C}=E_{k}(\mathcal{P})$ belong to $y+W$. In addition, we have observed that the ciphertexts $c=E_{K}(p)$ such that $E_{K}(p) \neq \mathbf{E}_{K}(p)$ are spread over the $2^{40}$ cosets of $W$.

The backdoor of BEA-1 is hence the following. First, choose a set $\mathcal{P}$ of $2^{16}$ plaintexts uniformly chosen in one coset $x+V$ and collect their ciphertexts $\mathcal{C}=E_{K}(\mathcal{P})$ encrypted under an unknown cipher key $K$. Then search for the most represented coset of $W$ in $\mathcal{C}$ and denote by $y$ one of its representatives. According to our experiments, this coset should have roughly $2^{16-11}=32$ elements and the second most represented coset is unlikely to have more than six elements. As a consequence of the preceding discussion, we know that the coset $x+V$ is mapped to $y+W$ by the secret encryption function $\mathbf{E}_{K}$. This information can then be used to recover the cipher key $K$ with a low computation cost, as detailed later in Sections 5.3 and 5.4.

To conclude this section, observe that no particular property of the key schedule has been used. It can be proven that each round of the key schedule preserves the linear partition $\mathcal{L}\left(\prod_{i=0}^{11} W_{i \bmod 4}\right)$, provided that the S-boxes $S_{i}$ are replaced with their

## Chapter 5 - Backdoored Encryption Algorithm 1

secret equivalents $\mathbf{S}_{i}$. This implies that if two cipher keys $K$ and $K^{\prime}$ are in the same coset of $\prod_{i=0}^{11} W_{i \bmod 4}$, then we can approximate the probability that each pair of round keys $k^{[i]}$ et $k^{\prime[i]}$ are in the same coset of $W$ by $\left(944^{3} \cdot 925 \cdot 2^{-40}\right)^{7} \approx 2^{-3.5}$. However, for this property to be easily exploitable, the round keys ought to stay in the same coset of $V$ instead of $W$ (which can be simply achieved by switching the mappings $M$ and ( $S_{0}\left\|S_{1}\right\| S_{2} \| S_{3}$ ) in the key schedule). Therefore, if compared with our cryptanalysis, this property appears not to be very useful and was intentionally left as a wrong track.

### 5.2.2. The Substitution Layer

The nature of the hidden property of BEA-1 having been emphasized, this and the following sections detail the design of the cipher's primitives and prove Theorems 5.2 and 5.4 stated above. As explained in introduction, these two sections are aimed at the reader who wants to understand how BEA-1 was made. For a first read, it is possible to jump directly to Section 5.3 explaining the basic principle of the cryptanalysis using the backdoor.

Let $\{0 *\}$ and $\{* 0\}$ denote respectively the subspaces $\left\{0_{5}\right\} \times \mathbb{F}_{2}^{5}$ and $\mathbb{F}_{2}^{5} \times\left\{0_{5}\right\}$ of $\mathbb{F}_{2}^{10}$. It should be noted that $\{* 0\}$ is a complement space of $\{0 *\}$ in $\mathbb{F}_{2}^{10}$. The design of each secret S-box $\mathbf{S}_{i}$ rests upon a permutation $\mathbf{S}_{i}^{\prime}$ of $\mathbb{F}_{2}^{10}$ preserving the linear partition $\mathcal{L}(\{0 *\})$. Following Theorem 4.4, we just need to choose a permutation $\rho_{i}$ of $\{* 0\}$ and a family $\left(\tau_{i, u}\right)_{u \in\{* 0\}}$ of permutations of $\{0 *\}$. Then, we define $\mathbf{S}_{i}^{\prime}$ for all $x=u+v$ in $\mathbb{F}_{2}^{10}$ to be

$$
\mathbf{S}_{i}^{\prime}(x)=\mathbf{S}_{i}^{\prime}(u+v)=\rho_{i}(u)+\tau_{i, u}(v),
$$

where $u$ is in $\{* 0\}$ and $v$ in $\{0 *\}$. The permutations $\rho_{i}$ and $\tau_{i, u}$ were selected following the method given in Section 4.2.3, in order to maximize the resistance of $\mathbf{S}_{i}^{\prime}$ against both differential and linear cryptanalysis.

Figure A. 1 in Appendix defines the linear mappings $L_{V_{i}}$ and $L_{W_{i}}($ for $0 \leq i<4)$ over the standard basis of $\mathbb{F}_{2}^{10}$. It is worthwhile to note that these mappings are automorphisms of $\mathbb{F}_{2}^{10}$. Moreover, $L_{V_{i}}(\{0 *\})=V_{i}$ and $L_{W_{i}}(\{0 *\})=W_{i}$. By virtue of Proposition 3.25 , we know that $L_{V_{i}}$ maps $\mathcal{L}(\{0 *\})$ to $\mathcal{L}\left(V_{i}\right)$ and that $L_{W_{i}}$ maps $\mathcal{L}(\{0 *\})$ to $\mathcal{L}\left(W_{i}\right)$. Last, but not least, define for each $0 \leq i<4$ the secret S-box $\mathbf{S}_{i}$ to be

$$
\mathbf{S}_{i}=L_{W_{i}} \circ \mathbf{S}_{i}^{\prime} \circ\left(L_{V_{i}}\right)^{-1} .
$$

These S-boxes are given in Figures A.4, A.6, A. 8 and A. 10 in Appendix. Obviously, $\left(L_{V_{i}}\right)^{-1}$ maps $\mathcal{L}\left(V_{i}\right)$ to $\mathcal{L}(\{0 *\})$, then $\mathbf{S}_{i}^{\prime}$ preserves $\mathcal{L}(\{0 *\})$, and $L_{W_{i}}$ maps $\mathcal{L}(\{0 *\})$ to $\mathcal{L}\left(W_{i}\right)$. This implies the following proposition.

Proposition 5.6. For each $0 \leq i<4$, the secret S-box $\mathbf{S}_{i}$ maps $\mathcal{L}\left(V_{i}\right)$ to $\mathcal{L}\left(W_{i}\right)$.
Remark 5.7. If the reader is interested in an explicit definition of the permutations $\rho_{i}$ and the families of permutations $\left(\tau_{i, u}\right)_{i \in\{* 0\}}$, they can be recovered in the following way. First, compute $\mathbf{S}_{i}^{\prime}=\left(L_{W_{i}}\right)^{-1} \circ \mathbf{S}_{i} \circ L_{V_{i}}$ using the tables of Figures A. 1 and A. 4
(or A.6, A.8, A.10). As noted previously, the permutation $\mathbf{S}_{i}^{\prime}$ preserves the linear partition $\mathcal{L}(\{0 *\})$. To obtain its decomposition, we just have to follow the proof of Theorem 4.4. Thus, for each $u$ in $\{* 0\}$, define $\rho_{i}(u)$ to be the unique element of $\{* 0\} \cup\left(\mathbf{S}_{i}^{\prime}(u)+\{0 *\}\right)$. It is not hard to see that $\rho_{i}(u)$ is simply equal to the element of $\mathbb{F}_{2}^{10}$ where the five leftmost bits are exactly the ones of $\mathbf{S}_{i}^{\prime}(u)$ and the five remaining bits are all zero. Lastly, for each $u$ in $\{* 0\}$, let $\tau_{i, u}$ be the permutation of $\{0 *\}$ defined to be $\tau_{i, u}(v)=\mathbf{S}_{i}^{\prime}(u+v)+\rho_{i}(u)$. Again, $\tau_{i, u}(v)$ is just the 10 -bit vector having its five leftmost bits all zero and its five rightmost bits identical to the ones of $\mathbf{S}_{i}^{\prime}(u+v)$. Naturally, the permutations $\rho_{i}$ and $\tau_{i, u}$ can be seen as permutations of $\mathbb{F}_{2}^{5}$ (instead of $\{* 0\}$ and $\{0 *\}$ ) to obtain the more convenient definition

$$
\mathbf{S}_{i}^{\prime}(u \| v)=\left(\rho_{i}(u) \| \tau_{i, u}(v)\right) .
$$

The modified S-boxes $S_{i}$ given in the specification of BEA-1 are such that $S_{i}(x)=\mathbf{S}_{i}(x)$ for almost all input $x$ in $\mathbb{F}_{2}^{10}$. For instance, $S_{0}(x)=\mathbf{S}_{0}(x)$ for all except 80 elements $x$ in $\mathbb{F}_{2}^{10}$. The images of these 80 particular points are emphasized in Figures A. 4 and A.5. These modifications were chosen so as to improve the differential and linear resistances of $S_{0}$ compared to the original secret S-box $\mathbf{S}_{0}$. More generally, $S_{i}$ and $\mathbf{S}_{i}$ have 80 different images for $i$ in $\{0,1,2\}$. The last modified S-box $S_{3}$ is less close to it secret equivalent since $S_{3}$ and $\mathbf{S}_{3}$ have 99 different images.

Consequently, if $x$ is uniformly distributed over $\mathbb{F}_{2}^{10}$, then the equality $S_{i}(x)=$ $\mathbf{S}_{i}(x)$ holds with probability $q_{i}$ where

$$
q_{0}=q_{1}=q_{2}=\frac{944}{1024} \quad \text { and } \quad q_{3}=\frac{925}{1024} .
$$

This implies that when $x$ is uniformly distributed over $\left(\mathbb{F}_{2}^{10}\right)^{8}$, the images of $x$ under the secret and the modified substitution layers are equal with probability $q=\left(\prod_{i=0}^{3} q_{i}\right)^{2}$.

Let $p=p^{[0]}$ be a plaintext. In the following, we use the notation of Theorem 5.4. If $k^{[i]}$ is uniformly distributed, then so is $p^{[i]}+k^{[i]}$. Thus, $p^{[i+1]}=F_{k}$ (i] $\left(p^{[i]}\right)$ is equal to $\mathbf{p}^{[i+1]}=\mathbf{F}_{k^{[i]}}\left(p^{[i]}\right)$ with probability $q$. Assuming moreover that the round keys are independent implies that the events $p^{[i]}=\mathbf{p}^{[i]}$ for each $1 \leq i \leq 11$ are independent. Therefore, the probability that the equalities $p^{[i]}=\mathbf{p}^{[i]}$ hold for all $1 \leq i \leq 11$ is given by $q^{11}$. This discussion proves Theorem 5.4.

### 5.2.3. The Diffusion Layer

Some components used to design the linear transformation $M$ are defined over the finite field $\mathbb{F}_{2^{5}}$. In order to have an explicit construction of this field, we consider the irreducible polynomial $X^{5}+X^{2}+1$ over $\mathbb{F}_{2}$ and define $\mathbb{F}_{2^{5}}$ to be the quotient ring $\mathbb{F}_{2}[X] /\left(X^{5}+X^{2}+1\right)$. Let $\alpha$ denote the equivalence class of $X$ in $\mathbb{F}_{2^{5}}$. By construction, the equality $\alpha^{5}+\alpha^{2}+1=0$ holds, or equivalently, $\alpha^{5}=\alpha^{2}+1$. Each element of $\mathbb{F}_{2^{5}}$ can hence be uniquely written as $\sum_{i=0}^{4} x_{i} \alpha^{i}$ where $\left(x_{4}, \ldots, x_{0}\right)$ belongs to $\mathbb{F}_{2}^{5}$. More precisely, the family $\left(\alpha^{i}\right)_{i<5}$ is a basis of $\mathbb{F}_{2^{5}}$ seen as a 5 -dimensional vector space over $\mathbb{F}_{2}$. The field $\mathbb{F}_{2^{5}}$ will then be identified with $\left(\mathbb{F}_{2}\right)^{5}$ via the isomorphism from $\mathbb{F}_{2}^{5}$

## Chapter 5 - Backdoored Encryption Algorithm 1

to $\mathbb{F}_{2^{5}}$ mapping $\left(x_{4}, \ldots, x_{0}\right)$ to $\sum_{i=0}^{4} x_{i} \alpha^{i}$. For instance, the element $\alpha^{2}+\alpha+1$ in $\mathbb{F}_{2^{5}}$ is identified with 07 in $\mathbb{F}_{2}^{5}$. Now define the $4 \times 4$ matrices $M_{U}$ and $M_{V}$ over $\mathbb{F}_{2^{5}}$ to be

$$
\left(\begin{array}{llll}
a & b & c & d \\
b & a & d & c \\
c & d & a & b \\
d & c & b & a
\end{array}\right) \quad M_{U}:\left\{\begin{array}{l}
a=\alpha^{4}+\alpha^{2}, \\
b=\alpha^{4}+\alpha^{3}+\alpha^{2}+\alpha+1, \\
c=\alpha^{3}+\alpha^{2}, \\
d=\alpha^{4}+\alpha^{2}+1,
\end{array} M_{V}:\left\{\begin{array}{l}
a=\alpha^{3}+\alpha^{2}+1, \\
b=\alpha^{4}+\alpha^{3}+\alpha^{2}+\alpha, \\
c=\alpha^{4}+\alpha^{2}+\alpha, \\
d=\alpha^{3}
\end{array}\right.\right.
$$

It can be verified that these matrices are MDS. In other words, the [8, 4]-linear code having $G=\left[\mathrm{Id}_{4}, M_{U}\right]$ as generator matrix has minimal distance equal to 5 , which is the maximum achievable.

Each of these matrices naturally induces an automorphism of $\left(\mathbb{F}_{2^{5}}\right)^{4}$, and hence of $\left(\mathbb{F}_{2}^{10}\right)^{4}$. For instance, $M_{U}$ maps the element $x=\left(x_{0}, x_{1}, x_{2}, x_{3}\right)$ to $x \times M_{U}$. Observe that we chose to see elements of $\left(\mathbb{F}_{2}^{10}\right)^{4}$ as row vectors to keep the common notation of linear codes.

Example 5.8. To illustrate this notation, let us compute the image of the element $x=(00,02,00,00)$ of $\left(\mathbb{F}_{2}^{10}\right)^{4}$ under the automorphism induced by $M_{U}$. First, $x$ is identified with the element $(0, \alpha, 0,0)$ of $\left(\mathbb{F}_{2^{5}}\right)^{4}$. Then,

$$
\begin{aligned}
& (0, \alpha, 0,0) \times M_{U}=\left(\alpha\left(\alpha^{4}+\alpha^{3}+\alpha^{2}+\alpha+1\right), \alpha\left(\alpha^{4}+\alpha^{2}\right), \alpha\left(\alpha^{4}+\alpha^{2}+1\right), \alpha\left(\alpha^{3}+\alpha^{2}\right)\right) \\
& =\left(\begin{array}{ccc}
\left.\alpha^{5}+\alpha^{4}+\alpha^{3}+\alpha^{2}+\alpha, \quad \alpha^{5}+\alpha^{3}, \quad \alpha^{5}+\alpha^{3}+\alpha, \quad \alpha^{4}+\alpha^{3}\right)
\end{array}\right. \\
& =\left(\quad \alpha^{4}+\alpha^{3}+\alpha+1, \alpha^{3}+\alpha^{2}+1, \alpha^{3}+\alpha^{2}+\alpha+1, \quad \alpha^{4}+\alpha^{3}\right) \text {. }
\end{aligned}
$$

Therefore, $(00,02,00,00) \times M_{U}=(1 \mathrm{~B}, 0 \mathrm{D}, 0 \mathrm{~F}, 18)$.
As was the case for the secret S -boxes $\mathbf{S}_{i}$, the linear transformation $M$ rests upon the linear transformation $M^{\prime}$ defined as follows:

$$
\begin{aligned}
& M^{\prime}:\left(\mathbb{F}_{2}^{10}\right)^{4} \longrightarrow\left(\mathbb{F}_{2}^{10}\right)^{4} \\
&\left(u_{i} \| v_{i}\right)_{i<4} \longmapsto\left(\rho(u)_{i} \| \tau_{u}(v)_{i}\right)_{i<4}
\end{aligned}
$$

where $\rho(u)=u \times M_{U}$ and $\tau_{u}(v)=v \times M_{V}+P_{U \rightarrow V}(u)$. The strength of this construction is that $M^{\prime}$ inherits the linear and differential branch numbers of $M_{U}$ and $M_{V}$, as stated in the proposition hereunder. But first, we introduce the following example.

Example 5.9. Let us compute the image of $x=(000,070,000,000)$ under $M^{\prime}$. As a first step, observe that $x$ can be written as

$$
x=(00\|00,03\| 10,00\|00,00\| 00)=\left(u_{i} \| v_{i}\right)_{i<4},
$$

where $u=(00,03,00,00)$ and $v=(00,10,00,00)$. Let $e_{9}=(00,02,00,00)$ and $e_{10}=(00,01,00,00)$. Then $u=e_{9}+e_{10}$, it is indeed its decomposition over the standard basis of $\left(\mathbb{F}_{2}^{5}\right)^{4}$. Thus, for any linear mapping $L$, it holds that $L(u)=L\left(e_{9}\right)+L\left(e_{10}\right)$. The image of $u$ under $\rho$ can hence be computed by

$$
\rho(u)=\rho\left(e_{9}\right)+\rho\left(e_{10}\right)=(1 \mathrm{~B}, 0 \mathrm{D}, 0 \mathrm{~F}, 18)+(1 \mathrm{~F}, 14,15,0 \mathrm{C})=(04,19,1 \mathrm{~A}, 14) .
$$

In the same way,

$$
\begin{aligned}
\tau_{u}(v) & =v \times M_{V}+P_{U \rightarrow V}\left(e_{9}\right)+P_{U \rightarrow V}\left(e_{10}\right) \\
& =(16,0 \mathrm{E}, 14,02)+(0 \mathrm{~F}, 11,0 \mathrm{C}, 16)+(11,0 \mathrm{E}, 02,0 \mathrm{~A})=(08,11,1 \mathrm{~A}, 1 \mathrm{E}) .
\end{aligned}
$$

Consequently, $M^{\prime}(x)=(04\|08,19\| 11,1 \mathrm{~A}\|1 \mathrm{~A}, 14\| 1 \mathrm{E})=(088,331,35 \mathrm{~A}, 29 \mathrm{E})$.
Proposition 5.10. The linear and the differential branch numbers of $M^{\prime}$ are both equal to 5 . Thus, $M^{\prime}$ is a perfect diffusion layer.

Proof. Let $x=\left(u_{i} \| v_{i}\right)_{i<4}$ be a nonzero element of $\left(\mathbb{F}_{2}^{10}\right)^{4}$. In order to prove that the differential branch number of $M^{\prime}$ is equal to 5 , we need to show that $\mathrm{w}_{10}(x)+$ $\mathrm{w}_{10}\left(M^{\prime}(x)\right)$ is greater than or equal to 5 . First, assume that $u=\left(u_{i}\right)_{i<4}$ is nonzero. Using the fact that $M_{U}$ is MDS, we obtain the inequality $\mathrm{w}_{5}(u)+\mathrm{w}_{5}\left(u \times M_{U}\right) \geq 5$. Next,

$$
\begin{aligned}
5 & \leq \mathrm{w}_{5}(u)+\mathrm{w}_{5}(\rho(u))=\mathrm{w}_{10}\left(\left(u_{i} \| 0\right)_{i<4}\right)+\mathrm{w}_{10}\left(\left(\rho(u)_{i} \| 0\right)_{i<4}\right) \\
& \leq \mathrm{w}_{10}\left(\left(u_{i} \| v_{i}\right)_{i<4}\right)+\mathrm{w}_{10}\left(\left(\rho(u)_{i} \| \tau_{u}(v)_{i}\right)_{i<4}\right)=\mathrm{w}_{10}(x)+\mathrm{w}_{10}\left(M^{\prime}(x)\right) .
\end{aligned}
$$

Now, suppose that $u=0$. It must be the case that $v \neq 0$ as $x$ is nonzero by definition. Again, it holds that $\mathrm{w}_{5}(v)+\mathrm{w}_{5}\left(v \times M_{V}\right) \geq 5$ because $M_{V}$ is also MDS. Then,

$$
\begin{aligned}
5 \leq \mathrm{w}_{5}(v)+\mathrm{w}_{5}\left(\tau_{0}(v)\right) & =\mathrm{w}_{10}\left(\left(0 \| v_{i}\right)_{i<4}\right)+\mathrm{w}_{10}\left(\left(0 \| \tau_{0}(v)_{i}\right)_{i<4}\right) \\
& =\mathrm{w}_{10}(x)+\mathrm{w}_{10}\left(M^{\prime}(x)\right) .
\end{aligned}
$$

We have proven that $\mathrm{w}_{10}(x)+\mathrm{w}_{10}\left(M^{\prime}(x)\right) \geq 5$ for any nonzero element $x$ of $\left(\mathbb{F}_{2}^{10}\right)^{4}$. Consequently, the differential branch number of $M^{\prime}$ is greater than or equal to 5 . The equality $\mathcal{B}_{\mathrm{D}}\left(M^{\prime}\right)=5$ follows as 5 is the maximum achievable. Similarly, it can be proven that $M^{\prime}$ has also the maximum linear branch number. It follows that $M^{\prime}$ is a perfect diffusion layer and the result is proven.

Recall that the notation $\{0 *\}$ denotes the subspace $\left\{0_{5}\right\} \times \mathbb{F}_{2}^{5}$ and that the linear mappings $L_{V_{i}}$ and $L_{W_{i}}$ (see Figure A.1) map respectively $\mathcal{L}(\{0 *\})$ to $\mathcal{L}\left(V_{i}\right)$ and $\mathcal{L}(\{0 *\})$ to $\mathcal{L}\left(W_{i}\right)$. It is then easily seen that $M^{\prime}$ maps $\{0 *\}^{4}$ to itself. Thus, $M^{\prime}$ preserves the partition $\mathcal{L}\left(\{0 *\}^{4}\right)$ by Proposition 3.25. Finally, define

$$
M=\left(L_{V_{0}}\left\|L_{V_{1}}\right\| L_{V_{2}} \| L_{V_{3}}\right) \circ M^{\prime} \circ\left(L_{W_{0}}\left\|L_{W_{1}}\right\| L_{W_{2}} \| L_{W_{3}}\right)^{-1} .
$$

From its definition, it is straightforward to check that $M$ maps the linear partition $\mathcal{L}\left(\prod_{i=0}^{3} W_{i}\right)$ to $\mathcal{L}\left(\prod_{i=0}^{3} V_{i}\right)$.
Example 5.11. We are going to compute $M(000,080,000,000)$. First, we have

$$
\begin{aligned}
& \left(L_{W_{0}}\left\|L_{W_{1}}\right\| L_{W_{2}} \| L_{W_{3}}\right)^{-1}(000,080,000,000) \\
& \quad \quad=\left(L_{W_{0}}^{-1}(000), L_{W_{1}}^{-1}(080), L_{W_{2}}^{-1}(000), L_{W_{3}}^{-1}(000)\right)=(000,070,000,000) .
\end{aligned}
$$

Then, the image of $(000,070,000,000)$ under $M^{\prime}$ is $(088,331,35 \mathrm{~A}, 29 \mathrm{E})$, as already established in Example 5.9. Finally,

$$
\begin{aligned}
M(000,080,000,000) & =\left(L_{V_{0}}\left\|L_{V_{1}}\right\| L_{V_{2}} \| L_{V_{3}}\right)(088,331,35 \mathrm{~A}, 29 \mathrm{E}) \\
& =(15 \mathrm{E}, 0 \mathrm{BF}, 1 \mathrm{E} 2,04 \mathrm{~F}) .
\end{aligned}
$$

## Chapter 5 - Backdoored Encryption Algorithm 1

Indeed, $L_{V_{0}}(088)=L_{V_{0}}(080)+L_{V_{0}}(008)=21 \mathrm{D}+343=15 \mathrm{E}$. The three other bundles are computed in the same manner.

Because each mapping $L_{V_{i}}$ or $L_{W_{i}}$ operates on different bundles and is invertible, it is clear that the linear and differential branch numbers of $M$ are the same as $M^{\prime}$. This discussion completes the proof of the following corollary.

Corollary 5.12. The linear mapping $M$ is a perfect diffusion layer which maps $\mathcal{L}\left(\prod_{i=0}^{3} W_{i}\right)$ to $\mathcal{L}\left(\prod_{i=0}^{3} V_{i}\right)$.

In conclusion, Proposition 3.23 ensures that any key addition preserves all the linear partitions, and hence it preserves $\mathcal{L}(V)$. Next, it has been proven in Section 5.2.2 that every secret S-box $\mathbf{S}_{i}$ maps $\mathcal{L}\left(V_{i}\right)$ to $\mathcal{L}\left(W_{i}\right)$. Thus, the secret substitution layer maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. It is clear that the ShiftRows operation is linear and maps $W$ to itself. According to Proposition 3.25, this mapping preserves $\mathcal{L}(W)$. Finally, the MixColumn operation maps $\mathcal{L}(W)$ to $\mathcal{L}(V)$ by Corollary 5.12. This discussion is summarized in Figure 5.3 and proves Theorem 5.2 previously given in Section 5.2.1.

### 5.3. Main Idea of the Cryptanalysis

As we have seen in Section 5.2.1, the cipher BEA-1 does not map a linear partition to another one, but behaves as though it did for a non-negligible fraction of the message space. This non-trivial property can be used to recover the cipher key in an operational cryptanalysis close to Harpes's basic partitioning cryptanalysis [52. But before considering the full cipher, we give the main idea of this attack.

### 5.3.1. A Detailed Example

To explain how to take advantage of this backdoor, we introduce a toy example. First, let us mention that the notation of this section is independent of the remainder of this chapter. The message space of this toy cipher is simply $\mathbb{F}_{2}^{6}$. Then, consider the subspaces $V$ and $W$ of $\mathbb{F}_{2}^{6}$ defined to be

$$
\begin{aligned}
V & =\operatorname{span}(01,02,10,20) \\
W & =\left\{\left(x_{3}, x_{2}, 0,0, x_{1}, x_{0}\right) \mid x \in \mathbb{F}_{2}^{4}\right\}, \\
, ~ \operatorname{pan}(01,02,04,10) & =\left\{\left(0, x_{3}, 0, x_{2}, x_{1}, x_{0}\right) \mid x \in \mathbb{F}_{2}^{4}\right\} .
\end{aligned}
$$

Thus, $\mathcal{L}(V)=\{x+V \mid x \in\{00,04,08,0 C\}\}$ and $\mathcal{L}(W)=\{y+W \mid y \in\{00,08,20,28\}\}$.
Let $\mathbf{S}$ be the permutation of $\mathbb{F}_{2}^{6}$ given in Figure 5.4. We define another permutation $S$ of $\mathbb{F}_{2}^{6}$ satisfying $S(x)=\mathbf{S}(x)$ for any input $x$ in $\mathbb{F}_{2}^{6}$ except $00,01,04,05,08,09$, OC and OD. The images of these eight specific points under $S$ are also given in Figure 5.4. By analogy with Section 5.2, the permutation $\mathbf{S}$ represents the secret S-box used to design the trapdoor whereas $S$ represents the modified S-box given in the specification of the algorithm. Lastly, define the following keyed mappings

$$
\begin{aligned}
\mathbf{F}_{k}: \mathbb{F}_{2}^{6} & \longrightarrow \mathbb{F}_{2}^{6} & F_{k}: \mathbb{F}_{2}^{6} & \longrightarrow \mathbb{F}_{2}^{6} \\
x & \longmapsto \mathbf{S}(x)+k, & x & \longmapsto S(x)+k,
\end{aligned}
$$

|  |  | . 0 | . 1 | . 2 | . 3 | . 4 | . 5 | . 6 | . 7 | . 8 | . 9 | . A | . B | . C | . D | . E | . F |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\mathbf{S}(x)$ | 0. | 1 C | 1E | 1F | 08 | 39 | 3A | 3C | 2A | 13 | 05 | 02 | 03 | 37 | 20 | 24 | 31 |
|  | 1 | OD | 18 | OA | 1A | 3B | 2D | 29 | 3E | 14 | 07 | 11 | 10 | 25 | 26 | 21 | 35 |
|  | 2 | 1B | 19 | OB | 1D | 2B | 2F | 2C | 28 | 15 | 01 | 16 | 06 | 27 | 36 | 30 | 32 |
|  | 3 | OC | 09 | OF | OE | 3F | 2E | 3D | 38 | 00 | 17 | 04 | 12 | 22 | 23 | 33 | 34 |
| $S(x)$ | 0 | 39 | 05 |  |  | 13 | 1C |  |  | 37 | 20 |  |  | 1E | 3A |  |  |

Figure 5.4: The secret and modified S-boxes.
representing respectively the secret and the modified round functions. Naturally, the key $k$ can be any element of $\mathbb{F}_{2}^{6}$.

It can be easily verified that the secret S-box $\mathbf{S}$ maps $\mathcal{L}(V)$ to $\mathcal{L}(W)$. In fact, we have

$$
\begin{array}{ll}
\mathbf{S}(00+V)=08+W, & \mathbf{S}(08+V)=00+W, \\
\mathbf{S}(04+V)=28+W, & \mathbf{S}(0 C+V)=20+W .
\end{array}
$$

In contrast with the secret permutation $\mathbf{S}$, the modified S-box $S$ does not map $\mathcal{L}(V)$ to $\mathcal{L}(W)$. However the equality $S(x)=\mathbf{S}(x)$ holds with probability ${ }^{56} / 64$ assuming that $x$ is uniformly distributed over $\mathbb{F}_{2}^{6}$. This can be stated equivalently as

$$
\#\left\{x \in \mathbb{F}_{2}^{6} \mid S(x)=\mathbf{S}(x)\right\}=2^{6}-8=56
$$

It should also be noted that this statement remains valid when considering their inverse mappings, that is $\#\left\{y \in \mathbb{F}_{2}^{6} \mid S^{-1}(y)=\mathbf{S}^{-1}(y)\right\}=56$. Indeed, if $x$ is an element of $\mathbb{F}_{2}^{6}$ such that $S(x)=\mathbf{S}(x)$, then $y=S(x)$ satisfies the equality $S^{-1}(y)=\mathbf{S}^{-1}(y)$. As a consequence,

$$
\#\left\{x \in \mathbb{F}_{2}^{6} \mid S(x)=\mathbf{S}(x)\right\} \leq \#\left\{y \in \mathbb{F}_{2}^{6} \mid S^{-1}(y)=\mathbf{S}^{-1}(y)\right\} .
$$

The converse inequality can be proven in the same way, establishing the equality.
Now, consider the subset $\mathcal{P}$ of $\mathbb{F}_{2}^{6}$ defined hereinafter. We assume that the round key is $k=37$. The image of $\mathcal{P}$ under $\mathbf{S}$ and its encryption with $\mathbf{F}_{37}$ are given below.

$$
\begin{aligned}
& \in(00+V) \quad \in(04+V) \quad \in(08+V) \in(0 C+V) \\
& \mathcal{P}=\{\overbrace{22}, \overbrace{04,05,06,15,16,17,27,34,35,36}, \overbrace{18,3 \mathrm{~A}}, \overbrace{\text { OD }, \text { OF }}\}, \\
& \mathbf{S}(\mathcal{P})=\{0 \mathrm{~B}, 39,3 \mathrm{~A}, 3 \mathrm{C}, 2 \mathrm{D}, 29,3 \mathrm{E}, 28,3 \mathrm{~F}, 2 \mathrm{E}, 3 \mathrm{D}, 14,04,20,31\}, \\
& \mathbf{F}_{37}(\mathcal{P})=\{\underbrace{3 \mathrm{C}}_{\in(28+W)}, \underbrace{0 \mathrm{OE}, \mathrm{OD}, 0 \mathrm{~B}, 1 \mathrm{~A}, 1 \mathrm{E}, 09,1 \mathrm{~F}, 08,19,0 \mathrm{~A}}_{\in(08+W)}, \underbrace{23,33}_{\in(20+W) \in(00+W)}, \underbrace{17,06\}} .
\end{aligned}
$$

It should be stressed that the coset $04+V$ is significantly more represented in $\mathcal{P}$ than any other coset of $V$. Since $\mathbf{F}_{37}$ maps the linear partition $\mathcal{L}(V)$ to $\mathcal{L}(W)$, the messages belonging to the same coset of $V$ are all mapped to the same coset of $W$. Therefore, the most represented coset of $W$ in $\mathbf{F}_{37}(\mathcal{P})$ has also ten elements.

## Chapter 5 - Backdoored Encryption Algorithm 1



Figure 5.5: Encryption with $\mathbf{F}_{37}$ and $F_{37}$.

As we have seen above, the modified round function $F_{37}$ does not map $\mathcal{L}(V)$ to $\mathcal{L}(W)$. Figure 5.5 displays the differences between the encryption of $\mathcal{P}$ with $\mathbf{F}_{37}$ and its encryption with $F_{37}$ by highlighting the messages $x$ in $P$ such that $S(x) \neq \mathbf{S}(x)$ (that is 04,05 and 0 D ) and their images throughout the encryption.

To explain these differences, let us first consider the set $\mathcal{Q}$ of the ten messages lying in both $\mathcal{P}$ and $04+V$. Knowing that the equality $S(x)=\mathrm{S}(x)$ holds with probability $56 / 64$ when $x$ is uniformly distributed, it seems reasonable to assume that only $10 \times 56 / 64=8.75$ messages of $\mathcal{Q}$ will remain in the same coset when computing their images under $S$. By comparing with the actual messages in $\mathcal{Q}$, we can see that this is a good approximation since eight messages in $S(\mathcal{Q})$ belong to the same coset of $W$.

$$
\begin{aligned}
\mathcal{Q} & =\{\begin{array}{l}
04,05
\end{array}, \begin{array}{l}
\neq(28+W) \\
S(\mathcal{Q})
\end{array}=\{\underbrace{13,1 \mathrm{C}, 15,16,17,27,34,35,36}_{\in(28+W)}, \underbrace{3 \mathrm{C}, 2 \mathrm{D}, 29,3 \mathrm{E}, 28,3 \mathrm{~F}, 2 \mathrm{E}, 3 \mathrm{D}}\}
\end{aligned} . \mathrm{P} \cap(04+V),
$$

Needless to say, there are also eight messages in $F_{37}(\mathcal{Q})$ lying in the same coset of $W$ because the key addition preserves $\mathcal{L}(W)$.

We focus now to the set $\mathcal{P}$ as a whole. According to the discussion above, we know that the most represented coset of $W$ in $F_{37}(\mathcal{P})$ has at least eight elements. We have seen that the images under $S$ of messages lying in the same coset may not stay together. Nonetheless, the converse can also be true and messages in different cosets may end up in the same coset. This is exactly what happens with the message 0D, as illustrated in Figure 5.5. Consequently, the most represented coset in $F_{37}(\mathcal{P})$ has actually nine elements.

The fact that the most represented coset may not only lose but occasionally


Figure 5.6: Decryption with the right key and with a wrong key.
retrieve elements, should be seen as a side effect. Its impact remains low when

- one coset has significantly more elements than all other cosets (say at least 5 times more), and
- when the number of messages is less than the total number of cosets.

We must nevertheless keep this fact in mind to understand why the right key will not necessarily have the best score.

It is now time to explain how to recover the round key using only the set $\mathcal{C}=F_{37}(\mathcal{P})$ of encrypted messages. First, we have to determine the most represented coset in $\mathcal{C}$. In our example, this coset is $08+W$ with nine messages, and $u=08$ is one of its representatives.

Now, assume that $k$ is the round key used to encrypt $\mathcal{C}$. We need to find the coset of $V$ which is mapped to $\mathbf{u}+W$ by the secret round function $\mathbf{F}_{k}$. According to Lemma 3.18, $F_{k}$ maps $\mathbf{t}+V$ to $\mathbf{F}_{k}(\mathbf{t})+W$. A representative of this coset of $V$ is then $\mathbf{t}=\mathbf{S}^{-1}(\mathbf{u}+k)$. Finally, the score of the guessed key $k$ is the number of messages $F_{k}^{-1}(c)=S^{-1}(c+k)$ which belong to the theoretical coset $\mathbf{t}+V$, that is to say

$$
\operatorname{score}(k)=\#\left\{c \in C \mid S^{-1}(c+k) \in(\mathbf{t}+V)\right\} .
$$

Figure 5.6 illustrates the scoring process applied to the right key (37) and to a wrong key (07). We naturally recover the set $\mathcal{P}$ and the coset $\mathbf{t}+V=34+V=04+V$ when using the right key. Thus, the score of $k=37$ is equal to 10 . In the same way, the score of $k=07$ is the number of decrypted messages in the coset $\mathbf{t}+V=32+V=00+V$, so $\operatorname{score}(07)=8$.

Let us now explain why a wrong key tends to have a lower score than the right key. First, the addition of the wrong key randomizes the cosets and the messages within.

Chapter 5 - Backdoored Encryption Algorithm 1

| Key | OB | 12 | 1 C | 37 | 03 | 05 | 10 | 1 D | 20 | 21 | 22 | 2 C | 2 F | 35 | 36 | 38 |
| :--- | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| Score | 11 | 10 | 10 | 10 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 |
| Key | $3 B$ | $3 C$ | $3 D$ | 00 | 01 | 02 | 04 | 06 | 07 | 08 | 09 | $0 A$ | $0 E$ | 0 F | 11 | 13 |
| Score | 9 | 9 | 9 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| Key | 18 | 19 | 1 E | 1 F | 24 | 25 | 26 | 27 | 2 A | 2 B | 2 D | 2 E | 30 | 34 | 39 | 3 A |
| Score | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| Key | OC | 0D | 14 | 15 | 16 | 17 | 1 A | 1 B | 23 | 28 | 29 | 31 | 32 | 33 | 3 E | 3 F |
| Score | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 |

Figure 5.7: The scores for each key.

Recall that when the input $x$ is uniformly distributed, the equality $S^{-1}(x)=\mathbf{S}^{-1}(x)$ holds with probability $56 / 64$. The most represented coset after the addition of the wrong key should then lose some elements by applying $S^{-1}$. Thus, the score of any wrong key should be less than or equal to 8 .

It goes without saying that the previous discussion gives just the main idea of the cryptanalysis. For some wrong keys, the side effects are significant and their scores can even be higher than the score of the right key, as shown in Figure 5.7. Indeed, the key 37 is one the four best keys, but is not the one which has the highest score (OB). For this reason, we will not only return the best key but also the NbCand candidate keys having the highest scores when running this cryptanalysis.

### 5.3.2. Formalization of the Attack

The aim of this section is to formalize and to generalize the cryptanalysis introduced previously in Section 5.3.1. As we have just seen, this attack really begins in Figure 5.6. The very first data needed is the set $\mathcal{C}$ containing the encrypted messages under the unknown key, given by

$$
\mathcal{C}=\{04,05,06,0 \mathrm{D}, 0 \mathrm{~F}, 15,16,17,18,22,27,34,35,36,3 \mathrm{~A}\} .
$$

Naturally, $\mathcal{C}$ is included in the set $\mathscr{C}=\mathbb{F}_{2}^{6}$ of all possible ciphertexts. Similarly, the set of all possible round keys is denoted by $\mathscr{K}=\mathbb{F}_{2}^{6}$. Next, define the keyed mapping

$$
\begin{aligned}
G: \mathscr{K} \times \mathscr{C} & \longrightarrow \mathbb{F}_{2}^{6} \\
(k, c) & \longmapsto S^{-1}(c+k) .
\end{aligned}
$$

Each mapping $G_{k}: c \mapsto G(k, c)$ is the inverse of the round function $F_{k}$. The secret counterpart of $G$ is $\mathbf{G}:(k, c) \mapsto \mathbf{S}^{-1}(c+k)$. Observe that for each round key $k$, the mapping $\mathbf{G}_{k}$ maps $\mathcal{L}(W)$ to $\mathcal{L}(V)$. It is also necessary to know the most represented coset $\mathbf{u}+W$ in $\mathcal{C}$. Using this notation, the cryptanalysis is formalized in Algorithm 7. Finally, to include potential information on the round keys, this attack processes only a subset $\mathcal{K}$ of $\mathscr{K}$.

More generally, the parameters can be outlined as follows.

```
Algorithm 7 - SelectKeys(G, G, K, C, u, V, NbCand)
Input. See Section 5.3.2.
Output. The set Cand containing the NbCand best keys together with their scores.
```

```
Cand \leftarrow []
```

Cand \leftarrow []
For each }k\in\mathcal{K}\mathrm{ do
For each }k\in\mathcal{K}\mathrm{ do
Computation of the score of }
Computation of the score of }
Score }\leftarrow
Score }\leftarrow
For each c\in\mathcal{C}}\mathrm{ do
For each c\in\mathcal{C}}\mathrm{ do
t}\leftarrow\mathbf{G}(k,\mathbf{u}
t}\leftarrow\mathbf{G}(k,\mathbf{u}
If G(k,c) lies in t + V then
If G(k,c) lies in t + V then
Score }\leftarrow\mathrm{ Score +1
Score }\leftarrow\mathrm{ Score +1
Saving k if it is one of the NbCand best keys
Saving k if it is one of the NbCand best keys
If the cardinality of Cand is lower than NbCand then
If the cardinality of Cand is lower than NbCand then
Insert ( }k,\mathrm{ Score) in Cand
Insert ( }k,\mathrm{ Score) in Cand
Else if Score is greater than the lowest score in Cand then
Else if Score is greater than the lowest score in Cand then
Remove the lowest scored key of Cand
Remove the lowest scored key of Cand
Insert ( }k,\mathrm{ Score) in Cand
Insert ( }k,\mathrm{ Score) in Cand
Return Cand

```
Return Cand
```

- The sets of all possible keys and ciphertexts are referred to as $\mathscr{K}$ and $\mathscr{C}$.
- The keyed mapping $G: \mathscr{K} \times \mathscr{C} \rightarrow E$ typically undoes (or partially undoes) one or two rounds of the encryption process.
- Its secret counterpart is denoted by $\mathbf{G}: \mathscr{K} \times \mathscr{C} \rightarrow E$. It is assumed that $\mathbf{G}_{k}$ maps a linear partition $\mathcal{L}(W)$ to another partition $\mathcal{L}(V)$ no matter the key $k$ used.
- The set of the given ciphertexts is denoted by $\mathcal{C}$. The set of the keys that must be scored by this attack is denoted by $\mathcal{K}$.
- It is assumed that there is a coset of $W$ containing significantly more ciphertexts than any other coset. The element $\mathbf{u}$ of $\mathscr{C}$ is a representative of this coset.
- Finally, NbCand is the number of candidate keys to return.

Remark 5.13. Taking a closer look at Algorithm 7, we can see that the structure Cand requires an efficient way to remove the lowest scored key. In our implementation, Cand is a sorted array of couples $(s, L)$ where $L$ is a list containing the keys having the score $s$. Since there are very few different scores, the sorted insertion in Cand is (almost) in constant time. Removing the lowest scored key is also in constant time. Thus, the time complexity of this cryptanalysis is $O(\# \mathcal{K} \times \# \mathcal{C})$.

### 5.4. Cryptanalysis of BEA-1 Using the Backdoor

The algorithm SelectKeys (see Algorithm 7) detailed into the previous section enables recovery of information on the last round key, using the fact that the round function acts as a function mapping a linear partition to another one with high

## Chapter 5 - Backdoored Encryption Algorithm 1

probability. In this section, we explain how this algorithm can be used to recover the full 120-bit cipher key in just a few seconds on a laptop computer.

This cryptanalysis requires $\mathrm{N}=2^{16}$ chosen plaintexts and their corresponding ciphertexts encrypted under one unknown cipher key $K$. As BEA-1 operates on 80 -bit blocks, this amounts to $2 \times 640 \mathrm{KiB}$ of data. The plaintexts only need to be uniformly chosen in one coset of $V$ and there is no requirement on the cipher key.

Our cryptanalysis is naturally divided in five distinct parts. First, we give a brief overview of each part. By hypothesis, all the plaintexts are in the same coset of $V$. As explained in Section 5.2.1, a coset of $W$ should be more represented among the ciphertexts. The first part is aimed at finding a representative $\mathbf{u}$ of this coset. The second part consists in using the algorithm SelectKeys to find $2^{15}$ candidates for the full 80 -bit last round key $k^{[11]}$. Next, relying on a property of the key schedule, SelectKeys is applied to these $2^{15}$ candidates to find the right last key in a third part. So far, we have recovered 80 bits of the cipher key. Knowing the last round key, it is then possible to undo the last round of each ciphertext. The fourth part is really close to the first one and provides $2^{15}$ candidates for the 40 remaining bits. Finally, deduce the $2^{15}$ candidate cipher keys from $k^{[11]}$ and the preceding candidates. The last part involves testing these cipher keys on the plaintext/ciphertext pairs available to find the right one.

The presentation of our cryptanalysis is structured as follows. First, we provide the full attack in Algorithm 5.4. Then, each part of this algorithm is detailed in one dedicated section. It should be noted that we keep the notation of Section 5.2 (and not that of Section 5.3) in the remainder of this chapter.

### 5.4.1. Part 1: Finding the Right Output Coset

Let $\mathcal{P}$ denote the set of the $2^{16}$ plaintexts uniformly chosen in one coset of $V$ and let $\mathcal{C}=\left\{E_{K}(p) \mid p \in \mathcal{P}\right\}$ denote the set of their ciphertexts. As said previously, we first need to find the most represented coset of $W$ in $\mathcal{C}$. Let $U_{i}$ be the subspace of $\mathbb{F}_{2}^{10}$ defined to be $U_{i}=L_{W_{i}}(\{* 0\})$ for each $0 \leq i<3$. Since $\{* 0\}$ is a complement space of $\{0 *\}$ and $L_{W_{i}}$ is an automorphism, we know that $U_{i}$ is a complement space of $L_{W_{i}}(\{0 *\})=W_{i}$. Define $U$ to be the subspace $\prod_{i=0}^{7} U_{i \bmod 4}$ of $\left(\mathbb{F}_{2}^{10}\right)^{8}$. Of course, $U$ is a complement space of $W$.

Let $c$ be a ciphertext and $u=\left(u_{i}\right)_{i<8}$ be in $U$. Because both $U$ and $W$ are product spaces, it is easily seen that $u$ is the unique representative in $U$ of the coset $c+W$ if, and only if, $c_{i}$ and $u_{i}$ are in the same coset of $W_{i \bmod 4}$ for each $i<8$. We deduce the following efficient way to compute the representative in $U$ of the coset $c+W$. First, precompute the four tables $\operatorname{RepW}_{i}$ such that, for each $x$ in $\mathbb{F}_{2}^{10}, \operatorname{RepW}_{i}[x]$ gives the representative in $U_{i}$ of $x+W_{i}$. These tables are just arrays of 1024 integers. Then, the representative of $c=\left(c_{i}\right)_{i<8}$ is just $u=\left(\operatorname{RepW}_{i \bmod 4}\left[c_{i}\right]\right)_{i<8}$.

To find the most represented coset of $W$ in $\mathcal{C}$, we first compute the representative in $U$ of each ciphertext as described above. Then, we search for the representative which occurs the most. Any naive algorithm should work since there are only $2^{15}$ representatives.

## Algorithm 8 - Cryptanalysis of BEA-1 Using the Backdoor

Input. The number N of plaintext/ciphertext pairs (typically, $\mathrm{N} \approx 2^{15}$ ).

- A set $\mathcal{P}$ of N plaintexts uniformly chosen in one coset of $V$.
- The corresponding ciphertexts encrypted under one (unknown) cipher key $K$. The set $\left\{E_{K}(p) \mid p \in \mathcal{P}\right\}$ of these ciphertexts in denoted by $\mathcal{C}$.
Output. The cipher key $K$ or "Failure" in case of failure.

```
\(\mathrm{NbCand} \leftarrow 2^{15}\)
Part 1: find the representative of the output coset.
\(-\mathbf{u} \leftarrow\) the element \(u \in U\) maximizing the cardinality of \(\mathcal{C} \cap(u+W)\)
Part 2: find the \(2^{15}\) best candidates for \(k^{[11]}\).
    \(E \leftarrow\{3\}\)
    Cand \(\leftarrow\left\{\left(k_{i}\right)_{i \in E} \mid k_{3} \in \mathbb{F}_{2}^{10}\right\}\)
    For each idx \(\in[7,0,4,1,5,2,6]\) do
        \(E \leftarrow E \cup\{\mathrm{idx}\}\)
        Define \(\mathbf{G}_{E}, G_{E}, \mathcal{C}_{E}\) and \(V_{E}\) as in Section 5.4.2
        \(\mathcal{K}_{E} \leftarrow\left\{\left(k_{i}\right)_{i \in E} \mid k_{\mathrm{idx}} \in \mathbb{F}_{2}^{10}\right.\) and \(\left.\left(k_{i}\right)_{i \in E \backslash\{\mathrm{idx}\}} \in \operatorname{Cand}\right\}\)
        Cand \(\leftarrow \operatorname{SelectKeys}\left(\mathbf{G}_{E}, G_{E}, \mathcal{K}_{E}, \mathcal{C}_{E},\left(\mathbf{u}_{i}\right)_{i \in E}, V_{E}\right.\), NbCand \()\)
    Part 3: find \(k{ }^{[11]}\) among its candidates.
    \(E \leftarrow\{0,2,5,7\}\)
    Define G, \(G\) and \(V^{\prime}\) as in Section 5.4.3
    Cand \(\leftarrow \operatorname{SelectKeys}\left(\mathbf{G}, G\right.\), Cand, \(\mathcal{C}_{E},\left(\mathbf{u}_{i}\right)_{i \in E}, V\), NbCand)
    \(k^{[11]} \leftarrow\) the key with the highest score in Cand
Part 4: find the \(2^{15}\) best candidates for \(\left(k_{i}^{[10]}\right)_{4 \leq i<8}\).
    Define \(\mathcal{C}^{\prime}\) and \(\mathbf{u}^{\prime}\) as in Section 5.4.4
    \(E \leftarrow\{4\}\)
    Cand \(\leftarrow\left\{\left(k_{i}^{\prime}\right)_{i \in E} \mid k_{4}^{\prime} \in \mathbb{F}_{2}^{10}\right\}\)
    For each idx \(\in[7,5,6]\) do
        \(E \leftarrow E \cup\{\mathrm{idx}\}\)
        Define \(\mathbf{G}_{E}, G_{E}, \mathcal{C}_{E}^{\prime}\) and \(V_{E}\) as in Section 5.4.4
        \(\mathcal{K}_{E}^{\prime} \leftarrow\left\{\left(k_{i}^{\prime}\right)_{i \in E} \mid k_{\text {idx }}^{\prime} \in \mathbb{F}_{2}^{10}\right.\) and \(\left(k_{i}^{\prime}\right)_{i \in E \backslash\{\mathrm{idx}\}} \in\) Cand \(\}\)
        Cand \(\leftarrow \operatorname{SelectKeys}\left(\mathbf{G}_{E}, G_{E}, \mathcal{K}_{E}^{\prime}, \mathcal{C}_{E}^{\prime},\left(\mathbf{u}_{i}^{\prime}\right)_{i \in E}, V_{E}\right.\), NbCand \()\)
    Part 5: find the cipher key \(K\).
    For each \(\left(k_{i}^{\prime[10]}\right)_{4 \leq i<8} \in\) Cand do
        \(\left(k_{i}{ }^{[10]}\right)_{4 \leq i<8} \leftarrow M\left(\left(k_{i}^{\prime[10]}\right)_{4 \leq i<8}\right)\)
        \(K \leftarrow\) the cipher key corresponding to \(\left(k_{i}{ }^{[10]}\right)_{4 \leq i<8}\) and \(k^{[11]}\)
        If \(E_{K}(p)=c\) for all plaintext/ciphertext pairs \((p, c)\) then
            Return \(K\)
Return "Failure"
```


## Chapter 5 - Backdoored Encryption Algorithm 1



Figure 5.8: Cryptanalysis using the backdoor (Part 2).

### 5.4.2. Part 2: Obtaining Candidates for the Last Round Key

This part is intended to find candidates for the last round key $k^{[11]}$ using the algorithm SelectKeys (see Algorithm 7) to undo the last round of BEA-1. However, if this algorithm is naively applied, then the last round has to be undone for each of the $2^{16}$ ciphertexts and $2^{80}$ possible values of $k^{[11]}$, yielding an order of $2^{96}$ time complexity.

To solve this problem, the $2^{15}$ candidates for $k^{[11]}$ are obtained bundle by bundle, as illustrated in Figure 5.8. First, we partially decrypt the bundles of index 3 and 7. We begin by these bundles since they both involve the S-box $S_{3}$, being the most different from its secret equivalent. Following the notation of SelectKeys, the set containing the ciphertexts is $\mathcal{C}_{\{3,7\}}=\left\{\left(c_{3}, c_{7}\right) \mid c \in \mathcal{C}\right\}$ and the set of the keys is $\mathcal{K}_{\{3,7\}}=\left\{\left(k_{3}, k_{7}\right) \mid k_{3}, k_{7} \in \mathbb{F}_{2}^{10}\right\}$. The mapping used to partially decrypt the last round of these ciphertexts is

$$
\begin{aligned}
G_{\{3,7\}}:\left(\mathbb{F}_{2}^{10}\right)^{2} \times\left(\mathbb{F}_{2}^{10}\right)^{2} & \longrightarrow\left(\mathbb{F}_{2}^{10}\right)^{2} \\
\left(\left(k_{3}, k_{7}\right),\left(c_{3}, c_{7}\right)\right) & \longmapsto\left(S_{3}^{-1}\left(c_{3}+k_{3}\right), S_{3}^{-1}\left(c_{7}+k_{7}\right)\right) .
\end{aligned}
$$

Its secret equivalent $\mathbf{G}_{\{3,7\}}$ is obtained by replacing $S_{3}$ with $\mathbf{S}_{3}$. The two remaining inputs of the algorithm are the representative $\mathbf{u}=\left(\mathbf{u}_{3}, \mathbf{u}_{7}\right)$ of the most represented coset of $\left(W_{3}\right)^{2}$, and the subspace $\left(V_{3}\right)^{2}$ of $\left(\mathbb{F}_{2}^{10}\right)^{2}$. It is worth observing that $\mathbf{G}_{\{3,7\}}$ maps $\mathcal{L}\left(\left(W_{3}\right)^{2}\right)$ to $\mathcal{L}\left(\left(V_{3}\right)^{2}\right)$ as required by the algorithm. Running SelectKeys with these arguments generates a set Cand containing $2^{15}$ candidates for $\left(k_{3}{ }^{[11]}, k_{7}{ }^{[11]}\right)$ instead of $2^{20}$.

From now on, each step seeks to add a new bundle to our candidates for the last round key $k{ }^{[11]}$. The next bundle to add has index 0 . Let $E$ denote the set $\{0,3,7\}$
of the current bundle's indices. Since we have no information on the value of $k_{0}{ }^{[11]}$, the set of the possible values for $\left(k_{i}{ }^{[11]}\right)_{i \in E}$ is

$$
\mathcal{K}_{E}=\left\{\left(k_{i}\right)_{i \in E} \mid k_{0} \in \mathbb{F}_{2}^{10},\left(k_{3}, k_{7}\right) \in \text { Cand }\right\}
$$

Following the idea of the first step, we define $\mathcal{C}_{E}=\left\{\left(c_{i}\right)_{i \in E} \mid\left(c_{i}\right)_{i<8} \in \mathcal{C}\right\}$ and

$$
\begin{aligned}
G_{E}:\left(\mathbb{F}_{2}^{10}\right)^{E} \times\left(\mathbb{F}_{2}^{10}\right)^{E} & \longrightarrow\left(\mathbb{F}_{2}^{10}\right)^{E} \\
\left(\left(k_{i}\right)_{i \in E},\left(c_{i}\right)_{i \in E}\right) & \longmapsto\left(S_{i \bmod 4}^{-1}\left(c_{i}+k_{i}\right)\right)_{i \in E}
\end{aligned}
$$

Then, define $\mathbf{G}_{E}$ by replacing $S_{i}$ with $\mathbf{S}_{i}$ and let $V_{E}$ denote the subspace $\prod_{i \in E} V_{i \bmod 4}$ of $\left(\mathbb{F}_{2}^{10}\right)^{E}$. The set Cand obtained by running SelectKeys with these parameters contains $2^{15}$ candidates for ( $k_{0}{ }^{[11]}, k_{3}{ }^{[11]}, k_{7}{ }^{[11]}$ ).

According to Algorithm 5.4, the index of the next bundle is 4. Actually, the order of the bundle's indices were chosen such as to involve the S-boxes $S_{3}$, then $S_{0}, S_{1}$ and finally $S_{2}$. The current indices are in the set $E=\{0,3,4,7\}$. Similarly, we define

$$
\mathcal{K}_{E}=\left\{\left(k_{i}\right)_{i \in E} \mid k_{4} \in \mathbb{F}_{2}^{10},\left(k_{0}, k_{3}, k_{7}\right) \in \operatorname{Cand}\right\}
$$

to include the information on $k^{[11]}$ gathered by the previous step. Finally, define $\mathcal{C}_{E}$, $G_{E}, \mathbf{G}_{E}$ and $V_{E}$ as above. Again, the algorithm SelectKeys yields $2^{15}$ candidates for $\left(k_{i}{ }^{[11]}\right)_{i \in E}$.

This time, let us take a closer look at the implementation of this step. Because $\# \mathcal{K}_{E}=2^{25}$ and $\# \mathcal{C}_{E}=2^{16}$, a straightforward implementation of SelectKeys requires $2^{41}$ partial round decryptions, as explained by Remark 5.13. Algorithm 9 provides our implementation of SelectKeys for this step. As we can see, the previous candidates are used to filter the ciphertexts before attacking $k_{4}$ by brute force. For each of the $2^{15}$ candidates, initializing the filter requires $2^{16}$ partial decryptions. On average, it remains roughly $2^{6}$ ciphertexts after the filtering process. The loop over $k_{4}$ hence requires $2^{16}$ partial decryptions. Consequently, this implementation performs about $2^{32}$ partial decryptions instead of $2^{41}$.

Naturally, the $2^{15}$ candidates for the full round key $k^{[11]}$ are obtained by repeating this method for the four remaining bundles. We will conclude by observing that the complexity of each step decreases since the filtering process improves as the algorithm progresses.

### 5.4.3. Part 3: Finding the Last Round Key

So far, we have found $2^{15}$ candidates for the 80 -bit key $k^{[11]}$. This part intends to recover the right key among these candidates, relying on the key schedule's structure. Let us consider the last round of the key schedule in order to derive a relation between $k^{[10]}$ and $k^{[11]}$. In Figure 5.1:

- $k^{[9]}=\left(k_{0}^{[9]}, \ldots, k_{7}^{[9]}\right)$ corresponds with $\left(k_{0}, \ldots, k_{7}\right)$,
- $k^{[10]}=\left(k_{0}{ }^{[10]}, \ldots, k_{7}{ }^{[10]}\right)$ corresponds with $\left(k_{8}, \ldots, k_{15}\right)$,
- $k^{[11]}=\left(k_{0}{ }^{[11]}, \ldots, k_{7}{ }^{[11]}\right)$ corresponds with $\left(k_{16}, \ldots, k_{23}\right)$.


## Chapter 5 - Backdoored Encryption Algorithm 1

```
Algorithm 9 - An implementation of the step idx=4 in part 2.
Cand }\leftarrow[
For each of the 2 25 candidates ( }\mp@subsup{k}{0}{},\mp@subsup{k}{3}{},\mp@subsup{k}{7}{}\mathrm{ ) for ( }\mp@subsup{k}{0}{[11]},\mp@subsup{k}{3}{[11]},\mp@subsup{k}{7}{[11]})\mathrm{ do
    Initialization of the filter over the ciphertexts
    Filter }\leftarrow
    (\mp@subsup{\mathbf{t}}{0}{},\mp@subsup{\mathbf{t}}{3}{},\mp@subsup{\mathbf{t}}{7}{})\leftarrow(\mp@subsup{\mathbf{S}}{0}{-1}(\mp@subsup{k}{0}{}+\mp@subsup{\mathbf{u}}{0}{}),\mp@subsup{\mathbf{S}}{3}{-1}(\mp@subsup{k}{3}{}+\mp@subsup{\mathbf{u}}{3}{}),\mp@subsup{\mathbf{S}}{3}{-1}(\mp@subsup{k}{7}{}+\mp@subsup{\mathbf{u}}{7}{}))
    For each c\in\mathcal{C}}\mathrm{ do
        (to,t , , t7 )\leftarrow (S S0
        If }\mp@subsup{t}{0}{}\in(\mp@subsup{\mathbf{t}}{0}{}+\mp@subsup{V}{0}{})\mathrm{ and }\mp@subsup{t}{3}{}\in(\mp@subsup{\mathbf{t}}{3}{}+\mp@subsup{V}{3}{})\mathrm{ and }\mp@subsup{t}{7}{}\in(\mp@subsup{\mathbf{t}}{7}{}+\mp@subsup{V}{3}{})\mathrm{ then
            Filter }\leftarrow\mathrm{ Filter }\cup{c
    Loop over the new bundle of the key
    For each }\mp@subsup{k}{4}{}\in\mp@subsup{\mathbb{F}}{2}{10}\mathrm{ do
        Score }\leftarrow
    \mp@subsup{t}{4}{}}\leftarrow\mp@subsup{\mathbf{S}}{0}{-1}(\mp@subsup{k}{4}{}+\mp@subsup{u}{4}{}
    For each c\inFilter do
            t
            If }\mp@subsup{t}{4}{}\in(\mp@subsup{\mathbf{t}}{4}{}+\mp@subsup{V}{0}{})\mathrm{ then
                Score }\leftarrow\mathrm{ Score +1
            Saving ( }\mp@subsup{k}{0}{},\mp@subsup{k}{3}{},\mp@subsup{k}{4}{},\mp@subsup{k}{7}{})\mathrm{ if its score is high enough
            If #Cand \leq 2 }\mp@subsup{}{}{15}\mathrm{ then
            Insert (( }\mp@subsup{k}{0}{},\mp@subsup{k}{3}{},\mp@subsup{k}{4}{},\mp@subsup{k}{7}{})\mathrm{ , Score) in Cand
            Else if Score is greater than the lowest score in Cand then
            Remove the lowest scored key of Cand
            Insert (( }\mp@subsup{k}{0}{},\mp@subsup{k}{3}{},\mp@subsup{k}{4}{},\mp@subsup{k}{7}{})\mathrm{ ,Score) in Cand
Return Cand
```



Figure 5.9: Cryptanalysis using the backdoor (Part 3).
It is then easily seen that

$$
\left(k_{0}^{[10]}, k_{1}^{[10]}, k_{2}^{[10]}, k_{3}^{[10]}\right)=\left(k_{0}^{[11]}, k_{1}^{[11]}, k_{2}^{[11]}, k_{3}^{[11]}\right)+\left(k_{4}^{[11]}, k_{5}^{[11]}, k_{6}^{[11]}, k_{7}^{[11]}\right) .
$$

Thus, the 40 leftmost bits of $k^{[10]}$ are determined by $k^{[11]}$. Using this equality, it is possible to partially decrypt the last two rounds for every candidate for $k^{[11]}$. Again, the algorithm SelectKeys is used to distinguish between candidates.

Instead of wasting time understanding the definition of $G$ stated hereinafter, we encourage the reader to compare it with Figure 5.9 which speaks for itself. Let us consider

$$
\begin{aligned}
G^{\prime}:\left(F_{2}^{10}\right)^{8} \times\left(\mathbb{F}_{2}^{10}\right)^{\{0,2,5,7\}} \longmapsto & \left(\mathbb{F}_{2}^{10}\right)^{4} \\
\left(\left(k_{i}\right)_{i<8},\left(c_{i}\right)_{i \in\{0,2,5,7\}}\right) \longmapsto & \left(S_{0}^{-1}\left(c_{0}+k_{0}\right)+k_{0}+k_{4}, S_{1}^{-1}\left(c_{5}+k_{5}\right)+k_{1}+k_{5},\right. \\
& \left.S_{2}^{-1}\left(c_{2}+k_{2}\right)+k_{2}+k_{6}, S_{3}^{-1}\left(c_{7}+k_{7}\right)+k_{3}+k_{7}\right) .
\end{aligned}
$$

Then, let $G$ be the mapping from $\left(F_{2}^{10}\right)^{8} \times\left(\mathbb{F}_{2}^{10}\right)^{\{0,2,5,7\}}$ to $\left(\mathbb{F}_{2}^{10}\right)^{4}$ given by

$$
G=\left(S_{0}\left\|S_{1}\right\| S_{2} \| S_{3}\right)^{-1} \circ M^{-1} \circ G^{\prime} .
$$

Define G in the same way as before and let $V^{\prime}=\prod_{i=0}^{3} V_{i}$. Finally, run Selectkeys as in line 12 of Algorithm 5.4. The candidate which has the highest score is then the last round key $k^{[11]}$.

To explain why Parts 2 and 3 of this cryptanalysis are complementary, let us take a closer look at the $2^{15}$ candidates obtained previously. Most of them are in fact really close to $k^{[11]}$, more precisely, they have at most three bundles different from $k^{[11]}$. This observation is not surprising because when decrypting the last round,

## Chapter 5 - Backdoored Encryption Algorithm 1

each bundle of the key affects only one bundle of the output. As a direct consequence, close candidates give rise to close one-round decrypted ciphertexts. This explains why the algorithm SelectKeys, as used in Part 2, may assign similar scores to close candidates.

By contrast, the mapping $G$ defined above yields very different outputs when used with close candidate keys. Such a property comes from the high diffusion provided by $M^{-1}$. Thus, this part is more effective where the previous part has its main weakness. Moreover, the side effects are limited here since we decrypt two rounds instead of one.

### 5.4.4. Part 4: Obtaining Candidates for the Remaining Bits

The round function of the key schedule being bijective, it is sufficient to know the 120 output bits of the last round to compute the cipher key. Until now, we have recovered the last round key $k^{[11]}$, accounting for 80 of these 120 bits. The 40 remaining bits are the 40 rightmost bits of $k^{[10]}$, also denoted by $\left(k_{i}{ }^{[10]}\right)_{4 \leq i<8}$. This fourth part intends to find $2^{15}$ candidates for these unknown bits.

Since the key $k^{[11]}$ is now known, it is possible to undo the last round for every ciphertext. The cryptanalysis is then reduced to the attack of the second to last round. However, the method used in Part 2 cannot be directly applied here since the second to last round involves the MDS mapping $M$. Let $x$ and $k$ be elements of $\left(\mathbb{F}_{2}^{10}\right)^{4}$ and observe that

$$
M(x)+k=M(x)+M\left(M^{-1}(k)\right)=M\left(x+M^{-1}(k)\right)=M\left(x+k^{\prime}\right)
$$

where $k^{\prime}=M^{-1}(k)$. Thus, the key addition and the mapping $M$ can be switched provided that the key is replaced. According to this observation, define

$$
\left(k_{i}^{\prime[10]}\right)_{4 \leq i<8}=M^{-1}\left(\left(k_{i}^{[10]}\right)_{4 \leq i<8}\right) .
$$

Therefore, the last two rounds of BEA-1 can equivalently be represented as in Figure 5.10 .

Thanks to this representation, candidates for the key $\left(k_{i}^{\prime[10]}\right)_{4 \leq i<8}$ can be obtained using SelectKeys as in Part 2. To this end, we first need to partially undo the last round using $k^{[11]}$. Following Figure 5.10, define

$$
\begin{aligned}
f:\left(\mathbb{F}_{2}^{10}\right)^{\{1,3,4,6\}} & \longrightarrow\left(\mathbb{F}_{2}^{10}\right)^{4} \\
\left(c_{i}\right)_{i \in\{1,3,4,6\}} & \longmapsto M^{-1}\left(S_{0}^{-1}\left(c_{4}+k_{4}^{[11]}\right), S_{1}^{-1}\left(c_{1}+k_{1}{ }^{[11]}\right)\right. \\
& \left.S_{2}^{-1}\left(c_{6}+k_{6}{ }^{[11]}\right), S_{3}^{-1}\left(c_{3}+k_{3}{ }^{[11]}\right)\right) .
\end{aligned}
$$

The set $\left\{f\left(\left(c_{i}\right)_{i \in\{1,3,4,6\}}\right) \mid c \in \mathcal{C}\right\}$ of these "new" ciphertexts is denoted by $\mathcal{C}^{\prime}$ and the corresponding coset representative is $\mathbf{u}^{\prime}=\mathbf{f}\left(\left(\mathbf{u}_{i}\right)_{i \in\{1,3,4,6\}}\right)$. To be more consistent with Figure 5.10, the bundles of $\mathbf{u}^{\prime}$ and of the elements of $\mathcal{C}^{\prime}$ are indexed from 4 to 7 included. The remainder of the attack is similar to Part 2 as the candidates are obtained bundle by bundle. The first step gets candidates for the bundle's indices 4


Figure 5.10: Cryptanalysis using the backdoor (Part 4).
and 7. The second and the third steps add the indices 5 and 6 respectively. If $E$ denotes the set of the current bundle's indices, then the parameters of SelectKeys are the set $\mathcal{C}_{E}^{\prime}=\left\{\left(c_{i}^{\prime}\right)_{i \in E} \mid\left(c_{i}^{\prime}\right)_{4 \leq i<8} \in \mathcal{C}^{\prime}\right\}$, the mapping

$$
\begin{aligned}
G_{E}:\left(\mathbb{F}_{2}^{10}\right)^{E} \times\left(\mathbb{F}_{2}^{10}\right)^{E} & \longrightarrow\left(\mathbb{F}_{2}^{10}\right)^{E} \\
\left(\left(k_{i}^{\prime}\right)_{i \in E},\left(c_{i}^{\prime}\right)_{i \in E}\right) & \longmapsto\left(S_{i \bmod 4}^{-1}\left(c_{i}^{\prime}+k_{i}^{\prime}\right)\right)_{i \in E},
\end{aligned}
$$

its equivalent $\mathbf{G}_{E}$ and the subspace $V_{E}=\prod_{i \in E} V_{i \bmod 4}$ of $\left(\mathbb{F}_{2}^{10}\right)^{E}$. The other details are given in Algorithm 5.4. At the end of this part, every candidate $k^{\prime}=\left(k_{i}^{\prime}\right)_{4 \leq i<8}$ for $\left(k_{i}^{\prime}{ }^{[10]}\right)_{4 \leq i<8}$ gives rise to a candidate $k=M\left(k^{\prime}\right)$ for $\left(k_{i}{ }^{[10]}\right)_{4 \leq i<8}$.

### 5.4.5. Part 5: Deducing the Cipher Key

Concatenating the candidates for $\left(k_{i}{ }^{[10]}\right)_{4 \leq i<8}$ with $k^{[11]}$ yields $2^{15}$ candidates for the output of the key schedule's last round. To obtain the corresponding candidates for the cipher key, we need to reverse the rounds of the key schedule.

Referring to Figure 5.1, the $i$-th round of the key schedule maps the element ( $X_{0}, X_{1}, X_{2}$ ) of $\left(\mathbb{F}_{2}^{40}\right)^{3}$ to ( $Y_{0}, Y_{1}, Y_{2}$ ) according to the following equalities

$$
Y_{0}=X_{0}+f_{i}\left(X_{2}\right), \quad Y_{1}=Y_{0}+X_{1}, \quad Y_{2}=Y_{1}+X_{2}
$$

where $f_{i}$ denotes the permutation of $\left(\mathbb{F}_{2}^{10}\right)^{4}$ defined for each $X$ to be

$$
f_{i}(X)=\left(3^{i} \bmod 2^{10}, 0,0,0\right)+\left(S_{0}\left\|S_{1}\right\| S_{2} \| S_{3}\right) \circ M(X) .
$$

Using this notation, it easily seen that

$$
X_{0}=Y_{0}+f_{i}\left(Y_{1}+Y_{2}\right), \quad X_{1}=Y_{0}+Y_{1}, \quad X_{2}=Y_{1}+Y_{2}
$$

## Chapter 5 - Backdoored Encryption Algorithm 1

These equalities describe how to reverse each round of the key schedule, and thus how to recover the $2^{15}$ candidate cipher keys.

Finally, it just remains to test these cipher key candidates to complete the cryptanalysis. To be efficient, choose one plaintext/ciphertext pair ( $p, c$ ) and check whether or not the encryption of $p$ under the candidate $K$ is equal to $c$. In case of equality, repeat this process for all pairs available to prevent false positive results. Otherwise, the candidate is discarded. Obviously, the right cipher key is the one which passes all tests.

### 5.5. Conclusion

When parallelized and optimized as described in Algorithm 9, our cryptanalysis of BEA-1 recovers the full 120 -bit cipher key in about 20 seconds on a laptop computer. Thanks to its small computing time, we performed several times this attack and verified experimentally that its success probability is greater than $95 \%$. When this attack fails, the cryptanalyst can generally still recover the cipher key with the same data but needs more than $2^{15}$ candidates in each step. Thus, using more candidates increases the success probability but also the time-complexity of the cryptanalysis.

As noted in Section 5.3, the main idea our cryptanalysis is really close to Harpes' partitioning cryptanalysis [52]. However, some significant differences emerge. First, the number of parts in the output partition is assumed to be small in a partitioning cryptanalysis. Typically, this number is equal to 2,4 or 8 . In contrast, the output partition used in our cryptanalysis consists of all the $2^{40}$ cosets of the subspace $W$.

Second, partitioning cryptanalysis considers classes of the last round keys where only a few bits influence the output cosets of the messages. Because its complexity is proportional to the number of key classes, a partitioning cryptanalysis is efficient only if this number is reasonably small. In the case of BEA-1, each bit of the last round key impacts the output cosets of the messages. In other words, whenever one bit of the last round key is changed, at least one plaintext is encrypted in another coset of $W$. Since there are $2^{80}$ possible last round keys, a basic partitioning cryptanalysis is ineffective on BEA-1. This problem was addressed in the second part of our cryptanalysis (see Section 5.4.2) as we introduced a trick to compute the best round keys bundle by bundle.

Additionally, a partitioning cryptanalysis updates for each key class as many counters as there are cosets in the output partition. In our algorithm SelectKeys presented in Section 5.3.2, we manage only one counter per key as we exploit the secret structure of the round function and the output coset of the ciphertext space. Lastly, our attack recovers the full 120-bit cipher key whereas a partitioning cryptanalysis recovers only a few bits of the last round key.

We should now compare probabilistic and non-probabilistic partition-based backdoor ciphers. By virtue of Theorem 5.2, BEA-1 can be transformed into a partitionbased backdoor cipher by simply replacing its S-boxes $S_{i}$ with their secret counterparts $\mathbf{S}_{i}$. Now, assume further that

- the last round of BEA-1 includes the MixColumns operation,
- the key schedule also uses the secret S-boxes and
- the mappings $M$ and $\left(\mathbf{S}_{0}\|\ldots\| \mathbf{S}_{3}\right)$ are switched in the round function of the key schedule (see Figure 5.1).
It is easily seen that the round function of this new version of BEA-1 preserves the linear partition $\mathcal{L}(V)$ and the same applies to the whole encryption function. As observed at the end of Section 5.2.1, when two cipher keys $K$ and $K^{\prime}$ are in the same coset of $\prod_{i=0}^{11} V_{i \bmod 4}$, then the derived round keys $k^{[i]}$ and $k^{\prime[i]}$ are pairwise in the same coset of $V$. As a consequence, this backdoor cipher is vulnerable to the key schedule dependent attack presented in Section 3.1.3. Using one or two known plaintexts, the coset containing the cipher key is obtained with at most $2^{60}$ encryptions and then the right cipher key is searched within the $2^{60}$ elements of this coset. Summarizing, this cryptanalysis recovers the cipher key using at most $2^{61}$ encryptions or $2^{60}$ on average. By comparison, our cryptanalysis of the probabilistic version requires $2^{16}$ chosen plaintexts but has a much better time complexity. Moreover, the differential probability and linear potential matrices of the modified S-boxes $S_{i}$ are much less suspicious than the ones of the secret S-boxes $\mathbf{S}_{i}$.

Before concluding this thesis, let us consider the two criteria to prevent partitionbased backdoors given in Section 4.4. We begin with Calderini's criterion. As well as the AES, the diffusion layer of BEA-1 is strongly proper over two rounds. It can be proven with an exhaustive search that for each secret S-box $\mathbf{S}_{i}$, any subspace $V$ of $\mathbb{F}_{2}^{10}$ such that $W=\mathbf{S}_{i}(V)+\mathbf{S}_{i}(0)$ is also a subspace of $\mathbb{F}_{2}^{10}$ is at most 6-dimensional. Consequently, the secret S-boxes are strongly 3 -anti-invariant. Since the smallest integer $r_{i}$ such that $2^{10} \times \mathrm{DP}_{\mathbf{S}_{i}}^{\max ^{2}} \leq 2^{r_{i}}$ is 6 , the conditions of Theorem 4.37 are not fulfilled and we hopefully cannot prove that non-probabilistic version of BEA-1 is not a partition-based backdoor cipher, as it is one. Nonetheless, it can be verified that every modified S-box $S_{i}$ is strongly 7 -anti-invariant. Calderini's criterion then proves that BEA-1 is not a partition-based backdoor cipher. This fact does not contradicts Theorem 4.37 since BEA-1 is a probabilistic partition-based backdoor cipher. However, this proves that Calderini's criterion does not apply to this broader family of backdoor ciphers.

Let us now consider our criterion given in Theorem 4.33. By simply looking at the maximum differential probability and linear potential of each S-box, we can see that the conditions are not fulfilled neither for BEA-1 or its non-probabilistic version. Moreover, since these maximum values are really close to the bounds of Figure 4.10, our criterion suggests that each S-box might almost maps a linear partition associated with a 5 -dimensional subspace to another one.

To conclude let us motivate future research around backdoor ciphers. Even if bydesign backdoors are undesirable in block ciphers, their study can contribute to design better ciphers and to improve our understanding of classical cryptanalysis. In fact, partition-based backdoor ciphers are closely related to invariant subspace, constantdimensional subspace trail and partitioning cryptanalysis. We proved in Chapter 3 that plausible partition-based backdoor ciphers must have S-boxes equivalent to imprimitive S-boxes. Then, we showed in Chapter 4 that such S-boxes are either highly resistant to differential cryptanalysis or to linear cryptanalysis but not both.

## Chapter 5 - Backdoored Encryption Algorithm 1

As a consequence, our study yields unexpected links between differential, linear and partitioning cryptanalysis. Combined with the complementary work of Calderini, we have now two criteria to prove that a cipher does not have a partition-based backdoor but further interesting researches should be dedicated to prove other criteria for the probabilistic version. Along a similar line, a new variation of differential cryptanalysis was recently proposed by Blondeau, Civino and Sala [16]. This new perspective is directly inspired by the family of backdoor ciphers based on hidden sums [19. In addition, searching for backdoors naturally implies to consider different properties than the ones addressed by classical cryptanalysis, thereby increasing the chance of discovering new effective attacks. Finally, it is worth recalling that the question whether backdoors that are both efficient and undetectable can be inserted in practical block ciphers remains open.


In this appendix, we give the specifications of the mappings used in our probabilistic partition-based cipher BEA-1.

|  | 200 | 100 | 080 | 040 | 020 | 010 | 008 | 004 | 002 | 001 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 334 | 259 | 21D | OE4 | 193 | 266 | 343 | 3ED | 354 | 17 |
|  | 3DA | 306 | 39E | 262 | 080 | 398 | 229 | 34C | 251 | 37B |
|  | 295 | 237 | 131 | 3D1 | 6B | OB | 155 | 30 | 37E | 318 |
| $L_{V_{3}}(x)$ | 290 | 15D | 0 | 2BE | 25F | 1D1 | 21E | 13 | OD | 15 |
| $L_{W_{0}}(x)$ | 3E8 | 386 | 067 | 190 | 158 | 16A | 11B | 30 | 05 | OB |
| $L_{W_{1}}(x)$ | 364 | 33E | 3 A 7 | 119 | 1D2 | 04B | 3B | OD5 | 027 | 2C8 |
|  | 324 | 188 | 3CB | 1B0 | 131 | 1A9 | 095 | 10 | 36F | 2 A |
|  | 262 | 1 A 5 | 34E | 0B7 | 3ED | 0F0 | 2FE | 191 | 332 |  |
| $\left(L_{V_{0}}\right)^{-1}$ | 3BF | 268 | OBB | 379 | 17 B | 055 | 06 | 2 F | 35 | 1 F |
| $\left(L_{V_{1}}\right)^{-1}(x)$ | 13D | OAD | 020 | 2C7 | 36 D | 2B4 | 314 | 047 | 0D7 | 4 |
| $\left(L_{V_{2}}\right)^{-1}(x)$ | 361 | 070 | 133 | 02A | 2B8 | 3CC | ODC | 21A | 08B | 18 |
| $\left(L_{V_{3}}\right)^{-1}(x)$ | 1E9 | 3D1 | OB | 245 | 0F6 | 35 | 1D | 074 | 31 |  |
| $\left(L_{W_{0}}\right)^{-1}(x)$ | 026 | 0E9 | 104 | 29D | 351 | 053 | 207 | 3F9 | 332 | 187 |
| $\left(L_{W_{1}}\right)^{-1}(x)$ | 142 | 1B0 | 07 | 3D | 196 | 088 | 2 E 0 | OB7 | 2BB | 398 |
| $\left(L_{W_{2}}\right)^{-1}(x)$ | 02D | OAA | 205 | 0F1 | 375 | 19A | 3AF | 1F2 | 339 | 265 |
| $\underline{\left(L_{W_{3}}\right)^{-1}(x)}$ | 0A6 | 3B3 | 045 | 32B | 1E4 | 29A | 2AD | 27A | 069 | 168 |

Figure A.1: The transformation mappings given over the standard basis of $\mathbb{F}_{2}^{10}$.

## Appendix A - Specifications of BEA-1 Building Blocks

| $x$ | $x \times M_{U}$ | $x \times M_{V}$ | $P_{U \rightarrow V}(x)$ |
| :---: | :---: | :---: | :---: |
| $(10,00,00,00)$ | $(07,06,1 \mathrm{E}, 17)$ | $(0 \mathrm{E}, 16,02,14)$ | $(07,01,1 \mathrm{C}, 18)$ |
| $(08,00,00,00)$ | $(11,03,0 \mathrm{~F}, 19)$ | $(07,0 \mathrm{~B}, 01,0 \mathrm{~A})$ | $(05,16,14,03)$ |
| $(04,00,00,00)$ | $(1 \mathrm{~A}, 13,15,1 \mathrm{E})$ | $(11,17,12,05)$ | $(0 \mathrm{~A}, 01,1 \mathrm{C}, 1 \mathrm{C})$ |
| $(02,00,00,00)$ | $(0 \mathrm{D}, 1 \mathrm{~B}, 18,0 \mathrm{~F})$ | $(1 \mathrm{~A}, 19,09,10)$ | $(02,1 \mathrm{~F}, 1 \mathrm{E}, 1 \mathrm{C})$ |
| $(01,00,00,00)$ | $(14,1 \mathrm{~F}, 0 \mathrm{C}, 15)$ | $(0 \mathrm{D}, 1 \mathrm{E}, 16,08)$ | $(01,1 \mathrm{~B}, 13,04)$ |
| $(00,10,00,00)$ | $(06,07,17,1 \mathrm{E})$ | $(16,0 \mathrm{E}, 14,02)$ | $(07,08,01,11)$ |
| $(00,08,00,00)$ | $(03,11,19,0 \mathrm{~F})$ | $(0 \mathrm{~B}, 07,0 \mathrm{~A}, 01)$ | $(02,1 \mathrm{E}, 1 \mathrm{~B}, 1 \mathrm{~F})$ |
| $(00,04,00,00)$ | $(13,1 \mathrm{~A}, 1 \mathrm{E}, 15)$ | $(17,11,05,12)$ | $(16,06,1 \mathrm{E}, 0 \mathrm{D})$ |
| $(00,02,00,00)$ | $(1 \mathrm{~B}, 0 \mathrm{D}, 0 \mathrm{~F}, 18)$ | $(19,1 \mathrm{~A}, 10,09)$ | $(0 \mathrm{~F}, 11,0 \mathrm{C}, 16)$ |
| $(00,01,00,00)$ | $(1 \mathrm{~F}, 14,15,0 \mathrm{C})$ | $(1 \mathrm{E}, 0 \mathrm{D}, 08,16)$ | $(11,0 \mathrm{E}, 02,0 \mathrm{~A})$ |
| $(00,00,10,00)$ | $(1 \mathrm{E}, 17,07,06)$ | $(02,14,0 \mathrm{E}, 16)$ | $(1 \mathrm{~F}, 0 \mathrm{C}, 08,1 \mathrm{~B})$ |
| $(00,00,08,00)$ | $(0 \mathrm{~F}, 19,11,03)$ | $(01,0 \mathrm{~A}, 07,0 \mathrm{~B})$ | $(17,15,17,16)$ |
| $(00,00,04,00)$ | $(15,1 \mathrm{E}, 1 \mathrm{~A}, 13)$ | $(12,05,11,17)$ | $(1 \mathrm{D}, 04,0 \mathrm{E}, 00)$ |
| $(00,00,02,00)$ | $(18,0 \mathrm{~F}, 0 \mathrm{D}, 1 \mathrm{~B})$ | $(09,10,1 \mathrm{~A}, 19)$ | $(11,0 \mathrm{E}, 19,15)$ |
| $(00,00,01,00)$ | $(0 \mathrm{C}, 15,14,1 \mathrm{~F})$ | $(16,08,0 \mathrm{D}, 1 \mathrm{E})$ | $(16,1 \mathrm{~F}, 06,14)$ |
| $(00,00,00,10)$ | $(17,1 \mathrm{E}, 06,07)$ | $(14,02,16,0 \mathrm{E})$ | $(0 \mathrm{~F}, 03,16,03)$ |
| $(00,00,00,08)$ | $(19,0 \mathrm{~F}, 03,11)$ | $(0 \mathrm{~A}, 01,0 \mathrm{~B}, 07)$ | $(0 \mathrm{~B}, 12,03,0 \mathrm{D})$ |
| $(00,00,00,04)$ | $(1 \mathrm{E}, 15,1 \mathrm{l}, 1 \mathrm{~A})$ | $(05,12,17,11)$ | $(1 \mathrm{~F}, 1 \mathrm{D}, 1 \mathrm{~B}, 02)$ |
| $(00,00,00,02)$ | $(0 \mathrm{~F}, 18,1 \mathrm{~B}, 0 \mathrm{D})$ | $(10,09,19,1 \mathrm{~A})$ | $(18,12,0 \mathrm{~A}, 15)$ |
| $(00,00,00,01)$ | $(15,0 \mathrm{C}, 1 \mathrm{~F}, 14)$ | $(08,16,1 \mathrm{E}, 0 \mathrm{D})$ | $(17,05,05,05)$ |

Figure A.2: The linear mappings over $\left(\mathbb{F}_{2}^{10}\right)^{4}$ associated with $M_{U}, M_{V}$ and the linear mapping $P_{U \rightarrow V}$.

| $x$ | $M(x)$ | $M^{-1}(x)$ |
| :---: | :---: | :---: |
| (200, 000, 000, 000) | (13E, 20F, 253, 0BC) | (2D8, 209, 353, 243) |
| (100, 000, 000, 000) | (35C, 13E, 212, 110) | ( $0 \mathrm{~F} 5,1 \mathrm{BD}, 210,210$ ) |
| (080, 000, 000, 000) | (32C, 199, 2C5, 07A) | (1E9, 3FE, 238, 329) |
| (040, 000, 000, 000) | (3C6, 010, 0EC, 261) | (002, 246, 2E2, 380) |
| (020, 000, 000, 000) | (231, 120, 322, 016) | (322, 3FD, 3D5, 0E5) |
| (010, 000, 000, 000) | (2D9, 10A, 0C4, 095) | (0AD, 337, 3C5, 2D4) |
| (008, 000, 000, 000) | (215, 11F, 1E0, 2E7) | (08D, 04D, 016, 34C) |
| (004, 000, 000, 000) | (23F, 15B, 0C7, 0A7) | ( $1 \mathrm{AB}, 11 \mathrm{E}, 05 \mathrm{~F}, 3 \mathrm{~A} 4)$ |
| (002, 000, 000, 000) | (344, 394, 342, 165) | (1AE, 1E9, 2CB, 245) |
| (001, 000, 000, 000) | $(112,1 \mathrm{BC}, 36 \mathrm{C}, 0 \mathrm{OC5})$ | (10B, 221, 09D, 398) |
| (000, 200,000,000) | (0E6, OED, 314, 289) | $(395,295,38 \mathrm{D}, 129)$ |
| (000, 100, 000, 000) | (17E, 011, 198, 3C5) | (2D7, 1F4, 378, 157) |
| (000, 080, 000, 000) | (15E, 0BF, 1E2, 04F) | (0BD, 1B1, 18E, 2AB) |
| (000, 040, 000, 000) | (006, 131, 32E, 12B) | (3AA, 29E, 239, 1C0) |
| (000, 020, 000, 000) | (39A, 062, 38C, 2EB) | (3D9, 069, 21B, 11B) |
| (000, 010, 000, 000) | (1F4, 1C5, 1FF, 31D) | (06D, 1BE, 3EB, 0BE) |
| (000, 008, 000, 000) | (022, 37D, 08D, 3D4) | (3D1, 236, 09D, 2F1) |
| (000, 004, 000, 000) | (13B, 2FA, 328, 38C) | (0EB, 2FD, 3C3, 176) |
| (000, 002, 000, 000) | (0CC, 32A, 01A, 2DB) | $(055,128,25 \mathrm{~A}, 17 \mathrm{~F})$ |
| (000, 001, 000, 000) | (237, 252, 004, 0F8) | (07D, 2BB, 037, 3C8) |
| (000, 000, 200, 000) | (009, 175, 254, 3ED) | (0A6, 050, 36D, 016) |
| (000, 000, 100, 000) | (2D5, 29F, 072, 04D) | $(263,36 C, 361,369)$ |
| (000, 000, 080, 000) | (09A, 1DD, 336, 34B) | ( $0 \mathrm{C} 8,111,34 \mathrm{~B}, 38 \mathrm{E})$ |
| (000, 000, 040, 000) | (269, 2CC, 27E, 1CD) | (169, 1A1, 02D, 39B) |
| (000, 000, 020, 000) | (1B2, 0A7, 178, 208) | (009, 1D9, 3CC, 131) |
| (000, 000, 010, 000 ) | (189, 2AB, 1A6, 39D) | $(141,222,031,28 \mathrm{~A})$ |
| (000, 000, 008, 000) | (0DC, 0B1, 061, 3DE) | (1C7, 3F1, 063, 33C) |
| (000, 000, 004, 000) | (019, 08E, 280, 1A7) | $(084,128,167,20 B)$ |
| (000, 000, 002, 000) | (38B, 1A6, 221, 260) | (0D0, 34D, 18C, 354) |
| (000, 000, 001, 000) | (075, 380, 371, 2E9) | (15E, 23B, 378, 376) |
| (000, 000, 000, 200) | (099, 176, 3BC, 031) | (03D, 208, 27E, 249) |
| (000, 000, 000, 100) | (38E, 3D2, 2CD, 21C) | $(005,38 \mathrm{~F}, 215,2 \mathrm{DF})$ |
| (000, 000, 000, 080) | (1C7, 259, 17E, OBE) | (14F, 3D2, 0E2, 1C7) |
| (000, 000, 000, 040) | (165, 3BA, 19B, 0F7) | $(211,2 \mathrm{D} 9,1 \mathrm{~B} 2,362)$ |
| (000, 000, 000, 020) | (37F, 282, 3A4, 3D8) | (13C, 355, 058, 07F) |
| (000, 000, 000, 010) | $(256,130,382,067)$ | (19A, 0E6, 364, 0F2) |
| (000, 000, 000, 008) | (370, 1D0, 3CD, 07F) | $(322,319,244,300)$ |
| (000, 000, 000, 004) | (22D, 1C8, 221, 18B) | (2BE, 1DD , 223, 1FA) |
| (000, 000, 000, 002) | (058, 044, 3A0, 281) | (04A, 1EC, 1B6, 3B4) |
| (000, 000, 000, 001) | (28D, 172, 3EA, 24E) | (015, 371, 2DC, 0E2) |

Figure A.3: Specification of the diffusion $M$ and its inverse $M^{-1}$.

Appendix A - Specifications of BEA-1 Building Blocks

|  | . 0 | 1 | 2 | 3 |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 00 | OBA | 026 | OAO | 1E1 | 183 | 3DB | 1A4 | 084 | 110 | 350 | 085 | 2E5 | 3B4 | 195 | 359 | 2F6 |
| 01. | 33A | 26B | 209 | 07E | 1 CE | 2E3 | OC | 136 | 12 | C8 | 3D | 05 | 040 | 3F2 | 09F | 322 |
| 02 | 11B | 7 F | 139 | 07D | 2CF | 02A | 268 | 227 | 10A | C5 | 12B | 01 | 16 | 20D | 1E7 | 35B |
| 03. | 313 | OCD | 11 E | 1E6 | 117 | 355 | 182 | OE6 | 094 | 1B9 | 19C | 28C | 255 | 336 | OA | 19D |
|  | 2BC | 1A9 | 31B | 02E | 82 | 2AE | 27 | 2E9 | 3A | DD | 01 | 2D | 30 | 35 | 159 |  |
|  | 3DD | 12A | 248 | 3C | 28B | 191 | 02 | 173 | 018 | 38D | 1A1 | 185 | 0 | 156 | 378 | 12 |
|  | 10B | 143 | 05D | 3FA | 038 | 3DE | 081 | 0F9 | 2D1 | FB | 1C7 | 30 | DC | 16A | 2D8 | 23F |
|  | 030 | 1EB | 3 | 311 | 36D | 3BD | 3C9 | 348 | 26 | 1 AF | 071 | 3E | 3BA | 3AB | 1B8 | 3CA |
| 08 | 290 | 18 | 21B | 0F6 | 3FF | 122 | 1B2 | 360 | 1D6 | 1B6 | 3D4 | 3BB | 3B | OEA | 09 | 308 |
|  | 349 | 86 | OAE | 15 | 253 | 058 | OBB | 3D5 | 14B | 1 A 3 | 23E | 053 | 35D | 277 | 38 | E2 |
|  | 233 | 2B8 | 2AF | OD | 1B1 | 105 | OB3 | 215 | 2A | 27F | 2DB | 17E | 12 | 3A2 | 18 E | AC |
| OB | 321 | 09C | 294 | 04 | 036 | 2F1 | 3D2 | 18 | 14C | 304 | 128 | 06 | 198 | 2F4 | 3DC | 370 |
| 0 C | 138 | 324 | $23 C$ | 1FD | 082 | 247 | 005 | OA | 0FO | 27 | 15 | 17B | 1A | 1 C | 04 | 132 |
| OD. | 12 F | OCC | 075 | 10 | 3E0 | 021 | 1A | 211 | 3E | 17A | 276 | 28 | OA9 | 12 | 1 | 048 |
|  | 201 | 8 F | 0B1 | 00 | 179 | 32E | 12 |  | 1 E 3 | 109 | 079 | 37 | 297 | 96 | 12 | 23 |
|  | 165 | OAC | 18B | OAB | 1FF | 13D | 25 | 3D3 | 11 | 22 B | 21 C | 1BE | 187 | 30E | 34 | 18 |
|  | 269 | 343 | 29 | 39 | 1 AD | 1D | 023 | 3ED | 1B | 35E | 2D | 04 | OF1 | 3F1 | 31 | A 7 |
|  | 287 | 3C3 | 2A5 | 213 | 3E4 | 3DA | OFD | 140 | 38 | 2C | 15 | 25 | 15F | 02 | 1F | 1 ED |
|  | 1 C 6 | 051 | 062 | 090 | 214 | 230 | 190 | 15D | OA1 | 18 | 03 | OB | 1DA | 23 | 3D | 383 |
|  | 331 | 06D | 02D | 009 | 2FC | 3AD | 2A | 363 | 1EF | 38 | 39A | 2DC | 3BF | 10 | 39 |  |
|  | 03E | ODE | 1BC | 067 | OCF | 155 | 2 CE | 240 | 05E | E8 | OC4 | 149 | 08C | 3E5 |  |  |
|  | 1D1 | 228 | 3D | OEO | 3F6 | 19 | 19 | 27D | 2B | 35C | OE3 | 171 | 180 | 022 | 00E | 358 |
|  | 161 | OEE | 365 | 15B | OC3 | 2CD | 3E1 | 06C | 119 | 283 | 31E | 2B | 212 | 226 | 07 | 382 |
|  | 38 C | 1D3 | 150 | OB2 | 22 C | 314 | 056 | 216 | 364 | 1 | 1E9 | 02 | 176 | 389 | 2F2 | 73 |
|  | 06F | 27 E | 027 | 14 | 17 | 26D | 1BA |  | 03 |  | 3C | 2F | 22 | E1 |  |  |
|  | 14 F | 293 | 144 | 0FB | 2F0 | 2F3 | OF4 | 1- | 0C6 | 06 | 02 | 31 | 3E | 2DD | 27 |  |
|  | 17C | 041 | 080 | 2C5 | 072 | 08D | 339 | 2A | 1F | 1D | 2F | 28 | 01 | 18 | 246 | 206 |
|  | 091 | 03F | 259 | 18F | 1C3 | 27 | 319 | 15 | OD | OBD | 2D | 06 | 000 | 37 | 2F6 | A9 |
|  | 142 | 0F5 | 3EF | 03B | 3F8 | 344 | 3BC | 265 | OE | 33 | 23 | 08 | OA | 174 | 267 | 6 |
|  | 112 | 1D0 | 01C | 29 | 2 C | OE9 | 2B6 | 301 |  | 30 | 369 | 1 C 0 |  | 1 F 7 | 08 |  |
|  | 3CB | 34D | 2BE | 28 | 09A | 39D | 23 | 262 | 33 | 2 F |  | 2 C | 06 | 27A | 31 |  |
|  | 327 | 26C | 325 | 167 | 05B | 36 | 36 | 004 | 3F7 | 0F7 | 20B | 22 | 222 | 2D2 | OC | 196 |
|  | 33 F | 347 | 17D | 349 | 146 | 17 | 367 | 18A | 1D | OB5 | 09 | 3BE | 2C1 | B | 2A | 1B |
|  | 11D | 10 | 342 | 169 | 366 | 2EC | 088 | 361 | 29 | 131 | 2F | 19 | 18 | 3B | 00 | 24F |
|  | 031 | 063 | 3B6 | 281 | 0A5 | 070 | CB | 07B | 27 | 2C | 39 | 32 | 1 C 1 | 396 | 27 |  |
|  | 160 | OFF | 1A2 | OD4 | 024 | 24B | 178 | 1BD | 32 | 2E | 28 | 29 | 21 | 24 | 10 | 42 |
|  | 141 | 256 | 229 | 218 | OEB | 26 | 145 | 050 | 03 | OE5 | 300 | 3A | 1 E 2 | 34E | 223 | 20A |
|  | 164 | 02F | OC5 | 21 | 1A6 | 25 |  | 32 | 1B4 | 2EA | 10 | 3D0 | 381 | 371 | 392 | 0 |
|  | C8 | $3 F 3$ | 1F2 | 10 | OD1 | 1 BF | 2D6 | 32 | 39 | 25 E | 24 | 34 | 33 | 203 | 3B5 | 23A |
|  | 09E | 09 | 2C8 | 3A | OF | 26 | 0 | 3B | 3E | 3C | 2BB | 2 B | 36E | 13 E | 2 C |  |
|  | 014 | 00F | ODA | 133 | 163 | 05C | 0A | 1 E 5 | 01 | 37 | 043 | 1F | 18 | 07A | 3F | 3D |
|  | OFE | 25F | 26E | 3B7 |  | 2E8 | 3B1 | 1B | 01 | 2C | 0 C | 11 | 001 | 27 | 1D |  |
|  | 16 | 1 C 9 | OAD | 23 |  | 3CF | 3EC | 24E | 3F | 1D |  | 2B | 2 C | 338 | 1B5 | 25 C |
|  | 181 | 052 | 24 | 1F | 11F | 2E | 332 | 32 C | 1 C | A8 | 2B4 | 34 | OD | 30 | 006 |  |
|  | 13 F | 130 | 19 | 3A | 2DE | 2E | 3CE | 34 | $3 C$ | EF | 20 | 31 | 23D | 34 C | 05 | 19 F |
|  | 1E0 | 07 | 3F9 | 21 | 337 | OD | 14D | 353 | 12 | OC | 38 | 114 | 0 | 3D | 05 | 288 |
|  | 04F | B2 | 2CB | 039 | 234 | 2B5 | 2E1 | 32 | 2F | 15 | 11 | 37 | 3 A | 09 | 373 | 7F |
|  | 21 E | 06B | 087 | 2FD | 2ED | 2B | EA | 12 |  | 16 | 2 F | 2E0 |  | 3C2 | 3 |  |
|  | 11 | 01D | 3E | 04 | 15 | 25 | 1D9 | 37 | 16 D | 20E | 09 | 2B1 | 340 | 22E | 241 |  |
|  | 1F5 | OED | 19 | 298 | 3A7 | 30 | C | 05 | 35 | OE | 33 | 046 | 151 | 24 | 1EE | 235 |
|  | 12 E | A6 | 1A5 | 06 | 3A | 29 | 11 | 066 | 09 | 03 | 38A | 1F8 | F | 3B | 134 | 356 |
|  | 225 | OC | 3D9 | 2E | 0A8 | OB | 1FE |  |  | 7 | 2 F |  | 7 | 045 | 1E8 | 5A |
|  | 36 | 36F | 37 | 375 | 04D | 1FA | 25 | 13B | 089 | 22 | 399 | 00B | 15 | 2D | 068 | 28 |
|  | 357 | ODD | OB | 1B | 2A | 23 | 1 CA | 3F | 00 | 33 | 2A | 20 | 3EB | 008 | 12 | OA |
|  | 09B | 37A | 284 | 2D4 | OF3 | 28E | 237 | 31 | ODF | 368 | 38 | 060 | 37 | 31C | 29 | 26 |
|  | 100 | 394 | 1 F | 04B | 91 | 39 | 30B | 00 | 07 | 2E | 01 | 231 | 29 B | 049 | 202 | 224 |
| 38. | OC9 | 2DA | 2A8 | 286 | 6 A | 189 | 130 | 27 | 1EC | 29D | 104 | 387 | 32 | 316 | 207 | 137 |
|  | ODC | 02B | 1D | 034 | 35 | 39 C | OB6 | 32 | 3E | 3A4 | OD9 | 24 | 2B3 | 0D6 | 33 | 25 |
| 3 A . | OCB | 1DB | 172 | 296 | 14 | 04A | 244 | 250 | 1 F | 2A | 2C6 | 346 | 09 | 388 | 328 | 3A3 |
| 3B. | 2 C 7 | 3E7 | 29E | 3 CO | OD5 | 22A | 1F4 | 168 | 3FD | 242 | 102 | 3C5 | 0F8 | 25 | 26 | 2D |
|  | 27C | 029 | 003 | 38B | 0 C | 380 | 10D | 295 | 303 | 197 | 33 | 219 | 13 A | 306 | 166 | 2D9 |
| . | 175 | 19A | 0D8 | 3D8 | A2 | 26F | 3B8 | 1 C | 148 | 30A | 0B8 | 24D | 1A | 121 | 15 |  |
| 3 E . | 25 A | 266 | 22F | 135 | OBO | 055 | 01E | 3AC | 083 | 28 | 34B | 1D5 | 3E9 | 393 | 2E | 037 |
| 3F | 20F | 0D7 | 1A8 | 1 AB | 16B | 36A | 352 | 204 | 2BD | 08B | 147 | 1AA | 35F | 03C | 309 | 33D |

Figure A.4: Specification of the secret S-box $\mathbf{S}_{0}$.

|  |  | 1 | 2 |  |  |  |  |  |  |  |  |  |  |  | E |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 00 | OBA | 026 | OA | E1 | 183 | 3DB | 1A | 08 | 110 | 350 | 08 | 2E | 3B | 195 | 359 |  |
| 01. | 33A | 26 | 209 | 217 | 1 CE | 2E3 | 0C0 | 13 | 129 | OC8 | 3D6 | 05 | 4 | 3F2 | 09 |  |
|  | 1 B | 07F | 139 | 07D | 2CF | 02A | 268 | 227 | 24 | 1 C 5 | 12B | $3 \mathrm{B6}$ | 16C | OD | 1E7 |  |
| 03. | 313 | OCD | 11E | 1E6 | 117 | 355 | 182 | 0E6 | 09 | B | 19 | 28 | 2B9 | 336 | OAF |  |
| 04. | 2BC | 1A9 | 31B | 02E | 82 | 2 AE | 27 | 2E9 | 3AA | 1DD | 013 | 2D | 30F | 35A | 159 |  |
|  | 11 C | 12A | 248 | 3 C 7 | 28B | 191 | 025 | 173 | 018 | 38D | 1A1 | 185 | 007 | 156 | 378 |  |
| 06. | 0C9 | 43 | 05D | 3F | 038 | 3DE | 81 | 0F9 | 2D1 | 3FB | 1C7 | 3E0 | 1DC | 16A | 2D8 |  |
| 07. | 030 | 1EB | 3AF | 311 | 36D | BD | 3C9 | 348 | 261 | 1 AF | 071 | 3EE | 3BA | 3 AB | 1B8 |  |
| 08. | 22B | 118 | 279 | 0F6 | 3FF | 12 | 1B | 360 | 1D | 1B6 | 3D | 3B | 3B3 | OEA | 097 |  |
| 09. | 3A9 | 86 | OAE | 15 | 253 | 05 | OBB | 3D5 | 01D | A3 | 23 | 053 | 35D | 277 | 384 |  |
| OA. | 233 | 2B8 | 2AF | ODO | 1B1 | 10 | OB3 | 215 | 2A | 27 F | 2DB | 17E | 12C | 3A2 | 18 E |  |
| OB. | 321 | 09C | 294 | $04 C$ | 036 | 2F1 | 3D2 | 18D | 18 | 349 | 12 | 069 | 198 | 2F | 3DC |  |
| OC. | 138 | 324 | 23 C | 1FD | 082 | 247 | 005 | A3 | OFO | 273 | 15 | 17 | 1 A 0 | 1C8 | 04E |  |
|  | 12 F | CC | 75 | 10E | 290 | 02 | 1 AE | 211 | 3E | 17A | 276 | 28 | B5 | 123 | 01F |  |
| OE. | 201 | 08F | 29A | 002 | 179 | 32E | 120 | 1 A | 1E3 | 109 | 079 | 37C | 297 | 096 | 12D |  |
| OF | 165 | OAC | 18B | OAB | 1FF | 23 | 25B | 3D3 | 111 | 7E | 21 C | 1BE | 187 | 30 | 34 |  |
| 10. | 269 | 343 | 29F | 395 | 1 AD | 1D2 | 023 | 2DE | 1B3 | 35E | 2D | 04 | 206 | 3 F | 310 |  |
|  | 287 | C3 | 2A5 | 213 | 3E4 | 3DA | FD | 140 | 38 | 2C2 | 154 | 25 | 15 | 02 | F |  |
|  | 1 C | 051 | 62 | 090 | 214 | 14B | 190 | 15D | OA | 18 | 032 | OB | 1DA | 23 | 3D1 |  |
|  | 33 | 06D | 02D | 009 | 2 FC | 3AD | 2AA | 363 | 1EF | 38 F | 39A | 2DC | 3BF | 106 | 39B |  |
|  | 03E | ODE | 1BC | 067 | OCF | 15 | 2 CE | 240 | 05 | 0E8 | 0C4 | 14 | 08 | 3E5 | 2A1 |  |
| 15 | 1D1 | 228 | 3DF | OEO | 3F6 | 193 | 19 | 27D | 2B | 35C | OE3 | 17 | 180 | 022 | 00 |  |
| 16 | 161 | OEE | 365 | 5 B | 0C3 | 2 CD | 3E1 | 06 C | 11 | 283 | OF | 3B9 | 212 | 226 | 076 |  |
|  | 38 C | 1D3 | 15 C | OB2 | 22 C | 314 | 056 | 216 | 36 | 3D | 1 E | 02 | 176 | 89 | 2F2 |  |
|  | 06F | 27 E | 02 | 14E | 177 | 26 | BA | OEC | 25A | 194 | 3C6 | 2F9 | 221 | E1 | 3F4 |  |
|  | 14F | 293 | 144 | OFB | 2F0 | 3E | 0F | 1CC | 0C6 | 06 | 02 | 315 | 3E2 | 2DD | 274 |  |
| 1 A | 0D3 | 041 | 080 | 2C5 | 072 | 08D | 339 | A3 | 1F | 1 D | 2F | 26 | 01 | OB | 275 |  |
| 1B | 091 | 03F | 25 | 18F | 1 C 3 | 27 | 319 | 15 | OD2 | OBD | 2D0 | 064 | 000 | 379 | 2F6 |  |
|  | 142 | 0F5 | 3EF | 03B | 3F8 | 344 | 3B | 265 | OE7 | 33 | 23 | 08E | 347 | 174 |  |  |
|  | 112 | 1D0 | 0 | 292 | 2C0 | 0E9 | 2B6 | 301 | 0C1 | 30D | 369 | 1 C | 1 E | 1F7 | 08 |  |
| 1 E . | 3 CB | 34D | 2B | 28F | A | 39 | 23 | 262 | 333 | 2F8 | 397 | 2C | 06 | 27 | 31 |  |
|  | 327 | 6 C | 325 | 167 | 05B | 36 | 362 | 004 | 3F | F7 | 20B | 22 | 222 | 2D2 | OCA |  |
|  | 33 F | 3B2 | 17D | 302 | 146 | 17 | 367 | 18A | 1DE | OB5 | 099 | 3B | 2C1 | OBC | 2A |  |
|  | 11D | 10 | 342 | 169 | 366 | 2E | 088 | 361 | 29 | 131 | 2 F | 199 | , | 3B0 | 00D |  |
|  | 2 B 7 | 063 | 3EB | 281 | 0 | 070 | 1 CB | 07B | 27 | 2C | 39 | 32B | 1C | 396 | 278 |  |
| 23. | 160 | OFF | 1A | OD4 | 024 | 24B | 17 | 1BD | 32 | 2EF | 28D | 39 | 21F | 24 | 10B |  |
|  | 141 | 256 | 22 | 218 | OEB | 26 | 145 | 050 | 03 | OE5 | 300 | 3 A | 1E2 | 34E | 22 |  |
| 25. | 16 | 02F | OC5 | 210 | 1A6 | 25 | 3F5 | 32D | 1B4 | 2EA | 1-4 | 3D | 381 | 371 | 2D9 |  |
|  | $3 \mathrm{C8}$ | 3F3 | 1F2 | 10 F | OD1 | 1B | D | 320 | 39 | 25E | 249 | 341 | 33B | 3 | 087 |  |
|  | 09E | 095 | 2C8 | 3 A 6 | OF2 | 263 | 108 | 307 | 3E8 | 3C | 2BB | 14 | 36 | 13E | 2 C 9 |  |
|  | 014 | 00F | OD | 133 | 163 | 05 | OA | 1 E 5 | 019 | 37D | 043 | 1FC | 18 | 07A | 3FE |  |
| 29. | OFE | 25F | 26 | 3B | 135 | 2E | 3B1 | 1 B 7 | 01 | 2CA | OC2 | 11 | 001 | 271 | 1D8 |  |
|  | 16 | 1 C | OAD | 23 | 299 | 3 | 3E | 24 E | 3F0 | 1D | 3CC | 2B | 2C3 | 338 | 1B5 |  |
| 2 B . | 181 | 052 | 243 | 1F3 | 11F | 2E | 332 | 32 | 03 | 3A | 2B | 34 | 03 | 305 | 006 |  |
| 2 C . | 13 F | 13C | 19E | 3A0 | 17 C | 2E | 3CE | 345 | 3CD | OEF | 20 | 31 | 23 | 06 | 05 |  |
|  | 1E0 | 3D8 | 3F9 | 103 | 337 | ODB | 14D | 353 | 12 | CE | 385 | 11 | 10 | 3D7 | 057 |  |
|  | 04F | 2B2 | 2CB | 39 | 234 | 2B | 2E1 | 32A | 2F | 115 | 11 | 37 | 3A | 092 | 373 |  |
|  | 21E | 2 AB | 37F | 2FD | 2ED | 2B | 1EA | 125 | 2 | 16 E | 33 | OAS | 2 F | 3C2 | 3C1 |  |
| 30. | 11A | A4 | 3EA | 047 | 157 | 25 | 1D | 10 | 16 | 20 | 098 | 2B | 34 | 22 | 24 |  |
|  | 1F5 | ED | 31 E | 298 | 3A7 | 30 C | 1 C | 05 | 35 | OE | 33 | 04 | 15 | 24 | 1EE |  |
|  | 12 E | 2A6 | 1A5 | 061 | 3A1 | 29 | 1 | 066 | 093 | 3 | 38A | 1 F | F | 08 | 134 |  |
|  | 225 | 20 C | 3D9 | 2E4 | OA8 | OBE | 1FE | 0FC |  | 37 | 2 F | 07C | 074 | 045 | 1E8 |  |
|  | 36B | 36F | 37 | 37 | 04D | 1FA | 25 | 13 | 08 | 22 | 399 | 00 | 158 | 2D5 | 06 |  |
| 35 | 357 | ODD | OBF | 1B0 | A7 | 23B | 25 | 3F | 00A | 330 | 2A | 200 | 1 | 008 | 126 |  |
| 36. | 09B | 37A | 284 | 2D4 | F3 | 28E | 237 | 31D | ODF | 368 | 386 | 060 | 37 | 31C | 033 |  |
| 37. | 100 | 94 | 1F9 | 4B | 91 | 39 | B | 00 C | 077 | 2EB | 3E | 231 | 29 | 049 | 202 |  |
| 38. | 132 | 2DA | 2A8 | 286 | 06A | 18 | 13 | 13D | 1 E | 29 | 104 | 38 | 32 | 316 | 20 |  |
| 39 | ODC | 02B | 1D7 | 21A | 354 | 39C | 0B6 | 329 | 285 | 3A4 | OD9 | 245 | 2B3 | 0D6 | 33E |  |
| 3 | OCB | 1DB | 172 | 296 | 92 | 04A | 244 | 250 | 1F6 | 2AD | 2C6 | 346 | 09D | 388 | 328 |  |
| 3 B . | $2 \mathrm{C7}$ | 3E7 | 29E | 3 CO | D5 | 22A | F | 168 | 3F | 242 | 102 | 3C5 | OF8 | 251 | 264 |  |
| 3 C . | 27 C | 029 | 003 | 38B | OC | 380 | OD | 295 | 303 | 197 | 1 CD | 219 | 13A | 306 | 166 |  |
| 3 D . | 175 | 19A | 0D8 | 28A | OA2 | 26F | 3B8 | 1 C 2 | 148 | 30A | 0B8 | 24D | 1 A | 121 | 15E |  |
| 3 E . | 0B4 | 266 | 22F | 2 FE | OBO | 055 | 01E | 3AC | 14A | 2E0 | 34B | 1D5 | 3E9 | 393 | 2E7 |  |
| 3F. | 20F | 0D7 | 1A8 | 1 AB | 16B | 36A | 352 | 204 | 2BD | 08B | 147 | 1AA | 35F | 03C | 309 |  |

Figure A.5: Specification of the modified S-box $S_{0}$.

Appendix A - Specifications of BEA-1 Building Blocks

|  | . 0 | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 00 | 021 | 09B | 74 | 3AB | ODF | 016 | 1FE | 004 | 07C | 3BE | 141 | 39 | 300 | 185 | 00C |  |
| 01 | 2 F | 3AA | 235 | 0B9 | 00 | 3CF | 14A | 18F | 356 | 363 | 055 | 2 E 4 | 16 | OCF | 373 | 379 |
|  | 2CA | 33B | 16 | 393 | 283 | 2E0 | 2B9 | 3E9 | 12 | 247 | 3AD | 07B | 288 | 146 | 30F |  |
| 03 | 15 C | 01F | 22 C | 0F8 | 10F | D | 367 | 343 | 1EC | 047 | 008 | 062 | 2CF | 019 | 36B | 48 |
|  | OB4 | 2E3 | 25E | 234 | OD2 | 1F8 | 184 | 2 FF | 2EB | 2BB | 3A | 34F | 312 | OB | 2EA |  |
|  | 1B1 | 2FE | 08 | 3CC | 216 | 337 | OD4 | 08D | 21F | 035 | 1F5 | 32A | 1AA | 182 | 24B | BF |
|  | 245 | 25 | 01E | 34 E | 375 | 197 | 292 | 1DD | 4D | 190 | 27E | 18D | 137 | 3 A3 | 228 | 392 |
|  | 01 | 340 | 389 | 114 | 3B | 28B | 32 | 21 | 1E7 | 30B | 38 | 335 | 09 | 088 | 038 |  |
|  | 305 | 38E | 112 | OAA | 01B | 60 | 3C1 | 10 | OE | 3D4 | OEF | 079 | 34 | 38 | 22E | 9 D |
|  | 1E6 | 087 | 278 | 20D | 25B | 060 | 215 | 2 C | 3E0 | 0A1 | 3F9 | 179 | 252 | 1B5 | 105 | 368 |
|  | 029 | 1 E | 2C | 2 C 5 | 03 | 233 | 20 | 133 | BD | 20B | 37D | AE | 115 | 116 | B2 | F3 |
|  | 266 | 333 | 08F | 050 | 1B9 | 328 | 26F | 1EA | A9 | 0E6 | 291 | 2ED | 05 | 162 | 1EE | 362 |
| 0 C | 15B | 351 | 20F | 17 | 08B | D5 | 25 | 27 | 14F | 2 F | 01 | 3E7 | 14B | 39 | 248 | OB2 |
| OD. | 119 | 3CD | 160 | 23E | 06 | ODO | 3C3 | 01 C | 171 | 3D3 | 34 | 061 | 16 | OFB | 1DF | 42 |
|  | 82 | 07 | 218 | 2E9 | 3B3 | 225 | 2F9 | 23 | 20 | 22 | 151 | 0C5 | 2A9 | FE | 096 |  |
|  | 0F2 | OD | 03A | 015 | 049 | 370 | 14C | 25 | 369 | 193 | 344 | 20E | 16 | 366 | 3 D | 87 |
|  | 24 C | 030 | 315 | 3CA | 2EE | 0C6 | 02C | 20 | 107 | OF1 | 3FE | 244 | 26C | 264 | 1 C 6 | C9 |
| 11 | OB1 | 090 | 36F | 28 | 1A | 19D | OB | 317 | 19B | 25 | 11 | OED | 395 | OBF | 37 | 3E4 |
| 12 | 35 C | 3FB | 103 | 2E | 36 | 11 E | 21 | 27 | 316 | 38 | 27 | 286 | 08 | 068 | 3D | F7 |
|  | 3C5 | 09 | 2FC | 09F | 2B | 332 | 05C | 38 | 3B | 091 | 2DD | 35 | 19F | 111 | 2 A | B0 |
|  | 091 | 32 | 106 | 10E | 012 | 273 | 2EC | 033 | 080 | 174 | 2DB | 1 C | 102 | 2D3 | 2 |  |
|  | 03F | 2D | 364 | 131 | OA | 275 | 00A | 38 | 052 | 3D | 339 | 11A | 211 | 02A | 27 F |  |
| 16 | 318 | 27B | 17B | 2D | 15 | 85 | 144 | 26 | 3 F 4 | 1EF | 09 | 3BB | 307 | 88 | 3B0 | OEB |
|  | 209 | 2CB | OBB | 3A5 | 12 | OAC | 02 | 02 | 3E6 | 0E5 | 22 | 12 | 15 | 2B7 | 0F9 |  |
|  | 054 | 32 | 3F6 | 03 | 05 | 29 | 23 | 2A |  |  |  | 23 | 1B3 |  | 380 |  |
|  | 0 C 7 | 360 | 0D6 | 265 | 34 | 17 F | 296 | 3E | 20 | 0A2 | F6 | 20 |  | 04 | 1D5 |  |
|  | 200 | 121 | 134 | 2 AB | 2FB | 72 | OD | 07 | 001 | 26 | 27A | 1FF | 29 | 3EB | 1FA |  |
|  | 253 | 006 | 128 | 195 | 14 E | 89 | 0F6 | 3A8 | 3D2 | 26 | 178 | 3E5 | 2C | OB7 | 303 | 81 |
|  | 097 | 22A | 32E | 166 | 30 | 0FC | 139 | 138 | OF | 1AC | FD | 29B | OAF | 041 | 2 C |  |
|  | 23B | 1F | 25D |  | 31 | 20A |  | 33 | 3C |  |  |  | 3E8 | 21 | 06E |  |
|  | 0 C 4 | 08 | 1B | 051 | 3E2 | 153 | 013 | OF | 2B6 |  | 17 | 2D | 2 | 3B | 33 |  |
|  | OB5 | 27 C | 3F | 39 | 19 | 099 | 0A9 | 32 | 35A | 36 | 2 C | 05D | 1F9 | 226 | 098 |  |
|  | 05A | 3AC | 33E | OE | OA | 186 | 10 | 17E | 12 | 32B | 110 | 05F | 1A | 390 | 3CE |  |
|  | 11F | 3D6 | 3D5 | 13 | 2B | 251 | 355 | 06 | 33 | 3D | 15 | 07A | 086 | 1B6 | 308 |  |
|  | ODC | 124 | 15F | 075 | 2E7 | 39E | 046 | 30 | 32 | 2CE |  |  | 267 | 066 | 394 |  |
|  | 06 | 371 | 2 AF | 12 | 378 | 319 | 2 | 1D | 37F | 3A | 21 | 15 | 31 | 3F | 23 |  |
|  | 071 | 31B | 256 | 3F3 | 33 | 80 | 30 C | 08 | 21 C | 058 | 1CD | 2D6 | 165 | 3A0 | 077 |  |
|  | 022 | 32F | 359 |  | 37 | 1 EB | 30A | 19 | 1C | 1BA | 06B | OAO | 17 | 183 | 28E | 2 A |
|  | 29 C | 130 | 323 | 122 | 33 | 201 | 3B1 | OBC | 25A | OD8 | 34B | 11B | 24 | 2E8 | 1F1 |  |
|  | 31 C | 254 | 346 | 37 | 11 | 000 | 24 | OC | 381 | OE9 | 22D | 01A | 161 | 3D0 | 07 |  |
|  | 295 | 175 | 04F | 3C4 | 1A | 2A2 | 191 | 2 F | 34 | 36 | 2E | 3D | 02 | 30 | 0F | 2F6 |
|  | 0C1 | 30D | 025 | 1F3 | 01 | 1D3 | 06 | 13 | 109 | 2D | 38 | 31 | 18C | OE1 | 23 |  |
|  | 36D | 3DB | 377 | 1DB | 16D | 090 | 024 | 24 | 07 |  | 31 | 2C9 | 149 | 20 | 08 |  |
|  | OEA | 05 | 250 | 2CD | 38 | 2 AO | OB | 16 | 12 D | 309 | 2D8 | 2AD | 3F0 | 3F | 1 C 8 |  |
|  | 268 | 2A3 | 1D6 | 28 | 1 C | 324 | 2A | 02 | 1DE | 3C7 | OD | 274 | 147 | 219 | 02 |  |
|  | 1D8 | 13F | 383 | 3DA | 3E | 26A | OA | 1D |  | 2 | 35 |  | OAB | 2A | 3D |  |
|  | 2D2 | 352 | 108 | OE3 | 27 | 22 |  | 29 |  | 06F | 00 |  | 0A4 | 19 | 23 |  |
|  | 06 | 258 | 348 |  | 17 | 2B4 |  | 3 C | 33 | 217 | 28 |  | 3B2 | 15 E | 03B |  |
|  | 2B8 | 2DO | 340 | 0F | OBD | 2 FO | 35 | 39 | 18 | 29A | 39 | 24 | 1 CB | 2 | A2 |  |
|  | 3 FC | 212 | 1B7 | 03 | 28 | 357 | 12 | 04 | 32 | 3A | 3B | 33 | 19 | 1B | 1 F |  |
|  | 1 E | OAD | 101 |  | 22 | 227 | OB | 34 |  | 220 |  | 298 | 3EF | OB | 2 F |  |
|  | O4 | OE4 | 02 | OD1 | 21B | 005 | 12 C | E | 13A | 3B | 09 | 0 | 05B | 0 | 37B |  |
|  | ODB | 2A | 27D | 39D | 3A | 214 |  | 1 AD | 2 E | 2D | 1D |  | 1 C 0 | 3D | 140 |  |
|  | 2B3 | 26 | 1F0 | $3 C$ | 3A | 04A | 03 | 2 C | OB | 07 | 1D | 1E | 16A | 145 | 170 | C8 |
|  | 00B | 35B | 1 AB | 127 | 2BF | 6 E | 2B | 24 | 1E1 | 063 | 33 | 2B | 136 | 3E | 38 |  |
|  | 23D | 2D1 | 42 | 372 | 3BA | ED | OF | 32 | C9 | 01 | 1 C | 39 | 3F8 | 26 | 1B | 187 |
| 38. | 034 | 3FD | 10 | 118 | 1D1 | 076 | 22B | 14 | 208 | 38 | 39 | OD | 3B | 19 | 3C | 3B5 |
| 39 | OE2 | 13 | , | 28 | 15 | 150 | 173 | 155 | 3DD | 15D | OCD | 163 | 1A0 | OC3 | 10C |  |
| 3A. | 180 | 1A6 | 321 | 00E | 276 | 03E | 25F | 3E | 18 | 3E | 1D0 | 1C | 26 | 205 | 17A | 3 F |
| 3B. | 35E | 036 | 35F | 2F8 | 067 | 2BA | 2A5 | 16 C | 3D | 2F | 297 | 18 | 113 | OFD | 31 | OE7 |
| 3 C . | 15A | 1B8 | 08A | 239 | 04B | 26 | 083 | 385 | 2 F | 19 C | 12E | 01 | 3BC | 224 | 135 | 29 |
| 3D. | 09A | 311 | 240 | 13E | OA5 | 24 E | 069 | 18B | FF | 236 | 36A | 1 A | 04 | 3 AE | 1 E | 31E |
| 3 E . | 132 | 23F | 222 | 070 | 2AE | 3EA | 249 | 023 | 293 | OBO | 330 | 21 | 28D | 1CE | 154 | 172 |
| 3 F | 1F4 | 056 | 00F | 2EF | 361 | 1D2 | OEO | 1C4 | 19E | 282 | 1B4 | 3F7 | 294 | 142 | 2D9 | OCE |

Figure A.6: Specification of the secret S-box $\mathbf{S}_{1}$.

|  | . . 0 | . 1 | . 2 | . 3 |  | . 5 | . 6 | . 7 | . 8 |  | . A | . ${ }^{\text {B }}$ |  | . D |  | .F |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 00. | 021 | 09B | 37A | 3AB | ODF | 016 | 1 FE | 004 | 07C | 3BE | 141 | 397 | 300 | 185 | 00 | A7 |
| 01. | 2FA | 3AA | 235 | OB9 | 003 | 3CF | 14A | 18F | 356 | 363 | 173 | 2E4 | 168 | OCF | 373 | 379 |
| 02. | 2CA | 326 | 16B | 393 | 283 | 2E0 | 2B9 | 3E9 | 12 F | 247 | 3D8 | 07B | 288 | 146 | 30F | 267 |
| 03. | 15C | 01F | 22C | 0F8 | 10F | 35D | 367 | 343 | 1EC | 047 | 008 | 062 | 2CF | 3D6 | 36B | 148 |
| 04 | OB4 | 2E3 | 25E | 234 | OD2 | 1F8 | 184 | 2FF | 2EB | 2BB | 3A1 | 34F | 312 | 10B | 2EA | 04D |
| 05. | $1 \mathrm{B1}$ | 2FE | 084 | 229 | 216 | 337 | OD4 | 08D | 21 F | 035 | 164 | 32A | 1A | 182 | 24B | 1BF |
| 06. | 245 | 257 | 01E | 34E | 375 | 197 | 292 | 1DD | 14D | 190 | 27E | 13D | 137 | 3А3 | 228 | 392 |
| 07 | 010 | 34C | 389 | 114 | 3B9 | 28B | 325 | 210 | 1 E 7 | 30B | 388 | 1A | 094 | 088 | 038 | 1C2 |
| 08 | 305 | 38E | 112 | OAA | 01B | 260 | 3C1 | 104 | 30E | 3D4 | OEF | 079 | 347 | 382 | 22E | 09D |
| 09. | 1E6 | 087 | 278 | 20D | 25B | 060 | 215 | 2 C 6 | 3E0 | 055 | 3F9 | 179 | 252 | 1B5 | 105 | 368 |
| OA | 029 | 1E9 | 2C4 | 2 C 5 | 037 | 233 | 204 | 133 | 3BD | 20B | 37D | 1 AE | 03D | 116 | 1B2 | 2F3 |
| OB. | 266 | 333 | 08F | 050 | 1B9 | 328 | 26F | 1EA | 1A9 | 0E6 | 291 | 2ED | 05E | 162 | 1EE | 362 |
| OC | 15B | 351 | 20F | 17D | 08B | 2D5 | 259 | 271 | 14F | 2F5 | 011 | 3E7 | 14B | 391 | 248 | OB2 |
| OD | 119 | 3CD | 160 | 23E | 06A | ODO | 3 C 3 | 01C | 171 | 3D3 | 349 | 061 | 16F | OFB | 1DF | 342 |
| OE. | 082 | 068 | 218 | 2E9 | 3B3 | 225 | 2F9 | 230 | 020 | 223 | 151 | OC5 | 2A9 | OFE | 096 | 045 |
| OF. | 0F2 | ODA | 03A | 015 | 049 | 370 | 14C | 255 | 369 | 193 | 38A | 20E | 0B1 | 3A6 | 039 | 387 |
| 10. | 24C | 030 | 315 | 3CA | 0A1 | 0C6 | 02C | 203 | 107 | 115 | 3FE | 244 | 26C | 264 | 1C6 | 1-9 |
| 11 | 123 | 090 | 36F | 28F | 1 A 3 | 19D | OBE | 317 | 19B | 25C | 117 | OED | 395 | OBF | 37E | 3E4 |
| 12 | 04C | 3FB | 103 | 2E6 | 3C8 | 11E | 3D1 | 279 | 316 | 38C | 277 | 286 | 081 | 074 | 21 | 1F7 |
| 13 | 3C5 | 095 | 2 FC | 09F | 2B5 | 332 | 05C | 31F | 324 | 09E | 2DD | 3FC | 19F | 111 | 2A7 | 2B0 |
| 14. | 091 | 329 | 106 | 10E | 012 | 273 | 2EC | 341 | 080 | 174 | 2DB | 1 C | 102 | 2D3 | 2E | 1B0 |
| 15 | 03F | 2D4 | 364 | 131 | 0A6 | 275 | 00A | 386 | 052 | 3DC | 339 | 11A | 211 | 02A | 27 F | ODD |
| 16. | 318 | 27B | 17B | 2D7 | 1E4 | 285 | AC | 269 | 3 F | 1EF | 093 | 3BB | 307 | 08E | 3B0 | OEB |
| 17 | 209 | 2CB | OBB | 3A5 | 129 | 1CA | 027 | 028 | 3E6 | 064 | 221 | 125 | 159 | 2B7 | 0F9 | 37C |
| 18. | 054 | 32D | 3F6 | 031 | 053 | 29F | 23C | 2A1 | OD9 | 237 | 336 | 232 | 1B3 | 1C1 | 380 | 2C1 |
| 19. | 1DA | 360 | 30C | 265 | 34A | 17F | 296 | 3E1 | 20C | 0A2 | 1F6 | 207 | 0F1 | 040 | 1D5 | 026 |
| 1 A | 200 | 121 | 134 | 2 AB | 2FB | 272 | 0D7 | 07E | 001 | 262 | 27A | 1 F | 299 | 3EB | 1 F | 39F |
| 1B | 253 | 006 | 128 | 36E | 14 E | 289 | 0F6 | 3A8 | 3D2 | 261 | 178 | 3E5 | 2 CO | 0B7 | 303 | 181 |
| 1 C | 097 | 22A | 32E | 166 | 306 | OFC | 139 | 138 | 3BF | 1AC | 1FD | 29B | OAF | 041 | 2CC | OCA |
| 1D. | 23B | 1F2 | 25D | OEC | 314 | 20A | 03C | 120 | 3C6 | OCO | 158 | 28C | 3E8 | 21E | 06E | 263 |
| 1 E | OC4 | 085 | 1BD | 051 | 3E2 | 153 | 013 | 0F3 | 2B6 | 1A8 | 17C | 2D | 2 C 7 | 3B7 | 33C | 29E |
| 1F | OB5 | 27C | 3F2 | 398 | 194 | 099 | OA9 | 320 | 35A | 366 | 2 C 2 | 05D | 1F9 | 226 | 098 | 04E |
| 20. | 05A | 3AC | 33E | 0E8 | OA7 | 186 | 1D8 | 17E | 126 | 32B | 110 | 05F | 1A5 | 390 | 3CE | 1FC |
| 21 | 11F | 019 | 3D5 | 13C | 2BD | 251 | 355 | 065 | 1F5 | 3DF | 152 | 07A | 086 | 1B6 | 308 | 188 |
| 22. | ODC | 124 | 15F | 075 | 2E7 | 39E | 046 | 302 | 32C | 2CE | 3CC | 3AF | 208 | 066 | 394 | 12B |
| 23. | 06D | 371 | 2AF | 12A | 378 | 319 | 24D | 1D7 | 37F | 3A2 | 21D | 157 | 31A | 3FF | 3B2 | 2DA |
| 24 | 071 | 31B | 256 | 3F3 | 33D | 280 | 144 | 08C | 21 C | 058 | 1 CD | 2D6 | 165 | 3A0 | 077 | 354 |
| 25 | 022 | 32F | 359 | 2BC | 374 | 1EB | 30A | 192 | 1 CF | 1BA | 06B | OAO | 177 | 183 | 28E | 2A8 |
| 26. | 29C | 130 | 323 | 122 | 331 | 201 | 3B1 | OBC | 25A | OD8 | 34B | 11B | 24F | 2E8 | 1F1 | 3 F 5 |
| 27. | 31C | 254 | 346 | 376 | 11C | 000 | 243 | 0C8 | 381 | OE9 | 22D | 01A | 161 | 3D0 | 07 F | 1 E 0 |
| 28. | 295 | 175 | 04F | 3 C 4 | 1AF | 2A2 | 191 | 2F7 | 34D | 36C | 2E2 | 3D7 | 0F7 | 18B | 0F5 | 2F6 |
| 29. | OC1 | 30D | 025 | 1F3 | 01D | 1D3 | 06C | 13B | 109 | 2DF | 38B | 2E5 | 18C | OE1 | 231 | 10D |
| 2 A . | 36D | 3DB | 377 | 1DB | 16D | 09C | 024 | 242 | 072 | 39B | 31D | 2C9 | 149 | 0FO | 089 | OA3 |
| 2 B . | OEA | 057 | 250 | 2CD | 38F | 2 AO | 0B3 | 169 | 12D | 309 | 2D8 | 2AD | 358 | 3F1 | 1C8 | 043 |
| 2 C . | 268 | 2 A 3 | 1D6 | 28A | 3EC | 18D | 2AA | 02F | 1DE | 3C7 | OD3 | 27 | 147 | 219 | 02D | 2B2 |
| 2 D . | OCC | 13F | 383 | 3DA | 3ED | 26A | OAE | 1DC | 301 | 2A4 | 350 | 2F | OAB | 2A6 | 39 | 014 |
| 2 E | 2D2 | 352 | 108 | OE3 | 270 | 3E3 | 02E | 29D | 1BE | 06F | 002 | 059 | OA4 | 198 | 23A | 044 |
| 2F. | OCB | 258 | 348 | 39C | 176 | 2B4 | 007 | 3C2 | 33F | 217 | 287 | 073 | 238 | 15E | 03B | 167 |
| 30. | 2B8 | 2D0 | 340 | 0F4 | OBD | 2FO | 353 | 100 | 18A | 29A | 399 | 246 | 1CB | 02B | 1 A 2 | 2E1 |
| 31. | 3 FO | 212 | 1B7 | 032 | 281 | 357 | 3AD | 048 | 322 | 3A9 | 3B6 | 33A | 196 | 1BB | 1 F | 19A |
| 32. | 1E2 | OAD | 101 | 033 | 22F | 227 | OB6 | 345 | 0C2 | 220 | 07D | 29 | 3EF | 0B8 | 2 F | ODE |
| 33 | 304 | OE4 | 202 | OD1 | 21B | 005 | 12C | OEE | 13A | 00 | 092 | 00D | 05B | 009 | 37B | 365 |
| 34. | ODB | 2AC | 27D | 39D | $3 A 7$ | 214 | 338 | 1 AD | 335 | 2DE | 1D9 | 1E5 | 1C0 | 3DE | 140 | 24A |
| 35. | 2B3 | 26B | 1F0 | 3C0 | 3A4 | 04A | 0A8 | 2C3 | OBA | 078 | 1D4 | 1E3 | 16A | 145 | 170 | 2C8 |
| 36. | 00B | 35B | 1 AB | 127 | 2BF | 16E | 2BE | 241 | 1E1 | 063 | 334 | 2B1 | 136 | 3EE | 3B8 | 1C5 |
| 37. | 23D | 2D1 | 042 | 372 | 3BA | 1ED | OFA | 327 | 0C9 | 018 | 1C3 | 396 | 3F8 | 26E | 1BC | 187 |
| 38. | 034 | 3FD | 310 | 118 | 1D1 | 076 | 22B | 143 | 38D | 33B | OE5 | OD5 | 3B4 | 199 | 3C9 | 3B5 |
| 39. | 0E2 | 195 | 10A | 284 | 156 | 150 | 11D | 155 | 3DD | 15D | OCD | 163 | 1A0 | 0C3 | 10C | 35C |
| 3 A . | 180 | 1A6 | 321 | 00E | 276 | 03E | 25F | 0D6 | 189 | 206 | 1D0 | 1CC | 26D | 205 | 17A | 3FA |
| 3 B . | 35 E | 036 | 35F | 2F8 | 067 | 2BA | 2A5 | 16C | 3D9 | 2 FD | 297 | 18E | 113 | OFD | 313 | 0E7 |
| 3 C . | 15A | 1B8 | 08A | 239 | 04B | 384 | 083 | 385 | 2F4 | 19C | 12E | 017 | 3BC | 224 | 135 | 290 |
| 3 D . | 09A | 311 | 240 | 13E | 0A5 | 24E | 069 | 3CB | 0FF | 236 | 36A | 1A4 | 344 | 3AE | 1E8 | 31E |
| 3 E . | 132 | 23F | 222 | 070 | 2AE | 3EA | 249 | 023 | 293 | OBO | 330 | 21A | 28D | 1 CE | 154 | 172 |
| 3 F . | 1F4 | 056 | 00F | 2EF | 361 | 1D2 | OEO | 1C4 | 19E | 282 | 1B4 | 3F7 | 294 | 142 | 2D9 | OCE |

Figure A.7: Specification of the modified S-box $S_{1}$.

Appendix A - Specifications of BEA-1 Building Blocks

|  | . 0 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 00 | 12E | 38B | 18E | 131 | 03 | 10 D | 2DE | 246 | 286 | 2BE | 31 | 384 | 21D | A5 | 06D |  |
| 01 | 2 A | 2CE | 264 | 085 | 374 | 3BB | 3B9 | 1B | ODE | 3B | 20 | 00 | 392 | 1B5 | OBA | 318 |
|  | 39 C | 2EE | 13 C | 125 | 22 | 063 | 27 E | 12 |  | 08 | 30 | 5 | 206 | OAO | 009 | 3 |
|  | 100 | 3F | 2 | 199 | 102 | 108 | 1D | 301 | 310 | 245 | OA | 116 | 02 | 3C | 028 | 332 |
|  | 1 E | 2E7 | ODA | 255 | OCB | 07 C | 2 AO | 240 | 150 | 165 | 258 | 2C8 | OC | 33 | 6B |  |
|  | 1 E | 138 | 39A | 0FF | 1A | 10C | 353 | 19B | 171 | 038 | 3BD | 000 | 3A2 | 1B8 | 282 | 2EB |
|  | 1 D 4 | 3D | 20F | 23 C | OD | 154 | 012 | ODF | OF | 237 | 04E | 155 | 2E | 189 | 01F |  |
|  | 1B | 381 | 273 | 123 | 05 | 2 C | 158 | 033 | 2D2 | 3D | 23B | 3B | 2F | 16 | 341 | 12 |
| 08. | 337 | 1E6 | 3BE | 327 | OBD | 96 | 2E4 | 107 | 1C2 | 263 | 2A | 2C | 244 | 19 | 36 |  |
| 09 | OA1 | 2 C 3 | 004 | 049 | 303 | A3 | 09E | 361 | 065 | 1B | 05 | 31 | 21B | 24 | 2B2 | 399 |
|  | 198 | 26 | 080 | 1B1 | 340 | 28A | 33C | 316 | FC | 37 F | 1 A8 | 134 | 17F | 3DF | 34F | 355 |
|  | 2D9 | 32A | 34A | 1D1 | 09D | 3FB | OBE | 348 | 383 | 036 | 3B6 | 22 | 22E | 2B6 | 3A6 | FA |
|  | 1 C | OB2 | 113 | 3E8 | 12 | 34 C | 153 | 33 | 07E | 01F | 01D | 213 | 29 | 0F8 | 130 | B9 |
| OD. | 182 | OA2 | 1A1 | 1 CD | 119 | 210 | 24 C | 020 | 097 | 3F0 | 280 | 112 | 04 | 14D | 1EB | 307 |
|  | 386 | OAE | 322 | 2 FE | 217 | 3D7 | 1 AF | 345 | 05B | 3F | 110 | 1 C 8 | 03 | 1C | 5 A | C0 |
|  | 3 F 1 | 23 | 338 | 1CB | 0F4 | 2B4 | 00F | 3 A | 242 | 03D |  | B3 | 003 | 11 | 3FA |  |
|  | 35 F | 0 C 5 | 261 | 2C1 | 15D | 28F | 390 | 1 C 9 | DD | 3C7 | 14 F | 11 | 066 | 04D | 03B | E9 |
|  | 2BA | 2FD | 347 | 191 | 04 | B8 | 194 | 14 | 256 | 360 | 32 | 257 | 1AE | 396 | 09B | 2CD |
|  | 1 E 7 | 3CD | 1FF | 269 | 040 | 3E7 | 08 | 216 | C9 | 33B | 3D | 1BC | 2B | 325 | 11B | 6F |
| 13 | 053 | 22A | 86 | 180 | 27 | 11F | 2A9 | 13E | 3E1 | OD4 | 24 | 12 | 2FC | 3 C 9 | FB | 31A |
|  | 3DE | 1D | 025 | 372 | 339 | 2C7 | 2ED | 25 F | 3E6 | 098 | 2EF | 247 | 0E8 | 2D | 05 |  |
|  | 2CC | 36 | 31F | 24B | 1D8 | 241 | 068 | 21 | 2AF | 3EA | 355 | 35C | 026 | 2B | 0B5 | EF |
| 16 | 35B | 233 | 05A | 1 BE | 291 | 368 | 13 | 03 | 29 | 14 | 26 | 1E4 | 37 | 07 | 3EB | 16 |
|  | 20B | 12D | 75 | 1BF | 12 | 1AA | 18B | 26 | 3F4 | 364 | OF7 | 057 | OB | 3C | 060 |  |
|  | 22B | 17 | 11C | OB1 | 23 | 3B4 | 05 | 2 F | 219 | 224 | 30 | 42 | 06F | 39 | 218 |  |
|  | 215 | 17 | 190 |  | 27 | 35 |  | 2E | 39 |  | 10 | 09 |  | 8 | 314 |  |
|  | ODC | 03F | 1AC | 1A6 | 132 | 152 | 195 | 3AD | 3E9 | 3C2 | 01 | 0F0 | OCD | 074 | 178 |  |
|  | 184 | 3E0 | 084 | 2 FB | 1A9 | B7 | 250 | 27B | 06 C | 13B | OFB | 296 | 29 | 30 | 350 |  |
| 1 C | 007 | 10E | 19 C | 055 | 35 | 034 | 175 | 103 | 272 | 02D | 2C | 21 C | 04 | 20D | OE3 | 29B |
|  | 13 | 1D | 162 | 376 | OBF | 1CA |  | 2B9 | 3FE | 388 | 133 | 29 | 33 | 304 | 1FE |  |
|  | 13D | 19 | 294 | 02B | 12 | 1E8 | 27 | 07B |  | 018 | 03 |  | OA | OE | 27 |  |
|  | 38D | 3B0 | 284 | 1FA | 1F5 | 00A | 3E2 | 02 | 22 | 285 | 34 | 311 | 07 | 2 F | 1C4 |  |
|  | 3 FF | 202 | 27 F | 2 F 9 | 30D | 35 | 33F | 30 | 3D8 | 2 | 3D2 | 30 | OEA | 073 | F1 | 289 |
|  | 3B5 | 09 | 111 | OB | 20 | 1BA |  | 24 | 39 | 15 |  | 336 | 39B | 017 | 25C |  |
|  | 1 EC | 2B | 144 | 1E9 | 193 | 16A |  | 344 | 295 |  | 2 B 7 |  | 38A | 17 | 292 |  |
|  | OF2 | 35 | 1EF | OBB | 1BB | 071 | 2D | 3 F | 3D1 | 037 | 2 AB | 330 | OBO | 2DB | 07A |  |
|  | 000 | 149 | OAF | 290 | 2EO | 122 | 28 | 32 | 3A | 3C3 | 1D | 2E | 37B | OB | 265 |  |
|  | 089 | 2CB | 15 | 081 | 18A | OE5 | 05 | 1 A 3 | 28 | OD | 276 | 32C | 0 C 3 | 30B | 22 | 1 C |
|  | 2 F | OA | 062 | 2AA | 18 | 091 | 20 | 15 | 230 | 320 | 38 | 28E | 21 | 3F | 11 E | E |
|  | 159 | 281 | 0C8 |  | ODD | 188 | 04F | 26 | 33 | 2 F 8 | 3 A 0 | 3B3 | 3 | OA | 1A2 |  |
|  | 302 | 36E | 38F | 19E | 21 | 142 | 24 | OB | 141 | 3EF | 1 CE | 262 | 14 | 36 | 346 |  |
|  | 1 E 3 | 14B | 3A9 | 3D | 1 C 6 | 3F8 | 070 | OD | 1E | 3BA | 248 | 146 | 20 | 243 | F6 | 205 |
|  | 0A7 | 20 | 2F6 | 00 | 26 | 26D | 2A | 31 | 2D | OD | 38E | 00 | 30A | 3E | 2C5 |  |
|  | 2D5 | 3A | 1D5 | 3A4 | 101 | 2D7 | 34E | 2B | 07 | 26C | 09 | F8 | 1F9 | 3A | 1F0 |  |
|  | 2 C 2 | 21A | 06A | OA | 1 | 109 | 16 | 15 | 16 | 38 | C | 27 | 279 | 369 | 342 |  |
| 2 D . | 01A | 016 | 352 | 173 | 34D | 5 | 18 | 23 | 25 | 23 | 16 | 03 | 03 | 1 C | 2EA |  |
|  | 18 | 078 | 18D | 01B | 11 | 393 |  | 39 |  |  | 24 |  | 29 | OA | 8 |  |
|  | 015 | 046 | 0C1 | 25 | OOD | 348 | 01 | 21 | 00 | 008 | 2 C | 32 | 1B2 | 1 B | 43 |  |
|  | 223 | OB | 054 |  | 0FD | 37 |  | 32 | 20 |  |  | 28 |  | 04 | 349 |  |
|  | 32F | O | 277 | 179 | 27 | 3F6 | 23 | 25 | 07 | 04A | 120 | 200 | 308 | 300 | 31 |  |
|  | 1ED | 048 | 30 C | 183 | OD | 39 F | 3B | OA | 3FD | 20 | 05 | C | 19 | 2 F | 22 |  |
|  | 1 F3 | 343 | 51 | 1F2 | 16 | 266 | 25 | 26F |  | 2B0 | 09 | 7B | 31 | F | 0E |  |
|  | 225 | 36C | 1EE | 25 | 05 | OE1 | 02 | 31 C | 3D | 1 A | 167 | 2A | 06B | 23 | 39 | 3 |
|  | 35 | 2 F | O0 | 391 | 2 | OF5 | 335 | 02C | 083 | 143 | 02A | 29E | 36F | 214 | 104 |  |
| 36. | OE4 | 1E5 | 19F | 2E | 1 F | 356 | 28 | 07 | 11 | OE | OE | 37 | 358 | 1D | 163 | 056 |
| 37. | 367 | 03A | 2D6 | 363 | 229 | DA | 08B | 382 | 270 | 2E | 2F | 168 | 027 | 2A | 170 | 28 |
|  | 2 A 3 | 08C | CF | 076 | 389 | 32B | 2E | 2A5 | 2C9 | 2A | 29 C | 3ED | 09C | OCC | 2A8 | 203 |
|  | OF | 293 | 29 F | 2 F | OE | 232 | OCE | 3 AB | 13 | 011 | 3DB | 22 | OD | 1 F | 22F | 236 |
| 3 A . | 17 | 1 A 4 | 27A | 12 | 329 | 324 | 06 | 36 | 02 | 2B8 | 3E | 0D6 | 3AC | 3A5 | 2 | 306 |
| 3B. | 16 E | ODB | 3C0 | 25B | 088 | 2D8 | 3BF | 380 | 259 | 2A1 | 1E | 37 | 02F | 029 | 2F | 2B |
| 3 C . | 2 C 4 | 136 | 2BB | 3B1 | 1DE | 3D5 | 01C | 25E | 2B3 | 069 | 0A6 | 10 | OD5 | 3DC | 118 | 2E |
| D | 2DD | 1D3 | 18 F | 371 | 064 | 260 | 0C7 | OEO | C | 1D0 | 3EE | OD | 37A | 387 | 3CB | 234 |
| S. | 3D0 | 15F | 3B2 | 08F | 15A | 013 | 331 | 328 | 06 | 25D | OF | 09 | 16 | 378 | 3CE | 139 |
| 3 F . | 005 | 09A | 12B | 061 | 231 | 1A0 | 3CF | 3CA | 2D | 192 | 086 | 357 | 22C | 12A | 3FC | 37E |

Figure A.8: Specification of the secret S-box $\mathbf{S}_{2}$.

|  |  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 12E | 38 | 18E | 131 | 039 | 10D | 2DE | 24 | 28 | 2BE | 315 | 38 |  |  | 06D |  |
| 01. | 2A2 | 2CE | 264 | 085 | 374 | 3BB | 3B9 | 1B | 3E | 3B | 20 | 00 | 39 | 1B5 | OBA |  |
| 02. | 390 | EE | 1DA | 125 | 019 | 063 | 27 | 2 | 19A | 082 | 305 | 0E3 | 206 | OAO | 009 |  |
| 03. | 100 | 3F3 | 2 AD | 199 | 102 | 108 | 1DB | 2 F 0 | 310 | 245 | 0A8 | 11 | 022 | 3C1 | 28 |  |
| 04 | 1E1 | 2E7 | ODA | 2B7 | OCB | 07 C | 2 AO | 240 | 150 | 165 | 258 | 2C | 0C4 | 334 | 36B |  |
| 05. | 1E0 | 138 | 39A | 0FF | 1A7 | 10C | 353 | 19B | 171 | 038 | 3BD | 000 | 3A2 | B8 | 28 |  |
| 06. | 1D4 | D | 20F | $23 C$ | 0D7 | 154 | 012 | ODF | 3 A | 237 | 09E | 15 | 2E2 | 189 |  |  |
|  | $1 \mathrm{B4}$ | 381 | 273 | 123 | 052 | 12 | 158 | 033 | 2D | 3D3 | 23B | 3B | 2F7 | 160 | 341 |  |
| 08. | 337 | 1E6 | 3BE | 327 | 1D3 | 045 | 2 E 4 | 107 | 1C2 | 263 | 2A4 | 2CF | 244 | 196 | 36A |  |
| 09. | OA | 2 C 3 | 004 | 049 | 209 | ЗАЗ | 221 | 36 | 01E | 1 B | 05D | 319 | 21B | 24 | 2B2 |  |
| OA | 198 | 26A | 080 | 1B1 | 40 | 28A | 330 | 316 | 0FC | 37F | 1A8 | 13 | 17 F | 3D | 34 |  |
|  | 2D9 | 32A | 34A | 1D1 | 09D | 3FB | BE | 3EA | 383 | 36 | 3B6 | 22 | 22 E | 2B6 | 3 A6 |  |
|  | 1 C 1 | B2 | 11 | 3E8 | 129 | 34 | 153 | 333 | 07 | 01F | 01D | 21 | 299 | 0F8 | 130 |  |
| OD. | 18 | OA2 | 1A1 | 3D5 | 119 | 10F | 24 C | 020 | 097 | 3F0 | 280 | 112 | 04C | 4D | 1EB |  |
| OE. | 386 | AE | 322 | 2FE | 0C5 | 3D | 1A | 345 | 05B | 3F5 | 110 | 1 C | 03 C | 1 C 5 | 35A |  |
| OF. | 3F1 | 5B | 338 | 1CB | OF4 | 2B4 | 00F | 3A1 | 24 | 3D | 29D | 1B | 00 | 114 | 3F |  |
| 10 | 35F | 217 | 26 | 2 C | 15D | 28 | 390 | 1C9 | 1D | C7 | 4 F | 11 | 066 | 04D | 03B |  |
|  | 2BA | 2FD | 347 | 19 | 044 | OB | 94 | 148 | 25 | 360 | 326 | 25 | 1AE | 396 | 98 |  |
|  | 1 E 7 | 3CD | 1FF | 269 | 040 | 3E | 08A | 216 | 0 | 33B | 3D9 | 1BC | 2B1 | 325 | 11B |  |
| 13. | 053 | 2 A | 186 | 180 | 27D | 11F | 2A9 | 13 E | 3E | OD4 | 24 | 1D2 | 2 F | 3C9 | 1F |  |
|  | 3DE | 1D7 | 025 | 372 | 39 | 2C | 2ED | 25 | OA | 09 | 2EF | 24 | OE | 2D3 | 105 |  |
| 15 | 2CC | 36D | 31F | 24B | 1D8 | 24 | 068 | 211 | 2A | A | 355 | 35 | 026 | 2BD | 238 |  |
|  | 35B | 233 | 05 | 1BE | 291 | 368 | 37 | 035 | 29 | 4 | 26B | 1 E 4 | 379 | 7 F | 3EB |  |
|  | 20B | 12D | 375 | 1BF | 12 F | 1 AA | 18B | 268 | 3F4 | 364 | 0F7 | 1CC | 0B9 | 5 | 0 |  |
| 18. | 22B | 17C | 11C | OB1 | 23A | 3B | 05F | 2F | 21 | 224 | OE5 | 04 | 06F | 39 | 21 |  |
| 19 | 1 D | 177 | 190 | 39 | 274 | 35 | OE2 | 2E9 | 39 | F1 | 01 | 09 | 7 D | 08E | 31 |  |
|  | ODC | 3 F | 1AC | 1A | 132 | 15 | 19 | 3AD | 3E | C2 | 1 BB | OF | OCD | 074 | 17 |  |
|  | 18 | 3E0 | 389 | 2FB |  | OB | 25 | 27 | 06C | 3 | OFB | 29 | 297 | 30F | 350 |  |
|  | 007 | 10E | 19 C | 055 | 51 | 034 | 17 | 103 | 272 | 02 | 2C0 | 21- | 04 | 20D | OEA |  |
| 1 D. | 13F | DF | 162 | 376 | OBF | 1C | 3E | 2B9 | 3F | 88 | 13 | OA | 33 A | 304 | F |  |
| 1 L | 13 D | OBD | 294 | 02B | 127 | 1 E | 275 | 07B | 14 | 18 | 031 | 1 C 6 | 0A3 | EC | 27 |  |
|  | 38 D | 3B0 | 28 | 1FA | $1 F 5$ | 00 | 3E2 | 02E | 22 | 28 | 34B | 31 | 075 | 2F1 | 1 C 4 |  |
|  | 3 FF | 202 | 27 | 2 | 30D | 13 | 33F | 301 | 3D | 2 C 6 | 3D2 | 30 | 05 | 07 | 1F1 |  |
|  | 3B5 | 3CE | 111 | OB4 | 20 E | 1B | 1 F | 24 | 39 | 15 | 366 | 336 | 39 | 017 | 25C |  |
| 22. | 1 EC | 2BC | 144 | 1E9 | 93 | 16A | 33D | 34 | 29 | 079 | 02 | 2D | 38 | 17 | 292 |  |
| 23 | OF | 35E | 1 EF | OBB | 106 | 07 | 2DA | 3 F | 084 | 037 | 2A | 33 | OBO | 2D | 07 |  |
|  | 00 C | 149 | OAF | 29 | 2E0 | 12 | 283 | 32E | 3 | 3C3 | 1D9 | 2 E | 37B | OBC | 265 |  |
|  | 089 | 2CB | 11 | 081 | 18A | 25 | 05 | 1 A | 28 | D | 27 | 32 | OC | 30B | 22 |  |
|  | 2F3 | 0A5 | 121 | 2AA | 210 | 091 | 208 | 3E | 230 | 320 | 385 | 28 E | 21. | 3F | 11 |  |
|  | 159 | 281 | 0C8 | 37 C | ODD | 18 | 04F | 26E | 33 | 2F8 | 3A | 3B3 | 3C8 | 227 | 1 A 2 |  |
| 28 | 302 | 6 E | 38 | 19 | 212 | 13 | 24D | OB3 | 141 | 3EF | 1 | 26 | 145 | 362 | 34 |  |
| 29. | 1 E | 4B | 3A9 | 3DD | 093 | 3F8 | 7 | OD3 | 1EA | 3BA | 2 | 146 | 201 | 24 | 1F6 |  |
|  | 1 CD | 20A | 2F6 | OOE | 67 | 26 | 2A | 1FC | 2D | D 1 | 38 | 006 | 30 | 3E | 2 |  |
| 2 B . | 2D5 | A7 | 1D5 | 3 A 4 | 101 | 2D | 34E | 2B | 072 | 26 | 090 | 1F8 | 1 F | 3A | 1F0 |  |
|  | 2 C 2 | 21A | 06 | OAB | 1EE | 109 | 16 B | 15 | 16 | 38 | 15 | 27 | 27 | 36 | 342 |  |
|  | 01A | 016 | 352 | 173 | 34D | 35 | 181 | 185 | 1A | 23F | 16 C | 030 | 21 | 1 C 3 | 2EA |  |
| 2E | ODE | 078 | 18 | 01 | 117 | 39 | 3F2 | 39 | 37 | 1 BD | 24 | 18 C | 29A | 0A4 | 08D |  |
| 2 F . | 015 | 065 | 0C1 | 251 | OD | 348 | 014 | 21 | 00 | 008 | 2 C | 321 | B | 1B | 04 |  |
| 30. | 223 | B6 | 054 | A | OFD | 37 | 31E | 32 | 20 | 15 | 10 | 28 | D | 041 | 34 |  |
|  | 32F | OED | 27 | 179 | 278 | 3 F | 23E | 25 | 07 | 4 | 12 | 20 | 308 | 30 | 312 |  |
|  | 1 ED | 048 | 30c | 183 |  | 39 | 3B |  |  |  | 050 | 1 C | 19 | 3BF | 046 |  |
|  | 1F3 | 43 | 05 | 1F2 | 169 | 26 | 25 | 26 | OF | 2B | 09 | 17 | 31 | 0F6 | 0E6 |  |
| 34. | 225 | 36C | 377 | 253 | 058 | OE1 | 2 | 31 | 3D | AD | 16 | 2A | 06B | 23D | 398 |  |
|  | 35D | FA | 00B | 391 | 99 | OF | 535 | 02 | 08 | 4 | 02A | 29E | 36F | 21 | 10 |  |
|  | 0 E 4 | 096 | 19 F | 2E1 | 1 FD | 30 | 28 D | 07 | 11A | E | OE | 370 | 358 | 1 D | 163 |  |
| 37. | 367 | 03 | 2D6 | 36 | 22 | 3D | 08 | 1E5 | 27 | 2E8 | 2FF | 16 | 10 A | 2AE | 170 |  |
| 38 | 2 A 3 | 08C | 1 CF | 076 | 3D1 | 32B | 2EC | 2A5 | 2C9 | 2A6 | 29 | 3ED | $09 C$ | OCC | 2A8 |  |
| 39. | OFE | 293 | 29F | 2F4 | E7 | 232 | OCE | 3 AB | 13A | 01 | 3DB | 220 | OD8 | 1 F | 22F |  |
| 3 A . | 062 | 1 A 4 | 27A | 128 | 29 | 324 | 6 | 365 | 024 | B8 | 3E | 0D6 | A | 3A5 | 172 |  |
| 3 B . | 16 E | ODB | 3CO | 25B | 88 | 2D8 | O3 | 38 | 259 | 2A1 | 1E | OB | 2 | 02 | 356 |  |
| $3 C$. | 2 C 4 | 03E | 2BB | 3B1 | 17E | 3CC | 01C | 25E | 2B3 | 069 | OA6 | 15C | 0D5 | 3DC | 118 |  |
| 3 D . | 2DD | 235 | 18F | 371 | 064 | 260 | 0C7 | OEO | 0C6 | 1D0 | 254 | OD9 | 37A | 387 | 3CB |  |
| 3 E . | 3D0 | 15F | 3B2 | 08F | 15A | 013 | 331 | 328 | 06E | 25D | 0F9 | 092 | 166 | 378 | 31D |  |
| 3F | 005 | 09A | 12B | 061 | 231 | 1A0 | 3CF | 3CA | 382 | 192 | 086 | 357 | 22C | 12A | 3FC |  |

Figure A.9: Specification of the modified S-box $S_{2}$.

Appendix A - Specifications of BEA-1 Building Blocks

|  | . 0 | 1 | 2 | . 3 |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 00 | 1 AD | 084 | 1B5 | 30A | 25 | 151 | 7 | 3F9 | 113 | 3B4 | 35B | 291 | 33 | 170 | 021 | 31 |
| 01. | OOE | FC | 23 | OBO | 376 | 259 | 2BC | 378 | 03 | 050 | 359 | 1FF | 26 | OD5 | 214 | BD |
| 02 | 1 AB | AB | 3AC | 036 | OE2 | 2F6 | 7A | OEA | 2C | FE | 24 E | 28 | 057 | 073 | 219 | EA |
| 03. | 2E2 | 27C | 032 | 162 | 285 | 13C | OB6 | 1ED | OB3 | 2F5 | 2C6 | 34B | 335 | 93 | 29 | 37A |
|  | 273 | 7 E | 30F | 2E7 | 14B | 3BC | 1 CE | 03 | 315 | 01A | 144 | 1 C | 20A | 349 | 36 | OD |
|  | 235 | 1D9 | 2F9 | OA | 052 | OE3 | 17 F | 061 | 02 | 140 | OE1 | 156 | 10E | 250 | 288 | BE |
|  | 07C | 2B8 | 05D | 242 | 192 | 0A8 | 3B0 | ODB | 12 | 2 AF | 063 | 3AF | 3D1 | 0C8 | 0A6 | 29 |
|  | 2B9 | 3B8 | 092 | 07 | 2A2 | 06E | 2C | 3 | OE | 0E7 | 019 | 1F1 | 07E | 1BB | 2 C | 251 |
| 08 | 36A | CA | 076 | 216 | 2E5 | OE6 | 1DD | 2FE | 390 | 27 | 1D2 | 39 | 2C5 | 02 | 05 | 396 |
|  | 0 F 4 | 65 | OFD | 150 | 027 | 111 | 2E | 29 | 3D | 11F | 2 A 1 | 158 | 388 | D3 | 3C | 86 |
|  | 38B | 279 | 064 | 1A4 | 028 | 34F | 1D5 | 35 | 2C | 257 | 3C4 | 35 | OB7 | 322 | 2C1 | 17 |
|  | 1DF | A9 | 137 | 3DC | 015 | 09 | 2AA | 2A4 | 3F | 1 A3 | 3DA | 08 | E8 | 343 | 36 | 11A |
| 0 C | OA5 | 38D | 328 | 348 | 292 | 308 | 3F | 059 | 31C | 1AC | 1E4 | 3BF | C | 36D | 1D8 | OED |
| OD. | 191 | D3 | D | 046 | E8 | 373 | 03 | 230 | 10 | 3C | 11E | 393 | 00B | 2D7 | 2D | 00F |
|  | 209 | 30 | 19D | 18 | 1B8 | 339 | 360 | 240 | 011 | 305 | 17A | 324 | 344 | 045 | 3F0 |  |
|  | 1 C 6 | OB4 | 08D | 18 | 035 | OC9 | 345 | OD3 | 37 | CA | 284 | 3E | 00D | 197 | 36 | 6B |
|  | 08B | OB | 18A | 218 | 3DE | 32A | 2CC | OAE | 25 | 3FC | 066 | 24 | 24D | 232 | OA2 |  |
|  | 2DB | 199 | 37F | 1E | 392 | 3F3 | 1-8 | 1CD | 136 | 2DO | 325 | 27B | 068 | 1F | 077 | 22D |
|  | 1 E 2 | 2F4 | OB2 | 2E9 | 3CC | 296 | 2E | 116 | 30 | 27 | 02 | 11B | 09 C | 25E | 15 | 195 |
|  | 3 A | 3F2 | 3D7 | 13 | 258 | 22 | OD | 26B |  | 1 E | 379 | 32 | 17 | 2D5 | OC | 9 F |
|  | 39E | 09E | 1FD | 15B | 126 | 2B3 | 5E | 012 | 21A | , | 356 | 154 |  | 017 | 21 |  |
|  | 1F8 | 261 | 3ED | 14 | 22F | 110 | 03 | 1B7 | 07 | 201 | 3C | OE | 2B6 | 107 | 3C | 302 |
|  | 19E | 21D | 1E5 | 205 | 25 | 3BD | 19 | 19 | 337 | 69 | 32 | OD | 3EE | 272 | OB | 3C2 |
|  | 01D | 37B | 3 CO | OA3 | 22E | 123 | 2A | ODE | 2A7 | FF | 3 A | 05 | 38 | 04 | 1B | 50 |
|  | 1 EE | 0A1 | 29D | 1F | 02 | 29 | 3A3 | 11 | 3B | 21 | 09A | 37E | 2 A | 0C2 | 377 |  |
|  | 149 | 04A | 0E9 | 36 | 3D6 | 2E3 | 20 | 35 | 17B | 0D | 13 | 3D | 36 | 36 | 33 |  |
|  | 1DC | 3B2 | 2B1 | 2 AB | 3F1 | 1FA | 06 | 06 | 02 | 211 | 23 | 28 | ODA | 34 | 20 | A8 |
|  | 28 F | 389 | 349 | 3F5 | 2FB | 1CF | 38 | 38 | OC | 08F | 0CO | 135 | 3A7 | 2BO | 34 | 30E |
|  | 163 | 3 C | 32F | 1E | OFA | 12 | 244 | 226 | 1 C | 35 E | 1A | 25 | 1 E | 3A | 146 | S |
|  | 148 | 353 | OFF | 37 |  | 2C0 | 26 |  | 117 | 1 E | 2A | 003 | 32 | AD | 1D |  |
|  | 072 | 18D | 297 | 39 | OC7 | 12D | 01 | 222 | 05 | 27 | 28 | 0 | 36 | 293 | 3E0 | 35 |
|  | 369 | 299 | 190 | 10F | 25B | 183 | 08 | 1B6 | 36 | 3AA | 3E1 | 31 | 2BA | 15C | OD | D |
|  | 342 | 2EE | 1 AE | 04 | A7 | 2CD | 2F8 | 03A | 01F | OBA | 18 | 09 | 2B7 | 382 | 16F | C5 |
|  | $1 \mathrm{B0}$ | 2D2 | 1CC | 3B | 26 | 15 | 24B | 1 E 7 | OD | OFC | 33 | 0F | 3BB | 25 C | 1 C 7 | D |
|  | 000 | 271 | OAA | 1C5 | 357 | 1E8 | 01E | 3FE | 08 | 24 | 31 | 29 | 16 | 13F | 212 |  |
|  | 141 | 1B9 | 2 C | 02E | 087 | OE | 13 | 26 | 17 | 24 | 22 | 206 | 13 | 00 | OAO | 23F |
|  | 02B | BB | 06F | 05E | 275 | 20 | 3B3 | 12A | 28 | 100 | 2AC | 22 | 263 | 0F9 | 1C0 | 21B |
|  | 203 | 03 | 35 | 295 | 088 | 008 | 3E | OD | 307 | 105 | 12 | 185 | A 7 | 3EC | 11C | 34 |
|  | 09 | 39D | 1B2 | 02A | 3B1 | 20 | 114 | 312 | 16 | 131 | 30 | 29 | 231 | 3E | 2D | 3D |
|  | 2C2 | 32 C | 3E6 | 2 F | 00 | 10 | 32 | 2F | 2D | 1BA | 2 FD | 35 | 25 |  | 282 |  |
|  | 338 | 14 F | 1B | 28B | 330 | 2F0 | 18 | 175 | 12 | 169 | 2D | 22 | 2F | 255 | C | 13D |
|  | 398 | 15 F | 16D | 2D | 2BD | OF | 3 F | 2ED | 14 | 161 | 01 | 04 | 17 | 28C | 05 | C1 |
|  | 1 A | 21F | 1DA | 27 F | 124 | 2B | 39C | 005 | 05 | 35F | 143 | 3CE | 19 | 043 | 12F |  |
|  | OC | 86 | 18B | 24 | 006 | 10 | 333 | 152 | 1 BF | 3FF | 3B7 | 1EC | 30B | 8 | 08 |  |
|  | 089 | 3CD | 1 F | 21 | 2EB | 30 | 2F | 13 | 20 | AD | 02 | OEC | 11 | 1 D | 3A |  |
|  | 311 | E6 | 3FB | OA | 2 E | 12 | 22 | 03 | OF | F | 20 | 16C | 28 | 18 | 33A |  |
|  | 033 | A | OCA | A5 | 010 | 31 | 3B |  | 3B | D | 19 | 2AD | 28 | 085 | 00A | 2B |
|  | 0F5 | 3AB | 1D0 | 2E6 | OEB | 2D | B2 |  | 065 | 88 | 18 | 36 | 33 | B8 | 2CE |  |
|  | 289 | 142 | 266 | 132 | 3E2 | 24 | 10 | 24 | 39 | 09B | 09 | 1 A | 22 | 375 | 320 |  |
|  | 33D | 18 | 3EB | 030 | 15A | 28 | 1A1 | 20 | 3C | 331 | 31 | 08 | 12 | 34E | 07 | 239 |
|  | 23 A | 300 | OB | 01 C | 2B | 1E0 |  | 18 | 32 | 3 | 26 | 37 | 1B | 36 | 26 | 3E |
|  | OC | 165 | OF6 | 19 C | 070 | OEO | 36 | 1D | 24 | 1 | 05 | 10 | 2D | 2B | 3DB | 92E |
|  | 30 C | 1CB | O | 1F7 | 15 | 2E0 | 01 | 236 | 2A3 | 22 | OBB | 14D | 18 | 278 | 155 |  |
|  | 178 | OCD | 37 | 07 | 3A | 23 | 04 | 2D | 39 | OB | 1B | 21 | 39 | 3F | OA | 004 |
|  | 34A | 055 | 04D | 14C | 33F | 13 | 301 | 05 | 3A | 11 | 2D | 07 | 3F | 391 | 040 | 326 |
|  | 2D8 | 00 | ODC | OD1 | 4 | 14 E | 20B | 1A5 | 16 | 168 | 05 | 22 | 318 | OCC | 16E | 172 |
| 38. | 1 CA | 2 C 4 | 3C3 | A9 | 3 F | 173 | 27E | 08A | 25D | 1 F | 01 | 17 | 4 | 16B | 38 | 76 |
|  | 31 D | 3E9 | 108 | 139 | 2C9 | 04C | 18 | 07 | 29 F | 381 | 316 | 03 | OCE | 06D | 34 | A |
| 3 A . | 122 | 2A8 | 1 C 3 | 04E | 368 | 351 | 202 | 38A | 225 | 189 | 19 | 306 | 026 | OFO | 248 | 08 |
| 3 B . | 05F | 19F | 2BE | 270 | 060 | 083 | 186 | 3D | 2AE | OC | 23D | 160 | 24 | 0F8 | 1EB | 385 |
|  | 374 | 177 | 3E4 | 358 | 1 FE | 099 | 120 | 1D | 3A4 | 310 | 030 | 1AF | 1F | OBE | 07 | 16A |
| . | 274 | 1D6 | 21C | 3FD | 3C6 | 238 | 234 | 262 | 3D5 | 31A | 395 | 27D | 3E8 | 128 | 00 | 29A |
| 3 E . | 32D | ODO | 341 | 26E | OB9 | 224 | 237 | OF | 2E4 | 12 C | 103 | 025 | 20 | 260 | 3AE | 269 |
| 3F | 07F | 03B | 03E | 007 | 182 | 159 | 091 | 3B6 | 3E3 | 384 | 264 | 0D6 | 36C | 256 | 221 | 24 |

Figure A.10: Specification of the secret S-box $\mathbf{S}_{3}$.

|  | . 0 | . 1 | 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  |  |  |  |  |  |  |  |  |  |  | 35 | 291 |  |  |  |  |
| 01 | OOE | 2 FC | 023 | OBO | 3A9 | 259 | BC | 378 | 031 | 50 | OD | 1FF | 26 C |  |  |  |
|  | 1 AB | OAB | 3A | 036 | OE2 | 2 F 6 | 07A | OEA | $2 C B$ | OFE | 24E | 280 | 138 | 073 | 19 |  |
| 03. | 2E2 | 27C | 032 | 162 | 285 | 13 C | 0B6 | 1 ED | OB3 | 2 F 5 | 2 C 6 | 34B | 335 | 1EF | 26 E |  |
| 04. | 273 | 17E | 30F | 2E7 | 14B | 3BC | 1 CE | 039 | 315 | 01A | 14 | 1 C | 20 | 7B | 362 |  |
| 05. | 235 | $1 \mathrm{D9}$ | 2F9 | OA4 | 052 | OE3 | OBD | 061 | 02 | 140 | OE | 156 | 10 | 250 | 288 |  |
| 06. | 07 C | 2B8 | 05D | 242 | 192 | OA8 | 3B0 | ODB | 129 | 2AF | 06 | 3AF | 3D1 | OC8 | A6 |  |
| 07. | $2 \mathrm{2B9}$ | 3B8 | OD2 | 078 | 2A2 | 06E | 2 CF | 3CF | OEF | OE7 | 01 | 1 F 1 | 07E | 1BB | 2 C 7 |  |
| 08. | 36A | 2 CA | 076 | 216 | 2E5 | OE6 | 1DD | 2 FE | 390 | 277 | 1D2 | 394 | 2 C 5 | 022 | 05A |  |
| 09. | OF4 | 265 | OFD | 150 | 057 | 111 | 2 EC | 29 C | 3DF | 11F | 13A | 158 | 38 | 1D3 | 3C8 |  |
| OA | 38B | 279 | 064 | 1 A 4 | 028 | 22F | 1D5 | 352 | 2 C 8 | 257 | 3 C 4 | 355 | 104 | 322 | 2 C 1 |  |
| OB | 1DF | 1 A 9 | 137 | 3DC | 015 | 096 | 2AA | 2 A 4 | 3 F 6 | 1 A | 3DA | 086 | 2 E 8 | 343 | 233 |  |
| OC | OA5 | 38D | 328 | 348 | 292 | 132 | $3 F 4$ | 059 | 310 | 1 AC | 1 C 6 | 3BF | 1 C 2 | 36 D | D8 |  |
|  | 191 | 3D3 | 3D4 | 3DE | OE8 | 373 | 034 | 23 C | 224 | 3C5 | 11E | 393 | OOB | 308 | 2DA |  |
|  | 209 | 230 | 19D | 184 | 188 | 339 | 360 | 2 D 7 | 011 | 305 | 17A | 324 | 34 | 28 |  |  |
|  | 317 | OB4 | 08D | 18E | 035 | OC9 | 345 | OD3 | 37D | 3 C | 284 | 3EF |  | 97 |  |  |
|  | 08B | 10B | 18A | 218 | 046 | 32A | 2 CC | OAE | 25 | 3 F | 066 | 246 | 4D | 232 | A2 |  |
|  | 2DB | 199 | 37F | 1E1 | 392 | $3 F 3$ | 1 C 8 | 1CD | 136 | 2DO | 325 | 27B | 068 | F5 |  |  |
| 12. | 12 F | 2 F 4 | OB2 | 2E9 | 3CC | 296 | 2EA | 116 | 30 | 276 | 02D | 266 | 09C | 25E |  |  |
| 13. | 3 A 1 | $3 F 2$ | 3D7 | 130 | 258 | 227 | OD4 | 26B | 027 | 1EA | 37 | 32 | 179 | 2D5 | C4 |  |
| 14. | 39E | 09E | 1 FD | 15B | 126 | 2 3 3 | 15E | 012 | 21A | 372 | 356 | 154 | 042 | 017 | 217 |  |
| 15 | 1 F 8 | 261 | 3ED | 14A | 1 FB | 110 | 037 | 1 B 7 | 079 | 045 | $3 \mathrm{C9}$ | OEE | $2 \mathrm{B6}$ | 107 | CB |  |
| 16. | 19 E | 21D | 1 E 5 | 205 | 25F | 3BD | 196 | 198 | 337 | 069 | 32E | ODF | 3EE | 201 | BC |  |
| 17. | 01D | 37B | 3 CO | оАЗ | 22E | 123 | 249 | ODE | 2 A 7 | 2FF | 3 A 5 | 05B | 38F | 047 | B4 |  |
| 18. | OCB | OA1 | 29D | 1 FC | 024 | 29B | 3A3 | 2A1 | 3BE | 215 | 09A | 37 E | 2AO | OC2 | 377 |  |
| 19. | 149 | 33B | 323 | 365 | 3D6 | 2 E 3 | 082 | 35A | 38 | OD7 | 134 | 3D0 | 36 | 336 | 334 |  |
| 1 A | 1 DC | 3B2 | 2B1 | 213 | 3 F 1 | 1FA | 380 | 06 | 020 | 211 | 033 | 28D | ODA |  |  |  |
| 1B | 28 F | 369 | 349 | 355 | 2FB | 1 C | 383 | 38 | 35 | 08F | 29 A | 135 | 3A7 | 2BO | 34 |  |
|  | 163 | 33 C | 32F | 093 | OFA | 125 | 244 | 22 | 1 C | 1 E | 1A | 25 | 1 E | 3A0 |  |  |
| 1D | 148 | 353 | OFF | 370 | 09D | 2 C | 268 | 04 | 11 | 1 E | 2A6 | 003 | 11B | OAD | 1D7 |  |
| 1 E | 072 | 18D | 297 | 39A | OC7 | 12D | 016 | 222 | 05 | 1 C | 28 | 095 | 36 | 293 | 3E0 |  |
| 1 F | 13 E | 299 | 190 | 10 F | 25B | 183 | 080 | 1B6 | 361 | 3AA | 3 E 1 | 318 | 2BA | 15 C | OD8 |  |
| 20 | 342 | 2 EE | 1 AE | 04F | 147 | 2 CD | 2 F 8 | 03A | 06 | OBA | 188 | 090 | 2 B 7 | 1 E 4 | 16 |  |
|  | 1 BO | 2D2 | 1 CC | 3B9 | 267 | 153 | 24B | 1E7 | 20 | OF | 2 E 6 | $0 \mathrm{F7}$ | 3BB | 376 |  |  |
|  | OOC | 271 | OAA | 1 C 5 | 357 | 1 E 8 | 01E | 3FE | 081 | 245 | 314 | 294 | 164 | 13F | 212 |  |
|  | 141 | 189 | 120 | 02E | 34 F | OE4 | 092 | 26 | 171 | 249 | 22B | 206 |  |  |  |  |
|  |  | 2BB | 06 F | 05E | 275 | 20 E | 3В3 |  |  |  | 2AC | 22A | 263 |  |  |  |
|  | 203 | 303 | 35 | 295 | 088 | 008 |  |  |  | 105 | 121 |  |  |  |  |  |
|  | 094 | 39 | 1B2 | 02A | 3B1 | 204 |  |  |  |  | 304 | 290 | 231 |  |  |  |
|  | 2 C 2 | 32 C | 3E | 04 | 009 | 10 C | 327 |  | 2 D 1 |  | 2 FD | 35D |  |  |  |  |
| 28 | 338 | 14F | 1B1 | 28B | 330 | 2 FO |  | 175 | 12 | 169 | 2D9 | 223 | 2 F 3 |  |  |  |
| 29 | 398 | 15 | 16 | 2DC | 2BD | OFB | 3FA | 2 ED | 14 | 161 | 01B | 04B | 17D |  |  |  |
| 2 A | 1 A 6 | 21 | 1DA | OE9 | 124 | 2BF |  | 00 | 05 | 35F | 143 | CE | 19A | 04 |  |  |
| 2 B | OCF | 286 | 18B | 243 | 006 | 106 | 333 | 152 | 18F | 3FF | 3B | 1E | 30B | 98 |  |  |
| 2 C . | 089 | 3 CD | 1 FO | 210 | EB | 309 | 2 F 7 | 13B | 20 D | 3AD | 02F | OEC | 11 | 6 |  |  |
| 2 D | 311 | 1 E 6 | 3FB | OAF | 2 E 1 | 12B | 220 | 03D | OF1 | 2FA | 208 | 16 | 28 | 181 | 33A |  |
| 2 E | 109 | 10A | OCA | 2 A | 10 | 31 F | 3BA | OB7 | 3B5 | 2DD | 193 | 2AD | 283 | 085 | OOA |  |
| 2 F . | 2 A 8 | 3AB | 1D0 | 2 F 1 | OEB | 2DF | 298 | 1 DE | 065 | 17 | 185 | 364 | 33 | OB | 2 CE |  |
| 30. | 289 | 142 | 2 B 2 | 0D6 | 3E2 | 24C | 101 | 24 | 39 | 098 | 097 | 1 A | 22 | 375 | 320 |  |
| 31. | 33D | 118 | 3EB | 03 C | 15A | 281 | 1A1 | 207 | 3C | 331 | 319 | 27A | 12 | 34 | 7B |  |
| 32. | 23A | 300 | OB5 | 010 | 2B5 | 1E0 | 39 F | 180 | 321 | 13 | 26F | 371 | 1B3 | 36 | 26D |  |
| 33 | OC6 | 165 | OF6 | 19 C | 070 | OEO | 367 | 002 | 24 | 38 | 053 | 27 F | 2D6 | 2 B | 3DB |  |
| 34 | 30 C | 1 AD | OE5 | 22 C | 15D | 2E0 | 013 | 23 | 243 | 228 | OBB | 14D | 018 | 278 | 155 |  |
| 35 | 178 | OCD | 370 | 07 | 3A | 23B | 049 | 2D4 | 397 | OBF | 1BC | 21 E | 39 | 358 |  |  |
|  |  | 055 | 04D | 14 C | 33 F | 1 | 301 | 05 C | зА2 | 112 | 2DE | 075 | 3 F | 391 |  |  |
|  | 2D8 | 000 | ODC | OD1 | 041 | 14 E | 067 | 160 | 166 | 168 | 051 | OA9 | 31B |  |  |  |
|  |  | 2 C 4 | 3 C 3 | 1 E 2 | 03 F | 17 | 27 | 08A | 25D | 1F9 | 01 | 17 | 04 | 16B |  |  |
|  | 31D | 3E9 | 108 | 139 | 2C9 | 04C | 187 | 071 | 29 | 381 | 316 | 038 | OCE |  | 34D |  |
|  | 122 | 225 | 1 C 3 | 04E | 368 | 351 | 202 | 38A | 102 | 189 | 194 | 306 | 026 | OFO | 248 |  |
| 3B | 05F | 19 F | 2BE | 270 | 060 | 083 | 186 | 3DD | 2AE | OC1 | 23D | 272 | 24 | OF8 | 1EB |  |
| 3 C | 374 | 177 | 3 E 4 | 358 | 1 FE | 099 | 2 AB | 1 D 4 | 3 A 4 | 310 | 030 | 1 AF | $1 F 4$ | OBE | 14 |  |
| 3 D | 274 | 1D6 | 21 C | 3FD | $3 \mathrm{C6}$ | 238 | 234 | 262 | D5 | 31A | 395 | 27D | 3E8 | 240 | , |  |
| 3 E | 32 D | 359 | 341 | 250 | -B9 | 115 | 237 | F | 2 E 4 | 12 | 103 | 025 | 20F | 260 | 3AE |  |
| 3 F | 07 F | 03B | 03E | 007 | 182 | 159 | 091 |  |  |  |  |  |  |  |  |  |

Figure A.11: Specification of the modified S-box $S_{3}$.

Appendix A - Specifications of BEA-1 Building Blocks

## Résumé long en français

Les trappes jouent un double rôle dans la cryptographie moderne. Même si elles sont essentielles en cryptographie asymétrique, leur rôle est tout autre lorsque l'on considère la cryptographie symétrique. Dans ce cas, une trappe désigne une faiblesse mathématique insérée volontairement au cœur du chiffrement, permettant à son concepteur de le casser efficacement. Une telle propriété est alors fortement indésirable. Pour qu'un chiffrement à trappe puisse inspirer confiance, il doit fournir les mêmes preuves de sécurité que tout autre chiffrement.

La première partie de cette thèse se concentre sur les analyses de sécurité par rapport aux deux principales cryptanalyses des chiffrements par blocs, à savoir les attaques différentielles et linéaires. Nous commençons par rappeler les fondements théoriques de ces deux cryptanalyses dans la section B.1. Nous détaillons ensuite notre algorithme permettant une évaluation automatique de la résistance des réseaux de substitutions-permutations aux cryptanalyses différentielle et linéaire dans la section B.2.

La seconde partie est quant à elle dédiée à l'étude d'une famille de chiffrements à trappes introduite par Paterson et Harpes. Ces chiffrements envoient une partition des messages clairs sur une partition des messages chiffrés indépendamment des clés utilisées. Tout d'abord, nous étudierons la structure de tels chiffrements dans la section B.3. Nous obtiendrons ensuite des bornes sur leur sécurité dans la section B. 4 puis nous expliquerons comment les primitives du chiffrement doivent être conçues pour atteindre ces bornes. Enfin, nous conclurons dans la section B. 5 en présentant BEA-1, un chiffrement à trappe grandeur nature développé à partir de notre théorie. Bien qu'il soit résistant aux cryptanalyses différentielle et linéaire, la connaissance de la trappe permet de retrouver la clé de 120 bits en seulement quelques secondes sur un portable.

## B. 1. Réseaux de substitutions-permutations

La cryptologie est la science des secrets. Elle a pour objectif de permettre à deux parties, appelées généralement Alice et Bob, de communiquer sur un canal non sécurisé. Un canal peut désigner n'importe quel moyen de communication, comme une ligne téléphonique ou un réseau informatique. Il est dit non sécurisé dès qu'une tierce

## Appendice B - Résumé long en français

partie peut intercepter ou modifier les messages envoyés. La cryptologie est divisée en deux parties complémentaires. D'une part, la cryptographie regroupe les différentes méthodes de protection de l'information. Cela inclut naturellement la confidentialité assurant qu'un adversaire interceptant un message ne peut obtenir aucune information sur son contenu. Cependant, la cryptographie s'intéresse également à l'intégrité (assurant que le message reçu est identique à celui envoyé) et à l'authenticité (prouvant l'identité de la source du message). D'autre part, la cryptanalyse a pour objectif de casser la sécurité assurée par la cryptographie.

La confidentialité s'obtient via un algorithme de chiffrement. Dans le contexte de la cryptographie à clé secrète, Alice et Bob doivent s'échanger une clé secrète avant de pouvoir communiquer sur un canal non sécurisé. Supposons qu'Alice souhaite communiquer avec Bob. L'information qu'elle souhaite partager s'appelle le message clair. Ensuite, à l'aide de la clé secrète et de l'algorithme de chiffrement, Alice chiffre le message clair et obtient un message chiffré qu'elle envoie à Bob. Ce dernier peut alors déchiffrer le message chiffré à l'aide de la clé secrète qu'il partage avec Alice et recouvre ainsi le message original.

## B.1.1. Définitions

Les algorithmes de chiffrement à clé secrète sont eux-mêmes divisés entre les chiffrements par blocs et les chiffrements par flots. Nous ne considérons dans cette thèse que les chiffrements par blocs ; cependant le lecteur peut se renseigner sur les chiffrements par flots en lisant par exemple [77]. Un chiffrement par blocs est un algorithme opérant sur des blocs de données de longueur fixée utilisant une clé secrète, appelée clé de chiffrement [39].

Définition B. 1 (Chiffrement par blocs). Soient $n$ et $\kappa$ deux entiers naturels non nuls. un chiffrement par blocs est une application $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ prenant en entrée un clé de chiffrement de $\kappa$ bits, un bloc de message clair de $n$ bits et produit le bloc chiffré $c=E(K, p)$ associé de $n$ bits.
De plus, pour toute clé de chiffrement $K$ dans $\mathbb{F}_{2}^{\kappa}$, l'application $E_{K}: p \mapsto E(k, p)$ doit être une permutation de $\mathbb{F}_{2}^{n}$.

L'entier $n$ correspond à la taille des blocs du chiffrement et $\kappa$ désigne la longueur de sa clé. L'application $E_{K}$ est appelée fonction de chiffrement associée à la clé de chiffrement $K$. Son inverse est appelée fonction de déchiffrement et est notée $D_{K}$. Remarquons enfin qu'un chiffrement par blocs seul ne peut chiffrer qu'un message de longueur fixe, généralement entre 64 et 128 bits. Pour chiffrer un message de longueur quelconque, on utilise conjointement au chiffrement par blocs un mode de chiffrement expliquant comment l'utiliser. Introduisons maintenant une famille majeure comprenant presque tous les chiffrements par blocs modernes.

Définition B. 2 (chiffrements itérés). Un chiffrement par blocs $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n}$ est dit itéré sur r rondes s'il est formé des deux applications suivantes.

- Un algorithme appelé cadenceur des clés de rondes transforme la clé de chiffrement $K$ dans $\mathbb{F}_{2}^{\kappa}$ en $r$ clés de rondes $k^{[0]}, \ldots, k^{[r-1]}$ dans $\mathbb{F}_{2}^{l}$.
- Une application $F: \mathbb{F}_{2}^{l} \times \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ appelée fonction de ronde, telle que pour toute clé de chiffrement $K$, la fonction de chiffrement peut s'écrire

$$
E_{K}=F_{k[r-1]} \circ \cdots \circ F_{k[0]} .
$$



Figure B. 1 : Représentation d'un chiffrement itéré (voir la définition B.2).

Remarque B.3. L'entier $l$ est appelé longueur des clés de rondes. L'application $F_{k}$ de $\mathbb{F}_{2}^{n}$ vers $\mathbb{F}_{2}^{n}$ envoyant un bloc $x$ sur $F(k, x)$ est appelée fonction de ronde associée à la clé de ronde $k$. Naturellement, chaque application $F_{k}$ doit être une permutation de $\mathbb{F}_{2}^{n}$. La figure B. 1 donne une représentation schématique d'un tel chiffrement.

Parmi les chiffrements itérés, on trouve les réseaux de substitutions-permutations (abrégés en SPN) qui sont directement inspirés des travaux de Shannon [91]. La fonction de ronde d'un SPN est constituée de trois étapes : l'ajout de clé, la couche de substitution et la couche de diffusion (ou de permutation). L'une des primitives d'un SPN est appelée boîte de substitution, ou simplement $S$-box.

Définition B. 4 (S-Box). Une $S$-box sur $n$ bits est une application de $\mathbb{F}_{2}^{n}$ vers $\mathbb{F}_{2}^{n}$. Dans cette thèse, nous supposerons que les S-boxes sont bijectives.

Dans la couche de substitution, le bloc de $n m$ bits est vu comme $m$ paquets de $n$ bits. Ensuite, $m$ S-boxes sont évaluées en parallèle sur chacun de ses paquets. À l'inverse, la couche de diffusion traite le bloc de données dans son ensemble.

Définition B. 5 (SPN). Soient $m$ et $n$ deux entiers naturels non nuls et $S_{0}, \ldots, S_{m-1}$ des S-boxes sur $n$ bits.

- L'ajout de la clé de ronde $k$ et notée $\alpha_{k}: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ et envoie $x$ sur $x+k$.
- La couche de substitution est notée $\sigma$ et envoie $\left(x_{i}\right)_{0 \leq i<m} \operatorname{sur}\left(S_{i}\left(x_{i}\right)\right)_{0 \leq i<m}$.
- La couche de diffusion est une permutation linéaire notée $\pi: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$. Un réseau de substitutions-permutations est un chiffrement itéré dont la fonction ronde est $F_{k}=\pi \circ \sigma \circ \alpha_{k}$.

En notant $k^{[0]}, \ldots, k^{[r]}$ les clés de rondes extraites de la clé de chiffrement $K$, la fonction de chiffrement d'un SPN est donc donnée par

$$
E_{K}=\alpha_{k[r]} \circ \underbrace{\pi \circ \sigma \circ \alpha_{k}[r-1]}_{F_{k}[r-1]} \circ \cdots \circ \underbrace{\pi \circ \sigma \circ \alpha_{k[0]}}_{F_{k[0]}} .
$$

Avant de conclure cette partie, nous introduisons une famille de couches de diffusion particulièrement utilisée dans les algorithmes de chiffrement à bas coûts.

Définition B. 6 (permutation des bits). Une application linéaire $\pi: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ est appelée permutation des bits s'il existe une permutation $\phi$ de $\llbracket 0, n m \llbracket$ vérifiant

$$
\pi\left(x_{0}, \ldots, x_{n m-1}\right)=\left(x_{\phi^{-1}(0)}, \ldots, x_{\phi^{-1}(n m-1)}\right) .
$$

## B.1.2. Cryptanalyse différentielle

La cryptanalyse différentielle, introduite par Biham et Shamir dans [13, 14] est aujourd'hui l'une des attaques majeures contre les chiffrements par blocs [39, 64]. Il s'agit d'une attaque à clairs choisis nécessitant le chiffrement de plusieurs pairs de messages clairs dont la différence est fixée. L'attaque exploite ensuite une distribution non uniforme parmi les différences entre les paires de chiffrés pour obtenir de l'information sur la dernière clé de ronde du chiffrement.

## B.1.2.a. Idée générale de l'attaque

La différence entre deux éléments $x$ et $x^{*}$ de $\mathbb{F}_{2}^{n}$ est définie par $x-x^{*}$ mais comme chaque élément de $\mathbb{F}_{2}^{n}$ est son propre opposé, elle s'écrit plus simplement $x+x^{*}$. La propriété principale utilisée dans la cryptanalyse différentielle est que pour toute clé de ronde $k$, on a

$$
\begin{equation*}
(x+k)+\left(x^{*}+k\right)=x+x^{*} . \tag{B.1}
\end{equation*}
$$

Autrement dit, la différence entre $x$ et $x^{*}$ est invariante sous l'ajout de la clé.
Une cryptanalyse différentielle efficace repose sur l'existence d'une différentielle de probabilité élevée, que nous définissons maintenant. Soit $f$ une application de $\mathbb{F}_{2}^{n}$ vers $\mathbb{F}_{2}^{n}$. Une différentielle relativement à $f$ est une paire $(a, b)$ d'éléments de $\mathbb{F}_{2}^{n}$. Étant donnée une différentielle ( $a, b$ ), les éléments $a$ et $b$ sont respectivement appelés motifs de différence d'entrée et de sortie. Ensuite, une différentielle ( $a, b$ ) prédit que
lorsque la différence entre deux entrées $x$ et $x^{*}$ vaut $a$, la différence entre leurs images $f(x)$ et $f\left(x^{*}\right)$ sera égale à $b$ avec une certaine probabilité. Clairement, la différence entre $x$ et $x^{*}$ vaut $a$ si et seulement si $x^{*}=x+a$. Aussi, une différentielle ( $a, b$ ) prédit que lorsque $x$ est uniformément distribué sur $\mathbb{F}_{2}^{n}$, la quantité $f(x)+f(x+a)$ sera égale à $b$ avec la probabilité définie comme suit.

Définition B. 7 (probabilité d'une différentielle). Soit $f: \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ une application. La probabilité de la différentielle $(a, b)$ relativement à $f$ est notée $\mathrm{DP}_{f}(a, b)$ et définie par

$$
\mathrm{DP}_{f}(a, b)=\frac{\#\left\{x \in \mathbb{F}_{2}^{n} \mid f(x)+f(x+a)=b\right\}}{2^{n}} .
$$

L'idée générale de l'attaque est la suivante. Supposons que $(a, b)$ est une différentielle sur $(r-1)$ rondes de probabilité $q$ pour une proportion significative des clés de chiffrement. Soit $K$ une clé de chiffrement inconnue de l'attaquant. Premièrement, on génère des paires de messages clairs de la forme $(p, p+a)$ et on récupère leur chiffré. Afin d'obtenir quelques paires chiffrées $\left(c, c^{*}\right)$ vérifiant $c+c^{*}=b$, il faut chiffrer aux alentours de $C \times q^{-1}$ paires de clairs avec $C \geq 5$. On suppose que $k$ est un candidat pour la dernière clé de ronde $k^{[r]}$. On déchiffre alors la dernière ronde pour chacune des paires $\left(c, c^{*}\right)$ avec le candidat $k$ puis on note

$$
y=\sigma^{-1}(c+k) \quad \text { et } \quad y^{*}=\sigma^{-1}\left(c^{*}+k\right) .
$$

Si la clé candidate $k$ est correcte, alors l'équation $y+y^{*}=b$ doit être satisfaite avec probabilité $q$ puisque $(a, b)$ est une différentielle sur $(r-1)$ rondes. Autrement, quand $k$ est un mauvais choix, on espère que l'équation $y+y^{*}=b$ soit vérifiée avec une probabilité significativement inférieure à $q$. Cette hypothèse est connue sous le nom d'hypothèse de randomisation par clé incorrecte [51].

De l'information peut alors être récupérée sur la dernière clé de ronde. Pour chaque candidat $k$, on déchiffre la dernière ronde de chaque paire $\left(c, c^{*}\right)$ puis on sauvegarde le nombre $N_{k}$ de paires $\left(y, y^{*}\right)$ vérifiant $y+y^{*}=b$. La clé $k$ maximisant le compteur $N_{k}$ a de forte chance d'être égale à la dernière clé de ronde $k^{[r]}$. En pratique, on déchiffre seulement partiellement la dernière ronde et l'on recouvre alors quelques bits de la dernière clé.

## B.1.2.b. Pistes différentielles

Maintenant que nous avons expliqué comment exploiter une différentielle de probabilité élevée dans une cryptanalyse, nous détaillons la théorie des différentielles. Nous considérons donc un SPN générique $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ sur $r$ rondes tel que pour toute clé de chiffrement $K$,

$$
E_{K}=F_{k}[r-1] \circ \cdots \circ F_{k}[0] \quad \text { avec } \quad F_{k[i]}=\pi \circ \sigma \circ \alpha_{k[i]} .
$$

Notons que ce SPN doit être vu comme une version restreinte composée de moins de rondes que le chiffrement réellement attaqué.

## Appendice B - Résumé long en français

La méthode habituelle pour déterminer des différentielles efficaces repose sur la notion de piste différentielle.

Définition B. 8 (piste différentielle). Une piste différentielle sur $r$-rondes est une famille $\mathcal{T}=\left(a^{[0]}, \ldots, a^{[r]}\right)$ de $(r+1)$ motifs de différences dans $\mathbb{F}_{2}^{n m}$. Soit $K$ une clé de chiffrement. La probabilité différentielle à clé fixée de $\mathcal{T}$ est définie par

$$
\mathrm{DP}_{E_{K}}(\mathcal{T})=\frac{\#\left\{x \in \mathbb{F}_{2}^{n m} \mid \forall 1 \leq i \leq r, E_{K}^{(i)}(x)+E_{K}^{(i)}\left(x+a^{[0]}\right)=a^{[i]}\right\}}{2^{n m}}
$$

Soit ( $x, x^{*}$ ) une paire de messages clairs. On dit que la paire $\left(x, x^{*}\right)$ suit la piste différentielle $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ si

- la différence entre $x$ et $x^{*}$ vaut $a^{[0]}$, et
- pour tout $1 \leq i \leq r$, la différence entre les chiffrés sur $i$ rondes de $x$ et $x^{*}$ vaut $a^{[i]}$.
Ainsi, la piste $\mathcal{T}$ prédit l'évolution d'une différence d'entrée au travers des différentes rondes du chiffrement alors qu'une différentielle prédit seulement sa différence de sortie. Ces deux concepts sont réunis dans la proposition suivante.

Proposition B.9. Soit ( $a, b$ ) une différentielle sur $r$ rondes et soit $K$ une clé de chiffrement. En notant $E_{a, b}$ l'ensemble des pistes $\left(a^{[i]}\right)_{i \leq r}$ vérifiant $a^{[0]}=a$ et $a^{[r]}=b$, on a

$$
\operatorname{DP}_{E_{K}}(a, b)=\sum_{\mathcal{T} \in E_{a, b}} \operatorname{DP}_{E_{K}}(\mathcal{T})
$$

Pour l'instant, nous avons seulement considéré les probabilités à clé fixée. Ces résultats peuvent cependant ne pas refléter l'efficacité moyenne d'une attaque réelle. Pour cela, nous introduisons la définition suivante.

Définition B. $10(\mathrm{DP}(\mathcal{T}))$. La probabilité différentielle moyenne d'une piste $\mathcal{T}$, notée $\operatorname{DP}(\mathcal{T})$, est sa probabilité différentielle à clé fixée moyenne lorsque les clés de rondes sont indépendantes et uniformément distribuées. Explicitement, on a

$$
\operatorname{DP}(\mathcal{T})=\frac{1}{\left(2^{n m}\right)^{r}} \times \sum_{K \in\left(\mathbb{F}_{2}^{n m}\right)^{r}} \operatorname{DP}_{E_{K}}(\mathcal{T})
$$

Théorème B.11. La probabilité d'une piste différentielle $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ est donnée par

$$
\operatorname{DP}(\mathcal{T})=\prod_{i=0}^{r-1} \mathrm{DP}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=\prod_{i=0}^{r-1} \prod_{j=0}^{m-1} \mathrm{DP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right)=\prod_{i, j \mid a_{j}{ }^{[i]} \neq 0} \operatorname{DP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right),
$$

où $b^{[i]}=\pi^{-1}\left(a^{[i+1]}\right)$ avec $i<r$.
Ce théorème est important en pratique puisqu'il permet de déterminer la probabilité différentielle d'une piste en multipliant quelques probabilités différentielles sur des S-boxes qui sont facilement calculables.

Définition B. 12 (EDP). La probabilité différentielle moyenne d'une différentielle $(a, b)$ sur $r$ rondes, notée $\operatorname{EDP}(a, b)$, est sa probabilité différentielle à clé fixée moyenne lorsque les clés de rondes sont indépendantes et uniformément distribuées.

Théorème B.13. Soit ( $a, b$ ) une différentielle sur $r$ rondes. En notant $E_{a, b}$ l'ensemble des pistes $\left(a^{[i]}\right)_{i \leq r}$ vérifiant $a^{[0]}=a$ et $a^{[r]}=b$, on a

$$
\operatorname{EDP}(a, b)=\sum_{\mathcal{T} \in E_{a, b}} \operatorname{DP}(\mathcal{T})
$$

La probabilité moyenne d'une différentielle est une valeur théorique qui reflète son efficacité. Cette note possède cependant deux inconvénients. Premièrement, l'ensemble $E_{a, b}$ croît généralement de manière exponentielle avec le nombre de rondes ce qui rend l'énumération complète des pistes le composant très difficile. Pour des SPN de taille réelle, il est donc presque impossible de calculer cette valeur. Elle peut cependant être approchée en utilisant plusieurs pistes différentielles de forte probabilité.

Deuxièmement, la probabilité moyenne d'une différentielle ne tient pas compte de l'effet de l'algorithme de cadencement des clés de rondes. Dans une cryptanalyse, on suppose tacitement que la probabilité à clé fixée d'une différentielle est proche de sa probabilité moyenne. Cette hypothèse est connue comme l'hypothèse d'équivalence stochastique 67].

## B.1.3. Cryptanalyse linéaire

Après la cryptanalyse différentielle, la cryptanalyse linéaire est l'attaque principale contre les chiffrements par blocs. Elle fut introduite par Matsui dans [74, 75] qui a proposé la première attaque capable de retrouver expérimentalement une clé du DES. Il s'agit d'une attaque à clairs connus, ce qui est un avantage comparé à la cryptanalyse différentielle.

## B.1.3.a. Idée générale de l'attaque

Une approximation linéaire de fort potentiel linéaire est la clé d'une cryptanalyse linéaire efficace. Commençons par définir ces deux concepts. Soit $f$ une application de $\mathbb{F}_{2}^{n}$ vers $\mathbb{F}_{2}^{n}$. Intuitivement, nous souhaitons approcher une combinaison linéaire des bits de sortie de $f$ par une combinaison linéaire de ses bits d'entrée. Nous voulons donc une relation de la forme

$$
\begin{equation*}
\langle a, x\rangle=\langle b, f(x)\rangle, \tag{B.2}
\end{equation*}
$$

où les vecteurs de $n$ bits $a$ et $b$ sont appelés les motifs de sélection de l'entrée et de la sortie de l'approximation. Aussi, une approximation linéaire de $f$ est simplement définie comme une paire $(a, b)$ d'éléments de $\mathbb{F}_{2}^{n}$. Une telle approximation est bien

## Appendice B - Résumé long en français

évidemment vérifiée avec une certaine probabilité, mais notons que si l'équation (B.2) n'est presque jamais satisfaite, l'équation

$$
\begin{equation*}
\langle a, x\rangle=\langle b, f(x)\rangle+1 \tag{B.3}
\end{equation*}
$$

est vérifiée avec une forte probabilité. Du point de vue de l'attaque, les équations (B.2) et (B.3) apportent la même quantité d'information. Le pire cas se produit lorsque l'équation (B.2) est satisfaite pour exactement la moitié des entrées $x$. Dans ce cas, le membre gauche n'apporte aucune information sur le droit. L'efficacité d'une approximation est alors caractérisée par sa corrélation, ou son potentiel.

Définition B. 14 (corrélation et potentiel linéaire). Soient $f: \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ une application et $(a, b)$ une approximation de $f$. La corrélation de $(a, b)$ est définie par

$$
\mathrm{C}_{f}(a, b)=2 \cdot \frac{\#\left\{x \in \mathbb{F}_{2}^{n} \mid\langle a, x\rangle=\langle b, f(x)\rangle\right\}}{2^{n}}-1
$$

Son potentiel linéaire LP est alors le carré de sa corrélation, c'est-à-dire

$$
\mathrm{LP}_{f}(a, b)=\mathrm{C}_{f}(a, b)^{2}
$$

Remarque B.15. La corrélation d'une approximation est comprise entre -1 et 1 . Son potentiel linéaire va donc de 0 à 1 . Plus la corrélation absolue (ou le potentiel linéaire) d'une approximation est proche de 1, plus l'approximation donne de l'information sur $f$.

Comme pour la cryptanalyse différentielle, nous considérons un SPN $E: \mathbb{F}_{2}^{\kappa} \times$ $\mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ sur $r$ rondes en supposant que la dernière ronde ne possède pas de couche de diffusion, ainsi

$$
E_{K}=\left(\alpha_{k[r]} \circ \sigma \circ \alpha_{k[r-1]}\right) \circ E_{K}^{(r-1)}
$$

Une cryptanalyse linéaire classique de $E$ repose sur une approximation ( $a, b$ ) de $E_{K}{ }^{(r-1)}$ ayant un fort potentiel linéaire pour la majorité des clés de chiffrement $K$. Soit $K$ une clé de chiffrement. Remarquons que

$$
\begin{aligned}
\langle a, x\rangle & =\left\langle b, E_{K}^{(r-1)}(x)+k^{[r-1]}\right\rangle \\
\Longleftrightarrow \quad\langle a, x\rangle & =\left\langle b, E_{K}^{(r-1)}(x)\right\rangle+\left\langle b, k^{[r-1]}\right\rangle .
\end{aligned}
$$

Puisque $\left\langle b, k^{[r-1]}\right\rangle$ ne dépend pas de $x$, la corrélation de l'approximation $(a, b)$ de $\alpha_{k[r-1]} \circ E_{K}^{(r-1)}$ est égale à celle de la même approximation de $E_{K}^{(r-1)}$ au signe près. Par conséquent

$$
\begin{align*}
\mathrm{C}_{R^{\prime}}(a, b) & = \pm \mathrm{C}_{R}(a, b)  \tag{B.4}\\
\operatorname{LP}_{R^{\prime}}(a, b) & =\operatorname{LP}_{R}(a, b)
\end{align*} \quad \text { avec } \quad\left\{\begin{array}{l}
R=E_{K}^{(r-1)} \\
R^{\prime}=\alpha_{k}^{[r-1]} \circ E_{K}^{(r-1)}
\end{array}\right.
$$

Notons $q$ le potentiel moyen de l'approximation $(a, b)$ des $(r-1)$ premières rondes. Pour que la cryptanalyse soit efficace, il faut environ $N=C \times q^{-1}$ couples de clairs/chiffrés $(p, c)$. On peut alors récupérer de l'information sur la dernière clé de
ronde de la manière suivante. Pour chaque clé candidate $k$ pour $k^{[r]}$, on calcule la valeur

$$
P_{k}=\left(2 \times \#\left\{(p, c) \mid\langle a, p\rangle=\left\langle b, \sigma^{-1}(c+k)\right\rangle\right\}-N\right)^{2} .
$$

La clé $k$ maximisant la valeur $P_{k}$ est alors probablement la dernière clé de ronde $k^{[r]}$. À nouveau, l'hypothèse que pour toute clé incorrecte $k$, la valeur $P_{k}$ est inférieure à $P_{k[r]}$ est appelée hypothèse de randomisation par clé incorrecte [51].

## B.1.3.b. Approximations et pistes linéaires

Cette section est consacrée à la théorie des approximations linéaires proposée par Daemen et Rijmen [39, 40]. Par analogie avec les pistes différentielles, nous introduisons le concept de piste linéaire. Même si l'application des pistes linéaires semble similaire à celle des pistes différentielles, ces deux concepts sont très différents par nature.

Définition B. 16 (piste linéaire). Une piste linéaire sur $r$ rondes est une famille $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ de $r+1$ motifs de sélection. La contribution de corrélation de $\mathcal{T}$ est définie par

$$
\mathrm{C}(\mathcal{T})=\prod_{i=0}^{r-1} \mathrm{C}_{\pi \sigma}\left(a^{[i]}, a^{[i+1]}\right)
$$

Lorsque l'on considère la corrélation à clé fixée d'une approximation sur rondes ou la moyenne de ces corrélations, la contribution de corrélation d'une piste linéaire n'est simplement qu'une variable intermédiaire. À l'inverse d'une piste différentielle, une piste linéaire ne possède pas d'interprétation concrète. En effet, une paire peut suivre une piste différentielle, mais dire que des messages suivent une piste linéaire n'a aucun sens. Une approximation ne considère par les messages séparément mais plutôt la fonction de chiffrement dans son ensemble.

Proposition B.17. Soit $\mathcal{T}=\left(a^{[i]}\right)_{i \leq r}$ une piste linéaire de corrélation non nulle. En notant $b^{[i]}$ l'élément $\pi^{\top}\left(a^{[i+1]}\right)$ pour tout entier naturel $i<r$, on a

$$
\mathrm{C}(\mathcal{T})=\prod_{i, j \mid a_{j}{ }^{[i]} \neq 0} \mathrm{C}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right) \quad \text { et } \quad \operatorname{LP}(\mathcal{T})=\prod_{i, j \mid a_{j}{ }^{[i]} \neq 0} \operatorname{LP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right)
$$

Présentons maintenant un résultat reliant les pistes linéaires aux approximations. La proposition suivante doit être vue comme l'homologue de la proposition B. 9 pour la cryptanalyse linéaire.

Proposition B.18. Soit $(a, b)$ une approximation linéaire sur $r$ rondes et soit $K$ une clé de chiffrement. Notons $E_{a, b}$ l'ensemble des pistes linéaires $\left(a^{[i]}\right)_{i \leq r}$ vérifiant $a^{[0]}=a, a^{[r]}=b$. Étant donnée une piste $\mathcal{T}$ dans $E_{a, b}$, on note $\langle\mathcal{T}, K\rangle$ l'élément $\sum_{i=0}^{r}\left\langle a^{[i]}, k^{[i]}\right\rangle$ de $\mathbb{F}_{2}$. La corrélation à clé fixée de $(a, b)$ est alors donnée par

$$
\mathrm{C}_{E_{K}}(a, b)=\sum_{\mathcal{T} \in E_{a, b}}(-1)^{\langle\mathcal{T}, K\rangle} \mathrm{C}(\mathcal{T})
$$

## Appendice B - Résumé long en français

Contrairement à la probabilité différentielle, la corrélation d'une approximation est une somme signée des contributions de corrélation de ses pistes associées. Quand plusieurs pistes de grandes corrélations absolues sont ajoutées avec le même signe, l'amplitude de la corrélation globale s'accroît. On parle dans ce cas d'interférence constructive. Autrement, quand ces pistes ont des signes différents, la corrélation globale peut s'approcher de zéro et on parle d'interférence destructive.

Définition B. 19 (ELP). Le potentiel linéaire moyen d'une approximation ( $a, b$ ) sur $r$ rondes, noté $\operatorname{ELP}(a, b)$, est le potentiel linéaire à clé fixée moyen lorsque les clés de rondes sont indépendantes et uniformément distribuées.

Théorème B.20. Soit ( $a, b$ ) une approximation linéaire sur $r$ rondes. En notant $E_{a, b}$ l'ensemble des pistes $\left(a^{[i]}\right)_{i \leq r}$ vérifiant $a^{[0]}=a$ et $a^{[r]}=b$, on a

$$
\operatorname{ELP}(a, b)=\sum_{\mathcal{T} \in E_{a, b}} \operatorname{LP}(\mathcal{T})
$$

Cette fois, la somme ne contient que des terme positifs donc il n'y a plus d'interférences destructives. Le potentiel linéaire moyen constitue un puissant indicateur de la résistance d'un chiffrement à la cryptanalyse linéaire. Néanmoins, nous devons garder à l'esprit que la corrélation réelle est fortement dépendante de la clé utilisée, comme le précise la proposition B.18. Enfin, le potentiel linéaire moyen possède les mêmes inconvénients que la probabilité différentielle moyenne. Cette valeur est pratiquement impossible à calculer précisément et on doit admettre l'hypothèse d'équivalence stochastique [51] pour l'assimiler à la résistance réelle d'un chiffrement.

## B.2. Évaluation de la sécurité des SPN

Les cryptanalyses différentielle [13] et linéaire [74] sont considérées comme les deux attaques principales contre les chiffrements par blocs [64]. Comme il est mentionné dans [41], tout nouveau système de chiffrement devrait au moins être accompagné d'une analyse détaillée prouvant sa résistance à ces deux attaques. Nous avons vu dans le chapitre précédent que la sécurité d'un système de chiffrement est évaluée par sa probabilité différentielle moyenne maximale ( maximum expected differential probability ou MEDP) ou son potentiel linéaire moyen maximal (MELP). Quand ces valeurs sont suffisamment basses, le chiffrement est sécurisé [57]. Cependant, calculer ces valeurs, voir simplement les majorer efficacement demeure un problème ouvert et les preuves classiques de sécurité se concentrent uniquement sur les pistes différentielles et linéaires. Un chiffrement est alors dit sécurisé en pratique lorsque la probabilité différentielle (ou le potentiel linéaire) de toutes les pistes est trop faible pour permettre une cryptanalyse efficace. Enfin, il convient de souligner que ces mesures de sécurité supposent implicitement que les clés de rondes soient choisies indépendamment et de manière uniforme. Le cryptanaliste suppose ensuite que ces mesures théoriques reflètent la sécurité réelle lorsque les clés de rondes sont extraites d'une clé maitresse fixée via un cadenceur de clés. Cette hypothèse, dite d'équivalence
stochastique [67], semble être vérifiée pour presque tous les chiffrements utilisés en pratique.

Pour se prémunir des cryptanalyses différentielle et linéaire, le concepteur d'un SPN doit tout d'abord choisir des S-boxes ayant une grande résistance contres ces deux attaques. Ces choix conditionnent la couche de substitution de chiffrement. Concernant la couche de diffusion linéaire, deux grandes familles se distinguent. D'une part, la diffusion du chiffrement peut être assurée pour une permutation des bits. Même si ces applications linéaires ne fournissent pas la meilleure sécurité, elles sont généralement choisies pour leur efficacité calculatoire. En effet, durant les dernière années, plusieurs chiffrements à bas coûts utilisant des permutations de bits ont été proposés [17, 36, 95]. Une liste récente détaillée peut être trouvée dans [15]. D'autre part, la diffusion peut reposer sur une application linéaire plus compliquée comme un produit matriciel sur un corps fini par exemple. De telles applications sont généralement plus coûteuses en calculs mais délivrent en contrepartie une grande diffusion qui assure que toutes les pistes activent un nombre minimal de S-boxes. En s'appuyant sur cette propriété, le concepteur peut calculer des bornes sur la probabilité différentielle maximale ou sur le potentiel linéaire maximal de n'importe quelle piste et prouve ainsi la sécurité pratique de son chiffrement.

Cependant, les bornes obtenues pour un SPN ayant une permutation des bits comme diffusion linéaire ne suffisent généralement pas pour démontrer sa sécurité. En effet, les permutations de bits ont le plus petit nombre de branches possible parmi toutes les permutations linéaires. La sécurité du chiffrement est alors difficile à établir sans une analyse détaillée. La même observation devrait s'appliquer aux chiffrements à trappes puisque la structure mathématique de la trappe réduit sévèrement le choix des primitives sur chiffrement. Aussi, les stratégies habituelles pour prévenir les cryptanalyses différentielle et linéaire peuvent ne plus s'appliquer. Cette discussion motive des méthodes alternatives pour démontrer la sécurité d'un chiffrement face à ces attaques.

Dans ce chapitre, nous présentons un algorithme entièrement automatique calculant une piste différentielle ou linéaire optimale dans un SPN. Cette contribution a été présentée dans [8]. Le premier algorithme calculant des pistes optimales fut introduit par Matsui dans [76] pour les chiffrements de Feistel. En l'exécutant plusieurs fois sur le DES, Matsui trouva une permutation des S-boxes rendant le DES plus résistant aux cryptanalyses différentielle et linéaire. Cependant, la complexité de l'algorithme étant trop élevée pour l'appliquer au chiffrement FEAL, deux améliorations successives furent proposées dans [87] puis [3]. Bien que l'algorithme de Matsui s'adapte aux SPN, la taille des blocs des chiffrements modernes (de 64 à 128 bits) le rend impraticable. Ce fait a également été mis en évidence par Collard et al. [37] qui ont alors présenté quelques améliorations pour l'appliquer au chiffrement Serpent. Pour finir, mentionnons qu'une autre variation fut proposée par Ali et Heys dans [1]. Leur algorithme ne peut cependant pas démontrer la sécurité pratique d'un chiffrement puisqu'il ne trouve pas nécessairement une piste optimale.

Notre algorithme est une adaptation de [3, 76, 87] pour les SPN. Nous introduisons plusieurs optimisations en portant une attention particulière aux chiffrements dont la diffusion linéaire est réalisée au moyen d'une permutation des bits.

## Appendice B - Résumé long en français

Après un rappel sur les cryptanalyse différentielle et linéaire, nous présenterons une adaptation directe de l'algorithme de Matsui pour calculer une piste optimale dans un réseau de substitutions-permutations. Nos différentes optimisations algorithmiques seront présentées dans la section B.2.2. Enfin, nous présenterons nos résultats et conclurons dans la section B.2.3.

## B.2.1. Recherche d'une piste optimale

## B.2.1.a. Rappels et définitions

Dans cette section, nous considérons un réseau de substitutions-permutations générique $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$ sur $r$ rondes défini pour toute clé de chiffrement $K$ par

$$
E_{K}=F_{k[r-1]} \circ \cdots \circ F_{k[0]} \quad \text { avec } \quad F_{k[i]}=\pi \circ \sigma \circ \alpha_{k[i]} .
$$

Notons que la dernière ronde comprend la couche de diffusion $\pi$ puisque les différentielles et les approximations linéaires utilisées dans une cryptanalyse s'applique sur un nombre de rondes inférieur à celui du chiffrement complet. Notons $S_{0}, \ldots, S_{m-1}$ les S-boxes sur $n$ bits de la couche de substitution. Rappelons que les matrices des probabilités différentielles et des potentiels linéaires d'une S-box $S$ sont respectivement définies pour tous $a$ et $b$ dans $\mathbb{F}_{2}^{n}$ par

$$
\begin{aligned}
\operatorname{DP}_{S}(a, b) & =2^{-n} \times \#\left\{x \in \mathbb{F}_{2}^{n} \mid S(x)+S(x+a)=b\right\} \\
\operatorname{LP}_{S}(a, b) & =\left(2^{-(n-1)} \times \#\left\{x \in \mathbb{F}_{2}^{n} \mid\langle a, x\rangle=\langle b, S(x)\rangle\right\}-1\right)^{2}
\end{aligned}
$$

La probabilité différentielle maximale et le potentiel linéaire maximal de $S$ sont alors définis par

$$
\operatorname{DP}_{S}^{\max }=\max \left\{\operatorname{DP}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}, \quad \operatorname{LP}_{S}^{\max }=\max \left\{\operatorname{LP}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}
$$

D'après les définitions B. 8 et B.16, une piste différentielle ou linéaire sur $r$ rondes est une famille $\left(a^{[0]}\right)_{i \leq r}$ de $r+1$ motifs dans $\mathbb{F}_{2}^{n m}$. Dans ce chapitre, il convient de spécifier pour chaque ronde les motifs en entrée et en sortie de la couche de substitution. Aussi, nous pouvons définir de manière équivalente une piste différentielle ou linéaire $\mathcal{T}$ comme une famille $\left(\left(a^{[i]}, b^{[i]}\right)_{i<r}\right.$ de $r$ paires de motifs d'entrée et de sortie tels que pout tout $i<r-1$,

$$
a^{[i+1]}= \begin{cases}\pi\left(b^{[i]}\right) & \text { pour les pistes différentielles }, \\ \left(\pi^{\top}\right)^{-1}\left(b^{[i]}\right) & \text { pour les pistes linéaires }\end{cases}
$$

De plus, dans le cas où la diffusion est réalisée par une permutation des bits $\pi$, on peut montrer que $\left(\pi^{\top}\right)^{-1}=\pi$ donc la même structure peut aussi bien représenter une piste différentielle que linéaire. Enfin, la probabilité d'une piste différentielle et le potentiel d'une piste linéaire $\mathcal{T}$ sont respectivement donnés par

$$
\begin{aligned}
& \operatorname{DP}(\mathcal{T})=\prod_{i=0}^{r-1} \operatorname{DP}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=\prod_{i, j \mid a_{j}[i] \neq 0} \operatorname{DP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}{ }^{[i]}\right), \\
& \operatorname{LP}(\mathcal{T})=\prod_{i=0}^{r-1} \operatorname{LP}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=\prod_{i, j \mid a_{j}[i] \neq 0} \operatorname{LP}_{S_{j}}\left(a_{j}{ }^{[i]}, b_{j}^{[i]}\right),
\end{aligned}
$$

comme établi dans le théorème B. 11 et la proposition B.17. Autrement dit, la probabilité différentielle d'une piste s'obtient en multipliant les probabilités différentielles de ses S-boxes actives.

Définition B. 21 (Piste optimale). Toute piste différentielle sur $r$ rondes de probabilité maximale parmi l'ensemble des pistes sur $r$ rondes est dite optimale. On définit de manière analogue une piste linéaire optimale. Dans ce cas, sa probabilité (ou potentiel) est notée $p_{o}^{(r)}$.

Dans le contexte de notre algorithme de recherche, un candidat pour un motif d'entrée $a$ dans $\mathbb{F}_{2}^{n m}$ est un motif de sortie $b$ tel que $\operatorname{DP}_{\sigma}(a, b)$ est non nul. Naturellement, si l'on recherche une piste linéaire optimale, cette condition devient $\operatorname{LP}_{\sigma}(a, b) \neq 0$. Si $\mathcal{T}=\left(\left(a^{[i]}, b^{[i]}\right)\right)_{i<r}$ est une piste sur $r$ rondes, on note $\mathcal{T}^{[i, j]}$ la piste extraite $\left(\left(a^{[k]}, b^{[k]}\right)\right)_{i \leq k \leq j}$. Pour terminer, on introduit la définition suivante.

Définition B. 22 (prolongement d'une piste). Soient $r_{1}$ et $r_{2}$ deux entiers tels que $0 \leq r_{1} \leq r_{2}$. Soient $\mathcal{T}_{1}$ et $\mathcal{T}_{2}$ deux pistes sur $r_{1}$ et $r_{2}$ rondes respectivement. On dit que la piste $\mathcal{T}_{2}$ prolonge $\mathcal{T}_{1}$ si $\mathcal{T}_{2}{ }^{[0, r-1]}=\mathcal{T}$. Dans ce cas, $\mathcal{T}_{2}=\mathcal{T}_{1} \| \mathcal{T}_{2}^{\left[r, r^{\prime}-1\right]}$.

## B.2.1.b. Principe général

Présentons maintenant une adaptation directe de l'algorithme de Matsui pour les réseaux de substitutions-permutations (SPN). Premièrement, nous expliquerons comment cet algorithme calcule une piste différentielle optimale. Nous détaillerons ensuite les changements à effectuer pour calculer une piste linéaire optimale.

Notons $R$ le nombre réel de rondes du SPN. L'algorithme présenté dans ce chapitre calcule une piste optimale sur $R$ rondes tout en ne nécessitant aucune connaissance sur le chiffrement. Il est construit à partir d'un second algorithme appelé OptTrailEst prenant les arguments suivants :

- un entier $r \geq 2$ représentant le nombre courant de rondes;
- les probabilités $\left(p_{o}^{(i)}\right)_{1 \leq i<r}$ des pistes optimales sur $i$ rondes;
- une estimation $p_{\mathrm{e}}^{(r)}$ de la probabilité $p_{\mathrm{o}}^{(r)}$ de la piste optimale recherchée.

Il renvoie une piste optimale sur $r$ rondes notée $\mathcal{T}_{o}^{(r)}$. La connaissance des probabilités $\left(p_{o}^{(i)}\right)_{1 \leq i<r}$ et de l'estimation $p_{\mathrm{e}}^{(r)}$ accélère la recherche. Ensuite, une gestion automatique de l'estimation $p_{e}^{(r)}$ sera proposée dans la section B.2.2.e, donnant lieu à l'algorithme OptTrail. Pour résumer, l'algorithme de recherche OptTrail prend seulement $r$ et $\left(p_{o}^{(i)}\right)_{1 \leq i<r}$ en entrées et produit toujours une piste optimale sur $r$ rondes.

Expliquons maintenant comment l'algorithme OptTrail peut être utilisé pour calculer une piste optimale sur $R$ rondes à partir de rien. Premièrement, observons que $p_{\mathrm{o}}^{(1)}$ se calcule facilement. Ensuite, on calcule

$$
\mathcal{T}_{\mathrm{o}}^{(r)}=\operatorname{OptTrail}\left(r,\left(p_{\mathrm{o}}^{(i)}\right)_{1 \leq i<r}\right) \quad \text { et } \quad p_{\mathrm{o}}^{(r)}=\mathrm{DP}\left(\mathcal{T}_{\mathrm{o}}^{(r)}\right)
$$

pour $r$ allant de 2 à $R$. Ce dernier calcul donne le résultat souhaité. Cette procédure est illustrée dans la figure B.2.

## Appendice B - Résumé long en français



Entrée. Le nombre $R$ de rondes du chiffrement.
Sortie. Une piste optimale $\mathcal{T}_{o}^{(R)}$ sur $R$ rondes.

```
\(p_{o}^{(1)} \leftarrow \max \left\{\operatorname{DP}_{\sigma}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n}\right)^{m}\right\}\)
    Pour \(r\) allant de 2 à \(R\) faire
        \(\mathcal{T}_{\mathrm{o}}^{(r)} \leftarrow \operatorname{OptTrail}\left(r,\left(p_{\mathrm{o}}^{(i)}\right)_{1 \leq i<r}\right)\)
        \(p_{\mathrm{o}}^{(r)} \leftarrow \operatorname{DP}\left(\mathcal{T}_{o}{ }^{(r)}\right)\)
    Renvoyer \(\mathcal{T}_{\mathrm{o}}{ }^{(R)}\)
```

Figure B. 2 : Utilisation de l'algorithme OptTrail.

Le reste de cette section est dédié à l'algorithme OptTrailEst donné dans la figure B.3. Expliquons maintenant son fonctionnement. Premièrement, on suppose que les conditions présentes aux lignes 9 et 18 sont toujours vraies et que l'estimation $p_{\mathrm{e}}^{(r)}$ est nulle. Sous cette hypothèse, l'algorithme parcourt implicitement les arbres de toutes les pistes sur $r$ rondes et en sauvegarde une de probabilité maximale dans la variable $\mathcal{T}_{\mathrm{o}}{ }^{(r)}$. Observons tout de même que la première et la dernière rondes ont un traitement particulier pour accélérer la recherche. Quand le programme atteint la fonction Round ( $s, \mathcal{T}^{(s-1)}, p^{(s-1)}$ ), la piste courante est

$$
\begin{aligned}
& \mathcal{T}^{(s-1)}=\left(\left(a^{[0]}, b^{[0]}\right), \ldots,\left(a^{[s-2]}, b^{[s-2]}\right)\right), \\
& \operatorname{DP}\left(\mathcal{T}^{(s-1)}\right)=\prod_{i=0}^{s-2} \operatorname{DP}_{\sigma}\left(a^{[i]}, b^{[i]}\right)=p^{(s-1)} .
\end{aligned}
$$

Le motif d'entrée $a^{[s-1]}$ pour cette ronde est égal à $\pi\left(b^{[s-2]}\right)$. Ensuite, pour chaque candidat $b^{[s-1]}$ pour $a^{[s-1]}$, la piste courante $\mathcal{T}^{(s-1)}$ est prolongée par ( $a^{[s-1]}, b^{[s-1]}$ ) et la procédure de recherche pour la ronde suivante est appelée. Par conséquent, le programme effectue un parcours en profondeur. Quand l'algorithme atteint la fonction LastRound(), il est simple de calculer le motif de sortie $b^{[r-1]}$ maximisant la probabilité de la dernière ronde. La piste est sauvegardée uniquement si sa probabilité est supérieure à la probabilité $p_{\mathrm{e}}^{(r)}$ de la meilleure piste $\mathcal{T}_{\mathrm{o}}^{(r)}$ trouvée à cet instant. Il reste donc à expliquer les conditions aux lignes 9 et 18 .

```
Algorithme 10 - OptTrailEst(r, ( }\mp@subsup{p}{0}{(i)}\mp@subsup{)}{1\leqi<r,}{},\mp@subsup{p}{\textrm{e}}{(r)}
```

Entrée. Le nombre de rondes courant $r$ (avec $r \geq 2$ ), les probabilités $\left(p_{\mathrm{o}}^{(i)}\right)_{1 \leq i<r}$ et une estimation $p_{\mathrm{e}}^{(r)}$ de $p_{\mathrm{o}}^{(r)}$
Sortie. Suivant l'estimation $p_{\mathrm{e}}^{(r)}$, cet algorithme renvoie :

- une piste sur $r$ rondes optimale $\mathcal{T}_{\mathrm{o}}{ }^{(r)}$ si $p_{\mathrm{e}}^{(r)} \leq p_{\mathrm{o}}{ }^{(r)}$;
- une piste vide si $p_{\mathrm{e}}^{(r)}>p_{\mathrm{o}}^{(r)}$.

```
\(\mathcal{T}_{\mathrm{o}}{ }^{(r)} \leftarrow()\)
Pour chaque motif de sortie \(b^{[0]}\) non nul faire
    Appeler FirstRound \(\left(b^{[0]}\right)\)
Renvoyer \(\mathcal{T}_{\mathrm{o}}{ }^{(r)}\)
Fonction FirstRound( \(\left.b^{[0]}\right)\)
    \(a^{[0]} \leftarrow \arg \max \left\{\mathrm{DP}_{\sigma}\left(a, b^{[0]}\right) \mid a \in \mathbb{F}_{2}^{n m}\right\}\)
    \(\mathcal{T}^{(1)} \leftarrow\left(\left(a^{[0]}, b^{[0]}\right)\right)\)
    \(p^{(1)} \leftarrow \operatorname{DP}_{\sigma}\left(a^{[0]}, b^{[0]}\right)\)
    Si \(p^{(1)}\) n'est pas inférieur à la borne de rang un alors
        Si \(r>2\) alors
            Appeler Round \(\left(2, \mathcal{T}^{(1)}, p^{(1)}\right)\)
        Sinon
            Appeler LastRound \(\left(\mathcal{T}^{(1)}, p^{(1)}\right)\)
Fonction Round \(\left(s, \mathcal{T}^{(s-1)}, p^{(s-1)}\right)\)
    \(a^{[s-1]} \leftarrow \pi\left(b^{[s-2]}\right)\)
    Pour chaque candidat \(b^{[s-1]}\) pour \(a^{[s-1]}\) faire
        \(p^{(s)} \leftarrow p^{(s-1)} \times \operatorname{DP}_{\sigma}\left(a^{[s-1]}, b^{[s-1]}\right)\)
        Si \(p^{(s)}\) n'est pas inférieur à la borne de rang \(s\) alors
            \(\mathcal{T}^{(s)} \leftarrow \mathcal{T}^{(s-1)} \|\left(a^{[s-1]}, b^{[s-1]}\right)\)
            Si \(s+1<r\) alors
                Appeler \(\operatorname{Round}\left(s+1, \mathcal{T}^{(s)}, p^{(s)}\right)\)
                Sinon
                Appeler LastRound \(\left(\mathcal{T}^{(s)}, p^{(s)}\right)\)
Fonction LastRound \(\left(\mathcal{T}^{(r-1)}, p^{(r-1)}\right)\)
    \(a^{[r-1]} \leftarrow \pi\left(b^{[r-2]}\right)\)
    \(b^{[r-1]} \leftarrow \arg \max \left\{\mathrm{DP}_{\sigma}\left(a^{[r-1]}, b\right) \mid b \in \mathbb{F}_{2}^{n m}\right\}\)
    \(p^{(r)} \leftarrow p^{(r-1)} \times \mathrm{DP}_{\sigma}\left(a^{[r-1]}, b^{[r-1]}\right)\)
    Si \(p^{(r)} \geq p_{\mathrm{e}}^{(r)}\) alors
        \(\mathcal{T}^{(r)} \leftarrow \mathcal{T}^{(r-1)} \|\left(a^{[r-1]}, b^{[r-1]}\right)\)
```



```
        \(p_{\mathrm{e}}^{(r)} \leftarrow p^{(r)}\)
```

Figure B. 3 : L'algorithme OptTrailEst.

Définition B. 23 (borne de rang $s$ ). Soit $\mathcal{T}$ une piste sur $s$ rondes avec $1 \leq s<r$. Sa probabilité est dite inférieure à la borne de rang s si

$$
\operatorname{DP}(\mathcal{T})<\frac{p_{\mathrm{e}}^{(r)}}{p_{\mathrm{o}}^{(r-s)}}
$$

Cette condition sur la probabilité de la piste courante permet d'élaguer l'arbre de recherche sans manquer de pistes optimales. Elle peut se réécrire en

$$
\operatorname{DP}(\mathcal{T}) \times p_{\mathrm{o}}^{(r-s)}<p_{\mathrm{e}}^{(r)}
$$

et elle signifie que même si la piste est prolongée par une piste optimale sur $(r-s)$ rondes, sa probabilité sera inférieure à $p_{\mathrm{e}}^{(r)}$.

L'importance de l'estimation $p_{\mathrm{e}}^{(r)}$ est maintenant claire. Si $p_{\mathrm{e}}^{(r)}>p_{\mathrm{o}}^{(r)}$, une piste prolongeable en une piste optimale sur $r$ rondes peut être coupée. De plus, aucune piste ne sera sauvegardée à cause de la condition à la ligne 25 . D'autre part, plus l'estimation $p_{\mathrm{e}}^{(r)}$ est proche de $p_{o}^{(r)}$, plus la condition d'élagage est efficace et donc plus la complexité de l'algorithme OptTrailEst est faible.

Théorème B.24. L'algorithme OptTrailEst peut calculer une piste linéaire optimale en remplaçant simplement toutes les occurrences de DP par LP et toutes les occurrences de $\pi(\ldots)$ par $\left(\pi^{\top}\right)^{-1}(\ldots)$.

## B.2.2. Optimisations

Remarquons tout d'abord que la première boucle de OptTrailEst appelle la fonction FirstRound pour chaque différence non nulle $b^{[0]}$. Puisqu'il y a $2^{n m}-1$ différences non nulles, on peut minorer la complexité de l'algorithme par $2^{64}$ ou $2^{128}$ pour des SPN de taille réelle. Aussi, cette partie doit être optimisée pour toute application pratique.

## B.2.2.a. Construction du premier motif de sortie

Comme nous venons de le souligner, le nombre d'appels à la fonction FirstRound() est un problème qu'il faut impérativement résoudre. Pour optimiser cette étape, une partition de l'ensemble des différences non nulles est introduite. Ensuite, nous donnerons une manière efficace de tester si aucune différence dans une partie peut être le début d'une piste optimale.

Pour chaque entier $w$ tel que $1 \leq w \leq m$, nous notons $\mathrm{DP}_{(w)}^{\max }$ la probabilité maximale d'une piste sur une ronde activant $w$ S-boxes. Autrement dit,

$$
\operatorname{DP}_{(w)}^{\max }=\max \left\{\operatorname{DP}_{\sigma}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n}\right)^{m} \text { tels que } \mathrm{w}_{n}(a)=w\right\},
$$

où $\mathrm{w}_{n}(a)$ désigne le poids par paquet de $a$. Ensuite, nous trions les probabilités $\mathrm{DP}_{S_{i}}^{\max }$ dans l'ordre décroissant. Cela revient à définir une permutation $\tau$ de $\llbracket 0, m \llbracket$ vérifiant pour tout $i<m-1$ l'inégalité

$$
\mathrm{DP}_{S_{\tau(i)}}^{\max } \geq \mathrm{DP}_{S_{\tau(i+1)}}^{\max }
$$

```
Algorithme 11 - OptTrailEst
    \mp@subsup{\mathcal{T}}{\textrm{o}}{(r)}}\mp@subsup{}{}{(r)
    Pour w allant de 1 à m faire
        Si DP (w)
        Quitter la boucle
        Sinon
        Pour chaque motif de sortie b [0] activant w S-boxes faire
            Appeler FirstRound(b[0])
Renvoyer }\mp@subsup{\mathcal{T}}{0}{(r)
```

Figure B. 4 : Première optimisation - construction de la première différence

Proposition B.25. Soit $w$ un entier tel que $1 \leq w \leq m$. Alors,

$$
\mathrm{DP}_{(w)}^{\max }=\prod_{i=0}^{w-1} \mathrm{DP}_{S_{\tau(i)}}^{\max }
$$

Remarque B.26. On a clairement $\mathrm{DP}_{(1)}^{\max } \geq \ldots \geq \mathrm{DP}_{(m)}^{\max }$. Aussi, la probabilité d'une piste optimale sur une ronde est donnée par

$$
p_{\mathrm{o}}^{(1)}=\max \left\{\mathrm{DP}_{\sigma}(a, b) \mid a, b \in\left(\mathbb{F}_{2}^{n m}\right)^{*}\right\}=\mathrm{DP}_{(1)}^{\max }=\mathrm{DP}_{S_{\tau(0)}}^{\max }
$$

Bien entendu, les matrices différentielles $\mathrm{DP}_{S_{i}}$ et les probabilités $\mathrm{DP}_{S_{i}}^{\max }$ et $\mathrm{DP}_{(i)}^{\max }$ sont pré-calculées avant d'initier la recherche.

Théorème B.27. Soient $w$ et $w^{\prime}$ deux entiers tels que $1 \leq w \leq w^{\prime} \leq m$. Si $\operatorname{DP}_{(w)}^{\max }$ est inférieur à la borne de rang un, alors il n'existe aucune piste sur $r$ rondes activant $w^{\prime} \mathrm{S}$-boxes dans la première ronde de probabilité supérieure ou égale à $p_{\mathrm{e}}^{(r)}$.

Nous avons exécuté l'algorithme final sur plusieurs SPN ayant une permutation des bits comme couche de diffusion. Avec $m=16$ et $n=4$, $\mathrm{DP}_{(4)}^{\max }$ était toujours inférieur à la borne de rang un, donc il y avait au plus $2^{21}$ différences de sortie à tester au lieu de $2^{64}$. Avec $m=16$ et $n=8$, l'écart était encore plus grand puisque $\mathrm{DP}_{(3)}^{\max }$ était toujours inférieur à la borne de rang un, donnant seulement $2^{21}$ différences à tester au lieu de $2^{128}$. L'algorithme optimisé à l'aide du théorème B. 27 est décrit dans la figure B. 4 .

## B.2.2.b. La fonction de ronde

En suivant l'algorithme de Matsui [76, les candidats de sortie dans la fonction Round sont construits récursivement. Notons $a$ la différence en entrée de la ronde courante. On sait que les candidats $b$ associés à $a$ peuvent être construits en choisissant un motif de sortie pour chaque S-box activée par $a$. Le théorème suivant établit que la condition d'élagage peut s'appliquer paquet par paquet.

## Appendice B - Résumé long en français

Théorème B.28. Soient $s$ un entier tel que $1 \leq s \leq r$ et $\mathcal{T}$ une piste sur $s$ rondes. Notons $x_{0}<\ldots<x_{w-1}$ les indices des S-boxes activées par $a^{[s-1]}$ où $w=\mathrm{w}_{n}\left(a^{[s-1]}\right)$. Soit $v$ un entier vérifiant $1 \leq v \leq w$. Si le produit

$$
\operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right)\left(\prod_{i=0}^{v-1} \mathrm{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \mathrm{DP}_{(w-v)}^{\max }
$$

est inférieur à la borne de rang $s$, alors pour tout motif $c$ vérifiant :

- $c_{x_{i}}=b_{x_{i}}{ }^{[s-1]}$ pour tout $i<v-1$ et
- $\mathrm{DP}_{S_{x_{v-1}}}\left(a_{x_{v-1}[s-1]}, c_{x_{v-1}}\right) \leq \mathrm{DP}_{S_{x_{v-1}}}\left(a_{x_{v-1}[s-1]}, b_{x_{v-1}[s-1]}\right)$
il n'existe aucune piste sur $r$ ronde prolongeant $\mathcal{T}^{[0, s-2]} \|\left(a^{[s-1]}, c\right)$ de probabilité supérieure ou égale à $p_{\mathrm{e}}^{(r)}$.


## B.2.2.c. Les S-Boxes actives à la ronde suivante

Supposons ici que la couche de diffusion $\pi$ est une permutation des bits. Notons $\mathrm{L}_{\text {ASB }}$ l'application de $\left(\mathbb{F}_{2}^{n}\right)^{m}$ vers $\mathbb{F}_{2}^{m}$ qui envoie un motif $c$ sur le vecteur de $m$ bits $\mathrm{L}_{\mathrm{ASB}}(c)=\left(x_{i}\right)_{i<m}$ où $x_{i}$ vaut un si et seulement si $c_{i}$ est non nul. En d'autres termes, $\mathrm{L}_{\mathrm{ASB}}(c)$ est une représentation compacte des S-boxes activées par le motif $c$ et $\mathrm{L}_{\mathrm{ASB}}$ se lit : liste des $S$-boxes actives.

Étant donnés deux éléments $L$ et $L^{\prime}$ de $\mathbb{F}_{2}^{m}$, on note $L \vee L^{\prime}$ leur $O U$ exclusif bit-à-bit. Soit $c$ un motif et $i<m$ un entier positif. On note $\left.c\right|_{i}$ l'élément de $\left(\mathbb{F}_{2}^{n}\right)^{m}$ ayant toutes ces composantes à zéro, exceptée celle d'indice $i$ valant $c-i$. Autrement dit,

$$
\left(x_{j}\right)_{j<m}=\left.c\right|_{i} \Longleftrightarrow \begin{cases}x_{i}=c_{i} & \text { et } \\ x_{j}=0_{n} & \text { if } j \neq i .\end{cases}
$$

Théorème B.29. On garde les notations du théorème B. 28 sauf que $s<r-1$. Soit $w^{\prime}$ le poids de Hamming de $\bigvee_{i=0}^{v-1} \mathrm{~L}_{\mathrm{ASB}}\left(\pi\left(\left.b^{[s-1]}\right|_{x_{i}}\right)\right)$. Si le produit

$$
\left[\operatorname{DP}\left(\mathcal{T}^{[0, s-2]}\right)\left(\prod_{i=0}^{v-1} \operatorname{DP}_{S_{x_{i}}}\left(a_{x_{i}}^{[s-1]}, b_{x_{i}}^{[s-1]}\right)\right) \times \mathrm{DP}_{(w-v)}^{\max }\right] \times \mathrm{DP}_{\left(w^{\prime}\right)}^{\max }
$$

est inférieur à la borne de rang $(s+1)$, alors pour tout motif $c$ vérifiant :

$$
c_{x_{i}}=b_{x_{i}}{ }^{[s-1]} \text { pour tout } i<v,
$$

il n'existe aucune piste sur $r$ rondes prolongeant $\mathcal{T}^{[0, s-2]} \|\left(a^{[s-1]}, c\right)$ de probabilité supérieure ou égale à $p_{\mathrm{e}}^{(r)}$.

La fonction Round optimisée à l'aide des théorèmes B. 28 et B. 29 est donnée dans la figure B. 5 .

```
Algorithme 12 - Round(s, \mathcal{T}}\mp@subsup{}{(s-1)}{(p)}\mp@subsup{p}{}{(s-1)}
Entrée. }\mathcal{T}=((\mp@subsup{a}{}{[0]},\mp@subsup{b}{}{[0]}),\ldots,(\mp@subsup{a}{}{[s-2]},\mp@subsup{b}{}{[s-2]})
    a}\mp@subsup{}{[s-1]}{\leftarrow}\leftarrow\pi(\mp@subsup{a}{}{[s-2]}
    b}\mp@subsup{}{}{[s-1]}\leftarrow\mp@subsup{0}{nm}{
    p
    \mathcal{T}}\mp@subsup{}{(s)}{\leftarrow
    w}\leftarrow\mp@subsup{\textrm{w}}{n}{}(\mp@subsup{a}{}{[s-1]}
    Noter }\mp@subsup{x}{0}{}<\ldots<\mp@subsup{x}{w-1}{}\mathrm{ les indices des S-boxes activées par a }\mp@subsup{|}{}{[s-1]}\mathrm{ .
    X \leftarrow(x0,\ldots, 和-1
    L(0)}\leftarrow\mp@subsup{0}{m}{
    Appeler RoundRec(s,1, 隹(s), p
    Fonction RoundRec(s,v, 隹(s), p
        Si v=w alors
            p}\mp@subsup{}{}{(s)}\leftarrow\mp@subsup{p}{}{(s,w-1)
            Si s+1<r alors
                Appeler Round(s+1, 仿(s), p}\mp@subsup{}{}{(s)}
            Sinon
                Appeler LastRound( }\mp@subsup{\mathcal{T}}{}{(s)},\mp@subsup{p}{}{(s)}
        Sinon
        x}\leftarrow\mp@subsup{x}{v-1}{
        Pour chaque }\mp@subsup{b}{x}{[s-1]}\mathrm{ triés par ordre décroissant selon
        DP
        p
        Si }\mp@subsup{p}{}{(s,v)}\times\mp@subsup{\textrm{DP}}{(w-s)}{\operatorname{max}}\mathrm{ est inférieur à la borne de rang s alors
                Quitter la boucle
                            Théorème B.28
            Si }\pi\mathrm{ est une permutation des bits alors
                L'v)}\leftarrow\mp@subsup{L}{}{(v-1)}\vee\mp@subsup{\textrm{L}}{\textrm{ASB}}{}(\pi(\mp@subsup{b}{}{[s-1]}\mp@subsup{|}{x}{})
                w
                Si p}\mp@subsup{p}{}{(s,v)}\times\mp@subsup{\textrm{DP}}{(w-s)}{\operatorname{max}}\times\mp@subsup{\textrm{DP}}{(\mp@subsup{w}{}{\prime})}{\operatorname{max}}\textrm{n}\mathrm{ 'est pas inférieur à la borne de
                    rang (s+1) alors
                Appeler RoundRec(s,v+1, 佒(s)},\mp@subsup{p}{}{(s,v)},\mp@subsup{L}{}{(v)},X) Théorème B.2
            Sinon
                Appeler RoundRec (s,v+1, 隹(s)},\mp@subsup{p}{}{(s,v)},\mp@subsup{L}{}{(v)},X
```

Figure B．5 ：Deuxième optimisation－la fonction de recherche Round

## Appendice B - Résumé long en français

Algorithme 13 - OptTrail $\left(r,\left(p_{o}^{(i)}\right)_{1 \leq i<r}\right)$
Entrée. Le nombre de rondes courant $r$ et les probabilités $\left(p_{o}^{(i)}\right)_{1 \leq i<r}$
Sortie. Une piste sur $r$ rondes optimale $\mathcal{T}_{o}{ }^{(r)}$

```
\({ }_{1} \mathcal{T}_{\mathrm{o}}{ }^{(r)} \leftarrow()\)
\(p_{\mathrm{e}}^{(r)} \leftarrow p_{\mathrm{o}}^{(r-1)}\)
Tant que \(\mathcal{T}_{\mathrm{o}}^{(r)}\) est vide faire
    \(p_{\mathrm{e}}^{(r)} \leftarrow p_{\mathrm{e}}^{(r)} / 2\)
        \(\mathcal{T}_{\mathrm{o}}{ }^{(r)} \leftarrow\) OptTrailEst \(\left(r,\left(p_{o}^{(i)}\right)_{1 \leq i<r}, p_{\mathrm{e}}^{(r)}\right)\)
Renvoyer \(\mathcal{T}_{o}{ }^{(r)}\)
```

Figure B. 6 : Gestion automatique de l'estimation.

## B.2.2.d. Le test sur la borne

L'ensemble des résultats précédents peuvent être préservés tout en renforçant la condition sur la borne. Supposons que nous ayons déjà trouvé une piste de probabilité supérieure ou égale à $p_{\mathrm{e}}^{(r)}$. L'estimation $p_{\mathrm{e}}^{(r)}$ est alors égale à la probabilité différentielle de cette piste. Maintenant, supposons que la probabilité de la piste courante $\mathcal{T}$ sur $s$ rondes vérifie $\operatorname{DP}(\mathcal{T}) \cdot p_{\mathrm{o}}^{(r-s)}=p_{\mathrm{e}}^{(r)}$. Dans ce cas, la probabilité $\mathrm{DP}(\mathcal{T})$ n'est pas inférieure à la borne de rang $s$ et l'algorithme teste tous ses prolongements possibles. Cependant, l'égalité précédente implique que dans le meilleur cas, nous trouverons une piste sur $r$ rondes de probabilité $p_{e}^{(r)}$. Étant donné qu'une telle piste est déjà connue, l'extension de $\mathcal{T}$ n'est pas nécessaire. Cette discussion montre que la définition B. 23 peut être renforcée comme suit.

Définition B. 30 (borne de rang $s$ ). Soit $\mathcal{T}$ une piste sur $s<r$ rondes. Sa probabilité est inférieure à la borne de rang $s$ si

$$
\left(\mathcal{T}_{\mathrm{o}}^{(r)}=() \text { et } \operatorname{DP}(\mathcal{T})<\frac{p_{\mathrm{e}}^{(r)}}{p_{\mathrm{o}}^{(r-s)}}\right) \quad \text { ou } \quad\left(\mathcal{T}_{\mathrm{o}}^{(r)} \neq() \text { et } \operatorname{DP}(\mathcal{T}) \leq \frac{p_{\mathrm{e}}^{(r)}}{p_{\mathrm{o}}^{(r-s)}}\right) .
$$

## B.2.2.e. Gestion automatique de l'estimation

Comme expliqué dans la section B.2.1.b, l'estimation $p_{e}^{(r)}$ conditionne la complexité de l'algorithme OptTrailEst. Plusieurs méthodes permettent d'obtenir de bonnes estimations de $p_{o}^{(r)}$. Citons par exemple l'utilisation de pistes itératives. Notre algorithme OptTrail est construit à partir d'une idée de Ohta, Moriai et Aoki [87] et possède deux avantages majeurs. Premièrement, la gestion de l'estimation est entièrement automatique et donc aucune étude de chiffrement n'est nécessaire. Ensuite, sa complexité est du même ordre de grandeur que l'algorithme OptTrailEst exécuté avec $p_{e}^{(r)}=p_{o}^{(r)} / 2$.

L'algorithme OptTrail est présenté dans la figure B.6. Pour comprendre son fonctionnement, il convient de rappeler que OptTrailEst ne trouve aucune piste quand $p_{e}^{(r)}>p_{o}^{(r)}$. Dans ce cas, la piste $\mathcal{T}_{o}^{(r)}$ reste vide après l'exécution de l'algorithme.

## B. 2 - Évaluation de la sécurité des SPN

Puisque $p_{\mathrm{o}}^{(r)} \leq p_{\mathrm{o}}^{(r-1)}$, on commence par lancer OptTrailEst avec $p_{\mathrm{e}}^{(r)}=p_{\mathrm{o}}^{(r-1)} / 2$ comme estimation. Cette estimation est alors divisée par deux après chaque exécution de OptTrailEst jusqu'à ce qu'une piste optimale soit trouvée, ce qui ce produit à partir du moment où la condition $p_{\mathrm{e}}^{(r)} \leq p_{\mathrm{o}}^{(r)}$ devient vraie.

De plus, nous avons observé expérimentalement que la complexité de l'algorithme OptTrailEst exécuté avec $p_{\mathrm{e}}^{(r)} \geq 2^{4} \cdot p_{\mathrm{o}}^{(R)}$ est négligeable comparée à celle de son exécution avec $p_{\mathrm{e}}^{(r)}=p_{\mathrm{o}}^{(R)} / 2$. Cela justifie que la complexité de OptTrail est à peu près la même que celle de OptTrailEst.

## B.2.3. Résultats

Nos expérimentations et simulations ont été réalisées sur un processeur AMD Phenom II X4 965 Black Edition 3.4 GHz. Le temps d'exécution de notre algorithme pour un chiffrement sur $R$ rondes comprend tous les pré-calculs ainsi que les $R-1$ appels à OptTrail, comme expliqué dans la section B.2.1.b.

Pour démontrer la sécurité pratique de Present [17] face à la cryptanalyse différentielle, ses auteurs ont démontré que la probabilité d'une piste sur 5 rondes est majorée par $2^{-20}$ et ont exhibé une piste de probabilité $2^{-21}$. Notre algorithme permet de démontrer en 0,3 seconde que cette borne est atteinte. Ils ont ensuite déduit que la probabilité d'une piste sur 25 rondes est majorée par $2^{-100}$. Notre algorithme a déterminé en 0,5 seconde que la probabilité d'une piste optimale vaut $2^{-110}$. Le nombre de ronde n'est ici pas problématique puisque le calcul d'une piste optimale sur 64 rondes ne prend que deux secondes.

La permutation des bits utilisée dans l'algorithme SmallPresent 69] (ainsi que dans Present) peut être généralisée pour tous entiers naturels $n$ et $m$. Notons $\phi_{n, m}$ la permutation de $\llbracket 0, n m \llbracket$ définie par

$$
\phi(i)=m(i \bmod n)+\left\lfloor\frac{i}{m}\right\rfloor .
$$

Nous avons construit un SPN opérant sur des blocs de 128-bits et similaire à Present pour tester l'efficacité de notre algorithme. Nous définissons $\pi$ comme la diffusion linéaire associée à la permutation des bits $\phi_{8,16}$ puis les S-boxes toutes égales à celle de l'AES [39]. En exécutant notre algorithme, nous obtenons en 7,1 secondes une piste différentielle optimale sur 13 rondes de probabilité $2^{-89}$.

Afin d'analyser la sécurité du chiffrement Puffin [36] contre la cryptanalyse différentielle, ses auteurs avaient majoré la probabilité d'une piste optimale sur 31 rondes par $2^{-62}$. Nous avons calculé une piste atteignant cette borne en 0,02 seconde.

Finalement, nous avons testé notre algorithme sur Iceberg [95]. Étant donné que la diffusion linéaire du chiffrement n'est pas réalisée au moyen d'une simple permutation des bits, l'optimisation présentée à la section B.2.2.c ne s'applique pas. Les concepteurs du chiffrement avaient majoré la probabilité d'une piste différentielle optimale sur 16 rondes par $2^{-160}$. Notre algorithme a prouvé qu'elle est en fait égale à $2^{-171,6}$ en 2,3 secondes. Ces résultats sont résumés dans la figure B.7.

|  | Taille <br> des blocs | Nombre <br> de rondes | Majorant | Meilleure <br> probabilité | Temps <br> d'exécution |
| :--- | :---: | :---: | :---: | :---: | :---: |
| Present | 64 | 5 | $2^{-20}$ | $2^{-20}$ | 0.3 s |
| Present | 64 | 25 | $2^{-100}$ | $2^{-110}$ | 0.5 s |
| Present-like | 128 | 13 | - | $2^{-89}$ | 7.1 s |
| Puffin | 64 | 31 | $2^{-62}$ | $2^{-62}$ | 0.02 s |
| ICeberg | 64 | 16 | $2^{-160}$ | $2^{-171.6}$ | 2.3 s |

Figure B.7: Liste des résultats

Pour conclure, nous avons présenté dans ce chapitre un algorithme générique calculant une piste différentielle ou linéaire optimale dans un réseau de substitutionspermutations. L'exécution de cet algorithme peut permettre de prouver la sécurité pratique d'un chiffrement par blocs. À l'inverse, si le chiffrement est faible, la piste renvoyée permet de l'attaquer efficacement avec une cryptanalyse différentielle ou linéaire. Spécialement optimisé pour les SPN dont la diffusion linéaire est assurée par une permutation des bits, nous avons trouvé des pistes différentielles optimales pour Present et Puffin en moins d'une seconde. Par conséquent, notre algorithme constitue un puissant outil pour le concepteur de SPN qui peut être exécuté plusieurs fois afin d'optimiser les primitives du chiffrement.

## B.3. Chiffrements à trappes basées sur des partitions

Les chiffrements à trappes étudiés dans cette thèse sont principalement une généralisation des idées présentées par Paterson dans [88]. Cet article présente un chiffrement à trappe inspiré du DES exploitant une faiblesse induite par sa fonction de ronde. En effet, l'action du groupe engendré par les fonctions de ronde sur l'espace des messages est imprimitive. Autrement dit, la fonction de ronde préserve une partition de l'espace de message indépendamment des clés de rondes utilisées. La même propriété reste naturellement vraie pour le chiffrement complet. Cette partition secrète constitue la trappe. Paterson a ensuite présenté un chiffrement à trappe composé de 32 rondes et utilisant une clé de 80 bits. Sa trappe peut compromettre sérieusement sa sécurité en utilisant $2^{32}$ clairs choisis. De plus, une fois combinée à un algorithme de cadencement des clés rondes bien choisi, elle permet de retrouver la clé avec quelques clairs connus et un effort de $2^{41}$ opérations. Même si les concepts mathématiques de la trappe sont donnés, aucun algorithme ne détaille la construction des S-boxes. Comme l'auteur le reconnait, la sécurité de son chiffrement à trappe face à la cryptanalyse différentielle n'est pas aussi élevée que ce que l'on pourrait attendre et la moitié des bits des chiffrés sont indépendants de la moitié des bits des messages clairs. Enfin, l'auteur se demandait si les partitions utilisées doivent être linéaires, c'est-à-dire constituées des classes d'un sous-espace vectoriel. Caranti and al. [31] répondirent ensuite à cette question en prouvant que si le groupe généré par les fonctions de rondes est imprimitif, alors la partition de l'espace des messages est nécessairement linéaire.

## B.3.1. Généralisations

Dans ce chapitre, nous considérons une généralisation des chiffrements à trappe imprimitifs introduite par Harpes dans sa thèse 50. Un chiffrement à trappe basée sur des partitions est un chiffrement envoyant une partition de l'ensemble des messages clairs sur une partition de l'ensemble des messages chiffrés, indépendamment de la clé utilisée. Cette notion généralise donc les chiffrements imprimitifs pour lesquels les partitions d'entrée et de sortie sont égales. Plus formellement, on introduit les deux définitions suivantes.

Définition B.31. Soient $f$ une permutation d'un ensemble $E$ et $\mathcal{A}, \mathcal{B}$ deux partitions de $E$. Notons $f(\mathcal{A})$ l'ensemble $\{f(A) \mid A \in \mathcal{A}\}$. On dit que $f$ envoie $\mathcal{A}$ sur $\mathcal{B}$ si $f(\mathcal{A})=\mathcal{B}$. De plus, si $\mathcal{A}=\mathcal{B}$, on dit que $f$ préserve la partition $\mathcal{A}$.

Définition B. 32 (chiffrement à trappe basée sur des partitions). Un chiffrement itéré $E$ opérant sur des blocs de $n$ bits est appelé un chiffrement à trappe basée sur des partitions s'il existe deux partitions $\mathcal{A}$ et $\mathcal{B}$ de $\mathbb{F}_{2}^{n}$ telles que pour toute clé de chiffrement $K$ dans $\mathbb{F}_{2}^{\kappa}$ on a

$$
E_{k}(\mathcal{A})=\mathcal{B}
$$

Comme $E_{K}$ doit être une permutation de $\mathbb{F}_{2}^{n}$ pour permettre le déchiffrement, on vérifie facilement que les partitions $\mathcal{A}$ et $\mathcal{B}$ ont nécessairement le même nombre de parties.

La cryptanalyse partitionnante est une attaque contre les chiffrements itérés par blocs introduite par Harpes dans [52]. De manière similaire à la cryptanalyse différentielle qui utilise une paire $(a, b)$ de motifs de différences, la cryptanalyse partitionnante considère une paire de partitions $(\mathcal{A}, \mathcal{B})$, où $\mathcal{A}$ représente la partition des messages clairs et $\mathcal{B}$ la partition de l'ensemble des entrées de la dernière ronde. Une paire $(\mathcal{A}, \mathcal{B})$ est dite efficace si pour presque toutes les clé de chiffrement, les entrées de la dernière ronde ne sont pas uniformément distribuées sur les blocs de $\mathcal{B}$ quand les messages clairs sont uniformément choisis parmi un bloc fixé $A$ de $\mathcal{A}$. Ensuite, l'attaque exploite ce comportement non-uniforme pour récupérer de l'information sur la dernière clé de ronde, de la même manière que le font les cryptanalyses différentielle et linéaire.

À la lumière de cette attaque, il convient de relâcher la définition d'un chiffrement à trappe basée sur des partitions afin d'inclure les chiffrements créés intentionnellement pour être faible à la cryptanalyse partitionnante. Pour éviter toute confusion, nous proposons la définition suivante.

Définition B. 33 (Chiffrement à trappe probabiliste). Un chiffrement itéré sur $r$ rondes $E: \mathbb{F}_{2}^{\kappa} \times \mathbb{F}_{2}^{n} \rightarrow \mathbb{F}_{2}^{n}$ est appelé un chiffrement à trappe probabiliste basée sur des partitions s'il existe une paire $(\mathcal{A}, \mathcal{B})$ de partitions de $\mathbb{F}_{2}^{n}$ vérifiant la propriété suivante : pour presque toutes les clés de chiffrement $K$ dans $\mathbb{F}_{2}^{\kappa}$ et pour chaque partie $A$ dans $\mathcal{A}$, il existe une partie $B_{A, K}$ dans $\mathcal{B}$ telle que pour toute autre partie $B$ on a

$$
\mathbb{P}_{x \in A}\left(E_{K}^{(r-1)}(x) \in B_{A, K}\right) \gg \mathbb{P}_{x \in A}\left(E_{K}^{(r-1)}(x) \in B\right) .
$$

Autrement dit, pour la majorité des clés de chiffrement $K$ dans $\mathbb{F}_{2}^{\kappa}$ et pour chaque partie $A$ de $\mathcal{A}$, la fonction de chiffrement sur $(r-1)$ notée $E_{K}{ }^{(r-1)}$ envoie une proportion significative des messages clairs dans $A$ sur une seule partie $B_{A, K}$ de $\mathcal{B}$ et les autres messages dans $A$ sont éparpillés dans les autres parties de $\mathcal{B}$. Naturellement, une telle propriété doit être voulue par le concepteur du chiffrement pour pouvoir parler de trappe. Nous discuterons à la fin de cette thèse de BEA-1, notre chiffrement à trappe inspiré des travaux de Paterson et Harpes et conçu avec la théorie que nous exposons maintenant.

## B.3.2. Réseaux de substitutions-permutations et partitions

L'objectif de cette section est l'étude d'un réseau de substitutions-permutations (SPN) envoyant une partition des messages clairs sur une partition des messages chiffrés. Quand la clé de chiffrement est fixée, la fonction de chiffrement $E_{K}$ est une simple permutation de l'espace des messages. Aussi, n'import quelle partition $\mathcal{A}$ des clairs est envoyée sur la partition $E_{K}(\mathcal{A})$ des chiffrés. Néanmoins, pour exploiter la trappe, le concepteur doit connaître la paire de partitions $\left(\mathcal{A}, E_{K}(\mathcal{A})\right)$. Le problème est que la partition de sortie $E_{K}(\mathcal{A})$ dépend a priori de la clé de chiffrement $K$, qui est inconnue de l'attaquant. La manière la plus simple pour résoudre ce problème consiste à imposer que les partitions $E_{K}(\mathcal{A})$ soient indépendantes de la clé $K$. En d'autres termes, nous souhaitons que toutes les partitions $E_{K}(\mathcal{A})$ soient égales à une partition fixée $\mathcal{B}$.

Comme pour les cryptanalyses différentielle et linéaire, la prise en compte exacte l'algorithme de cadencement des clés de rondes est un problème difficile. Aussi, le cadenceur de clés sera délibérément omis tout au long de cette section. Cela revient à considérer un SPN envoyant une partition $\mathcal{A}$ sur une partition fixée $\mathcal{B}$ indépendamment des clés de rondes utilisées.

Comme nous le verrons dans le prochain résultat, l'étude de tels chiffrements repose sur un type particulier de partitions formées des classes modulo un sous-espace vectoriel. Ces partitions ont déjà été introduites par Harpes [50, Définition 4.4].

Définition B. 34 (partition linéaire). Soit $\mathcal{A}$ une partition de $\mathbb{F}_{2}^{n}$. Notons $V$ sa partie contenant $0_{n}$. La partition $\mathcal{A}$ est dite linéaire si $V$ est un sous-espace vectoriel de $\mathbb{F}_{2}^{n}$ et si chaque partie dans $\mathcal{A}$ est une classe modulo $V$ dans $\mathbb{F}_{2}^{n}$, c'est-à-dire si

$$
\mathcal{A}=\left\{x+V \mid x \in \mathbb{F}_{2}^{n}\right\}=\mathbb{F}_{2}^{n} / V
$$

Cette partition est alors notée $\mathcal{L}(V)$.

## B.3.3. De la fonction de chiffrement à la substitution

Pour exposer les prochains résultats, nous fixons plusieurs notations en considérant un réseau de substitutions-permutations générique. Soient $m, n$ et $r$ trois entiers naturels non nuls. Soient $S_{0}, \ldots, S_{m-1}$ des S-boxes sur $n$ bits.

- L'addition de la clé de ronde $k$ est notée $\alpha_{k}: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}, x \mapsto x+k$.
- La couche de substitution est notée $\sigma$ et envoie $\left(x_{i}\right)_{i<m} \operatorname{sur}\left(S_{i}\left(x_{i}\right)\right)_{i<m}$.
- La couche de diffusion est une permutation linéaire notée $\pi: \mathbb{F}_{2}^{n m} \rightarrow \mathbb{F}_{2}^{n m}$.

La fonction de ronde $F_{k}$ associée à la clé de ronde $k$ est définie par $F_{k}=\pi \sigma \alpha_{k}$. Enfin, la fonction de chiffrement associée aux clés de rondes $K=\left(k^{[0]}, \ldots, k^{[r]}\right)$ dans $\left(\mathbb{F}_{2}^{n m}\right)^{r+1}$ est définie par

$$
E_{K}=\alpha_{k[r]} F_{k[r-1]} \ldots F_{k[0]} .
$$

Nous pouvons maintenant présenter nos principaux résultats sur les chiffrements à trappe préservant une partition.

Théorème B.35. Soient $\mathcal{A}$ et $\mathcal{B}$ deux partitions de $\mathbb{F}_{2}^{n m}$. Supposons pour chaque $(r+1)$-uplet de clés de ronde $K=\left(k^{[0]}, \ldots, k^{[r]}\right)$ dans $\left(\mathbb{F}_{2}^{n m}\right)^{r+1}$ que la fonction de chiffrement $E_{K}$ envoie $\mathcal{A}$ sur $\mathcal{B}$. Posons

$$
\mathcal{A}^{[0]}=\mathcal{A} \quad \text { et } \quad \forall 1 \leq i \leq r, \mathcal{A}^{[i]}=(\pi \sigma)^{i}(\mathcal{A}) .
$$

Alors,

- $\mathcal{A}^{[r]}=\mathcal{B}$;
- pour tout $0 \leq i<r$ et pour tout $k^{[i]}$ dans $\mathbb{F}_{2}^{n m}, F_{k}\left[{ }^{[i]}\left(\mathcal{A}^{[i]}\right)=\mathcal{A}^{[i+1]}\right.$;
- pour tout $0 \leq i \leq r$, la partition $\mathcal{A}^{[i]}$ est linéaire.

Corollaire B.36. On conserve les notations du théorème précédent. Pour tout $0 \leq i \leq r$, on note $V^{[i]}$ la partie de $\mathcal{A}^{[i]}$ contenant 0 . On sait alors que $\mathcal{A}^{[i]}=\mathcal{L}\left(V^{[i]}\right)$. Soit $i<r$ un entier naturel. Alors,

$$
\sigma\left(\mathcal{L}\left(V^{[i]}\right)\right)=\mathcal{L}\left(W^{[i]}\right) .
$$

où $W^{[i]}$ désigne le sous-espace vectoriel $\pi^{-1}\left(V^{[i+1]}\right)$. En particulier, la couche de substitution doit envoyer une partition linéaire sur une autre.

La figure B. 8 illustre schématiquement les résultats du théorème B. 35 ainsi que de son corollaire B.36. Cette représentation souligne que la partition d'entrée est toujours

## Appendice B - Résumé long en français

| Hypothèse | Théorème B. 35 | Corollaire B. 36 |
| :---: | :---: | :---: |
| $\mathcal{A}$ | $\mathcal{A}^{[0]}$ | $\mathcal{L}\left(V^{[0]}\right)$ |
| $E_{K}$ | $F_{k[0]}$ | $\oplus k^{[0]}$ |
|  |  | $\mathcal{L}\left(V^{[0]}\right)$ |
|  |  | $\sigma$ |
|  |  | $\mathcal{L}\left(W^{[0]}\right)$ |
|  |  | $\pi$ |
|  | $\mathcal{A}^{[1]}$ | $\mathcal{L}\left(V^{[1]}\right)$ |
|  | $\vdots$ | ! |
|  | $\mathcal{A}^{[r-1]}$ | $\mathcal{L}\left(V^{[r-1]}\right)$ |
|  |  | $\oplus k^{[r-1]}$ |
|  |  | $\mathcal{L}\left(V^{[r-1]}\right)$ |
|  | $F_{k}{ }^{[r-1]}$ | $\sigma$ |
|  |  | $\mathcal{L}\left(W^{[r-1]}\right)$ |
|  |  | $\pi$ |
|  | $\mathcal{A}^{[r]}$ | $\mathcal{L}\left(V^{[r]}\right)$ |
|  | $\oplus k^{[r]}$ | $\oplus k^{[r]}$ |
| $\mathcal{B}$ | $\mathcal{A}^{[r]}$ | $\mathcal{L}\left(V^{[r]}\right)$ |

Figure B. 8 : Illustration du théorème B. 35 et de son corollaire B. 36 .
transformée de la même façon au travers des différentes opérations du processus de chiffrement. Jusqu'à présent, nous avons donc expliqué que lorsqu'un SPN envoie une partition $\mathcal{A}$ des messages clairs sur une partition $\mathcal{B}$ des chiffrés indépendamment des clés de rondes, alors sa couche de substitution doit nécessairement envoyer au moins une partition linéaire sur une autre. En conséquence, notre étude peut être restreinte à la couche de substitution sans perte de généralité. Pour cela, nous rappelons la définition suivante.

Définition B. 37 (mur). Soit $E$ un sous-ensemble de $\llbracket 0, m \llbracket$. Le mur associé $E$ que l'on note Wall $_{E}$, est défini par

$$
\operatorname{Wall}_{E}=\left\{x \in\left(\mathbb{F}_{2}^{n}\right)^{m} \mid \forall i \in E^{c}, x_{i}=0_{n}\right\} .
$$

Remarque B.38. La notion de mur a été introduite par Aragona et Calderini [4), 22]. On voit facilement que

$$
\mathrm{Wall}_{E}=\prod_{i=0}^{m-1} \operatorname{Wall}_{E}^{[i]} \quad \text { avec } \quad \operatorname{Wall}_{E}^{[i]}= \begin{cases}\left\{0_{n}\right\} & \text { if } i \in E^{c} \\ \mathbb{F}_{2}^{n} & \text { if } i \in E\end{cases}
$$

Ainsi, un mur correspond au produit cartésien de sous-espaces triviaux pour chaque S-box.

Les sous-espaces $\mathrm{Wall}_{E}$ sont essentiels pour l'étude de la couche de substitution puisque cette dernière préserve toujours la partition $\mathcal{L}\left(\mathrm{Wall}_{E}\right)$, indépendamment de ses S-boxes.

Théorème B.39. Soient $n \geq 2$ et $m$ deux entiers strictement positifs. Soient $S_{0}, \ldots, S_{m-1}$ des S-boxes sur $n$ bits. Notons $\sigma$ la permutation de $\left(\mathbb{F}_{2}^{n}\right)^{m}$ envoyant $\left(x_{i}\right)_{0 \leq i<m} \operatorname{sur}\left(S_{i}\left(x_{i}\right)\right)_{0 \leq i<m}$. Enfin, considérons deux sous-espaces $V$ et $W$ de $\left(\mathbb{F}_{2}^{n}\right)^{m}$ tels que $\sigma$ envoie $\mathcal{L}(V)$ sur $\mathcal{L}(W)$. En supposant que $V$ n'est pas un mur, au moins l'une des S-boxes envoie une partition linéaire non triviale sur une autre.

## B.3.4. Analyse des résultats

Dans un premier temps, supposons que tous les $V^{[i]}$ sont des murs. Si un tel cas se produit, la couche de diffusion du chiffrement ne joue probablement pas son rôle (ou sinon le nombre de rondes est trop faible). Comme c'est généralement le cas, supposons qu'il n'y ait pas de diffusion linéaire dans la dernière ronde du SPN. Alors, les partitions d'entré et de sortie sont toutes deux linéaires et associées à des murs. Cela implique que certains bits des chiffrés sont indépendants de certains bits des messages clairs. Une telle propriété doit naturellement être évitée dans tout bon chiffrement. Afin de caractériser une diffusion linéaire ne possédant pas cette faiblesse, Calderini a introduit la définition suivante dans [23].

Définition B. 40 (diffusion fortement propre sur $r$ rondes). La couche de diffusion est dite fortement propre sur rondes si pour chaque mur propre $W$, il existe un entier $1 \leq i<r$ tel que $\pi^{i}(W)$ n'est pas un mur.

## Appendice B - Résumé long en français

Supposons maintenant que la couche de diffusion est fortement propre sur $r$ rondes. Alors au moins l'un des $V^{[i]}$ n'est pas un mur. Ce second cas est nettement plus intéressant que le précédent. En vertu du théorème B. 39 , au moins l'une des S-boxes doit envoyer une partition linéaire non triviale sur une autre.

En résumé, nous avons prouvé dans cette section que tout chiffrement à trappe basée sur des partitions ayant une diffusion fortement propre doit avoir au moins une S-box envoyant une partition linéaire non triviale sur une autre. La section suivante cherche alors à concevoir de telles S -boxes tout en maximisant leur résistance aux cryptanalyses différentielle et linéaire.

## B.4. Analyse d'une S-box à trappe

En poursuivant l'étude menée dans la section précédente, nous devons maintenant étudier la résistance aux cryptanalyses différentielle et linéaire des S-boxes envoyant une partition linéaire sur une autre. On peut alors montrer que si $S_{1}$ est une S -box envoyant $\mathcal{L}(V)$ sur $\mathcal{L}(W)$, alors il existe une S -box $S_{2}$ préservant $\mathcal{L}(V)$ qui possède les mêmes propriétés différentielles et linéaires que $S_{1}$. Autrement, on peut supposer sans perte de généralité que $V=W$ dans cette étude. Par conséquent, nous considérons dans toute cette section

- un sous-espace vectoriel non trivial $V$ de $\mathbb{F}_{2}^{n}$ de dimension $d$,
- un sous-espace supplémentaire $U$ de $V$, et
- une S-box $S$ sur $n$ bits préservant la partition linéaire $\mathcal{L}(V)$.

Puisque $U$ est un supplémentaire de $V$, l'espace $\mathbb{F}_{2}^{n}$ est égal à la somme directe $U \oplus V$. Autrement dit, tout élément $x$ de $\mathbb{F}_{2}^{n}$ s'écrit de manière unique sous la forme $x=u+v$ avec $u$ et $v$ des éléments de $U$ et $V$ respectivement. Notons [ $u$ ] la classe $u$ modulo $V$. Ainsi, $[u]=u+V$ est l'unique partie dans $\mathcal{L}(V)$ contenant $u$ et nous avons

$$
\mathcal{L}(V)=\{[u] \mid u \in U\} .
$$

Puisque $V$ est de dimension $d$, son complémentaire $U$ est de dimension $n-d$. De plus, on a les inégalités

$$
1 \leq d \leq n-1 \quad \text { et } \quad 1 \leq n-d \leq n-1
$$

car $V$ est par hypothèse un sous-espace non trivial de $\mathbb{F}_{2}^{n}$.

## B.4.1. Structure d'une S-box à trappe

Le théorème suivant précise la structure interne des permutations préservant une partition linéaire. Un résultat similaire fut introduit par Harpes [50, Theorem 5.6]. Cependant, notre formulation sera plus appropriée pour exposer les autres résultats de cette section.

Théorème B. 41 (décomposition d'une S-box imprimitive). Soit $S$ une S-box sur $n$ bits préservant $\mathcal{L}(V)$. Il existe une unique permutation $\rho$ de $U$ et une unique famille de permutations $\left(\tau_{u}\right)_{u \in U}$ de $V$ telles que, pour tout $x=u+v$ dans $\mathbb{F}_{2}^{n}$,

$$
S(u+v)=\rho(u)+\tau_{u}(v)
$$

Réciproquement, si $\rho$ est une permutation de $U$ et si $\left(\tau_{u}\right)_{u \in U}$ est une famille de permutations de $V$, alors l'application $S^{\prime}$ définie par la relation $S^{\prime}(u+v)=\rho(u)+\tau_{u}(v)$ préserve $\mathcal{L}(V)$.

Ce théorème est fondamental pour notre étude puisqu'il fournit une construction générale pour obtenir une S-box imprimitive à l'aide de plusieurs permutations définies sur de plus petits ensembles. Intuitivement, ce résultat peut s'expliquer comme suit. Nous savons déjà que la partition linéaire $\mathcal{L}(V)$ est formée des classes modulo $V$. En permutant les éléments de chaque classe [ $u$ ], la partition entière est préservée. La manière exacte de permuter les éléments de la classe [u] est représentée par la permutation $\tau_{u}$ de $V$, à savoir $u+v$ est envoyé sur $u+\tau_{u}(v)$. Par conséquent, il nous faut une famille $\left(\tau_{u}\right)_{u \in U}$ pour représenter toutes ses permutations locales. Jusqu'ici, chaque classe est envoyée sur elle-même. Il reste donc à expliquer comment les classes sont permutées. C'est la permutation $\rho$ de $U$ qui assure ce rôle. Ainsi, la classe $[u$ ] est envoyée sans permutation interne sur $[\rho(u)]$. Autrement dit, chaque élément $u+\tau_{u}(v)$ est envoyé sur $\rho(u)+\tau_{u}(v)$. En résumé, la famille $\left(\tau_{u}\right)_{u \in U}$ décrit comment les éléments sont déplacés à l'intérieur de chaque classe et la permutation $\rho$ explique comment $S$ permute les classes entres elles.

## B.4.2. Analyses différentielle et linéaire

Premièrement, rappelons quelques résultats basiques sur les propriétés différentielles et linéaires d'une S-box. Considérons une S-box $S$ sur $n$ bits ainsi que deux éléments $a$ et $b$ de $\mathbb{F}_{2}^{n}$. La probabilité de la différentielle $(a, b)$ et la corrélation de l'approximation $(a, b)$ relativement à $S$ sont définies par

$$
\begin{aligned}
\operatorname{DP}_{S}(a, b) & =2^{-n} \times \#\left\{x \in \mathbb{F}_{2}^{n} \mid S(x)+S(x+a)=b\right\}, \\
\mathrm{C}_{S}(a, b) & =2^{-(n-1)} \times \#\left\{x \in \mathbb{F}_{2}^{n} \mid\langle a, x\rangle=\langle b, S(x)\rangle\right\}-1 .
\end{aligned}
$$

Le potentiel linéaire de l'approximation $(a, b)$ de $S$ est alors le carré de sa corrélation, c'est-à-dire $\operatorname{LP}_{S}(a, b)=\mathrm{C}_{S}(a, b)^{2}$. La probabilité différentielle maximale $\mathrm{DP}_{S}^{\max }$, la corrélation absolue maximale $\mathrm{C}_{S}^{\max }$ et le potentiel linéaire maximal $\mathrm{LP}_{S}^{\max }$ de $S$ sont définis par

$$
\begin{aligned}
\mathrm{DP}_{S}^{\max } & =\max \left\{\mathrm{DP}(a, b) \mid a \in\left(\mathbb{F}_{2}^{n}\right)^{*}, b \in \mathbb{F}_{2}^{n}\right\}, \\
\mathrm{C}_{S}^{\max } & =\max \left\{|\mathrm{C}(a, b)| \mid a \in \mathbb{F}_{2}^{n}, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}, \\
\mathrm{LP}_{S}^{\max } & =\max \left\{\mathrm{LP}(a, b) \mid a \in \mathbb{F}_{2}^{n}, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}\right\}=\left(\mathrm{C}_{S}^{\max }\right)^{2} .
\end{aligned}
$$

Notons enfin que nous avons les inégalités suivantes

$$
\begin{equation*}
\mathrm{C}_{S}^{\max } \geq 2^{-\frac{n-1}{2}}, \quad \mathrm{LP}_{S}^{\max } \geq 2^{-(n-1)} \tag{B.5}
\end{equation*}
$$

## Appendice B - Résumé long en français

Maintenant, supposons que $S$ préserve la partition $\mathcal{L}(V)$. Le théorème B. 41 établit l'existence d'une permutation $\rho$ de $U$ et des permutations $\left(\tau_{u}\right)_{u \in U}$ de $V$ telles que

$$
S(u+v)=\rho(u)+\tau_{u}(v)
$$

pour tout élément $x=u+v$ de $\mathbb{F}_{2}^{n}$. Nous fixons cette décomposition pour le reste de la section.

Étant donné ce résultat, il est naturel de se demander si les propriétés différentielles et linéaires de $S$ sont reliées à celles des permutations de sa décomposition. Cependant, ces propriétés sont définies pour des fonctions booléennes vectorielles alors que les permutations $\rho$ et $\tau_{u}$ sont définies sur des sous-espaces propres de $\mathbb{F}_{2}^{n}$. Pour y remédier, nous allons identifier $U$ avec $\mathbb{F}_{2}^{n-d}$ et $V$ avec $\mathbb{F}_{2}^{d}$ à l'aide de deux isomorphismes puis considérer les permutations induites par $\rho$ et les $\tau_{u}$ sur ces espaces.

Notation B.42. Soient $\mathcal{B}_{\mathcal{U}}=\left(u_{i}\right)_{i<n-d}$ et $\mathcal{B}_{\mathcal{V}}=\left(v_{i}\right)_{i<n-d}$ deux bases respectives de $U$ et $V$. Posons

$$
\begin{aligned}
L_{U}: \mathbb{F}_{2}^{n-d} & \longrightarrow U & L_{V}: \mathbb{F}_{2}^{d} & \longrightarrow V \\
\left(x_{n-d-1}, \ldots, x_{0}\right) & \longmapsto \sum_{i=0}^{n-d-1} x_{i} u_{i}, & \left(y_{d-1}, \ldots, y_{0}\right) & \longmapsto \sum_{i=0}^{d-1} y_{i} v_{i} .
\end{aligned}
$$

On voit facilement que $L_{U}$ et $L_{V}$ sont tous deux des isomorphismes d'espaces vectoriels. On définit alors $\bar{\rho}$ comme la permutation $L_{U}^{-1} \circ \rho \circ L_{U}$ induite par $\rho$ sur $\mathbb{F}_{2}^{n-d}$. De la même manière, pour chaque $u$ dans $U$, on définit $\bar{\tau}_{u}$ comme la permutation $L_{V}^{-1} \circ \tau_{u} \circ L_{V}$ induite par $\tau_{u}$ sur $\mathbb{F}_{2}^{d}$.

## B.4.2.a. Matrices de corrélations et potentiels linéaires

Jusqu'ici, nous avons divisé notre S-box imprimitive $S$ en plusieurs permutations puis transformé ses permutations afin d'étudier leurs propriétés différentielles et linéaires. Commençons par étudier la matrice de corrélation de $S$. Notre premier résultat relie certains de ses coefficients à ceux de la matrice de corrélation de $\bar{\rho}$. Même si le prochain théorème ne prend en compte que quelques coefficients de $\mathrm{C}_{S}$, il est très important en pratique puisque ces coefficients sont généralement les plus grands en valeur absolue. Ils conditionnent donc la résistance de $S$ à la cryptanalyse linéaire.

Théorème B.43. Soient $a$ et $b$ deux éléments de $V^{\perp}$. Notons $a^{t}$ et $b^{t}$ leurs images respectives par $L_{U}^{\top}$. Alors,

$$
\mathrm{C}_{S}(a, b)=\mathrm{C}_{\bar{\rho}}\left(a^{t}, b^{t}\right) \quad \text { et donc } \quad \operatorname{LP}_{S}(a, b)=\operatorname{LP}_{\bar{\rho}}\left(a^{t}, b^{t}\right)
$$

Remarque B.44. Notons que les paires ( $a^{t}, b^{t}$ ) définies dans le théorème précédent sont toutes distinctes. Par conséquent, $\mathrm{C}_{\bar{\rho}}$ est une sous-matrice de $\mathrm{C}_{S}$.

Corollaire B.45. Le potentiel linéaire maximal de $S$ est minoré par $2^{-(n-d-1)}$.

## B.4.2.b. Probabilités différentielles

De la même manière, nous allons maintenant nous intéresser aux liens entre les probabilités différentielles de $S$ et celles des permutations de sa décomposition. À l'inverse du théorème B.43, le résultat suivant prend en compte l'ensemble des coefficients de la matrice $\mathrm{DP}_{S}$ et met ainsi en évidence sa structure globale.

Théorème B.46. Soient $a=u_{a}+v_{a}$ et $b=u_{b}+v_{b}$ deux éléments de $\mathbb{F}_{2}^{n}$. Notons $u_{a}^{\prime}$ et $u_{b}^{\prime}$ leurs images par $L_{U}^{-1}$. On a

$$
\sum_{i \in\left[u_{a}\right]} \mathrm{DP}_{S}(i, b)=\sum_{j \in\left[u_{b}\right]} \operatorname{DP}_{S}(a, j)=\operatorname{DP}_{\bar{\rho}}\left(u_{a}^{\prime}, u_{b}^{\prime}\right) .
$$

En particulier, $\mathrm{DP}_{S}(a, b) \leq \mathrm{DP}_{\bar{\rho}}\left(u_{a}^{\prime}, u_{b}^{\prime}\right)$ et donc $\mathrm{DP}_{S}^{\max } \leq \mathrm{DP}_{\bar{\rho}}^{\max }$.
Le prochain résultat est l'analogue du théorème B. 43 pour les probabilités différentielles. De même, il considère seulement quelques coefficients de $\mathrm{DP}_{S}$ mais généralement les plus grands. En conséquence, il sera utilisé pour obtenir une borne inférieure sur la résistance de $S$ à la cryptanalyse différentielle.

Théorème B.47. Soient $v_{a}$ et $v_{b}$ deux éléments de $V$. Notons $v_{a}^{\prime}$ et $v_{b}^{\prime}$ leurs images respectives par $L_{V}^{-1}$. Alors,

$$
\operatorname{DP}_{S}\left(v_{a}, v_{b}\right)=\frac{1}{2^{n-d}} \sum_{u \in U} \operatorname{DP}_{\bar{\tau}_{u}}\left(v_{a}^{\prime}, v_{b}^{\prime}\right)
$$

En particulier, la sous-matrice $\left(\operatorname{DP}_{S}\left(v_{a}, v_{b}\right)\right)_{v_{a}, v_{b} \in V}$ est uniquement déterminée par $\left(\mathrm{DP}_{\bar{\tau}_{u}}\right)_{u \in U}$.

Corollaire B.48. La probabilité différentielle maximale de $S$ est minorée par le plus petit multiple de $2^{-(n-1)}$ directement supérieur ou égal à $\frac{1}{2^{d}-1}$.

## B.4.2.c. Conception d'une S-Box à trappe

En s'appuyant sur les résultats précédents, nous allons obtenir un algorithme pour construire des S-boxes à trappe basée sur partitions atteignant presque les bornes des corollaires B.45, B. 48 résumées dans la figure B.9. Commençons par résumer les conditions obtenues.

- D'après les théorèmes B. 43 et B. 46 , le potentiel linéaire maximal et la probabilité différentielle maximale de la permutation $\bar{\rho}$ doivent être les plus faibles possibles.
- De plus, le théorème B. 47 précise que la somme des matrices $\mathrm{DP}_{\bar{\tau}_{u}}$ doit avoir les plus petits coefficients possibles.

Remarque B.49. Si $d$ est proche de 0 , la S-box est faible à la cryptanalyse différentielle. À l'inverse si $d$ est proche de $n$, elle est faible à la cryptanalyse linéaire. Ainsi, une s-box à trappe résistante à ces deux cryptanalyses doit vérifier $d \approx \frac{n}{2}$.

## Appendice B - Résumé long en français



Figure B. 9 : Bornes inférieures sur la probabilité différentielle maximale et sur le potentiel linéaire maximal d'une S -box envoyant $\mathcal{L}(V)$ sur $\mathcal{L}(W)$ où $V$ et $W$ sont deux sous-espaces de $\mathbb{F}_{2}^{n}$ de dimension $d$.

Soit $n$ un entier naturel non nul. On choisit deux sous-espaces propres $V$ et $W$ de $\mathbb{F}_{2}^{n}$ de dimension $d$ ainsi qu'un isomorphisme $L$ de $V$ vers $W$. Détaillons maintenant comment concevoir une bonne S -box envoyant $\mathcal{L}(V)$ sur $\mathcal{L}(W)$. Premièrement, on choisit un supplémentaire $U$ de $V$ dans $\mathbb{F}_{2}^{n}$ puis on construit les isomorphismes $L_{U}$ et $L_{V}$. Ensuite, on procède comme suit.

1. On construit une permutation $\bar{\rho}$ de $\mathbb{F}_{2}^{n-d}$ étant (presque) optimale relativement aux cryptanalyses différentielle et linéaire.
2. On construit une famille de permutations $\left(\bar{\tau}_{u}\right)_{u \in U}$ de $\mathbb{F}_{2}^{d}$ telle que la somme (notée SDP) de leurs matrices de probabilités différentielles vérifie la propriété :

$$
\frac{1}{2^{n-d}} \times \max _{a, b \in\left(\mathbb{F}_{2}^{n}\right)^{*}} \operatorname{SDP}(a, b) \text { est proche de la borne du corollaire B. } 48 .
$$

3. On définit alors la permutation $S$ de $\mathbb{F}_{2}^{n}$ par

$$
S(u+v)=\left(L_{U} \circ \bar{\rho} \circ L_{U}^{-1}\right)(u)+\left(L_{V} \circ \bar{\tau}_{u} \circ L_{V}^{-1}\right)(v) .
$$

4. Si $\mathrm{DP}_{S}^{\max }$ et $\mathrm{LP}_{S}^{\max }$ sont proches des bornes données dans la figure B.9, alors $L \circ S$ est une bonne S-box envoyant $\mathcal{L}(V)$ sur $\mathcal{L}(W)$. Sinon, on retourne à l'étape 1 .

En pratique, on obtient une S-box à trappe dont les propriétés différentielles et linéaires sont proches des bornes de la figure B. 9 après un nombre restreint d'itérations.

## B.4.3. Se prémunir des trappes basées sur des partitions

Pour conclure cette partie théorique sur les chiffrements à trappes basées sur des partitions, nous présentons un critère dérivé de nos résultats pour démontrer qu'un chiffrement ne possède pas une telle trappe. Dans la section précédente, nous avons considéré un SPN générique envoyant une partition des messages clairs sur une partition des messages chiffrés indépendamment des clés de rondes utilisées. Nous avons montré que lorsque sa couche de diffusion linéaire est fortement propre, au moins l'une de ses S-boxes envoie une partition linéaire non triviale sur une autre. Nous avons ensuite étudié les propriétés différentielles et linéaires de telles S-boxes dans la présente section. De cette étude, nous avons déduit des bornes supérieures sur leur résistance aux cryptanalyses différentielle et linéaire. En conséquence, si toutes les S-boxes d'un SPN ont des résistances plus élevées que ce qu'il est atteignable avec des S-boxes à trappe, le chiffrement n'a pas de trappe basée sur des partitions. Cela démontre le théorème suivant.

Théorème B.50. Considérons un réseau de substitutions-permutations sur nm bits constitué de $m$ S-boxes sur $n$ bits. Supposons que sa couche de diffusion soit fortement propre sur $r$ rondes. Si chaque S -box $S_{i}$ est telle que pour tout $1 \leq d \leq n-1$, les valeurs $\mathrm{LP}_{S_{i}}^{\max }$ et $\mathrm{DP}_{S_{i}}^{\max }$ sont inférieures aux bornes données dans la figure B.9, alors le SPN n'a pas de trappe basée sur des partitions valable pour des clés de rondes indépendantes.

## Appendice B - Résumé long en français

De plus, si les valeurs $\mathrm{LP}_{S_{i}}^{\max }$ et $\mathrm{DP}_{S_{i}}^{\max }$ sont significativement inférieures aux bornes de la figure B.9, alors il est peu probable que le SPN ait une trappe probabiliste basée sur des partitions. Par exemple, ce critère permet de montrer que l'AES [39] n'a pas de trappe (probabiliste) basée sur des partitions. Comme expliqué dans [23], sa couche de diffusion est fortement propre sur deux rondes. De plus, la probabilité différentielle maximale et le potentiel linéaire maximal de sa S-box sont bien en-dessous des bornes de la figure B.9, pour toute les dimensions $d$ possibles du sous-espace $V$. Par conséquent, cette S-box n'envoie aucune partition linéaire sur une autre.

## B.5. Conclusion

En guise d'application de notre théorie des chiffrements à trappes (probabilistes) basées sur des partitions, nous avons conçu BEA-1 (pour Backdoored Encryption Algorithm), un chiffrement à trappe largement inspiré de l'AES, le standard actuel de chiffrement par blocs. L'algorithme BEA-1 est prouvé résistant en pratique aux cryptanalyses différentielle et linéaire. Cependant, la cryptanalyse utilisant la trappe secrète permet de retrouver entièrement la clé maitresse de 120 bits en 20 secondes sur un ordinateur portable. L'attaque ne requiert que $2^{16}$ blocs de messages clairs choisis ce qui représente moins de 2 Mo de données. Comme son temps d'exécution est faible, nous avons effectué la cryptanalyse plusieurs fois et vérifié que sa probabilité de succès est supérieure à $95 \%$. En cas d'échec, l'attaquant peut tout de même retrouver la clé de chiffrement la plupart du temps avec les mêmes données mais les paramètres de la cryptanalyse doivent être modifiés manuellement et l'attaque a une plus grande complexité.

L'idée générale de notre cryptanalyse est proche de la cryptanalyse partitionnante de Harpes [52] avec cependant quelques différences significatives. Premièrement, la cryptanalyse partitionnante suppose que le nombre de parties composant la partition de sortie est faible, typiquement égal à 2 , 4 ou 8 . À l'inverse, la partition utilisée dans notre trappe est composée des $2^{40}$ classes d'un sous-espace vectoriel.

Ensuite, la cryptanalyse partitionnante considère des classes de candidats pour la dernière clé de ronde où seulement quelques bits conditionnent les classes des chiffrés. Comme sa complexité est proportionnelle au nombre de classes de clés, cette attaque n'est efficace seulement si ce nombre est raisonnablement petit. Dans le cas de BEA-1, chaque bit de la dernière clé de ronde influence les classes des chiffrés. Puisqu'il y a $2^{80}$ clés possibles pour la dernière ronde, une cryptanalyse partitionnante basique n'est pas appliquable sur BEA-1.

De plus, une cryptanalyse partitionnante utilise pour chaque classe de clés autant de compteurs qu'il y a de parties dans la partition de sortie. Notre cryptanalyse n'utilise quant-à-elle qu'un seul compteur par clé. Enfin, notre attaque permet de retrouver l'ensemble des 120 bits de la clé de chiffrement alors qu'une cryptanalyse partitionnante n'obtient que quelques bits de la dernière clé de ronde.

Comme dernière remarque sur notre chiffrement à trappe BEA-1, nous souhaitons souligner que le critère énoncé en fin de section B. 4 suggère que chacune de ses S-
boxes peut envoyer presque sûrement une partition linéaire associée à un sous-espace de dimension cinq sur une autre telle partition. En utilisant les résultats précédents, une étude des matrices différentielles et des matrices de corrélation de chaque S-box révèle alors les sous-espaces utilisés et donc une partie de la trappe.

Pour conclure, notons que même si l'existence d'une trappe est une propriété non désirable dans un chiffrement par blocs, leur étude peut contribuer à la conception de chiffrements plus sécurisés ainsi qu'à améliorer notre compréhension des cryptanalyses classiques. En effet, les chiffrements à trappes basées sur des partitions sont étroitement liés aux sous-espaces invariants, aux pistes de sous-espaces de dimension constante ainsi qu'à la cryptanalyse partitionnante. Nous avons montré dans la section B. 3 que les chiffrements étudiés doivent avoir des S-boxes équivalentes à des S-boxes imprimitives. Ensuite, nous avons montré dans la section B. 4 que de telles S-boxes peuvent être fortement résistantes soit à la cryptanalyse différentielle, soit à la cryptanalyse linéaire, mais pas au deux. En conséquence, notre étude a établi des liens inattendus entre les cryptanalyses différentielle, linéaire et partitionnante. En combinant nos travaux avec ceux de Calderini, nous disposons maintenant de deux critères permettant de montrer qu'un chiffrement n'a pas de trappe basée sur des partitions. Dans la même lignée, citons les travaux récents de Blondeau, Civino et Sala [16] proposant une nouvelle variante de la cryptanalyse différentielle directement inspirée d'une famille de chiffrements à trappes basées sur des sommes cachées [19]. De plus, la recherche de trappes nous fait naturellement considérer des propriétés différentes de celles utilisées dans les cryptanalyses classiques, augmentant ainsi nos chances de découvrir de nouvelles attaques efficaces. Enfin, soulignons que la question de savoir si des trappes efficaces et indétectables peuvent être insérées dans des chiffrements de confiance aux yeux de la communauté reste ouverte.

Appendice B - Résumé long en français

## Bibliography

[1] Kashif Ali and Howard M Heys. An Algorithm to Analyze Block Cipher Resistance to Linear and Differential Cryptanalysis. In Proceedings of Newfoundland Electrical and Computer Engineering Conference (NECEC 2006), 2006.
[2] Vesela Angelova and Yuri Borissov. Plaintext Recovery in DES-like Cryptosystems Based on S-boxes with Embedded Parity Check. Serdica Journal of Computing, 7(3):257p-270p, 2013.
[3] Kazumaro Aoki, Kunio Kobayashi, and Shiho Moriai. Best Differential Characteristic Search of FEAL. In Fast Software Encryption, pages 41-53. Springer, 1997.
[4] Riccardo Aragona, Marco Calderini, Antonio Tortora, and Maria Tota. On the Primitivity of PRESENT and Other Lightweight Ciphers. arXiv preprint arXiv:1611.01346, 2016.
[5] Riccardo Aragona, Andrea Caranti, Francesca Dalla Volta, and Massimiliano Sala. On the Group Generated by the Round Functions of Translation Based Ciphers Over Arbitrary Finite Fields. Finite Fields and Their Applications, 25:293-305, 2014.
[6] John Bamberg. Permutation Group Theory. RMIT Summer Course notes, 2006.
[7] Arnaud Bannier and Nicolas Bodin. A New Drawing for Simple Venn Diagrams Based on Algebraic Construction. Journal of Computational Geometry, 8:153173, 2017.
[8] Arnaud Bannier, Nicolas Bodin, and Eric Filiol. Automatic Search for a Maximum Probability Differential Characteristic in a Substitution-Permutation Network. In System Sciences (HICSS), 2015 48th Hawaii International Conference on, pages 5165-5174. IEEE, 2015. Best Paper Awards.
[9] Arnaud Bannier, Nicolas Bodin, and Eric Filiol. Partition-Based Trapdoor Ciphers. Cryptology ePrint Archive, Report 2016/493, 2016. http://eprint iacr.org/2016/493.
[10] Arnaud Bannier and Eric Filiol. Mathematical Backdoors in Symmetric Encryption Systems - Proposal for a Backdoored AES-like Block Cipher. In 1st

## BIBLIOGRAPHY

International Workshop on Formal methods for Security Engineering (ForSE), February 2017.
[11] Arnaud Bannier and Eric Filiol. Operational Cryptanalysis Based on Backdoors Exploitation in an AES-like Cipher. In RusCrypto'17, March 2017.
[12] Arnaud Bannier and Eric Filiol. Partition-based Trapdoor Ciphers. InTech editions, 2017. ISBN:978-953-51-3386-5 (Print), ISBN:978-953-51-3385-8 (Online).
[13] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. Journal of CRYPTOLOGY, 4(1):3-72, 1991.
[14] Eli Biham and Adi Shamir. Differential Cryptanalysis of the Data Encryption Standard, volume 28. Springer, 1993.
[15] Alex Biryukov and Léo Paul Perrin. State of the Art in Lightweight Symmetric Cryptography. 2017.
[16] Céline Blondeau, Roberto Civino, and Massimiliano Sala. Differential Attacks: Using Alternative Operations. Cryptology ePrint Archive, Report 2017/610, 2017. http://eprint.iacr.org/2017/610.
[17] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. PRESENT: An Ultra-lightweight Block Cipher. In Cryptographic Hardware and Embedded Systems-CHES 2007, pages 450-466. Springer, 2007.
[18] KA Browning, JF Dillon, MT McQuistan, and AJ Wolfe. An APN Permutation in Dimension Six. Finite Fields: theory and applications, 518:33-42, 2010.
[19] Carlo Brunetta, Marco Calderini, and Massimiliano Sala. Algorithms and Bounds for Hidden Sums in Cryptographic Trapdoors. arXiv preprint arXiv:1702.08384, 2017.
[20] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials. IEEE Transactions on Information Theory, 52(3):1141-1152, 2006.
[21] Stanislav Bulygin and Michael Walter. Study of the Invariant Coset Attack on PRINTcipher: More Weak Keys with Practical Key Recovery. IACR Cryptology ePrint Archive, 2012:85, 2012.
[22] Marco Calderini. On Boolean Functions, Symmetric Cryptography and Algebraic Coding Theory. PhD thesis, University of Trento, 2015.
[23] Marco Calderini. A Note on Some Algebraic Trapdoors for Block Ciphers. arXiv preprint arXiv:1705.08151, 2017.
[24] Marco Calderini and Massimiliano Sala. On Differential Uniformity of Maps that May Hide an Algebraic Trapdoor. In International Conference on Algebraic Informatics, pages 70-78. Springer, 2015.
[25] Marco Calderini and Massimiliano Sala. Elementary Abelian Regular Subgroups as Hidden Sums for Cryptographic Trapdoors. arXiv preprint arXiv:1702.00581, 2017.
[26] Peter J Cameron. Permutation Groups, volume 45. Cambridge University Press, 1999.
[27] Anne Canteaut. Lecture Notes on Cryptographic Boolean Functions. Inria, 2016. https://www.rocq.inria.fr/secret/Anne.Canteaut/poly.pdf.
[28] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. A New Characterization of Almost Bent Functions. In Fast Software Encryption, volume 99, pages 186-200. Springer-Verlag, 1999.
[29] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Binary m-sequences With Three-valued Crosscorrelation: A Proof of Welch's Conjecture. IEEE Transactions on Information Theory, 46(1):4-8, 2000.
[30] A Caranti, Francesca Dalla Volta, and Massimiliano Sala. On Some Block Ciphers and Imprimitive Groups. Applicable algebra in engineering, communication and computing, 20(5-6):339-350, 2009.
[31] A Caranti, F Dalla Volta, Massimiliano Sala, and Francesca Villani. Imprimitive Permutations Groups Generated by the Round Functions of Keyalternating Block Ciphers and Truncated Differential Cryptanalysis. arXiv preprint math/0606022, 2006.
[32] Andrea Caranti, Francesca Dalla Volta, and Massimiliano Sala. An Application of the O'Nan-Scott Theorem to the Group Generated by the Round Functions of an AES-like Cipher. Designs, Codes and Cryptography, 52(3):293-301, 2009.
[33] Claude Carlet. Vectorial Boolean Functions for Cryptography. Boolean models and methods in mathematics, computer science, and engineering, 134:398-469, 2010.
[34] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems. Designs, Codes and Cryptography, 15(2):125-156, 1998.
[35] Florent Chabaud and Serge Vaudenay. Links Between Differential and Linear Cryptanalysis. In Advances in Cryptology-EUROCRYPT'94, pages 356-365. Springer, 1995.
[36] Huiju Cheng, Howard M Heys, and Cheng Wang. Puffin: A Novel Compact Block Cipher Targeted to Embedded Digital Systems. In Digital System Design Architectures, Methods and Tools, 2008. DSD'08. 11th EUROMICRO Conference on, pages 383-390. IEEE, 2008.

## BIBLIOGRAPHY

[37] Baudoin Collard, F-X Standaert, and J-J Quisquater. Improved and Multiple Linear Cryptanalysis of Reduced Round Serpent. In Information Security and Cryptology, pages 51-65. Springer, 2008.
[38] Don Coppersmith and Edna Grossman. Generators for Certain Alternating Groups With Applications to Cryptography. SIAM Journal on Applied Mathematics, 29(4):624-627, 1975.
[39] Joan Daemen and Vincent Rijmen. The Design of Rijndael. Springer Verlag, 2002.
[40] Joan Daemen and Vincent Rijmen. Probability Distributions of Correlation and Differentials in Block Ciphers. Journal of Mathematical Cryptology JMC, 1(3):221-242, 2007.
[41] Joan Daemen and Vincent Rijmen. The Design of Rijndael: AES-the Advanced Encryption Standard. Springer Science \& Business Media, 2013.
[42] John D Dixon and Brian Mortimer. Permutation Groups, volume 163. Springer Science \& Business Media, 1996.
[43] Hans Dobbertin. Almost Perfect Nonlinear Power Functions on GF (2n): the Niho Case. Information and Computation, 151(1-2):57-72, 1999.
[44] Hans Dobbertin. Almost Perfect Nonlinear Power Functions on GF (2/sup n/): the Welch Case. IEEE Transactions on Information Theory, 45(4):1271-1275, 1999.
[45] Robert Gold. Maximal Recursive Sequences With 3-valued Recursive Crosscorrelation Functions. IEEE transactions on Information Theory, 14(1):154156, 1968.
[46] Jay Goldman and Gian-Carlo Rota. The Number Of Subspaces Of a Vector Space. Technical report, DTIC Document, 1969.
[47] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace Trail Cryptanalysis and its Applications to AES - Extended Version. http://eprint. iacr.org/2016/592.
[48] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace Trail Cryptanalysis and its Applications to AES. IACR Transactions on Symmetric Cryptology, 2016(2):192-225, 2017.
[49] Jian Guo, Jérémy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki, and Siang Meng Sim. Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs. IACR Transactions on Symmetric Cryptology, 2016(1):33-56, 2016.
[50] Carlo Harpes. Cryptanalysis of Iterated Block Ciphers. PhD thesis, Diss. Techn. Wiss. ETH Zürich, Nr. 11625, 1996. Ref.: JL Massey; Korref.: U. Maurer, 1996.
[51] Carlo Harpes, Gerhard G Kramer, and James L Massey. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 24-38. Springer, 1995.
[52] Carlo Harpes and James L Massey. Partitioning Cryptanalysis. In International Workshop on Fast Software Encryption, pages 13-27. Springer, 1997.
[53] Henk DL Hollmann and Qing Xiang. A Proof of the Welch and Niho Conjectures on Cross-correlations of Binary m-sequences. Finite Fields and Their Applications, 7(2):253-286, 2001.
[54] G Hornauer, W Stephan, and Ralph Wernsdorf. Markov Ciphers and Alternating Groups. Lecture Notes in Computer Science, 765:453-460, 1994.
[55] Alexander Hulpke. Notes on Computational Group Theory. Department of Mathematics. Colorado State University, 2010.
[56] Burton S Kaliski, Ronald L Rivest, and Alan T Sherman. Is the Data Encryption Standard a Group? (Results of Cycling Experiments on DES). Journal of Cryptology, 1(1):3-36, 1988.
[57] Masayuki Kanda, Youichi Takashima, Tsutomu Matsumoto, Kazumaro Aoki, and Kazuo Ohta. A Strategy for Constructing Fast Round Functions With Practical Security Against Differential and Linear Cryptanalysis. In Selected Areas in Cryptography, pages 264-279. Springer, 1999.
[58] Tadao Kasami. The Weight Enumerators for Several Classes of Subcodes of the 2nd Order Binary Reed-Muller Codes. Information and Control, 18(4):369-394, 1971.
[59] Auguste Kerckhoffs. La cryptographie militaire. Journal des sciences militaires, pages 5-83, 1883.
[60] Lars Knudsen. Truncated and Higher Order Differentials. In Fast Software Encryption, pages 196-211. Springer, 1995.
[61] Lars Knudsen, Gregor Leander, Axel Poschmann, and Matthew JB Robshaw. PRINTcipher: A Block Cipher for IC-printing. In International Workshop on Cryptographic Hardware and Embedded Systems, pages 16-32. Springer, 2010.
[62] Lars R Knudsen. Block Ciphers - Analysis, Design and Applications. PhD thesis, Aarhus University, Denmark, 1994.
[63] Lars R Knudsen. Block Ciphers-A Survey. Lecture notes in computer science, 1528:18-48, 1998.
[64] Lars R Knudsen and Matthew JB Robshaw. The Block Cipher Companion. Springer, 2011.

## BIBLIOGRAPHY

[65] Marc Krasner and Léo Kaloujnine. Produit complet des groupes de permutations et problème d'extension de groupes. III. Acta Sci. Math.(Szeged), 14:69-82, 1951.
[66] Gilles Lachaud and Jacques Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. IEEE transactions on information theory, 36(3):686-692, 1990.
[67] Xuejia Lai, James L Massey, and Sean Murphy. Markov Ciphers and Differential Cryptanalysis. In Advances in Cryptology-EUROCRYPT'91, pages 17-38. Springer, 1991.
[68] Serge Lang. Linear Algebra. 3rd corr. Printing 1993 (Undergraduate Texts in Mathematics), 1987.
[69] Gregor Leander. Small Scale Variants Of The Block Cipher PRESENT. IACR Cryptology ePrint Archive, 2010:143, 2010.
[70] Gregor Leander, Mohamed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. Advances in Cryptology-CRYPTO 2011, pages 206-221, 2011.
[71] Gregor Leander, Brice Minaud, and Sondre Rønjom. A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 254-283. Springer, 2015.
[72] Gregor Leander and Axel Poschmann. On the Classification of 4 Bit S-boxes. In Arithmetic of Finite Fields, pages 159-176. Springer, 2007.
[73] James L Massey. Cryptography: Fundamentals and Applications. In Copies of transparencies, Advanced Technology Seminars, volume 109, page 119, 1993.
[74] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In Advances in Cryptology-EUROCRYPT'93, pages 386-397. Springer, 1994.
[75] Mitsuru Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard. In Advances in Cryptology - Crypto'94, pages 1-11. Springer, 1994.
[76] Mitsuru Matsui. On Correlation Between the Order of S-boxes and the Strength of DES. In Advances in Cryptology - EUROCRYPT'94, pages 366-375. Springer, 1995.
[77] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. Handbook of Applied Cryptography. CRC press, 1996.
[78] Sean Murphy, Kenneth Paterson, and Peter Wild. A Weak Cipher that Generates the Symmetric Group. Journal of Cryptology, 7(1):61-65, 1994.
[79] Kaisa Nyberg. Perfect Nonlinear S-boxes. In Advances in Cryptol-ogy-EUROCRYPT'91, pages 378-386. Springer, 1991.
[80] Kaisa Nyberg. Differentially Uniform Mappings for Cryptography. In Advances in cryptology-Eurocrypt'93, pages 55-64. Springer, 1993.
[81] Kaisa Nyberg. On the Construction of Highly Nonlinear Permutations. In Advances in Cryptology-EUROCRYPT'92, pages 92-98. Springer, 1993.
[82] Kaisa Nyberg and Lars R Knudsen. Provable Security Against Differential Cryptanalysis. In Crypto, volume 92, pages 566-574. Springer, 1992.
[83] National Institute of Standards and Technology. Data Encryption Standard. Federal Information Processing Standard (FIPS), Publication 46, 1977.
[84] National Institute of Standards and Technology. DES Modes of Operation. Federal Information Processing Standard (FIPS), Publication 81, 1980.
[85] National Institute of Standards and Technology. Advanced Encryption Standard. Federal Information Processing Standard (FIPS), Publication 197, 2001.
[86] National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation. Special Publication 800-38A, 2001.
[87] Kazuo Ohta, Shiho Moriai, and Kazumaro Aoki. Improving the Search Algorithm for the Best Linear Expression. In Advances in Cryptology - CRYPT0'95, pages 157-170. Springer, 1995.
[88] Kenneth G Paterson. Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers. In Fast Software Encryption, pages 201-214. Springer, 1999.
[89] Vincent Rijmen and Bart Preneel. A Family of Trapdoor Ciphers. In Fast Software Encryption, pages 139-148. Springer, 1997.
[90] Joseph Rotman. An Introduction to the Theory of Groups, volume 148 of Graduate Texts in Mathematics. Springer-Verlag, New York, fourth edition, 1995.
[91] Claude E Shannon. Communication Theory of Secrecy Systems. Bell Labs Technical Journal, 28(4):656-715, 1949.
[92] Vladimir Michilovich Sidelnikov. On the Mutual Correlation of Sequences. In Soviet Math. Dokl., volume 12, pages 197-201, 1971.
[93] Neil JA Sloane et al. The On-line Encyclopedia of Integer Sequences, 2017. http://oeis.org.
[94] Rüdiger Sparr and Ralph Wernsdorf. Group Theoretic Properties of Rijndaellike Ciphers. Discrete Applied Mathematics, 156(16):3139-3149, 2008.
[95] Francois-Xavier Standaert, Gilles Piret, Gael Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat. ICEBERG: An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware. In Fast Software Encryption, pages 279-298. Springer, 2004.

## BIBLIOGRAPHY

[96] Anne Tardy-Corfdir and Henri Gilbert. A Known Plaintext Attack of FEAL4 and FEAL-6. In Advances in Cryptology-CRYPTO'91, pages 172-182. Springer, 1992.
[97] Ralph Wernsdorf. The One-round Functions of the DES Generate the Alternating Group. In Eurocrypt, pages 99-112. Springer, 1992.
[98] Ralph Wernsdorf. The Round Functions of Rijndael Generate the Alternating Group. In FSE, pages 143-148. Springer, 2002.
[99] Helmut Wielandt. Finite Permutation Groups. Academic Press, 1964.
[100] Hongjun Wu, Feng Bao, Robert H Deng, and Qin-Zhong Ye. Cryptanalysis of Rijmen-Preneel Trapdoor Ciphers. In Advances in Cryptology-Asiacrypt'98, pages 126-132. Springer, 1998.

## Analyse combinatoire des chiffrements par blocs avec trappes

Résumé. Les trappes jouent un double rôle dans la cryptographie moderne. Même si elles sont essentielles en cryptographie asymétrique, leur rôle est tout autre lorsque l'on considère la cryptographie symétrique. Dans ce cas, une trappe désigne une faiblesse mathématique insérée volontairement au cœur du chiffrement, permettant à son concepteur de le casser efficacement. Une telle propriété est alors fortement indésirable. Pour qu'un chiffrement à trappe puisse inspirer confiance, il doit fournir les mêmes preuves de sécurité que tout autre chiffrement. La première partie de cette thèse se concentre sur les analyses de sécurité par rapport aux deux principales cryptanalyses des chiffrements par blocs, à savoir les attaques différentielles et linéaires.
La seconde partie est quant à elle dédiée à l'étude d'une famille de chiffrements à trappes introduite par Paterson et Harpes. Ces chiffrements envoient une partition des messages clairs sur une partition des messages chiffrés indépendamment des clés utilisées. Tout d'abord, nous étudions la structure de tels chiffrements puis obtenons des bornes sur leur sécurité. Nous expliquons ensuite comment les primitives du chiffrement doivent être conçues pour atteindre ces bornes. Enfin, nous présentons BEA-1, un chiffrement à trappe grandeur nature développé à partir de cette théorie. Bien qu'il soit résistant aux cryptanalyses différentielle et linéaire, la connaissance de la trappe permet de retrouver la clé de 120 bits en seulement quelques secondes sur un portable.

Mots clés : cryptographie, trappes, partitions.

## Combinatorial Analysis of Block Ciphers With Trapdoors

Abstract. Trapdoors are a two-face key concept in modern cryptography. Even if they are essential in asymmetric cryptography, their role is reversed in symmetric cryptography. In this case, the aim is to insert hidden mathematical weaknesses which enable one who knows them to break the cipher, making the existence of a trapdoor a strongly undesirable property. For a backdoor cipher to be trusted, it must provide the same security proofs than any other cipher. The first part of this thesis focuses on a security analysis with respect to the two mains attacks on block ciphers, namely differential and linear cryptanalysis.
The second part is devoted to the study of a family of backdoor ciphers introduced by Paterson and Harpes. These ciphers maps a partition of the plaintexts to a partition of the ciphertexts independently of the keys used. First the structure of such ciphers is investigated and bounds of their security are obtained. We then explain how the basic components of a backdoor cipher can be designed to achieve these bounds. Finally we introduce BEA-1, a real-size backdoor cipher based on this theory. This cipher resists differential and linear cryptanalysis whereas the knowledge of the trapdoor enables recovery of the full 120-bit cipher key in just a few second on a laptop computer.

Keywords: Cryptography, Trapdoors, Partitions.


ARTS ETMÉTIERS ParisTech

