HAL
open science

Attaques électromagnétiques ciblant les générateurs d'aléa

Pierre Bayon

To cite this version:

Pierre Bayon. Attaques électromagnétiques ciblant les générateurs d'aléa. Micro et nanotechnologies/Microélectronique. Université Jean Monnet - Saint-Etienne, 2014. Français. NNT : 2014STET4003 . tel-01160026

HAL Id: tel-01160026

https://theses.hal.science/tel-01160026v1

Submitted on 4 Jun 2015

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.

Thèse

pour obtenir le grade de docteur
de l'Université Jean Monnet

Discipline : **Microélectronique**
Équipe : **Systèmes Embarqués Sécurisés**

Attaques électromagnétiques ciblant les générateurs d'aléa

Pierre BAYON

La soutenance de thèse est prévue pour le 31 janvier, 2014 avec le jury suivant

Rapporteur :	
Olivier Sentieys	**IRISA, France**
François-Xavier Standaert	**UCL, Belgique**
Directeur de thèse :	
Lilian Bossuet	**LaHC, France**
Codirecteur de thèse :	
Alain Aubert	**LaHC, France**
Examinateur :	
Viktor Fischer	**LaHC, France**
Robert Fouquet	**LaHC, France**
Julien Francq	**CASSIDIAN, France**
Philippe Maurine	**LIRMM, France**

Table des matières

Table des matières i

Liste des figures v

Liste des tableaux xi

Glossaire xiii

Unités xv

Remerciements xvii

Introduction xix

1 Securité des systèmes de génération d'aléa 1
- 1.1 Les générateurs de nombres aléatoires 2
  - 1.1.1 La génération d'aléa dans la cryptographie matérielle 2
  - 1.1.2 Générateur de nombres réellement aléatoires 3
  - 1.1.3 Générateur à base d'oscillateurs en anneau de [Sunar et al., 2007] et amélioré par [Wold and Tan, 2008]. 6
- 1.2 Attaques sur les générateurs d'aléa 9
  - 1.2.1 Pourquoi attaquer un générateur d'aléa ? 9
  - 1.2.2 Modèle de menaces sur les générateurs de nombres réellement aléatoires 10
  - 1.2.3 Attaques sur les générateurs de nombres aléatoires 10
- 1.3 Conclusion 17

2 Les ondes électromagnétiques : une menace pour la cryptographie matérielle ? 19
- 2.1 Utilisation du rayonnement électromagnétique comme canal d'attaque 20
  - 2.1.1 Le canal électromagnétique comme moyen de récupération d'information 20
  - 2.1.2 Le canal électromagnétique comme canal d'attaque active . . 33
  - 2.1.3 Le canal caché électromagnétique et la génération d'aléa ? . . 37
- 2.2 Bancs de tests électromagnétiques et circuits électroniques ciblés . . 40
  - 2.2.1 Banc d'analyse 41
  - 2.2.2 Caractérisation de la sonde d'analyse 42
  - 2.2.3 Banc d'injection harmonique 45
  - 2.2.4 Cartes électroniques 47
- 2.3 Conclusion 49

3 Utilisation du rayonnement électromagnétique des circuits intégrés comme source d'information sur les générateurs d'aléa 51
3.1 Objectif 53
3.2 Différentes techniques de cartographie 53
3.2.1 Cartographie temporelle 54
3.2.2 Cartographie à analyse fréquentielle 54
3.2.3 WGMSI - Mesure d'incohérence dans la densité spectrale de puissance 55
3.2.4 Cartographie de corrélation croisée 57
3.3 Présentation de l'analyse électromagnétique appliquée aux générateurs d'aléa 58
3.4 Résultats de cartographie sur les TRNGs 60
3.4.1 Résultats de cartographie sur Altera CycloneIII 60
3.4.2 Résultats de cartographie sur Microsemi Fusion 78
3.5 Différence analyse locale et globale 83
3.5.1 Principe 83
3.5.2 Résultat sur l'IMP#3 (Altera Cyclone III) 85
3.6 Conclusion 86

4 Attaque en faute sur générateur d'aléa par injection électromagnétique harmonique 89
4.1 Présentation de l'attaque 91
4.1.1 Les cibles 91
4.1.2 Paramètres de l'attaque 93
4.2 Influence de l'injection électromagnétique harmonique sur les oscillateurs en anneau 93
4.2.1 Choix de la fréquence d'injection 93
4.2.2 Étude de l'évolution de l'information mutuelle lors de l'attaque 94
4.2.3 Visualisation de l'effet à l'oscilloscope 96
4.2.4 Réduction de la phase entre les deux oscillateurs 96
4.3 Une maîtrise complète du flot de bits produit par le générateur . . . 98
4.3.1 Effet de la dépendance des oscillateurs sur le flot de sortie du générateur de nombres aléatoires 98
4.3.2 Contrôle dynamique du biais 99
4.4 Une étude du comportement des oscillateurs en anneau sous injection électromagnétique harmonique 101
4.4.1 Le modèle d'Adler et sa généralisation aux oscillateurs numériques 101
4.4.2 Analyse du comportement des oscillateurs en anneau en simulation 102
4.4.3 Effet du verrouillage des oscillateurs sur la sortie du générateur 114
4.5 Un modèle électrique et mathématique de l'effet de l'attaque sur l'extracteur d'entropie 115

4.5.1 Étude du comportement de l'extraction d'entropie sous injection électromagnétique 116
4.5.2 Modélisation électrique 118
4.5.3 Modèle mathématique 122
4.5.4 Discussion sur l'impact de la perturbation sur l'extracteur d'entropie 130
4.6 Conclusion 132

5 Résumé des contributions et perspectives 135

Liste des publications 137

Bibliographie 139

Annexe A : Notion d'électromagnétisme 147
A.1 Modèle théorique : les équations de Maxwell 147
A.2 Zone de rayonnement ? 148
A.3 Circuit intégré et électromagnétisme ? 150

Table des figures

1.1 Schéma de principe d'un générateur de nombres aléatoires 4
1.2 Historique d'apparition des publications relatives aux différents principes de génération de nombres réellement aléatoires. 5
1.3 Schéma de principe du générateur proposé par [Sunar et al., 2007]. . 6
1.4 Schéma de principe du générateur amélioré, proposé par [Wold and Tan, 2008]. 7
1.5 Principe de l'accumulation de l'incertitude temporelle dans un oscillateur en anneau. 8
1.6 Modèle de menaces sur les générateurs de nombres réellement aléatoires. 10
1.7 Schéma de l'expérimentation effectuée sur deux oscillateurs en anneau par les auteurs de [Markettos and Moore, 2009]. 12
1.8 Mesure du signal de sortie de deux oscillateurs (en jaune la sortie S1 et en bleu la sortie S2 signalées sur la Figure 1.7, avec de gauche à droite : pas d'injection de signal, injection d'un signal harmonique de 24 MHz et d'amplitude pic à pic égale à 900mV. Figure extraite de [Markettos and Moore, 2009]. 13
1.9 Schéma de l'expérimentation effectuée sur un microcontrôleur sécurisé embarquant un générateur d'aléa par les auteurs de [Markettos and Moore, 2009]. 14
1.10 Suite de bits produites par le générateur d'aléa embarqué dans le microcontrôleur avec de gauche à droite : pas d'injection, une injection à 1.822 MHz et une injection à 1.929 MHz. Figure extraite de [Markettos and Moore, 2009]. 14

2.1 Historique des attaques passives qui utilisent le canal caché électromagnétique. 21
2.2 Historique des attaques actives qui utilisent le canal caché électromagnétique. 22
2.3 Différence entre une trace de consommation de puissance et une trace du rayonnement électromagnétique. Figure tirée de [Peeters et al., 2007]. 26
2.4 Bobinage typiquement utilisé pour effectuer des analyses électromagnétiques [Gandolfi et al., 2001]. 29
2.5 Bobinage ayant une résolution spatiale en dessous du millimètre [Peeters et al., 2007]. 30
2.6 Sonde LANGER utilisée dans notre banc de mesure. 30
2.7 Sonde d'injection à base d'allume-gaz utilisée par [Schmidt and Hutter, 2007] 34
2.8 Résultats de simulation - de haut en bas : horloge utilisée pour échantillonner la bascule D, signal en sortie de l'oscillateur en anneau, courant fourni par l'alimentation. 39

2.9 Résultats de simulation - de haut en bas : horloge utilisée pour échantillonner les deux bascules D, signal en sortie du premier oscillateur en anneau, signal en sortie du deuxième oscillateur en anneau, courant fourni par l'alimentation. 40
2.10 Schéma de principe du banc d'analyse électromagnétique. 41
2.11 Schéma de principe de l'expérience de caractérisation de la sonde d'analyse. 43
2.12 Carte de la réponse fréquentielle et locale de la sonde pour une ligne située sur un PCB et orientée à 0 ° 43
2.13 Cartes de la réponse fréquentielle et locale de la sonde pour une ligne située sur un PCB et orientée à 0 °, 45 ° et 90 ° 44
2.14 Schéma de principe du banc d'injection électromagnétique de signal harmonique. 46
2.15 Micro-sonde uni-polaire. 46
2.16 Schéma de principe des cartes utilisées. 47
2.17 Photo de la carte mère et d'une carte fille à gauche. Photo d'une carte fille Altera Cyclone III à droite. 48
2.18 Présentation de l'attaque électromagnétique combinée. 49

3.1 Principe de quadrillage d'un circuit intégré pour réaliser des cartes du rayonnement électromagnétique. 53
3.2 Principe de la technique de cartographie électromagnétique basée sur l'analyse fréquentielle 55
3.3 Densité spectrale de puissance d'une trace du rayonnement électromagnétique au dessus d'un générateur d'aléa (les contributions des oscillateurs se situent entre [325-331 MHz]). 59
3.4 Principe de l'analyse différentielle adaptée à l'analyse du rayonnement électromagnétique des générateurs d'aléa. 60
3.5 Schéma descriptif de l'agencement des blocs (floorplan) pour les trois implantations sur la cible Altera CycloneIII. 61
3.6 Carte résultante d'une analyse temporelle du rayonnement électromagnétique pour l'IMP#1 pour une tension d'alimentation de cœur à 1.25 V. 62
3.7 Moyenne des densités spectrales de puissance, sur tout le circuit, pour l'IMP#1 pour une tension d'alimentation de cœur à 1.25 V. 63
3.8 Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#1 pour une tension d'alimentation de cœur à 1.25 V et de 1.38 V. 64
3.9 Zoom sur la différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#1 pour une tension d'alimentation de cœur à 1.25 V et de 1.38 V. 64

3.10 Cartes résultantes de l'analyse fréquentielle pour l'IMP#1 pour différents paramètres : a) V = 1.25 V et $\delta f = [290-295MHz]$ b) V = 1.38 V et $\delta f = [290-295MHz]$ c) V = 1.25 V et $\delta f = [325-331MHz]$ d) V = 1.38 V et $\delta f = [325-331MHz]$. 66
3.11 Carte résultante pour l'IMP#1 de la différence entre la carte a) et la carte b) de la Figure 3.10 67
3.12 Carte résultante pour l'IMP#1 de la différence entre la carte c) et la carte d) de la Figure 3.10 67
3.13 Carte résultante d'une analyse temporelle du rayonnement électromagnétique pour l'IMP#2 pour une tension d'alimentation de cœur à 1.25 V. 68
3.14 Moyenne des densités spectrales de puissance, sur tout le circuit, pour l'IMP#2 pour une tension d'alimentation de cœur à 1.25 V. 69
3.15 Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#2 pour une tension d'alimentation de cœur à 1.25 V et de 1.38 V. 69
3.16 Zoom sur la différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#2 pour une tension d'alimentation de cœur à 1.25 V et de 1.38 V. 70
3.17 Cartes résultantes de l'analyse fréquentielle pour l'IMP#2 pour différents paramètres : a) V = 1.25 V et $\delta f = [293-298MHz]$ b) V = 1.38 V et $\delta f = [293-298MHz]$ c) V = 1.25 V et $\delta f = [328-334MHz]$ d) V = 1.38 V et $\delta f = [328-334MHz]$. 71
3.18 Carte résultante pour l'IMP#2 de la différence entre la carte a) et la carte b) de la Figure 3.17 72
3.19 Carte résultante pour l'IMP#2 de la différence entre la carte c) et la carte d) de la Figure 3.17 72
3.20 Carte résultante d'une analyse temporelle du rayonnement électromagnétique pour l'IMP#3 pour une tension d'alimentation de cœur à 1.24 V. 73
3.21 Moyenne des densités spectrales de puissance, sur tout le circuit, pour l'IMP#3 pour une tension d'alimentation de cœur à 1.24 V. 74
3.22 Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#3 pour une tension d'alimentation de cœur à 1.24 V et de 1.30 V. 74
3.23 Zoom sur la différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#3 pour une tension d'alimentation de cœur à 1.24 V et de 1.30 V. 75
3.24 Cartes résultantes de l'analyse fréquentielle pour l'IMP#3 pour différents paramètres : a) V = 1.24 V et $\delta f = [294-299MHz]$ b) V = 1.30 V et $\delta f = [294-299MHz]$ c) V = 1.24 V et $\delta f = [307-312MHz]$ d) V = 1.30 V et $\delta f = [307-312MHz]$. 76
3.25 Carte résultante pour l'IMP#3 de la différence entre la carte a) et la carte b) de la Figure 3.24 77

3.26 Carte résultante pour l'IMP#3 de la différence entre la carte c) et la carte d) de la Figure 3.24 77
3.27 Schéma descriptif de l'agencement des blocs (floorplan) pour l'implantation sur la cible Microsemi Fusion. 78
3.28 Carte résultante d'une analyse temporelle du rayonnement électromagnétique pour l'IMP#4 pour une tension d'alimentation de cœur à 1.5 V. 79
3.29 Moyenne des densités spectrales de puissance, sur tout le circuit, pour l'IMP#4 pour une tension d'alimentation de cœur à 1.5 V. 79
3.30 Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#4 pour une tension d'alimentation de cœur à 1.5 V et de 1.7 V. 80
3.31 Zoom sur la différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#4 pour une tension d'alimentation de cœur à 1.5 V et de 1.7 V. 80
3.32 Cartes résultantes de l'analyse fréquentielle pour l'IMP#4 pour différents paramètres : a) V = 1.5 V et $\delta f = [331 - 354MHz]$ b) V = 1.7 V et $\delta f = [331 - 354MHz]$ c) V = 1.5 V et $\delta f = [376 - 399MHz]$ d) V = 1.7 V et $\delta f = [376 - 399MHz]$. 81
3.33 Carte résultante pour l'IMP#4 de la différence entre la carte a) et la carte b) de la Figure 3.32 82
3.34 Carte résultante pour l'IMP#4 de la différence entre la carte d) et la carte c) de la Figure 3.32 82
3.35 Sonde LANGER RF-R400-1 utilisée pour la mesure à deux sondes. . 84
3.36 Principe d'analyse à base d'une sonde qui mesure le rayonnement électromagnétique local et d'une sonde qui mesure le rayonnement électromagnétique global. 84
3.37 Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#3 pour la méthode de mesure à deux sondes. . 85
3.38 Carte résultante de la méthode à deux sondes. 86

4.1 Implantation des oscillateurs en anneau pour la Cible#1 (cette figure ne représente pas un floorplan précis de l'implantation). 91
4.2 Architecture de test du générateur de nombre aléatoires - Cible#2 . 92
4.3 Rapport $DFTRi = Y_{f_{inj}}/Y_{f_{RO_i}}$ en fonction de la fréquence d'injection pour les signaux de sorties de chaque oscillateur en anneau (RO_1 à RO_4). 95
4.4 Transformée de Fourier des signaux V_1 et V_3 sous : a) des conditions normales de fonctionnement b) une perturbation électromagnétique harmonique avec une fréquence égale à 309.7 MHz et avec $P_{transmise}$ = 3 mW. 95

4.5 Superposition en persistance de traces acquises successivement (trait gras) et traces moyennes (trait fin) de V_1 et V_3 pendant : a) des conditions de fonctionnement normales et b) une attaque électromagnétique harmonique avec $P_{transmise}$ = 3 mW et f_{inj} = 309.7 MHz. . 97
4.6 a) Différence de phase entre V_1 et V_3 au cours du temps b) Histogramme des phases. 97
4.7 Flots de bits (120x32) produits par le générateur de nombres aléatoires sous des puissances différentes d'injection et une fréquence d'injection de 309.7 MHz - De la gauche vers la droite : a) Pas d'injection b) $P_{tranmise}$ = 210 μW c) $P_{tranmise}$ = 260 μW d) $P_{tranmise}$ = 300 μW 99
4.8 a) Signal modulé en amplitude en entrée de l'amplificateur de puissance - b) Flot de bit en sortie du générateur (à lire de bas en haut et de gauche à droite) - c) Biais en % de la suite de bits génerée. . . 100
4.9 Modélisation électrique proposée par Adler du phénomène de verrouillage des oscillateurs. 102
4.10 Circuit utilisé en simulation pour étudier le phénomène de verrouillage. 103
4.11 Spectres fréquentiels des sorties des deux oscillateurs pour des conditions normales de fonctionnement. 104
4.12 Zone de verrouillage pour le premier oscillateur. 105
4.13 Zones de verrouillage pour deux oscillateurs. 106
4.14 Spectres fréquentiels des sorties des deux oscillateurs pour une fréquence d'injection de 309 MHz et pour un courant de 20 μA (point B sur la Figure 4.13) 107
4.15 Amplitude de la fréquence nominale du premier oscillateur dans le spectre fréquentiel de la sortie de l'oscillateur en fonction du courant d'injection pour plusieurs fréquences d'injection différentes. 108
4.16 Amplitude de la fréquence d'injection dans le spectre fréquentiel de sa sortie en fonction du courant d'injection pour plusieurs fréquences d'injection. 108
4.17 Durée entre les fronts consécutifs des deux oscillateurs pour plusieurs paramètres d'injection. 109
4.18 Zone de verrouillage pour le premier oscillateur pour une plage fréquentielle de 250 MHz à 1 GHz. 110
4.19 Signal de sortie, et son spectre fréquentiel, du premier oscillateur pour une fréquence d'injection de 640 MHz et une intensité de 180 μA (jeu 1). 111
4.20 Signal de sortie, et son spectre fréquentiel, du premier oscillateur pour une fréquence d'injection de 640 MHz et une intensité de 50 μA (jeu 2). 112
4.21 Signal de sortie, et son spectre fréquentiel, du premier oscillateur pour une fréquence d'injection de 640 MHz et une intensité de 145 μA. . . 112
4.22 Evolution de la fréquence d'interférence 113
4.23 Circuit utilisé pour étudier l'effet du verrouillage des oscillateurs sur la sortie du générateur. 114

4.24 Résultats de simulation pour différents paramètres d'injection. De haut en bas : Horloge, sortie pour f_{inj} = 285 MHz et I_{pert}= 0 μA, sortie pour f_{inj} = 285 MHz et I_{pert}= 5 μA et sortie pour f_{inj} = 285 MHz et I_{pert}= 15 μA. 115
4.25 Schéma de principe du circuit utilisé pour étudier l'effet de l'injection électromagnétique sur l'extraction d'entropie. 116
4.26 Observation des signaux S_{FF1}, S_{FF2}, S_{XOR} et H pour étudier l'effet de la perturbation électromagnétique sur la porte OU exclusif. 117
4.27 Observation des signaux H, S_{XOR} et S_{FF3} pour vérifier le comportement de la bascule FF3 sous l'effet de la perturbation électromagnétique. Le signal $S_{FF3normal}$ est une reconstruction du signal que l'on devrait obtenir en sortie de la bascule FF3 sans perturbation électromagnétique. 118
4.28 Premier modèle de l'effet de l'injection électromagnétique harmonique sur les bascules D - superposition d'un générateur de signal sinusoïdal sur l'arbre d'horloge. 119
4.29 Second modèle de l'effet de l'injection électromagnétique harmonique sur les bascules D - superposition de générateurs de signaux sinusoïdaux sur les deux rails d'alimentation. 120
4.30 Résultat de simulation pour le premier modèle. 120
4.31 Résultat de simulation pour le second modèle. 121
4.32 Topologie classique du réseau d'alimentation et de l'arbre d'horloge d'un FPGA 122
4.33 Front descendant du signal d'horloge pour différents réglages de la perturbation sinusoïdale. 123
4.34 Représentation du canal électromagnétique et du processus relatif à l'attaque. 125
4.35 Zoom sur un front descendant de l'horloge perturbée (H_{pert}) dans le but d'expliquer le choix pour la construction des inégalitées. 127
4.36 Graphique de la fonction $f(x)$ qui représente l'inéquation finale de l'Equation 4.17, pour x allant de -1 à 1. 128
4.37 Graphique qui donne la probabilité de succès de l'attaque en fonction des paramètres de l'attaque avec Vdd = 3.3 V et T_F = 20 ns. 129
4.38 Résultats de simulation électrique pour les trois jeux de paramètres. De haut en bas : signal d'horloge H, sortie de la bascule pour le premier jeu ($S_{FF-310MHz}$), le second jeu $S_{FF-185MHz}$ et le troisième jeu $S_{FF-45MHz}$ de paramètres d'injection. 130

A.1 Répartition des zones de champ en fonction de la distance avec l'antenne. 149
A.2 Modèle de rayonnement magnétique d'un fil considéré infini. 151
A.3 Vue en coupe d'une portion d'un circuit intégré. 152

Liste des tableaux

1.1 Tableau récapitulatif des différentes attaques sur les générateurs d'aléa. 16

2.1 Tableau récapitulatif des différences entres les deux types d'attaques actives qui exploitent le canal caché électromagnétique. 37
2.2 Mise en évidence des différences de conception entre les principes de génération d'aléa et les autres modules cryptographiques 38
2.3 Valeur de l'amplitude du champ mesurée à l'oscilloscope pour différentes orientations de sonde. 45

4.1 Valeurs de l'information mutuelle, obtenues pour différentes puissances d'injection, pour les différents couples d'oscillateurs en anneau. 96
4.2 Paramètres statistiques du flot de bits de sortie du générateur. . . . 99

A.1 Taille de la zone de champ proche en fonction de la fréquence de la source. 150

Glossaire

AES : Algorithme standard de chiffrement symétrique (Advanced Encryption Standard)

ARQS : Approximation des régimes quasi-stationnaires

ASIC : Circuit intégré propre à une application (Application Specific Integrated Circuit)

CEM : Compatibilité électromagnétique

CEMA : Analyse de corrélation du rayonnement électromagnétique (Correlation ElectroMagnetic Analysis)

CMOS : Technologie de fabrication des transistors modernes (Complementary Metal Oxide Semiconductor)

COMP128 : Implantation des algorithmes A3 et A8 définis dans les standards de télécommunications mobiles.

CPA : Analyse de corrélation de la consommation de courant (Correlation Power Analysis)

DEMA : Analyse différentielle du rayonnement électromagnétique (Differential ElectroMagnetic Analysis)

DES : Premier algorithme standard de chiffrement symétrique (Data Encryption Standard)

DPA : Analyse différentielle de la consommation de courant (Differential Power Analysis)

EM : ElectroMagnétique

EMA : Analyse électromagnétique (ElectroMagneticAnalysis)

EPROM : Mémoire morte reprogrammable (Erasable Programmable Read Only Memory)

FIFO : Système de mémoire de type premier arrivé, premier sorti (First In - First Out)

FPGA : Composant électronique disposant d'un réseau de portes programmables (Field Programmable Gate Array)

GTEM : Cellule émettrice utilisée en compatibilité électromagnétique (Gigahertz Transverse ElectroMagnetic)

NSA : Agence américaine de sécurité (National Security Agency)

OTAN : Organisation du traité nord atlantique

PCB : Circuit imprimé (Printed Circuit Board)

PLL : Boucle à verrouillage de phase (Phase-Locked Loop)

PRNG : Générateur de nombres pseudo-aléatoires (Pseudo Random Number Generator)

RAM : Mémoire vive (Random Access Memory)

RO : Oscillateur en anneau (Ring Oscillator)

RSA : Algorithme de chiffrement à clé publique

SEMA : Analyse simple du rayonnement électromagnétique (Simple ElectroMagnetic Analysis)

SPA : Analyse simple de la consommation de courant (Simple Power Analysis)

SRAM : Mémoire statique (Static Random Access Memory)

TRNG : Générateur de nombres réellement aléatoires (True Random Number Generator)

Unités

V :	Volt
A :	Ampère
W :	Watt
Hz :	Hertz
$^\circ$ C :	Degré Celsius
s :	Seconde
F :	Farad ($A.V^{-1}.s$)
C :	Coulomb ($A.s$)
H :	Henry ($V.A^{-1}.s$)

Remerciements

Je tiens à remercier en tout premier lieu les membres du jury qui ont accepté d'évaluer mes travaux accomplis pendant ces trois années de doctorat. Merci à M. François-Xavier Standaert - Professeur à l'UCL et M. Olivier Sentieys - Professeur à l'Université de Rennes d'avoir accepté d'être rapporteur de ce manuscrit.

Merci également à Philipe Maurine, HDR au LIRMM et Julien Francq de la société CASSIDAN pour avoir accepté d'examiner mon manuscrit et de faire partie de mon jury.

Merci à Robert Fouquet de m'avoir proposé initialement de réaliser un thèse au sein du laboratoire Hubert Curien.

Merci à Lilian Bossuet d'avoir encadré mes travaux, d'avoir su m'apporter de l'aide d'un point de vue scientifique, et également d'avoir été patient avec moi.

Merci à Alain Aubert d'avoir co-encadré mes travaux et de m'avoir donné un regard critique toujours utile pour améliorer mes travaux.

Merci à Viktor Fischer pour m'avoir accueilli au sein de l'équipe et pour ses bons conseils dans le but d'améliorer toujours l'écriture de mes articles scientifiques.

Merci à Florent Bernard et Pierre-Louis Cayrel pour l'aide qu'ils ont pu m'apporter quand mes connaissances mathématiques faisaient défaut.

Merci à Nathalie Bochard pour l'aide qu'elle a toujours su m'apporter sur le plan technique.

Merci à Patrick Haddad pour les discussions toujours intéressante et constructive qu'on a pu avoir ensemble.

Merci à tout les membres de l'équipe pour la bonne ambiance générale qui y règne et qui rend le travail beaucoup plus facile.

Merci à François Poucheret et Philippe Maurine pour m'avoir donné la chance de travailler en collaboration avec eux à Montpellier. L'accueil au LIRMM a toujours été très bon et je les remercie pour cela.

Merci à mes parents qui ont m'ont toujours aidé. Merci également à mes amis.

Introduction

Contexte

Anciennement réservée à des utilisations purement militaires, la protection des communications, ou encore cryptographie, s'est de plus en plus tournée vers des utilisations publiques (bancaires, télécommunications, etc...) du fait de la démocratisation et de l'utilisation de plus en plus intensive de nombreux appareils nomades (carte à puce, téléphone portable, tablette, ...). Protéger la totalité des communications représente un enjeu important de notre société, surtout dans un cadre d'utilisation nomade, où, la consommation de courant et la place sont contraintes.

Les principes cryptographiques utilisés en cryptographie sont supposés mathématiquement sûrs (jusqu'à preuve du contraire), et sont embarqués dans les applications précédemment citées soit sous forme logicielle (calcul effectué par un microprocesseur) ou matérielle (calcul effectué dans un circuit électronique dédié). Cependant, ces implantations, même si l'algorithme est sûr, recèlent des faiblesses. Il est notamment possible d'extraire, en étudiant précisément l'activité des circuits (consommation de courant par exemple), une information secrète enfouie dans ces circuits.

Il est également possible de perturber le fonctionnement d'un circuit intégré afin d'insérer une faute dans le calcul. En ayant une maîtrise de la faute produite (nombre de bits fautés, position de l'erreur dans le calcul), cette dernière permet par la suite d'effectuer une analyse de la propagation de la faute (cette propagation étant dépendante de la clé privée).

Ces deux types d'attaques représentent donc une menace importante pour la protection des données et des communications et s'appuient sur différentes techniques dont notamment l'exploitation émergente des champs électromagnétiques.

C'est dans ce contexte que s'inscrit le projet EMAISeCi (ElectroMagnetic Analysis and Injection of Secure Circuits), financé par l'Agence Nationale de la Recherche, pour lequel les travaux présentés dans ce manuscrit ont été réalisés. Ce projet s'articule autour de plusieurs entités, académiques et industrielles, à savoir :

- CEA-LETI,
- École Nationale Supérieure des Mines de Saint-Etienne,
- Laboratoire Hubert Curien,
- LIRMM, porteur du projet,
- ST Microelectronics,
- TIMA.

La motivation principale de la mise en place de ce projet est l'étude de l'utilisation du canal caché électromagnétique non seulement pour les attaques passives, mais aussi et surtout pour les attaques actives visant des implantations cryptogra-

phiques matérielles. Du point de vue des attaques actives, le travail se concentre sur l'étude de la faisabilité et la mise en place de nouvelles techniques d'attaque.

Objectif

Nous avions pour mission, au sein de notre équipe, d'étudier les attaques (passives et actives) utilisant le canal caché électromagnétique sur la génération d'aléa.

Contribution

Les principales contributions présentées dans ce manuscrit sont :

- Développement d'un banc d'analyse du rayonnement électromagnétique. Le matériel qui compose ce banc est particulièrement adapté à l'étude du rayonnement électromagnétique des générateurs d'aléa. Ce banc a déjà été dupliqué par la société CASSIDIAN Cyber Security et prochainement par le laboratoire Lab-STICC.
- Développement d'une analyse du rayonnement électromagnétique adaptée au générateur d'aléa à base d'oscillateurs en anneau. Cette analyse permet de retrouver la position et la fréquence des oscillateurs qui composent le générateur.
- Mise en évidence de la possibilité d'attaquer les générateurs à base d'oscillateurs en anneau en injectant un champ électromagnétique harmonique.
- Réalisation d'un modèle électrique du phénomène de verrouillage des oscillateurs en anneau induit par le champ électromagnétique harmonique.
- Réalisation d'un modèle électrique et mathématique de l'effet du champ électromagnétique harmonique sur les bascules D qui composent le générateur d'aléa.

Organisation du manuscrit

Le Chapitre 1 présente la théorie liée aux éléments du contexte dans lequel s'inscrit la thèse. Dans ce chapitre, nous montrerons la place de la génération d'aléa dans la cryptographie. Nous présenterons également les techniques de génération d'aléa dans l'électronique moderne, et nous détaillerons particulièrement le générateur utilisé comme cas d'étude dans ce manuscrit. Ensuite, nous réaliserons un bref aperçu des différentes techniques d'attaques matérielles existantes (en omettant volontairement les attaques utilisant le canal caché électromagnétique). Enfin nous argumenterons sur l'intérêt d'attaquer la génération d'aléa.

Le Chapitre 2 présente un état de l'art détaillé des attaques qui utilisent le canal caché électromagnétique. Nous présentons également dans ce chapitre le matériel - c'est à dire le banc d'analyse électromagnétique, celui d'injection électromagnétique, et les cartes électroniques - utilisé pour réaliser les travaux expérimentaux effectués pendant ces trois années.

Le Chapitre 3 détaille les différentes techniques de cartographie exploitant le rayonnement électromagnétique des circuits électroniques. Nous présentons la méthode de cartographie que nous avons développée pour analyser le rayonnement électromagnétique des générateurs d'aléa, puis nous donnons les résultats de cette analyse pour différentes implantations de générateur d'aléa, et ce, sur des cibles avec des technologies différentes.

Enfin le Chapitre 4 présente une étude expérimentale de l'effet d'une perturbation électromagnétique harmonique sur des oscillateurs en anneau premièrement, puis sur un générateur d'aléa ensuite. Dans ce chapitre, nous étudions également, d'un point de vue théorique (par des simulations électriques), en constituant des modèles électriques et mathématiques, l'interaction de l'injection électromagnétique harmonique sur les oscillateurs en anneau et le générateur d'aléa. Cette étude nous permet de conclure sur le danger d'une telle attaque sur un système cryptographique.

Chapitre 1

Securité des systèmes de génération d'aléa

Ce chapitre pose le cadre dans lequel les travaux présentés dans ce manuscrit s'inscrivent. Nous présenterons dans ce chapitre la place de la génération d'aléa dans la cryptographie moderne. Nous étudierons également le générateur de nombre réellement aléatoire retenu comme cas d'étude. Enfin, nous étudierons les attaques matérielles sur ces générateurs et l'intérêt de telles attaques.

1.1 Les générateurs de nombres aléatoires

Les générateurs de nombres aléatoires sont très utilisés pour plusieurs types d'applications, que ce soit les jeux de hasard, les simulations nécessitant de l'aléa (méthode de Monte-Carlo par exemple) ou encore la cryptographie matérielle. Nous allons nous intéresser particulièrement à leur utilisation dans ce dernier domaine.

1.1.1 La génération d'aléa dans la cryptographie matérielle

La génération d'aléa est une partie intégrante d'un système cryptographique, au même titre que les chiffreurs à clé publique ou privée, les fonctions de hachage, etc. Elle peut être utilisée pour générer :

- des clés secrètes,
- des vecteurs d'initialisation,
- des masques pour des contremesures contre l'analyse de la consommation de courant,
- ...

Le principe de Kerckhoffs, sur lequel se base la cryptographie moderne (volonté de créer des standards cryptographiques bien étudiés et mathématiquement sûrs), exprime clairement que le secret ne doit résider que dans la clé de chiffrement. Il est donc important, dans un système cryptographique, de faire particulièrement attention aux modules qui vont stocker ces clés ou encore les générer. Il est donc irréaliste de penser que la sécurité du système cryptographique se résume seulement à la protection du chiffreur (un système cryptographique où seul le chiffreur est protégé peut être vu comme un colosse au pied d'argile). En effet, la sécurité globale d'un système (en règle général) dépend de la sécurité de tous les blocs qui le constituent. Il est donc important que la sécurité de chaque élément qui constitue le système cryptographique soit étudiée et vérifiée (et tout particulièrement les éléments qui manipulent la clé secrète, dont le générateur de nombres aléatoires fait partie).

Typiquement, on peut trouver deux types de générateurs de nombres aléatoires dans un système cryptographique :

- Les générateurs de nombres réellement aléatoires, basés sur un processus d'extraction d'entropie issue d'un bruit physique. Nous détaillerons plus en détail dans la section suivante ce type de générateurs.
- Les générateurs de nombres pseudo-aléatoires, basés sur un algorithme complexe (par exemple un algorithme utilisant une suite de Fibonacci ou une congruence linéaire). Dans ce cas une suite déterministe permet de produire un flux de bits qui possède des propriétés statistiques proches du hasard. Ces générateurs permettent, au contraire des générateurs de nombres réellement aléatoires, d'obtenir un débit élevé.

C'est pour ce type de générateurs (pseudo-aléatoires) que les tests statistiques FIPS 140.2 FIPS [2001], NIST (Rukhin et al. [2001]) ou encore DIEHARD (Marsaglia [1995]), qui permettent de tester la qualité de la suite produite, ont été introduits. L'utilisation première de ces tests n'est donc pas de tester les flux de bits

produits par les générateurs de nombres réellement aléatoires. Cependant ils sont la plupart du temps utilisés pour attester de la qualité de ces générateurs, ce qui conduit parfois à qualifier de "réellement aléatoire" une suite déterministe. Afin d'éviter ce type d'erreur, une refonte de l'AIS31 (méthode d'évaluation des générateurs d'aléa proposée par le gouvernement allemand) est en cours et elle inclut l'obligation de soumettre un modèle de la source d'aléa exploitée dans le cas de générateur de nombres réellement aléatoires.

Nous allons maintenant nous intéresser aux générateurs de nombres réellement aléatoires qui constituent les cibles des travaux présentés dans ce manuscrit.

1.1.2 Générateur de nombres réellement aléatoires

Comme cela a été dit précédemment, les générateurs de nombres réellement aléatoires (TRNG pour True Random Number Generator) ou encore générateur de nombres aléatoires physiques (PRNG - Physical Random Number Generator) sont des générateurs d'aléas basés sur l'exploitation d'une source physique d'aléa. Cette source d'aléa peut être de nature diverse, tant que cette dernière est basée sur des phénomènes purement aléatoires. Par exemple, elle peut être liée à l'apparition de particules dans le vide ([Symul et al., 2011],[ANU, 2011]) ou encore à la réflexion ou transmission à travers une surface semi-réfléchissante d'un photon ([QUANTIS, 2006]). L'extraction de l'entropie de ces deux sources d'aléas dites quantiques (car basées sur des phénomènes très fortement liés à la physique quantique), ne sont pas facilement (voir pas du tout) implantables dans un circuit numérique classique. Il convient de noter que le deuxième générateur ([QUANTIS, 2006]), commercialisé sous forme d'un circuit dédié à la génération d'aléa, est très onéreux (environ 1000 dollars). Ces générateurs, conçus pour des applications bien particulières, sont en dehors du cadre des travaux dans lesquels s'inscrivent cette thèse. Ainsi nous les laisserons de côté pour nous concentrer sur les générateurs de nombres réellement aléatoires intégrables dans des circuits intégrés numériques avec les technologies disponibles aujourd'hui.

Dans le cadre de l'utilisation embarquée dans un circuit intégré numérique d'un générateur de nombres réellement aléatoires, ce dernier est composé (le schéma présenté à la Figure 1.1 résume la constitution d'un générateur réellement aléatoire) :

- D'une source de bruit numérique : cette source de bruit comporte deux parties, une source d'aléa physique et un extracteur d'entropie qui permet de transformer la composante physique aléatoire en un signal numérique. Cette source de bruit numérique doit bien évidemment fournir le plus d'entropie par bit possible, avec le meilleur débit possible, et être insensible aux variations environnementales (température, tension d'alimentation). La source de bruit physique, qui se base la plupart du temps sur l'exploitation de bruits intrinsèques aux transistors, est supposée comme étant non manipulable.
- D'un système de post-traitement des données (cryptographique ou arithmétique) : ce module peut être ajouté à la sortie de la source de bruit numérique dans le but d'améliorer les propriétés statistiques de la suite produite, sans

pour autant ajouter de l'entropie à la suite (en général, seule l'entropie par bit peut augmenter, car pour la plupart des systèmes de post-traitement, plusieurs bits sont compressés pour n'en former qu'un).

– D'un système de tests embarqués : le système de tests embarqués permet d'évaluer en temps réel (ou non suivant la complexité du test opéré - un test complexe peut être chronophage et entraîner une surconsommation d'énergie) la qualité de la source de bruit numérique. Il peut également vérifier que le générateur n'est pas complètement hors service. Les nouveaux standards de tests des générateurs de nombres réellement aléatoires imposent la conception d'un test adapté au générateur proposé. Cette partie du générateur est donc, au même titre que la source de bruit numérique, d'une grande importance quant à la sécurité globale du système cryptographique.

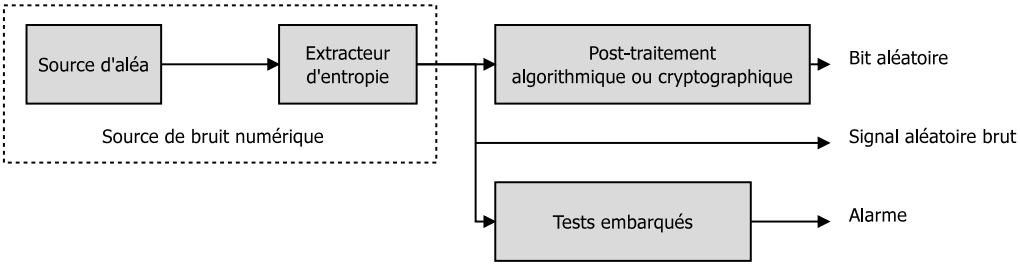

FIG. 1.1 – Schéma de principe d'un générateur de nombres aléatoires

On retrouve dans la littérature trois grands types de générateurs implantables dans un circuit intégré numérique :

– Les générateurs utilisant les incertitudes temporelles (ou encore jitter en anglais) d'horloges.
– Les générateurs utilisant la métastabilité des bascules.
– Les générateurs hybrides (qui sont un mélange d'une source d'aléa physique et d'une source purement déterministe). La structure déterministe utilise périodiquement la sortie du générateur comme graine pour renouveler la génération déterministe de nombres aléatoires.

La Figure 1.2 présente un historique d'apparition de différents principes de génération d'aléa. Il est évident, en regardant cette figure, que la principale source d'aléa utilisée dans les circuits électroniques numériques est l'incertitude temporelle.

Dans la suite, nous ne détaillerons pas le principe de fonctionnement de tous les générateurs existants, le but n'étant pas de faire un état de l'art complet de la génération d'aléa dans les circuits numériques modernes, mais nous nous intéresserons seulement au seul générateur utilisé dans la suite comme cas d'étude. Les deux articles inscrits en blanc dans la Figure 1.2 ([Sunar et al., 2007] et [Wold and Tan, 2008]) décrivent le principe du générateur que nous avons choisi d'utiliser comme cas d'étude. Ces générateurs, à base d'oscillateurs en anneau sont les plus utilisés et étudiés, et ils sont surtout les plus faciles à implanter dans un circuit intégré numérique. Nous détaillerons par la suite ces principes.

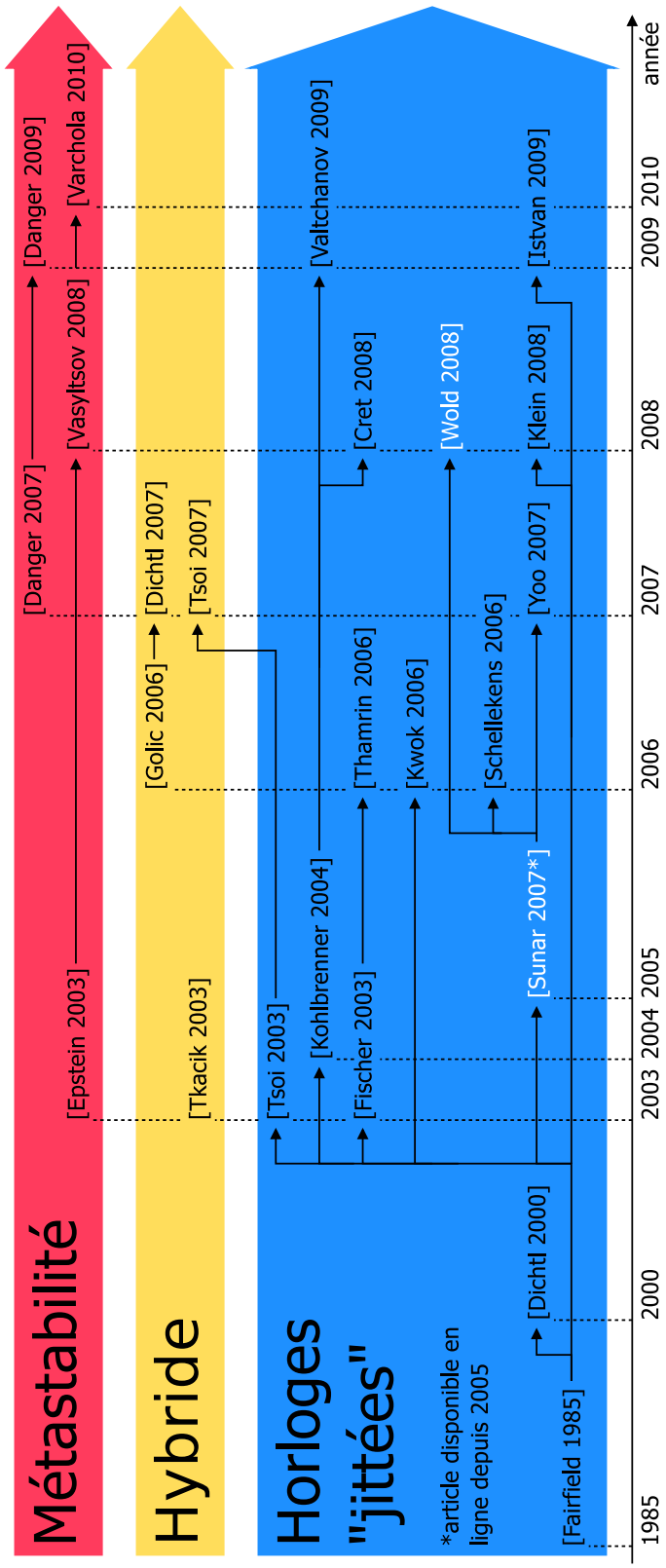

FIG. 1.2 – Historique d'apparition des publications relatives aux différents principes de génération de nombres réellement aléatoires.

Dans la suite, pour faciliter la lecture, les termes générateur de nombres aléatoires ou générateur d'aléa feront référence aux générateurs de nombres réellement aléatoires.

1.1.3 Générateur à base d'oscillateurs en anneau de [Sunar et al., 2007] et amélioré par [Wold and Tan, 2008].

Ce générateur est bien évidemment classé dans les générateurs utilisant l'incertitude temporelle d'horloges (une grande partie des générateurs identifiés dans la Figure 1.2 est réalisée sur la base d'une structure d'oscillateurs en anneau). L'une des principales raisons de sa vaste utilisation vient du fait que l'oscillateur en anneau (ou RO pour Ring Oscillator) est la source d'horloge la plus facile à implanter dans un circuit numérique (que ce soit un ASIC ou un FPGA).

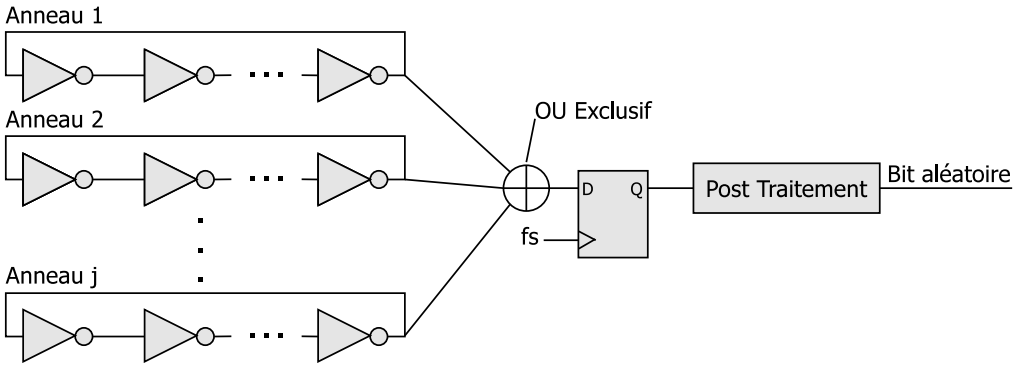

FIG. 1.3 – Schéma de principe du générateur proposé par [Sunar et al., 2007].

Nous avons choisi de nous intéresser plus particulièrement au principe proposé par les auteurs de [Sunar et al., 2007]. Le schéma de principe du générateur est présenté à la Figure 1.3. Il est composé d'un groupe d'oscillateurs en anneau dont les sorties sont combinées via un arbre de OU-Exclusifs. La sortie de cet arbre est ensuite échantillonnée par une horloge (fs).

Cependant, si les fréquences des oscillateurs en anneau sont élevées (elles sont en général de l'ordre de la centaine de MHz), cette structure ne fonctionne pas correctement. En effet, les transitions à l'entrée de l'arbre de OU-Exclusifs sont trop fréquentes et il n'est pas possible d'imaginer une structure combinatoire qui puisse gérer autant de transitions avec les technologies actuelles. La sortie de l'arbre de OU-Exclusif n'est donc pas, pour ce générateur une sortie purement numérique, mais une sortie analogique dûe aux sollicitations trop rapides en entrée de l'arbre. L'aléa est certes présent en sortie du générateur (la bascule finale vient échantillonner une sortie analogique, ce n'est pas un cadre d'utilisation classique et la sortie de la bascule n'est pas constante), mais ne correspond pas au modèle d'aléa (basé sur l'incertitude des horloges produites par les oscillateurs) présenté dans l'article. Ce générateur n'a été testé par ses auteurs qu'en simulation, c'est donc pour cela que la structure n'a pas été mise en défaut lors de cette première étude.

Pour résoudre ce problème d'arbre d'OU-Exclusifs, les auteurs de [Wold and Tan, 2008] ont légèrement modifié l'implantation proposée dans [Sunar et al., 2007] (voir Figure 1.3) en insérant des bascules intermédiaires entre la sortie de chaque oscillateur et l'arbre d'OU-Exclusifs. Le schéma de principe de cette implantation est visible à la Figure 1.4. Les bascules assurent le bon fonctionnement de l'arbre de OU-Exclusifs, quel que soit le nombre d'oscillateurs en anneau et quelles que soient leurs fréquences.

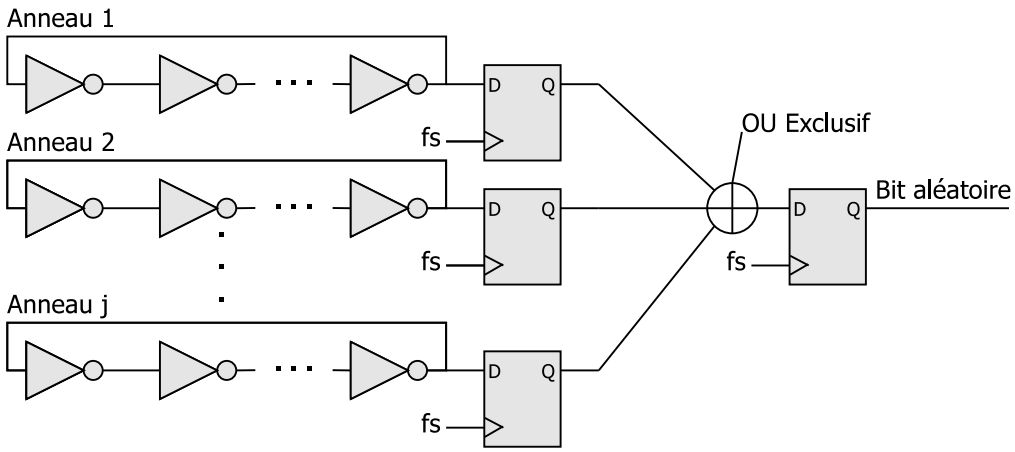

FIG. 1.4 – Schéma de principe du générateur amélioré, proposé par [Wold and Tan, 2008].

Pour les deux principes, il est important de noter, que chaque oscillateur est supposé être indépendant de tous les autres. En pratique, cela signifie que chaque oscillateur a une fréquence différente. Les différences de fréquence (naturelle) sont dues aux légères différences des paramètres des transistors (le processus de fabrication n'est pas linéaire sur tout le circuit) et les différences entre les temps de propagation entre chaque inverseur. Il est d'ailleurs intéressant d'ajouter que ces différences de fréquence de chaque oscillateur introduisent une composante pseudo-aléatoire au flux de bits généré par le générateur. Les auteurs de [Bochard et al., 2010] ont remarqué que des suites binaires produites par un générateur de type [Wold and Tan, 2008] en simulation ModelSim (donc avec des signaux d'horloges sans incertitude temporelle) passent les tests FIPS 140.2 si le nombre d'oscillateurs est supérieur à 18 (ce nombre va dépendre des fréquences de fonctionnement des oscillateurs, mais aussi de la fréquence d'échantillonnage).

La Figure 1.5 présente le phénomène d'accumulation de l'incertitude temporelle. On suppose que le premier front sélectionné comme point de départ de l'observation est fixe (temporellement parlant). Les fronts suivants vont être influencés par le bruit des transistors et vont donc avoir une incertitude temporelle. Cette incertitude temporelle peut avoir des répartitions différentes suivant divers influences. Il est bien évident que les fronts descendants ont eux aussi des incertitudes temporelles, mais pour ne pas surcharger la figure, nous ne les avons pas représentées.

Dans la Figure 1.5, nous avons choisi de représenter cette répartition comme une pure gaussienne (qui est recherchée en terme de génération d'aléa), mais cette répartition peut potentiellement contenir une composante déterministe (par exemple, si l'étage d'alimentation de la carte sur laquelle se trouve le circuit est de mauvaise qualité, elle peut influencer cette répartition). A chaque nouveau front, l'incertitude temporelle va s'accumuler, et donc la déviation standard de la répartition associée à cette incertitude va augmenter également (sa moyenne va quant à elle rester la même, la fréquence moyenne de l'oscillateur n'étant pas influencée par le jitter). De manière à assurer une influence de l'incertitude temporelle sur le bit aléatoire produit, il est nécessaire d'attendre suffisamment longtemps de manière à avoir accumulé suffisamment de jitter (la représentation de la Figure 1.5 n'est pas réaliste, la quantité de jitter n'est pas aussi importante, il faut en général compter une taille de jitter égale à environ 1/1000 de la période du signal étudié). En règle général, plus la fréquence d'échantillonnage est lente, plus le bit aléatoire produit a une chance d'être influencé par l'incertitude temporelle et donc d'être réellement aléatoire. Cette propriété est étudiée dans [Yoo et al., 2010], qui montre que plus le rapport entre la fréquence nominale de l'oscillateur et la fréquence d'échantillonnage est grand, plus la suite binaire produite par le générateur est de bonne qualité. Les auteurs de [Yoo et al., 2010] montrent également que le rapport entre la fréquence d'échantillonnage ne doit pas être un multiple de la fréquence moyenne des oscillateurs sous peine de réduire la qualité de l'aléa produit par le générateur.

En résumé, plus le nombre d'oscillateurs est important et plus leurs fréquences sont élevées, plus la composante pseudo-aléatoire du générateur sera importante. Plus la fréquence d'échantillonnage est faible, plus la composante purement aléatoire sera importante également (elle est aussi dépendante du nombre d'oscillateurs).

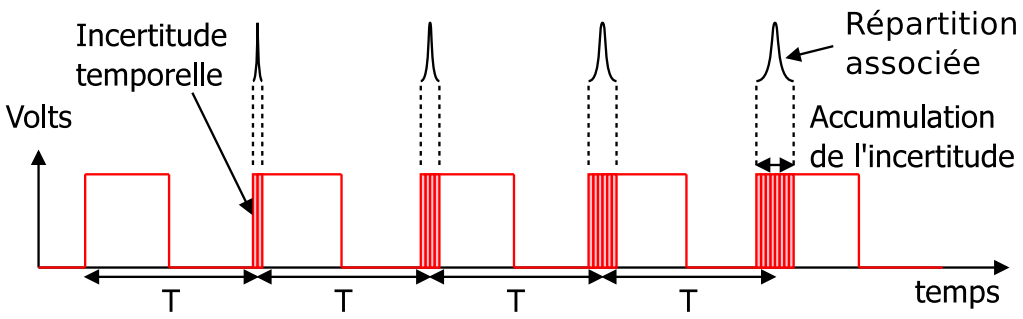

FIG. 1.5 – Principe de l'accumulation de l'incertitude temporelle dans un oscillateur en anneau.

Dans la suite, nous allons nous intéresser aux différentes techniques d'attaques sur les implantations matérielles de la génération d'aléa.

1.2 Attaques sur les générateurs d'aléa

Cette partie va présenter l'enjeu des attaques matérielles sur les générateurs d'aléa. Nous montrerons d'abord l'intérêt qu'il peut y avoir d'attaquer un générateur d'aléa. Nous présenterons ensuite un modèle de menaces et enfin un état de l'art des attaques sur les générateurs d'aléa.

1.2.1 Pourquoi attaquer un générateur d'aléa ?

D'un point de vue général, il est commun dans la communauté que l'étude de la robustesse des générateurs soit souvent délaissée au profit des autres blocs composant le système cryptographique, et notamment le chiffreur. Le chiffreur est certes une pièce maîtresse du système et requiert ainsi une attention particulière, mais il est également possible de corrompre l'intégrité totale du système cryptographique en attaquant le générateur.

Effectivement, qu'il soit utilisé pour de la génération de masque pour une contremesure contre l'analyse de la consommation de puissance, ou qu'il soit directement utilisé pour générer une clé secrète, la défaillance d'un générateur d'aléa peut être critique. Prenons un exemple simple - imaginons un système cryptographique simple, composé d'un chiffreur et d'un générateur, ce dernier fournissant une nouvelle clé secrète de 8 bits à intervalle régulier au chiffreur. Le générateur est bien sûr censé fournir une suite de bits ayant des propriétés statistiques convenables.

Une clé de 8 bits nous donne 256 clés possibles. Imaginons qu'un attaquant soit capable de biaiser le générateur de manière à lui faire produire plus de 0 que de 1. Par exemple, s'il peut, avec son attaque, obtenir au moins 6 bits (sur 8) à 0 (flot de bits produit par le générateur d'aléa biaisé à 50%), alors il est capable de réduire le champ de recherche sur les clés possibles à 37 clés, soit une réduction de clés de 7 fois. Ceci est bien sur un exemple simple, mais sur une clé de plus grande taille, si l'attaquant est capable de s'assurer un nombre de bits à une certaine valeur, il peut potentiellement accélérer une attaque par force brute, ou encore réduire la force d'une contremesure par masquage.

D'une manière générale, si l'attaquant fixe k bits à 0 ou 1 de la suite de n bits, le nombre de clés C possibles est donné par l'Equation 1.1.

$$C = \sum_{i=k}^{n} \binom{n}{i} = \sum_{i=k}^{n} \frac{n!}{i!(n-i)!} \tag{1.1}$$

Enfin, il peut être également intéressant de préférer attaquer le générateur plutôt que le chiffreur, car dans la plupart des systèmes cryptographiques, ce dernier est l'élément qui est le plus protégé (et donc par extension le plus dur et coûteux à attaquer).

1.2.2 Modèle de menaces sur les générateurs de nombres réellement aléatoires

La Figure 1.6 présente un modèle de menace sur la génération d'aléa. On retrouve la composition classique d'un générateur de nombres réellement aléatoires. Deux types d'attaques existent : actives et passives. Sur la Figure 1.6, les flèches en direction des modules représentent des attaques actives, et les autres des attaques passives.

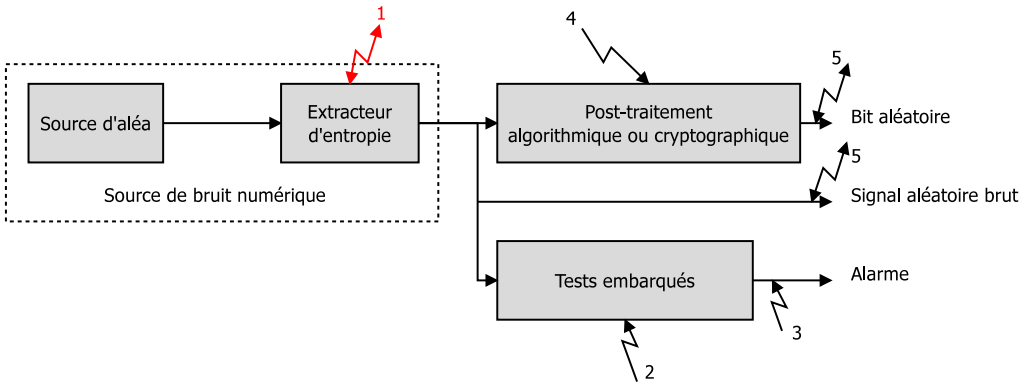

FIG. 1.6 – Modèle de menaces sur les générateurs de nombres réellement aléatoires.

Nous avons choisi de perturber, au plus proche de la source la génération d'aléa, à savoir l'extraction d'entropie (flèche rouge sur la Figure 1.6). Cependant, comme exposé dans la Figure 1.6, il se peut que la source numérique de bruit soit accompagnée soit d'un algorithme de post-traitement, ou encore d'un test embarqué. Dans ce cas là, il peut être nécessaire de venir également influencer ces modules, notamment le test embarqué (ou sa sortie), de manière à ce que l'attaque ne soit pas détectée.

1.2.3 Attaques sur les générateurs de nombres aléatoires

Dans cette partie, nous allons présenter les différentes attaques sur les générateurs de nombres réellement aléatoires jusqu'à présent publiées. Pour introduire cette section, nous donnerons les bases concernant les attaques sur les implantations matérielles cryptographiques.

1.2.3.1 Attaques matérielles

De manière générale, pour n'importe quel module d'un système cryptographique, on discerne deux types d'attaques, à savoir :

- Les attaques passives : Ces attaques ont pour but la collecte d'information sur le circuit ciblé. Elles visent principalement la collecte de la clé secrète de chiffrement manipulée par le chiffreur. Ces attaques vont utiliser différents canaux d'attaques passives (encore appelé canaux cachés), dont :

  - La consommation de courant du circuit, simple [Kocher, 1996] (Simple Power Analysis - SPA) ou différentiel [Kocher et al., 1999] (Differential Power Analysis - DPA).
  - Le son émis lors de la commutation des transistors d'un circuit (voir [Shamir and Tromer, 2004]).
  - Le rayonnement électromagnétique : Ce canal caché est détaillé dans le chapitre suivant.
  - Les photons émis lors de la commutation des transistors d'un circuit (voir [Ferrigno and Hlavac, 2008], [Skorobogatov, 2009] ou [Di-Battista et al., 2010]).
- Les attaque actives : Ces attaques ont pour but de perturber le fonctionnement d'une structure embarquée dans le circuit électronique ou encore par exemple d'injecter une faute dans un calcul, pour ensuite effectuer une analyse de la propagation de l'erreur comme par exemple dans [Piret and Quisquater, 2003] (la propagation de l'erreur va directement dépendre de la clé de chiffrement dans le cas où le calcul ciblé est un chiffreur à clé privée). Comme pour les attaques passives, ces attaques peuvent jouer sur plusieurs canaux de façon à perturber les circuits intégrés, dont :
  - les plages de fonctionnement des composants que ce soit en tension d'alimentation, en température ou en fréquence d'horloge (voir par exemple [Guilley et al., 2008]).
  - l'effet des photons sur les transistors, dont notamment les attaques qui exploitent l'émission photonique d'un LASER ([Skorobogatov and Anderson, 2002] ou [Schmidt and Hutter, 2007]).
  - l'effet de glitchs sur les signaux d'horloge ou sur l'alimentation ([Schmidt and Herbst, 2008] ou [Fukunaga and Takahashi, 2009]).
  - les champs électromagnétiques - comme pour les attaques passives qui utilisent ce type de canal, les attaques actives seront détaillées dans le chapitre suivant.

Ces attaques actives ou passives peuvent être de trois différents types :

- Attaques invasives : Ce type d'attaques est destructive pour la puce attaquée. Ces attaques nécessitent donc une préparation préalable du circuit à l'aide de différentes techniques (abrasion chimique ou mécanique, découpe de puce, faisceau d'ions focalisé ...). Ce sont des techniques très utilisées pour des études en rétro-ingénierie, dans le but par exemple de reconstituer le schéma électronique d'un circuit entier. Il est également possible de venir réaliser des mesures directement sur une interconnexion du circuit électronique.
- Attaques semi-invasives : Ce type d'attaques n'entraîne pas forcement la destruction de la puce. Elles utilisent des techniques similaires à celles utilisées pour des attaques invasives, mais le traitement de la puce s'arrête avant la couche de passivation de manière à ce que la puce puisse encore fonctionner par la suite. Ce type d'attaques a été notamment largement présenté dans [Skorobogatov, 2005].
- Attaques non-invasives : Ce type d'attaques n'implique en général pas le des-

truction de la puce, si l'attaquant a pris les précautions pour ne pas forcer la puce à fonctionner en dehors de sa zone limite de fonctionnement. En effet, aucun traitement de la puce n'est nécessaire pour ce type d'attaques.

1.2.3.2 Attaques pratiques sur les générateurs d'aléa

La première attaque pratique sur un générateur de nombres aléatoires a été présentée par les auteurs de [Markettos and Moore, 2009]. Cette attaque a été effectuée sur des générateurs à base d'oscillateurs en anneau. Elle consiste simplement à superposer sur le réseau d'alimentation d'un circuit un signal harmonique de manière à impacter les portes logiques avec ce signal perturbateur.

Les auteurs ont tout d'abord étudié l'effet d'une injection sur deux oscillateurs en anneau réalisés à l'aide de circuits CMOS embarquant des portes inverseuses (74HC04). Le premier oscillateur est composé de trois portes inverseuses, alors que le deuxième est composé de cinq portes inverseuses (voir la Figure 1.7). Cette différence de composition va entraîner une différence de fréquence importante entre les deux oscillateurs, comme on peut le voir sur la partie gauche de la Figure 1.8 entre le signal jaune (qui provient de l'oscillateur composé de trois portes inverseuses, signal noté S1 sur la Figure 1.8) et le signal bleu (qui provient de l'oscillateur composé de cinq portes inverseuses, signal noté S2 sur la Figure 1.8). En effet, sur la partie gauche de la Figure 1.8, l'oscilloscope est réglé pour se synchroniser sur le signal jaune, on voit alors, grâce au mode persistance de l'oscilloscope que le signal bleu n'est pas du tout synchronisé avec le signal jaune. Les signaux ont donc une fréquence complètement différente. Les auteurs ont par la suite appliqué une perturbation harmonique sur la masse des portes CMOS, de 900 mV pic à pic et de fréquence égale à 24 MHz (on suppose ici que cette fréquence est proche de la fréquence de fonctionnement des deux oscillateurs - les auteurs ne donnent pas d'information sur les fréquences des oscillateurs). Les signaux de sortie des deux oscillateurs, dans ce cas de figure, sont visibles dans la partie droite de la Figure 1.8. Du fait de cette injection de signal harmonique, les oscillateurs sont maintenant synchronisés, ou encore verrouillés (comme définis dans [Bochard et al., 2010]).

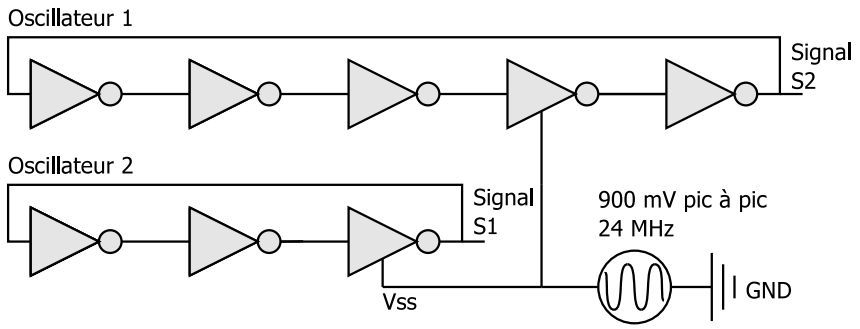

FIG. 1.7 – Schéma de l'expérimentation effectuée sur deux oscillateurs en anneau par les auteurs de [Markettos and Moore, 2009].

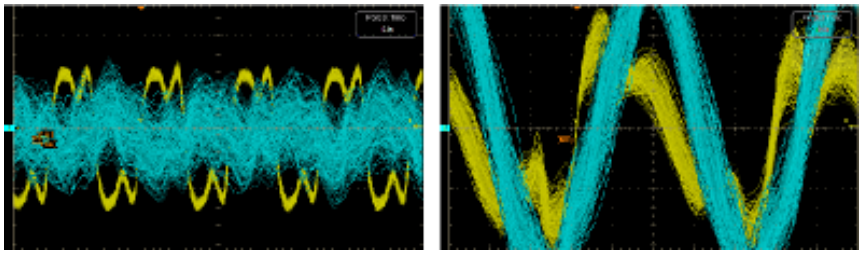

FIG. 1.8 – Mesure du signal de sortie de deux oscillateurs (en jaune la sortie S1 et en bleu la sortie S2 signalées sur la Figure 1.7, avec de gauche à droite : pas d'injection de signal, injection d'un signal harmonique de 24 MHz et d'amplitude pic à pic égale à 900mV. Figure extraite de [Markettos and Moore, 2009].

Par la suite, les auteurs de [Markettos and Moore, 2009] ont ciblé un microcontrôleur sécurisé (de type 8051) habituellement utilisé dans des distributeurs de billets de banque (ce microcontrôleur, au moment de la publication de l'article était toujours recommandé par le constructeur pour les nouveaux terminaux bancaires). Ce microcontrôleur embarque un générateur d'aléa basé sur la différence de fréquence entre deux oscillateurs en anneau. Une suite binaire produite par ce générateur (dans des conditions de fonctionnement normale) est montrée, à gauche, à la Figure 1.10. Le principe de perturbation est le même qu'utilisé précédemment (à savoir une superposition d'un signal harmonique sur l'alimentation du circuit), et est présenté à la Figure 1.9. L'amplitude pic à pic de la perturbation injectée est cette fois ci égale à 500 mV, de manière à rester dans des conditions de fonctionnement tolérées par le composant. On voit dans la Figure 1.10, le flot de bits produit par le générateur sous l'influence d'une perturbation à 1.822 MHz (figure du milieu sur la Figure 1.10) et d'une perturbation à 1.929 MHz (figure de droite sur la Figure 1.10). On note clairement l'apparition de motifs (différents pour les deux fréquences) qui dénote une réduction de l'aléa produit par le générateur due au verrouillage des oscillateurs sur la fréquence d'injection.

Bien évidemment, la fréquence maximale du signal harmonique qu'il sera effectivement possible d'injecter à l'intérieur du circuit va dépendre fortement des caractéristiques à la fois de la carte, mais aussi du circuit ciblé. En effet, plusieurs éléments peuvent filtrer ce type de signal : régulateur, pad d'alimentation, bounding, etc. Les auteurs de [Markettos and Moore, 2009] ont injecté des signaux de très faible fréquence ($<$ 50 MHz). Pour des oscillateurs en anneau de haute fréquence ($>$200 MHz) intégrés dans des circuits numériques récents, ce type de technique risque d'être impossible à appliquer, les différents éléments cités précédemment ayant une bande passante en général beaucoup plus faible. Nous montrerons, dans le Chapitre 4, que le rayonnement électromagnétique permet de réaliser le même type d'attaque, et ce sans limitation de fréquence.

D'autres articles, qui peuvent être vus comme des articles décrivant des attaques, traitent de la résistance de générateur d'aléa à des perturbations environnementales (en général modification de la température ou la tension d'alimentation), mais aussi

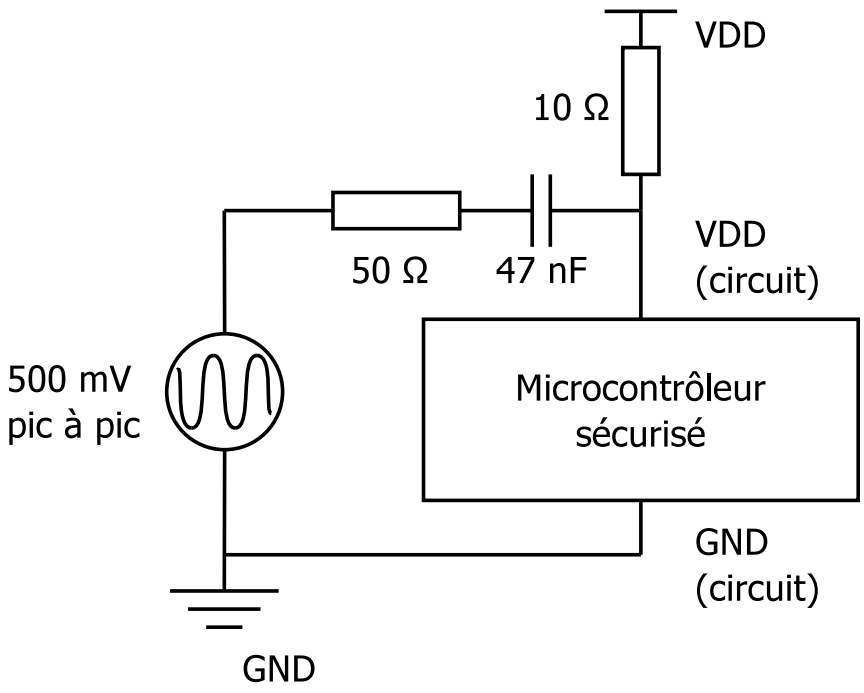

FIG. 1.9 – Schéma de l'expérimentation effectuée sur un microcontrôleur sécurisé embarquant un générateur d'aléa par les auteurs de [Markettos and Moore, 2009].

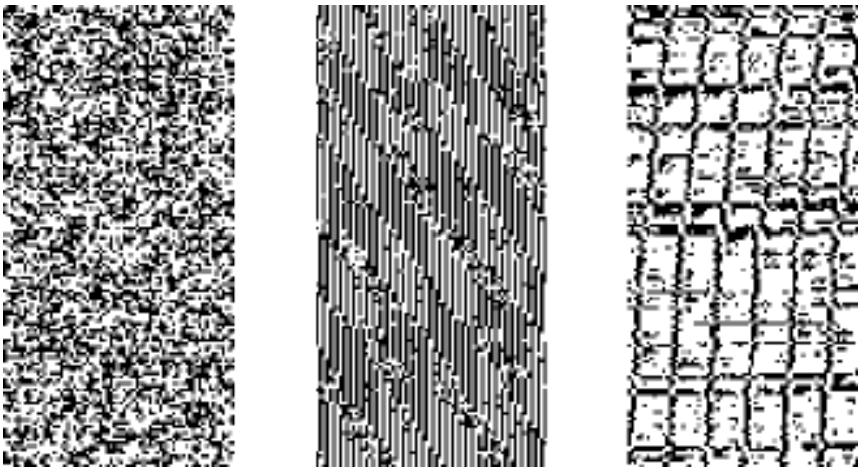

FIG. 1.10 – Suite de bits produites par le générateur d'aléa embarqué dans le microcontrôleur avec de gauche à droite : pas d'injection, une injection à 1.822 MHz et une injection à 1.929 MHz. Figure extraite de [Markettos and Moore, 2009].

pour certains, de la résistance aux perturbations dues à la logique environnante. C'est notamment le cas dans [Santoro et al., 2009] où les auteurs testent trois principes de génération d'aléa différents tous basés sur des oscillateurs en anneau ([Sunar et al., 2007], [Vasyltsov et al., 2008] et [Dichtl and Golic, 2007]). Les auteurs testent

à la fois la résistance du générateur aux variations de température (25 °C, 55 °C et 75 °C) mais aussi à l'application d'une forte activité logique autour de lui. Les auteurs appliquent les tests FIPS à la suite de bits générée par les différents générateurs pour évaluer leurs robustesses aux variations de température. Ils remarquent que les trois principes ne réagissent pas de la même façon. Par exemple, le générateur de [Dichtl and Golic, 2007] est peu sensible aux différences de température en l'absence de bloc logique environnant et devient sensible lorsque des blocs logiques l'entourent. Le générateur de [Vasyltsov et al., 2008] est quant à lui sensible aux différences de température quelque soit la présence ou non de logique environnante. Seul le générateur [Sunar et al., 2007] n'est pas sensible aux perturbations, mais comme présenté précédemment, ce générateur n'exploite pas réellement les incertitudes temporelles des oscillateurs, mais plutôt un signal analogique en sortie d'une porte OU-Exclusif trop sollicitée.

Les auteurs de [Yoo et al., 2010], étudient également la sensibilité d'un générateur de [Sunar et al., 2007] aux variations de température et de tension d'alimentation. Les auteurs proposent d'utiliser plusieurs configurations du générateur en gardant une fréquence d'échantillonnage fixe à 100 MHz. Les auteurs ont utilisé des générateurs avec 16, 32, ... 256 oscillateurs (le pas d'incrémentation du nombre d'oscillateurs est égal à 16) avec des oscillateurs constitués d'un nombre de portes inverseuses différent, 7, 11, 15, 19, 23, 27. Pour évaluer la suite de bits générée par le générateur, les auteurs ont utilisé les tests statistiques DIEHARD. De manière générale, les auteurs remarquent que les générateurs sont d'autant moins sensibles aux différences de tension ou de température que le nombre d'oscillateurs (pour des oscillateurs composés du même nombre de portes inverseuses) qui composent le générateur est important. De la même façon, ils remarquent que plus les oscillateurs sont lents (donc plus ils comportent de portes inverseuses), moins bonne est la qualité de la suite produite à nombre d'oscillateurs égal. Jouer sur les paramètres de fonctionnement permet ainsi de ralentir les oscillateurs. En sous-alimentant ou en réchauffant le circuit, les oscillateurs ralentissent, et ainsi les propriétés statistiques des suites produites par le générateur seront en moyenne moins bonnes que les suites produites par le même générateur pour les paramètres de fonctionnement nominaux.

Enfin les auteurs de [Simka et al., 2011] testent le principe de génération proposé par [Fischer and Drutarovsky, 2003]. Ce générateur utilise comme source d'aléa et extracteur d'entropie une boucle à verrouillage de phase. Il est possible, sur différentes technologies de FPGA de choisir le type de filtre de la boucle à verrouillage de phase. Les auteurs montrent que le réglage de ce filtre impacte directement la sensibilité (et donc les propriétés statistiques de la suite produite) aux variations de température. Cependant les variations de température (qui sont négatives) sont réalisées à l'aide d'une bombe d'air froid (utilisée en électronique pour détecter des pannes de composants par exemple). Il est donc difficile, avec un tel procédé, de contrôler proprement la température du circuit. Il serait donc intéressant de reprendre ce type d'étude avec une étuve par exemple (avec laquelle il est facile de maintenir précisément le circuit à une température voulue).

Le Tableau 1.1 résume les différentes attaques existantes sur les générateurs

d'aléa. Toutes les attaques sur les générateurs d'aléa présentées dans cette partie sont clairement axées de manière à perturber l'extracteur d'entropie (attaque 1 sur la Figure 1.6), mais agissent sur des canaux d'attaque qui vont perturber globalement tout le circuit (que ce soit pour les modifications de la température ou de la tension d'alimentation du circuit, ou de la superposition d'un signal harmonique sur l'alimentation de la puce).

Référence	Attaque	TRNG	Canal
[Markettos 2009]	1	RO	Signal harmonique sur l'alimentation
[Santoro 2009]	1	RO	Température
[Yoo2010]	1	RO	Température et alimentation
[Simka 2011]	1	PLL	Température

TAB. 1.1 – Tableau récapitulatif des différentes attaques sur les générateurs d'aléa.

Le canal caché électromagnétique (que nous présenterons dans la suite), nous semble être le meilleur candidat pour attaquer les générateurs d'aléa. Nous pensons qu'il est possible, sans réaliser de modification de la carte ou du circuit (donc dans le cadre des attaques non invasives), et à distance, d'effectuer à la fois une attaque active et passive du générateur.

1.3 Conclusion

Nous avons, dans ce chapitre, posé les bases dans lesquels s'inscrivent les travaux présentés dans ce manuscrit. Nous avons également montré l'intérêt d'attaquer la génération d'aléa, et nous avons fourni un modèle de menaces. A partir de là, il est légitime de se poser quelques questions :

- Est-il possible d'utiliser le canal électromagnétique comme canal d'attaque sans contact d'un générateur d'aléa à base d'oscillateurs en anneau ?
- Plus précisément, est il possible, en étudiant, le rayonnement électromagnétique d'obtenir de l'information (notamment l'emplacement et les fréquences) sur le générateur ?
- Est-il possible via ce canal de perturber ce générateur ?
- Enfin, comment modéliser l'effet induit par l'injection électromagnétique sur le générateur ?

Nous répondrons à ces différentes questions tout au long du manuscrit. Dans un premier temps, nous allons, dans le prochain chapitre, nous focaliser sur la description des attaques qui exploitent le canal caché électromagnétique.

Chapitre 2

Les ondes électromagnétiques : une menace pour la cryptographie matérielle ?

Dans le chapitre précédent nous avons introduit les attaques matérielles ciblant des circuits dédiés à la cryptographie. Nous avons volontairement omis de traiter les attaques qui utilisent le canal caché électromagnétique pour en discuter plus en détail dans ce chapitre. Enfin, nous réaliserons une description détaillée des bancs de tests utilisés pour la réalisation des travaux présentés dans ce manuscrit. Une annexe détaillant les principes fondamentaux de l'électromagnétisme est jointe afin d'appréhender au mieux les attaques électromagnétiques présentées dans ce chapitre.

Sommaire du chapitre

1.1 Les générateurs de nombres aléatoires 2

1.1.1 La génération d'aléa dans la cryptographie matérielle 2

1.1.2 Générateur de nombres réellement aléatoires 3

1.1.3 Générateur à base d'oscillateurs en anneau de [Sunar et al., 2007] et amélioré par [Wold and Tan, 2008]. 6

1.2 Attaques sur les générateurs d'aléa 9

1.2.1 Pourquoi attaquer un générateur d'aléa ? 9

1.2.2 Modèle de menaces sur les générateurs de nombres réellement aléatoires 10

1.2.3 Attaques sur les générateurs de nombres aléatoires 10

1.2.3.1 Attaques matérielles 10

1.2.3.2 Attaques pratiques sur les générateurs d'aléa 12

1.3 Conclusion 17

2.1 Utilisation du rayonnement électromagnétique comme canal d'attaque

Il est intéressant de noter que l'étude du rayonnement électromagnétique qui provient des circuits intégrés et l'étude de l'effet d'un rayonnement électromagnétique sur des circuits intégrés sont, de nos jours, relativement communes dans le développement de circuits. En effet, l'électronique étant de plus en plus diffusée depuis quelques années, nous vivons dans un environnement aujourd'hui où beaucoup d'appareils électroniques cohabitent entre eux. Il est donc nécessaire pour chaque circuit intégré en cours de conception de s'assurer qu'il puisse correctement fonctionner dans un environnement bruité, ou, dans le cas d'un système embarqué, autour d'autres systèmes embarqués. L'étude de la compatibilité électromagnétique (CEM) se rapproche fortement des études effectuées en cryptographie matérielle qui traitent de l'étude du rayonnement électromagnétique comme canal d'attaque. Il est donc naturel qu'une partie des méthodes et matériels ait été empruntée à cette branche de l'électronique.

La Figure 2.1 et la Figure 2.2 montrent un historique des différentes attaques, respectivement passives et actives, qui utilisent le canal électromagnétique. On peut noter que le canal caché électromagnétique est efficace à la fois pour récupérer de l'information contenue dans un circuit intégré (attaque passive par analyse), et pour perturber son fonctionnement (attaque active par injection de fautes).

Nous allons tout d'abord nous intéresser à l'analyse de l'émission électromagnétique des systèmes cryptographiques.

2.1.1 Le canal électromagnétique comme moyen de récupération d'information

Comme on peut le voir sur la Figure 2.1, le rayonnement électromagnétique d'un système est différent en fonction de la distance à laquelle se trouve l'appareil de mesure. On distingue en général deux types de champ, le rayonnement en champ proche, et le rayonnement en champ lointain. Comme leurs noms l'indiquent, l'un est mesuré au plus proche de la source, alors que l'autre est mesuré à distance. Nous discutons des différences entre ces deux champs en annexe (Annexe A). Les techniques et matériels relatifs à l'étude de chaque champ sont bien sûr différents.

Nous allons d'abord nous intéresser à l'étude du rayonnement en champ lointain pour ensuite détailler l'étude du rayonnement en champ proche.

2.1.1.1 Découverte de la fuite d'information inopinée des circuits électriques

La découverte de la possible utilisation du canal caché électromagnétique comme source d'information remonte à la seconde guerre mondiale. Cette découverte a été effectuée par un chercheur de l'entreprise BELL. Ce chercheur a en effet remarqué qu'il était possible d'observer, lors du chiffrement d'un texte par un système de

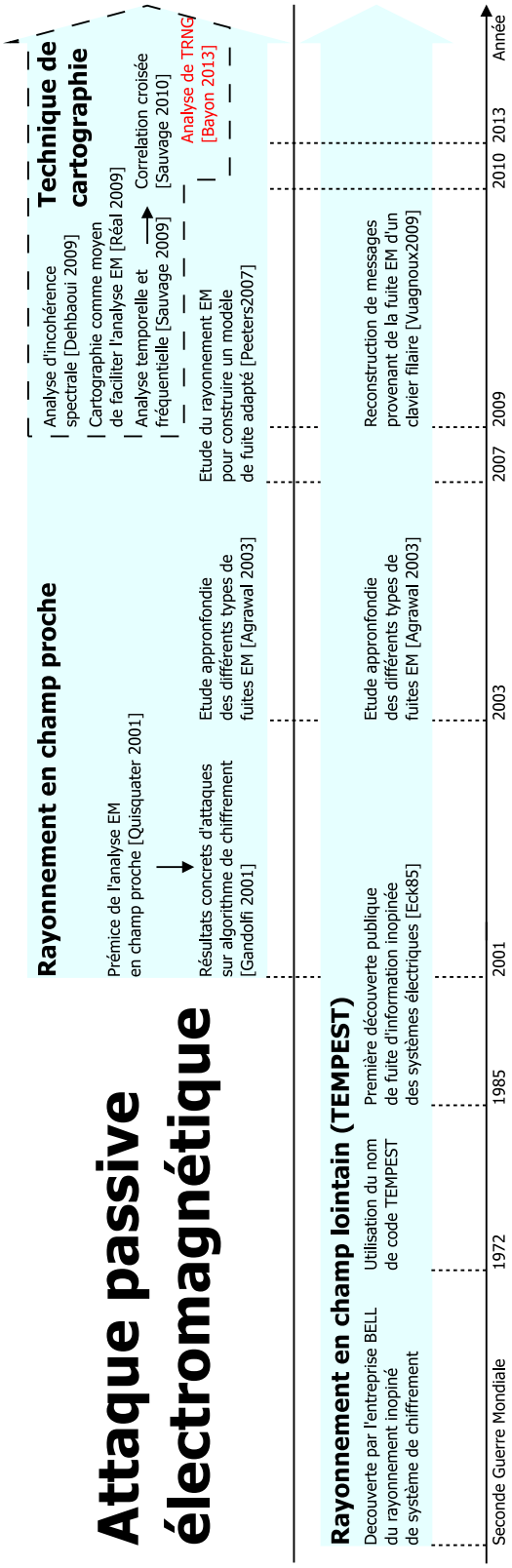

FIG. 2.1 – Historique des attaques passives qui utilisent le canal caché électromagnétique.

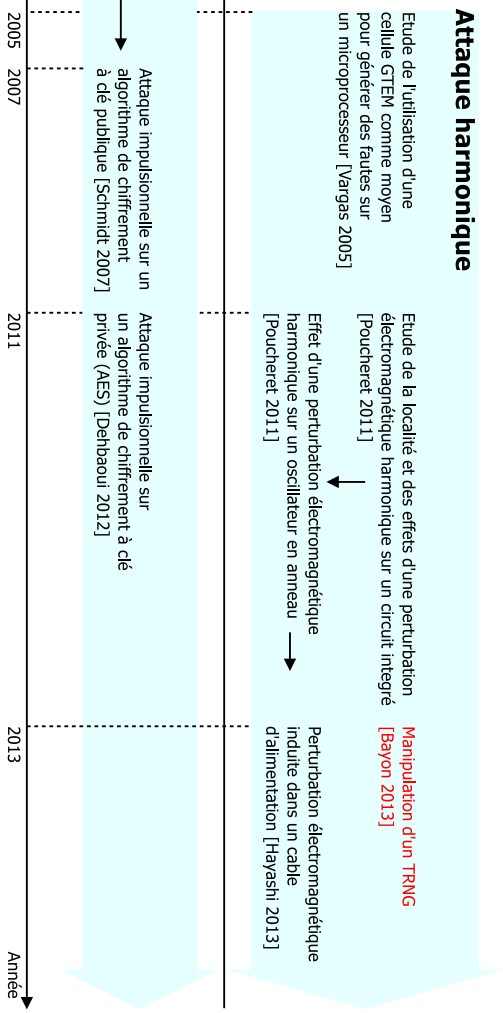

FIG. 2.2 – Historique des attaques actives qui utilisent le canal caché électromagnétique.

chiffrement dédié, une impulsion sur un oscilloscope non relié au système de chiffrement. Par la suite, l'étude de ces impulsions a permis à ce chercheur de remonter directement au texte en clair.

La fuite d'information a lieu sous trois formes :

- Radiation électromagnétique du système de chiffrement.
- Courant induit dans les câbles (alimentation et communication).
- Champ électromagnétique dû à l'utilisation de relais électromécaniques.

Les contremesures proposées pour se prémunir de tout risque consistent tout simplement à empêcher la mesure de tout rayonnement par utilisation d'un blindage autour du système cryptographique et par l'utilisation de filtres sur les câbles de signaux ou d'alimentation.

Le danger ici, se situe dans le cas d'attaquants qui ont accès à des antennes performantes qui leur permettent de capter des fuites d'informations à longue distance (> 50 mètres). La détection de ces impulsions peut se faire facilement à travers n'importe quelle surface non blindée, il est donc possible d'imaginer un scénario où une personne mal intentionnée est située dans un immeuble voisin d'une organisation sensible (ambassade, organisation relative à la défense d'un pays, ...) qui manipule des données nécessitant le secret.

Plusieurs cas d'utilisation de ce type de techniques par des ennemis ont été identifiés par les États-Unis durant la guerre froide, dont notamment l'espionnage d'ambassades situées dans des pays de l'Est. La mesure de la fuite n'était pas forcement une mesure du champ électromagnétique - cela pouvait aussi être des mesures acoustiques entre autres - mais la mesure du rayonnement électromagnétique proposait l'avantage de ne nécessiter aucun outil posé au plus proche de la source.

Plus tard cette technique sera identifiée par la NSA, sous le nom de code TEMPEST [NSA, 2007]. Il faudra attendre 1985 pour voir le premier article scientifique public traitant de l'utilisation du rayonnement électromagnétique de machines [van Eck, 1985]. La technique présentée ici permet de reconstruire à l'aide d'une antenne et d'un récepteur de télévision classique l'image affichée par un écran à base de tube cathodique. Le matériel d'espionnage utilisé est relativement simpliste et à faible coût. Seul un ajustement, facile à réaliser, sur le récepteur est nécessaire, si sa fréquence de rafraichissement de l'image est différente de celle de l'écran espionné. Les auteurs font état d'une reconstruction possible à une centaine de mètres pour le matériel cité plus haut. Avec un matériel plus performant, cette distance peut être étendue à un kilomètre. A noter que les écrans espionnés lors de cette étude n'étaient pas modifiés et émettaient des radiations en deçà des limites autorisées (études CEM préliminaires à la vente de chaque matériel électrique).

Cette étude démontre donc la possibilité d'espionner à bas coût tout ce qui peut être affiché sur un écran, ceci posant à la fois des problèmes de sécurité mais aussi de protection de la vie privée (il est possible d'imaginer quelqu'un en train d'espionner l'écran d'une tierce personne pour récupérer des informations personnelles - bancaire, santé, etc ...). L'article [van Eck, 1985] fait état de l'existence de deux standards militaires qui font office de référence pour tester le matériel destiné à une utilisation gouvernementale (NACSIM 5100A TEMPEST Standard pour les

États-Unis et AMSG720B pour l'OTAN) mais dont le contenu n'est pas public.

L'auteur propose différentes contremesures dont les plus efficaces sont :

- le blindage de l'écran avec une coque métallique - ne supprime pas complètement la fuite, car il faut bien sûr laisser une ouverture pour l'écran en lui même, mais permet de réduire la distance d'efficacité du matériel de réception d'un facteur au moins cinq.
- le changement de la méthode de rafraichissement de l'image (linéaire) pour une méthode plus complexe. Cela n'empêche pas la reconstruction, mais la rend plus compliqué.

D'autres articles scientifiques plus récents traitent de l'étude de cette technique d'espionnage, dont notamment [Vuagnoux and Pasini, 2009] qui propose une méthode de reconstruction de messages tapés sur un clavier filaire (PS/2, USB, et clavier d'ordinateur portable).

L'étude du champ électromagnétique en champ lointain permet de récupérer de l'information qui sort d'un système. Si cette information est en clair, il est alors facile de la lire. Si cette information est chiffrée, il est nécessaire de venir étudier le système plus en détail. Pour cela une analyse du champ électromagnétique proche peut donner de très bons résultats.

2.1.1.2 L'analyse du champ électromagnétique en champ proche

Le premier article qui présente l'utilisation d'une mesure du rayonnement électromagnétique en champ proche, en provenance d'un système cryptographique, dans le but de récupérer de l'information sur ce dernier est [Quisquater and Samyde, 2001]. Les auteurs de cet article font état de l'utilisation d'une simple bobine comme antenne réceptrice. Grâce à ce dispositif simple, il est possible de récupérer un champ magnétique émis par un circuit électronique intégré. Ce champ magnétique est directement lié à la consommation de courant du composant soumis au test, et par conséquence, les principes d'analyse utilisés pour les traces de consommation de puissance peuvent être directement utilisés ; seul le médium d'acquisition est différent. La méthode classique d'analyse différentielle de la consommation de courant proposée par [Kocher et al., 1999] (DPA) devient alors DEMA (Differential ElectroMagnetic Analysis), la méthode d'analyse par corrélation proposée par [Brier et al., 2004] (CPA) devient CEMA (Correlation ElectroMagnetic Analysis), et ainsi de suite en fonction du canal caché exploité. L'utilisation du canal électromagnétique permet d'effectuer une mesure locale, sans contact et non invasive. Cette mesure est plus ou moins locale suivant le matériel utilisé (cette notion de localité est fortement dépendante de la sonde : forme, caractéristiques). C'est cette propriété qui rend l'analyse électromagnétique intéressante par rapport à une analyse de consommation de puissance. En effet, lors d'une analyse de la consommation de puissance, l'attaquant mesure le courant consommé par tous les blocs qui constituent le circuit ciblé. La contribution qui correspond à la fuite du secret est noyée dans du bruit. Par contre, lors d'une analyse électromagnétique, il est possible de récupérer, en utilisant une sonde suffisamment petite, des traces électromagnétiques qui représentent

seulement la consommation de courant d'une partie du circuit. En d'autres mots, la mesure du champ électromagnétique permet de sélectionner le bloc fonctionnel sur lequel l'analyse sera effectuée. Face à une mesure globale (type DPA), il est possible d'utiliser des contremesures (technique de masquage) qui vont cacher la fuite d'information, mais face à une mesure locale (notamment une mesure du champ proche électromagnétique), il est nécessaire d'avoir une contremesure qui agisse au niveau local ; il est évident que ce type de contremesure n'est pas simple à réaliser et est surtout coûteuse.

Les premiers résultats pratiques de récupération de secret exploitant le canal caché électromagnétique, sur des circuits industriels qui réalisent des opérations cryptographique ont été présentés dans [Gandolfi et al., 2001]. Cette étude a été effectuée sur un circuit de type carte à puce, qui ne contient pas de protection logicielle, et qui embarque un chiffreur à clé privée de type DES, un algorithme d'authentification et de génération de clé (COMP128) et un algorithme à clé publique de type RSA. Les auteurs de cette étude remarquent que la mesure du champ électromagnétique a en général un moins bon rapport signal sur bruit qu'une mesure de consommation de puissance, mais que l'analyse électromagnétique reste tout de même plus performante car la signature qui correspond au calcul du bloc cryptographique est plus marquée. Les auteurs remarquent que les meilleurs résultats obtenus l'ont été avec une simple sonde magnétique (bobine en cuivre) "faite maison" dont les dimensions sont environ de l'ordre de la taille du bloc cryptographique étudié. Les autres sondes utilisées étaient des sondes magnétiques intégrées ou encore une tête de lecture d'un disque dur.

Sur les deux premières cibles, à savoir le chiffreur à clé privée et l'algorithme d'authentification, les auteurs ont souhaité comparer les techniques de DEMA et de DPA. Les traces de consommation de puissance et du rayonnement électromagnétique ont été acquises en même temps, ceci permet ainsi de comparer correctement les deux techniques. Même si la DPA permet dans les deux cas de retrouver le secret, la DEMA s'avère être beaucoup plus performante et précise. En effet, lors de l'évaluation de la clé, la DEMA, à l'inverse de la DPA, ne crée pas de faux positif.

Sur l'exponentiation modulaire de l'algorithme RSA, les auteurs ont comparé les techniques de SPA (Simple Power Analysis) et SEMA (Simple ElectroMagnetic Analysis). A contrario de l'analyse différentielle, la SPA et la SEMA ne fournissent pas un résultat identique. Dans le cas présenté ici, il existe des positions de sonde pour lesquels il est possible en analysant la trace électromagnétique de retrouver la clé privée lors de l'opération d'exponentiation, chose qui n'est pas possible de faire avec la trace de consommation de puissance. En effet, sur la trace de consommation de puissance, la clé ne ressort pas clairement, l'information est noyée dans trop de bruit. Les auteurs de l'article précisent que cela ne veut pas forcément signifier que la SEMA est supérieure à la SPA, mais que les deux analyses sont bel et bien différentes (et donc, peuvent potentiellement se révéler complémentaires). En d'autres mots, rien ne prouve qu'il n'existe pas des cas pour lesquels la SPA fonctionnerait alors que la SEMA échouerait.

La DPA nécessite un modèle de fuite. Les deux modèles de fuite les plus utilisés

(distance et poids de Hamming), ont tout naturellement été utilisés de la même façon pour l'EMA. Le problème inhérent à l'utilisation de ces deux modèles pour l'EMA est que, certes, les traces de courant sont relativement semblables à des traces électromagnétiques, que l'analyse EMA fonctionne très bien en utilisant ces deux modèles, mais qu'au final la capacité de l'EMA à trouver le secret n'est pas exploitée au maximum car le modèle de fuite n'est pas adapté. C'est ce que les auteurs de [Peeters et al., 2007] se sont efforcés de prouver. Ils partent du principe qu'aujourd'hui dans les technologies CMOS, la principale consommation de courant des transistors correspond à la charge/décharge des capacités parasites. C'est ce courant là qui entraîne une fuite électromagnétique. Au contraire des traces de consommation de puissance, les traces du rayonnement électromagnétique permettent de différencier les moments où ces capacités parasites des transistors se chargent du moment où ces capacités se déchargent. Cette propriété est illustrée sur la Figure 2.3 où l'on peut clairement voir des pics à la fois positifs et négatifs sur la trace du rayonnement électromagnétique (Figure 2.3 à droite), alors que ceux sur la trace de la consommation de puissance sont tous positifs (Figure 2.3 à gauche). Les modèles habituellement utilisés ne prennent pas en compte ce type d'information. Les auteurs ont donc construit un modèle, « Signed distance model », qui exploite ce type d'information. Ce modèle se révèle être plus efficace que les deux modèles habituellement utilisés : pour une attaque qui cible une table de substitution d'un chiffreur sur 8 bits, moins de 50 traces du rayonnement électromagnétique sont nécessaires pour retrouver la bonne clé en utilisant le « Signed distance model », alors qu'il en faut environ 1000 lors de l'utilisation du poids de Hamming.

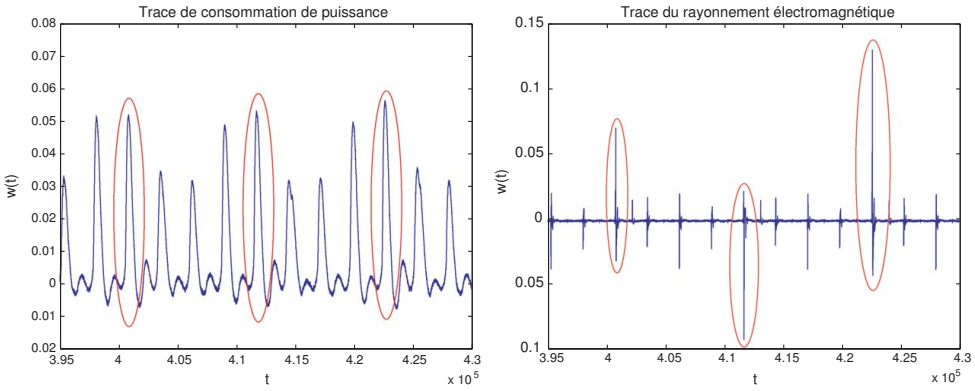

FIG. 2.3 – Différence entre une trace de consommation de puissance et une trace du rayonnement électromagnétique. Figure tirée de [Peeters et al., 2007].

Beaucoup d'articles supplémentaires traitent de l'étude de l'utilisation du canal électromagnétique comme médium pour réaliser une attaque de type DEMA ou CEMA sur différents algorithmes (chiffrement, authentification, ...). Le but ici n'est pas de faire une liste complète des avancées dans ce domaine, la plupart des articles font uniquement usage du canal caché électromagnétique comme médium

d'acquisition, et n'apportent pas de nouveauté sur le canal caché électromagnétique lui-même, ou sur son exploitation ; la contribution de ces articles se trouve souvent dans l'amélioration de l'algorithme utilisé pour retrouver la clé. Nous nous limiterons à la description des travaux présentés ci-dessous.

2.1.1.3 Étude comparative des fuites électromagnétiques

Comme cela a été montré précédemment, plusieurs types de fuites non intentionnelles existent. Les auteurs de [Agrawal et al., 2003] essayent de lister ces différents types de fuite, et surtout leurs provenances. Il existe deux types d'émanations :

- Directe : due aux courants qui circulent dans les transistors, dans les lignes à l'intérieur du circuit, etc. Ce sont les émanations qui sont exploitées dans les travaux présentés dans la section précédente.
- Indirecte : ce sont des émanations provenant du possible couplage entre des blocs de calculs avec des blocs analogiques beaucoup plus gros (horloge, alimentation). Il est courant pour ce type d'émanation de retrouver l'information dans des signaux modulés (amplitude, phase ou fréquence).

Il existe également deux moyens de propagation de la fuite électromagnétique, elle peut être rayonnée ou conduite (comme présenté dans la section qui traite de l'analyse en champ lointain).

Les auteurs de [Agrawal et al., 2003] font le constat que la fuite électromagnétique est dépendante de la constitution du circuit ciblé. Dans certains cas, par exemple, si un bloc qui manipule une donnée à protéger se trouve trop près d'un bloc analogique (par exemple un bloc d'horloge), il est possible que le rayonnement du bloc analogique contienne des informations sur la donnée sensible (du fait du couplage des deux blocs). Cette information ne peut pas directement être extraite du rayonnement (émanation indirecte). En effet, il est souvent nécessaire d'appliquer une démodulation en fréquence (à la fréquence de l'horloge par exemple). Il est intéressant de voir qu'une même trace électromagnétique, démodulée différemment, ne laisse pas forcément apparaître la même information (c'est à dire ne représente pas la même fuite).

Les auteurs expliquent que le rayonnement électromagnétique peut être vu comme une source multiple de canaux d'attaques. Même avec une seule sonde, il est possible d'obtenir plusieurs canaux différents en effectuant des démodulations avec des porteuses différentes par exemple. Il est même possible de combiner ces différents canaux afin de rendre une attaque plus efficace.

2.1.1.4 Localisation de blocs cryptographiques enfouis dans un circuit intégré

Le but des différentes analyses présentées ci-dessus est clair, il s'agit de retrouver à l'aide du canal électromagnétique le secret enfoui à l'intérieur du circuit (la clé utilisée pour chiffrer). Comme dit précédemment, l'avantage premier du canal caché électromagnétique par rapport au canal de la consommation de puissance est

la possibilité d'effectuer une attaque localisée uniquement sur la partie sensible du circuit où l'opération ciblée s'exécute. Cela permet de retrouver le secret plus efficacement et de contourner des contre-mesures qui agissent au niveau global. Cet avantage peut se retrouver être un inconvénient. Plus la sonde est petite, plus la mesure du champ électromagnétique est localisée. Il est alors difficile, sans connaissance préalable du circuit intégré, de choisir une position adéquate pour réaliser les mesures du rayonnement électromagnétique de la partie ciblée. L'attaquant se pose deux questions :

- La zone qui rayonne le plus (en terme d'amplitude) est-elle la zone qui est la plus propice à l'attaque électromagnétique ?
- Est-il possible de trouver un indicateur rapidement calculable qui permette de définir la zone où l'attaque est la plus efficace ?

Depuis 2009, plusieurs travaux ([Sauvage et al., 2009], [Real et al., 2009], [Sauvage et al., 2010] et [Dehbaoui et al., 2009]) ont apporté de nouvelles méthodes dites de cartographie électromagnétique (initialement introduit par [Quisquater and Samyde, 2001] en 2001). Ces techniques permettent de construire des cartes qui représentent la fuite électromagnétique d'un circuit. Les cartes résultantes d'une cartographie optique comme dans [Skorobogatov, 2005] sont beaucoup plus précises que ce que l'on peut espérer obtenir avec une cartographie basée sur l'acquisition du champ électromagnétique. Cependant, les cartes obtenues avec les techniques de cartographie électromagnétique sont plus représentatives de la fuite d'information que du layout en lui même, et elles présentent l'avantage de ne pas être limitées par la taille de gravure des transistors (il n'est en effet pas possible d'étudier un circuit avec une finesse de gravure inférieur à 250 nm avec les techniques présentées dans [Skorobogatov, 2005]) ou encore par le nombre de couches de métallisation qui constituent le circuit. Il est également important d'insister de nouveau sur le fait qu'au même titre que les analyses du champ électromagnétique présentées précédemment, les techniques de cartographie ne nécessitent aucune modification du circuit (comme le nécessitent les techniques de cartographique optique). La chaîne d'acquisition des traces électromagnétiques est identique (à l'exception de la nécessité d'utiliser une table XY pour déplacer le circuit par rapport à la sonde) à celle utilisée pour l'EMA.

Les différentes méthodes utilisées par ces techniques de cartographie ne sont pas discutées dans cette section. Les principes, les points forts et faibles de chaque technique seront détaillés dans le Chapitre 3.

Si la cartographie est censée accélérer l'analyse, il ne faut pas que cette dernière soit plus longue à réaliser que l'analyse en elle même au point le moins efficace pour réaliser l'attaque. Par exemple, il est possible de réaliser une attaque de type EMA sur une capacité de découplage externe au circuit comme cela a été prouvé dans [Agrawal et al., 2003] et [Sauvage et al., 2009]. Même si cette attaque se révèle être globale (le rayonnement électromagnétique mesuré au dessus de cette capacité résulte des contributions de tous les blocs du circuit), elle présente tout de même l'avantage de ne pas nécessiter de modification au niveau de la carte. Il est donc bon de se demander si réaliser l'attaque décrite juste au dessus n'est pas plus rapide que

de réaliser la cartographie, puis l'attaque au point le plus efficace.

2.1.1.5 Matériel pour l'analyse en champ proche

En ce qui concerne la sonde utilisée pour récupérer le champ électromagnétique qui émane du circuit, il est important d'insister sur le fait que le champ électromagnétique perpendiculaire à sa surface n'a qu'une composante magnétique (par contre, il est possible de récupérer d'autres champs électromagnétiques, sur les côtés du circuit par exemple, qui ont à la fois une composante électrique et magnétique) [Gandolfi et al., 2001]. Les premières sondes utilisées dans ce domaine de recherche étaient des bobinages de fil de cuivre "fait maison" (Figure 2.4). Ce type de sonde est largement utilisée, fonctionnelle et très bon marché. Le seul point noir revient à la fabrication. En effet, pour des bobinages avec une résolution spatiale en dessous du millimètre, la fabrication peut devenir difficile et nécessiter un équipement spécial comme cela fut le cas pour [Peeters et al., 2007], où pour réaliser la sonde présentée dans la Figure 2.5, un microscope et un fer à souder spécial ont été nécessaires. Globalement, en excluant les sondes nécessitant un matériel spécial lors de la fabrication, cette approche permet de limiter le coût de revient de l'attaque, mais une autre option est envisageable. En effet, beaucoup d'entreprises spécialisées dans la vente de produit de compatibilité électromagnétique vendent des sondes utilisables pour de l'analyse électromagnétique. Notamment, les auteurs de [Sauvage et al., 2009] conseillent l'utilisation de sondes industrielles, comme par exemple celle présentée à la Figure 2.6, que nous avons utilisée pour les travaux décrits dans ce manuscrit. Ces sondes permettent d'éviter tout problème d'adaptation d'impédance, et bénéficient de meilleures performances et permettent de ne pas se soucier de la fabrication de la sonde.

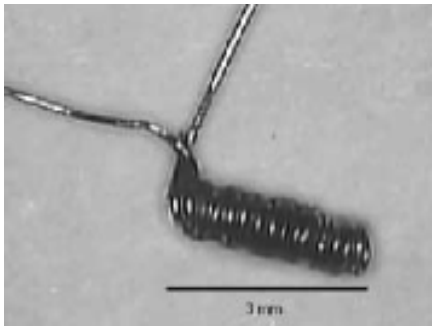

FIG. 2.4 – Bobinage typiquement utilisé pour effectuer des analyses électromagnétiques [Gandolfi et al., 2001].

Qu'elles soient industrielles ou "faites maison", les sondes magnétiques présentent l'avantage d'avoir une grande bande-passante, ce qui permet l'étude sur des composants qui mettent en jeu des fréquences élevées (notamment les FPGAs). En contrepartie, leur tension de sortie est limitée (au maximum 50mV en présence d'un circuit qui rayonne fortement, et ce même pour une sonde industrielle). De ce

FIG. 2.5 – Bobinage ayant une résolution spatiale en dessous du millimètre [Peeters et al., 2007].

FIG. 2.6 – Sonde LANGER utilisée dans notre banc de mesure.

fait, la plupart des auteurs préconisent l'utilisation d'un étage d'amplification entre la sonde et l'oscilloscope utilisé. Cet étage d'amplification est en général constitué d'un amplificateur faible bruit qui permet d'avoir un rapport signal sur bruit le plus fort possible.

Au contraire des études réalisées en compatibilité électromagnétique, l'utilisation d'une cage de Faraday n'est pas obligatoire, comme préconisée dans [Gandolfi et al., 2001]. Cependant la cage de Faraday réduit le bruit, et permet d'améliorer légèrement les performances des attaques (en terme de nombre de traces du rayonnement électromagnétique nécessaires pour réussir l'attaque) ; elle est donc optionnelle.

Pour conclure cette analyse, il est intéressant de parler de l'étude effectuée dans [Mounier et al., 2012]. En effet, les auteurs de cette étude se sont efforcés de caractériser plusieurs sondes qui ont des topologies différentes. L'étude se base sur l'analyse d'une ligne de type microstrip, comme l'on peut en trouver sur tous les PCB, traversée par un courant sinusoïdal. Le but de cette étude est de construire l'image électromagnétique de cette ligne en fonction de la fréquence du courant et de la position de la sonde par rapport à la ligne. L'étude a été également faite sur des lignes en silicium et sur un circuit de type carte à puce. Les auteurs de cette étude ont lié l'efficacité d'une attaque EMA avec les caractérisations de sondes obtenues sur les différents cas d'études. Le même type de caractérisation a été réalisé sur la sonde que nous avons utilisé. Cette étude est présentée dans le prochain chapitre (Chapitre 3).

2.1.1.6 Contremesures contre l'analyse en champ proche ?

Même si la menace que représente l'analyse électromagnétique n'est pas connue depuis longtemps, il n'a pas fallu longtemps pour imaginer des contremesures, et ce déjà dans l'article qui a introduit l'utilisation du canal électromagnétique comme canal d'attaque passive [Quisquater and Samyde, 2001]. Ces contremesures peuvent se classer en deux catégories comme cela est proposé par [Agrawal et al., 2003] :

- **Réduction de l'amplitude du signal électromagnétique**. Ce sont en général des contremesures liées à la conception et au packaging du circuit :
  - Cage de Faraday autour du circuit [Quisquater and Samyde, 2001]. Il est évident que l'analyse serait fortement contrariée par la cage de Faraday, mais cela ne supprimerait pas complètement les fuites d'information. En effet, il est impensable de réaliser une cage de Faraday parfaite, la connexion du circuit vers le monde extérieur nécessite toujours des points de passage pour les interconnexions, ce qui crée automatiquement une fuite d'information. Cependant, avec l'utilisation d'une cage de Faraday, il n'est plus possible de tirer avantage de la localité du canal électromagnétique, mais elle entraîne une hausse importante du coût de fabrication du circuit.
  - Oscillateurs au dessus du circuit [Gandolfi et al., 2001]. Le but de ces oscillateurs est de perturber l'analyse en incluant un bruit permanent. Cette contremesure requiert l'utilisation des couches supérieures de métallisation pour réaliser ces oscillateurs. Elle entraîne également une surconsommation de courant, ce qui peut être critique pour un système embarqué autonome. Avec la connaissance de la fréquence de fonctionnement de ces oscillateurs, il est imaginable de réaliser un filtrage sur la trace du rayonnement électromagnétique récupérée qui pourrait rendre la contremesure inefficace.
  - Répartition intelligente des couches de métal supérieures de manière à réaliser un maillage qui permet de contenir une partie du rayonnement électromagnétique [Quisquater and Samyde, 2001]. Le but de cette contremesure est de rendre l'analyse plus difficile à effectuer en réduisant l'amplitude du champ rayonné par le circuit (déjà faible comme signifié plus haut). Cela force l'attaquant à augmenter la sensibilité de son matériel d'acquisition (l'amplificateur de puissance doit avoir un gain plus important et une figure de bruit plus faible), et donc augmente le coût de l'attaque. D'un point de vue contremesure, le surcoût ne se situe pas au niveau de la fabrication (le processus de fabrication reste le même), mais au niveau du temps de conception (routage des différents niveaux de métallisation, enfouissement des interconnexions et transistors qui manipulent l'information à protéger).
  - Réduction de la consommation de puissance, celle ci est directement liée avec le rayonnement électromagnétique du circuit. Cette réduction de consommation se fait déjà avec la miniaturisation de la gravure des transistors, ce qui rend l'EMA plus difficile à réaliser au fur à et mesure que la taille de gravure diminue. Au même titre que la contremesure précédente, cela n'empêche pas l'analyse, mais réduit l'amplitude du champ rayonné par le circuit.
- **Réduction de la fuite d'information contenue dans le signal électromagnétique**. Ce sont toutes les contremesures qui tendent à réduire l'empreinte des calculs effectués par le circuit dans la fuite. Les contremesures DPA/SPA sont d'ailleurs en général proposées comme étant fonctionnelles pour lutter contre la DEMA/SEMA, tant que la mesure reste globale.
  - Ré-actualisation de la clé secrète.

- Masquage du chiffrement avec un nombre aléatoire [Coron and Goubin, 2000] [Akkar and Giraud, 2001].
- Utilisation de logique double-rail [Tiri and Verbauwhede, 2004].

Les contremesures adaptées à la DPA réduisent la fuite d'information au niveau global (donc dans la trace de consommation de puissance). Dans le cas d'une EMA, si la mesure est locale, il est possible de pouvoir récupérer le rayonnement d'un bloc où la contremesure ne sera pas effective, et donc ainsi la rendre caduque. Par exemple, dans le cas d'utilisation de technique de masquage, au début de chaque chiffrement, une valeur aléatoire est ajoutée à la clé ou au texte en clair - cette valeur est ensuite retirée à la fin du chiffrement - de façon à lier la fuite d'information à la valeur aléatoire (et plus seulement à la clé). Il est dans ce cas là beaucoup plus difficile de réaliser une attaque basée sur l'analyse de consommation de puissance (comme présenté dans le Chapitre 1, c'est dans ce genre d'exemple, qu'il est intéressant de vouloir attaquer le générateur implanté dans le circuit). Quelle que soit la technique de masquage utilisée, la clé est forcément manipulée, en clair, à un endroit du circuit. Si l'attaquant est capable de mesurer le rayonnement électromagnétique à cette position, il peut contourner la contremesure.

Une remarque intéressante est faite par les auteurs de [Gandolfi et al., 2001] : aucune contremesure n'est auto-suffisante et ne peut assurer qu'une analyse électromagnétique est impossible à réaliser sur le circuit où cette dernière est implantée. La proposition faite est de coupler plusieurs contremesures, suivant le niveau de protection requis par l'application et surtout le coût de revient du produit final, sachant que la plupart des contremesures proposées précédemment entraînent un surcoût non négligeable, notamment celles relatives à la réduction de la force du signal électromagnétique. Par exemple, une combinaison intéressante de contremesures pour protéger au maximum un circuit intégré contre l'analyse électromagnétique est l'utilisation d'une cage de Faraday avec une technique de réduction de la fuite d'information (masquage, logique double-rail, ...). Comme expliqué précédemment, la cage de Faraday bloque l'exploitation des fuites électromagnétiques locales (rayonnement électromagnétique à la surface du circuit), alors que la technique de réduction de la fuite d'information empêche l'exploitation de la fuite globale (fuite qui ne peut être bloquée par aucune contremesure de réduction de l'amplitude du signal électromagnétique).

Cependant, il est nécessaire de vérifier lors de l'utilisation d'une combinaison de contremesures que chaque contremesure n'entre pas en concurrence directe avec une autre, et ne la rende pas inefficace. Il est aussi important de vérifier si ces contremesures peuvent avoir un effet cumulatif : les auteurs de [Schaumont and Tiri, 2007] montrent qu'en combinant l'utilisation d'une logique double rail et une technique de masquage, les effets des deux contremesures ne s'additionnent pas et ne rendent donc pas le système plus robuste.

2.1.2 Le canal électromagnétique comme canal d'attaque active

Comme présenté sur la Figure 2.2, les attaques actives qui utilisent le canal caché électromagnétique peuvent être classées en deux catégories :

- Attaques impulsionnelles : les premières attaques de ce type ont vu le jour en 2002. Pour celles-ci, une forte impulsion électrique (ou un fort courant) est déchargée dans une sonde, positionnée au dessus du circuit, ce qui crée ainsi un fort champ électromagnétique très concentré dans le temps. La perturbation s'effectue sur un bref instant, mais est riche en fréquence.
- Attaques harmoniques : elles sont plus récentes, les premiers travaux présentant des attaques de ce type ont été publiés en 2011. Un fort champ électromagnétique harmonique est constamment appliqué à un circuit. La perturbation est constante, mais se concentre sur une seule fréquence.

Ces attaques ont pour but de perturber le fonctionnement du bloc cryptographique ciblé. Nous verrons dans la suite que les deux types d'attaques sont différentes et n'entraînent pas le même effet sur les circuits intégrés.

2.1.2.1 Attaque impulsionnelle

L'utilisation du canal caché électromagnétique comme canal d'attaque active, a été introduit en 2002 dans [Quisquater and Samyde, 2002]. Les auteurs utilisent le principe de courant de Foucault en vue de perturber le fonctionnement d'un circuit intégré : il est possible d'induire avec l'aide d'une bobine, un courant dans une surface conductrice. Les auteurs de [Quisquater and Samyde, 2002] ont été capables de réaliser une faute sur plusieurs bits (sans pour autant réellement définir le nombre exact) d'un bloc mémoire (RAM et EPROM) d'un processeur par l'utilisation d'une bobine composée de plusieurs centaines de spires qui encercle une tige métallique (ce qui permet de concentrer fortement le champ magnétique au bout de la bobine) reliée à un système de flash d'appareil photo utilisé comme générateur d'impulsion électrique. Si l'injection est trop brutale, il est possible de rendre la mémoire et le processeur inutilisables pour quelques heures. L'effet perturbatif du champ magnétique sur le circuit est évident, mais il est difficile de maîtriser précisément le nombre de fautes créées.

La deuxième attaque électromagnétique pratique ([Schmidt and Hutter, 2007]) est apparue 5 ans après celle introduite par [Quisquater and Samyde, 2002]. Les auteurs décrivent dans cet article une attaque sur un module RSA logiciel implanté dans un micro-contrôleur 8 bits (système type carte à puce). A l'instar de [Quisquater and Samyde, 2002], l'attaque proposée est relativement simple à réaliser et ne nécessite pas beaucoup de matériel. En effet, le champ électromagnétique perturbateur est créé par l'apparition d'un arc électrique. Au même titre que la foudre par exemple, un arc électrique dégage un fort champ électromagnétique. L'arc électrique en lui même est généré à l'aide d'une forte impulsion électrique provenant d'un allume-gaz piezzo-électrique, que l'on peut trouver dans toutes les quincailleries, et de deux électrodes qui sont en réalité des bouts de câbles coaxiaux (voir Figure 2.7).

FIG. 2.7 – Sonde d'injection à base d'allume-gaz utilisée par [Schmidt and Hutter, 2007]

Plus la distance entre les deux électrodes est importante, plus le champ est fort, mais, si la distance entre les deux électrodes est plus importante que la distance entre l'électrode et un autre conducteur (notamment le circuit), l'arc se créera entre l'électrode émettrice et ce dernier, qui entraîne une possible destruction du circuit.

Les auteurs sont capables de réaliser une faute lors de l'exécution du calcul de la signature RSA, ce qui permet donc l'application d'une attaque en faute. Ils constatent également que l'attaque peut causer des sauts d'instruction au niveau du processeur et des erreurs fatales au niveau des mémoires réversibles en quelques heures.

A l'inverse des attaques actives présentées au Chapitre 1 (notamment celle à base de laser), ces deux attaques sont très bas coût.

Enfin, l'attaque la plus avancée en terme d'impulsion électromagnétique est présentée dans [Dehbaoui et al., 2012a]. A l'aide d'un banc d'injection d'impulsion électromagnétique avancé (les éléments qui composent le banc n'ont rien à voir avec ce qui a été présenté avant en terme de coût d'achat - présence d'une cage de Faraday, d'un générateur d'impulsion en tension avec une faible incertitude temporelle, ...), les auteurs sont capables, grâce à l'injection d'une impulsion de haut voltage et avec des fronts très rapprochés, de fauter le calcul effectué par un chiffreur à clé privée (AES) embarqué sur une station d'émulation de carte à puce à base de micro-contrôleur 8 bits. Les auteurs s'intéressent en particulier au dernier tour de l'AES, et étudient l'effet de l'impulsion électromagnétique suivant sa position temporelle par rapport au début du calcul. Les auteurs sont capables en choisissant correctement la position de l'impulsion, de fauter seulement un seul octet du calcul (dû à l'architecture 8 bits du micro-contrôleur). L'octet n'est pas le même suivant la position temporelle choisie, mais pour une position donnée, l'octet fauté est toujours le même et est forcé toujours à la même valeur (cette valeur diffère en fonction de l'octet ciblé). L'attaquant peut donc choisir l'octet qu'il choisit d'impacter, mais il ne peut pas choisir la valeur de cet octet. Cette faute mono-octet permet aux auteurs d'appliquer avec succès une attaque en faute proposée par [Piret and Quisquater, 2003] sur le neuvième round de l'AES. L'attaque a été réalisée sur des circuits avec

des capots ouverts et fermés (dans les deux cas, l'attaque est réalisable). Ces travaux tout comme ceux présentés dans ce manuscrit font partie des contributions du projet ANR EMAISeCi.

2.1.2.2 Attaque harmonique

L'attaque harmonique est définie comme une attaque où le champ électromagnétique émis par la sonde est composé d'une seule fréquence. Elle est appliquée au circuit cible sur une durée en général longue (comparativement à une impulsion).

La première méthode envisagée par les auteurs de [Vargas et al., 2005] propose l'utilisation d'une cellule GTEM (Gigahertz Transverse ElectroMagnetic) - habituellement utilisée en CEM pour étudier l'influence des perturbations électromagnétiques d'une source sinusoïdale à fréquence fixe sur un composant - pour fauter un circuit intégré.

En pratique ce type de cellule se révèle ne pas être adapté à la génération de faute unitaire, tout le circuit se retrouve être soumis à la perturbation et ceci entraîne un défaut de fonctionnement du circuit. Cette méthode n'est pas adaptée à la génération de fautes précises (mono-octet par exemple), mais peut permettre de réaliser une attaque par déni de service sur un composant.

Une autre approche est apportée par les auteurs de [Poucheret et al., 2011a]. Ils ont utilisé, comme moyen d'injection, une sonde micro-métrique reliée à une chaîne d'amplification, et ce dans le but de localiser le champ électromagnétique produit par la sonde. Ils ont, pour prouver la localité du rayonnement électromagnétique produit par ce banc d'injection, effectué des tests d'injection (avec une fréquence de 1 GHz) sur un circuit non alimenté (avec tout les plots d'entrée/sortie reliés à la masse). Le circuit utilisé est un circuit de tests en technologie 350 nm, qui a la particularité d'avoir un réseau d'alimentation presque complètement réalisé en Métal 1 (la couche de métallisation la plus enfouie). Pour mesurer l'effet de l'injection sur le circuit, ils ont mesuré la tension induite par l'injection aux bornes d'alimentation du circuit. Dans le but de prouver la localité de l'injection harmonique, les auteurs ont réalisé une carte qui reflète l'amplitude de la tension induite sur l'alimentation par l'attaque en fonction de la position de la sonde. La carte montre que l'injection harmonique se couple directement avec le réseau d'alimentation (en métal 1) et que les lignes de métallisation supérieures (trois niveaux de métallisation au dessus) jouent le rôle de bouclier contre l'injection électromagnétique. Il est donc possible de superposer à l'alimentation d'un circuit un signal sinusoïdal en choisissant subtilement la position de la sonde.

Les auteurs de [Poucheret et al., 2011b] ont poursuivi l'étude de l'effet de l'injection électromagnétique harmonique sur un circuit en technologie 90 nm. Ce circuit est encore un circuit de tests technologiques sur lequel est situé un oscillateur en anneau et un diviseur de fréquence (compteur de Johnson). Le premier effet observé de l'injection harmonique à 1 GHz sur l'oscillateur est une augmentation de la tension de l'alimentation de ce dernier. Pour une injection à 0.75 mW sur un rail d'alimentation de l'oscillateur, il est possible d'accélérer de 47 % sa fréquence par rapport à

sa fréquence nominale. Cela est comparable à la fréquence de l'oscillateur sous une alimentation de 1.4 V (le circuit est alimenté par une alimentation stabilisée à 1.2 V pendant l'attaque). L'injection harmonique apporte de l'énergie directement liée à la puissance transmise à la sonde. Les auteurs retrouvent la même propriété de localité de l'injection électromagnétique sur ce circuit. Plus la sonde est éloignée du rail d'alimentation, plus l'effet sur l'oscillateur diminue.

Une autre attaque, proposée par les auteurs de [Hayashi et al., 2013] consiste à réaliser le même type d'injection électromagnétique harmonique, mais cette fois ci sur le câble d'alimentation du circuit. Les auteurs de cet article utilisent une bobine magnétique qui vient entourer le câble d'alimentation et induit un courant perturbateur. Cette attaque est notamment intéressante si l'attaquant n'a pas la possibilité d'accéder directement au circuit (par exemple cas d'attaque d'une salle de serveur, ...). L'attaque proposée ici cible un FPGA dans lequel un chiffreur à clé privée (AES) est implanté. L'attaque est réalisée sans signal de synchronisation par rapport aux calculs effectués dans le FPGA. Les auteurs repèrent deux types de fautes :

- Arrêt du fonctionnement du chiffrement.
- Création de glitchs sur l'horloge.

Plus la puissance d'émission est grande, plus l'occurrence des fautes est importante. Il est important de noter que cette attaque est réalisée alors que des composants de filtrage sont présents sur la carte ciblée.

2.1.2.3 Comparatif

Les attaques actives qui utilisent le canal électromagnétique peuvent être classées en deux types :

- Les attaques dites harmoniques : consistent en l'injection d'un signal sinusoïdal. Ce type d'attaque permet de fauter sur l'ensemble de la durée, l'ensemble du circuit [Vargas et al., 2005] et [Hayashi et al., 2013], ou seulement une partie du circuit [Poucheret et al., 2011a], [Poucheret et al., 2011b]. Ce type d'attaque n'est pas capable de créer une faute mono-bit (ou même encore mono-octet). Il n'est donc pas réellement possible avec une attaque de ce type de réaliser une attaque en faute lors d'un chiffrement.
- Les attaques dites impulsionnelles [Schmidt and Hutter, 2007],[Dehbaoui et al., 2012a] et [Dehbaoui et al., 2012b] : consistent à l'envoi d'une impulsion ou d'un train d'impulsions courtes, chaque impulsion a une amplitude très importante (en général, l'amplitude de l'impulsion est supérieure à 100 V). Ce type d'attaque permet de réaliser en général une ou des fautes sur une seule partie de l'opération réalisée par le circuit. Ces attaques correspondent à des attaques lasers, en ayant tout de même beaucoup moins de précision au niveau de la faute injectée ; ce n'est plus une cellule qui est attaquée ici, mais plutôt un bloc de plusieurs cellules suivant le type de sonde et sa position au dessus du circuit.

Un tableau récapitulatif des effets des deux différents types d'attaque est disponible (Tableau 2.1).

	Attaque harmonique	Attaque impulsionnelle
Type de faute	Faute globale sur un calcul	Permet la création de faute précise (un seul octet, voir moins, impacté)
Coût	Moyen : environ 50 000 euros	De faible à moyen, compris entre 100 et 50 000 euros
Analogie	Superposition d'un signal sinusoïdal sur l'alimentation	Glitch, Laser

TAB. 2.1 – Tableau récapitulatif des différences entres les deux types d'attaques actives qui exploitent le canal caché électromagnétique.

Dans le cadre des travaux présentés dans ce manuscrit, nous étudierons les effets des perturbations harmoniques, comme ce qui a été initié dans [Poucheret et al., 2011a], mais d'un point de vue de la génération d'aléa, car cela semble être une méthode très efficace pour impacter les générateurs d'aléa.

2.1.3 Le canal caché électromagnétique et la génération d'aléa ?

Le constat est rapide à faire, avant les travaux présentés dans ce manuscrit, aucune attaque utilisant le canal caché électromagnétique, que ce soit active ou passive, ciblant les générateurs d'aléa n'a été publiée. Nos travaux sont donc précurseurs dans le domaine et suscitent un intérêt croissant, notamment de la part des industriels.

Pourtant, comme on peut le voir précédemment, beaucoup d'articles traitent de l'utilisation, sur différents types d'algorithmes utilisés en cryptographie, du canal caché électromagnétique. Quelles sont les raisons qui font que les générateurs de nombres aléatoires ne sont pas régulièrement plus attaqués ?

Pour essayer de répondre à cette question, d'un point de vue de l'attaque passive, nous allons tout d'abord faire une rapide comparaison d'une structure de générateur de nombres aléatoires standard, et d'un module cryptographique standard (que ce soit un algorithme de chiffrement à clé publique ou privée, hachage, authentification, etc...).

D'après le Tableau 2.2, on voit clairement que la première différence se situe au niveau de la taille des structures. Une structure de générateur d'aléa est en général constituée de moins de 200 cellules logiques élémentaires (bascule, mémoire, porte logique), alors qu'un module cryptographique est en général constitué de plus de 1000 cellules logiques élémentaires. Cette différence de composition entraîne directement une différence dans la consommation de courant des deux structures. En effet, une bascule aura tendance à consommer plus fortement qu'une cellule logique classique (ET, OU, OU-Exclusif, ...) et surtout à générer un fort pic de consommation lorsque cette dernière recopie la valeur d'entrée.

	Module cryptographique	Générateur d'aléa
Surface	Grande : Grand nombre de cellules mémoires >100 portes logiques >100 bascules	Faible : Peu, voire pas de cellules mémoires Environ 100 portes logiques < 100 bascules
Fréquence	< 100 MHz	> 100 MHz
Propriété	Système synchrone	Système fortement asynchrone
Résultat	Consommation importante → Rayonnement fort	Consommation faible → Rayonnement faible

TAB. 2.2 – Mise en évidence des différences de conception entre les principes de génération d'aléa et les autres modules cryptographiques

Pour illustrer cette différence, nous avons réalisé une simple simulation électrique en comparant la consommation de courant entre une bascule et un oscillateur en anneau. Nous avons placé une bascule qui échantillonne (suivant une horloge de fréquence 20 MHz) toujours la même valeur, à savoir un 1 ; et un oscillateur en anneau composé de 21 inverseurs (qui donne une fréquence d'oscillateur proche de 70 MHz). Ces deux structures partagent la même source d'alimentation, et nous avons simplement simulé le courant fourni par cette source. Cette simulation a été réalisée en utilisant Spectre (le simulateur de la suite de logiciel Cadence) sur une technologie AMS 350 nm. Le résultat de cette simulation est représenté dans la Figure 2.8. On voit clairement dans la consommation de courant les différents pics qui correspondent à la bascule et à l'oscillateur en anneau. Ce qu'on peut remarquer premièrement, est la différence de consommation nette entre la bascule et l'anneau (donc une structure purement composée de portes logiques). Comme annoncé dans le Tableau 2.2, cette différence de consommation est encore plus accentuée par le fait que, la consommation des bascules s'effectue au moment des fronts d'horloge, donc synchrone avec l'horloge. Ainsi, plus le nombre de bascules est important, plus ce pic est important. A contrario, les oscillateurs en anneau eux, du fait des variations du processus de fabrication, de la différence de temps de propagation entre les étages, ont des fréquences légèrement différentes, même ils sont composés du même nombre d'éléments. L'appel de courant de chaque anneau ne se fait donc pas forcément en même temps. Il n'y a donc pas d'effet cumulatif de consommation comme cela est le cas pour les bascules. Il est donc évidemment plus dur de faire ressortir l'information qui correspond aux oscillateurs en présence de structures fortement synchrones. Cet effet est illustré par la Figure 2.9. Nous avons, pour cette simulation, mis deux bascules et deux oscillateurs en anneau (de fréquences différentes). On voit clairement sur la consommation de courant que les contributions des oscillateurs sont indiscernables par rapport aux contributions des bascules.

Nous allons montrer dans le Chapitre 3 qu'il est tout de même possible de récupérer des informations importantes sur les oscillateurs, ceci même en présence d'un

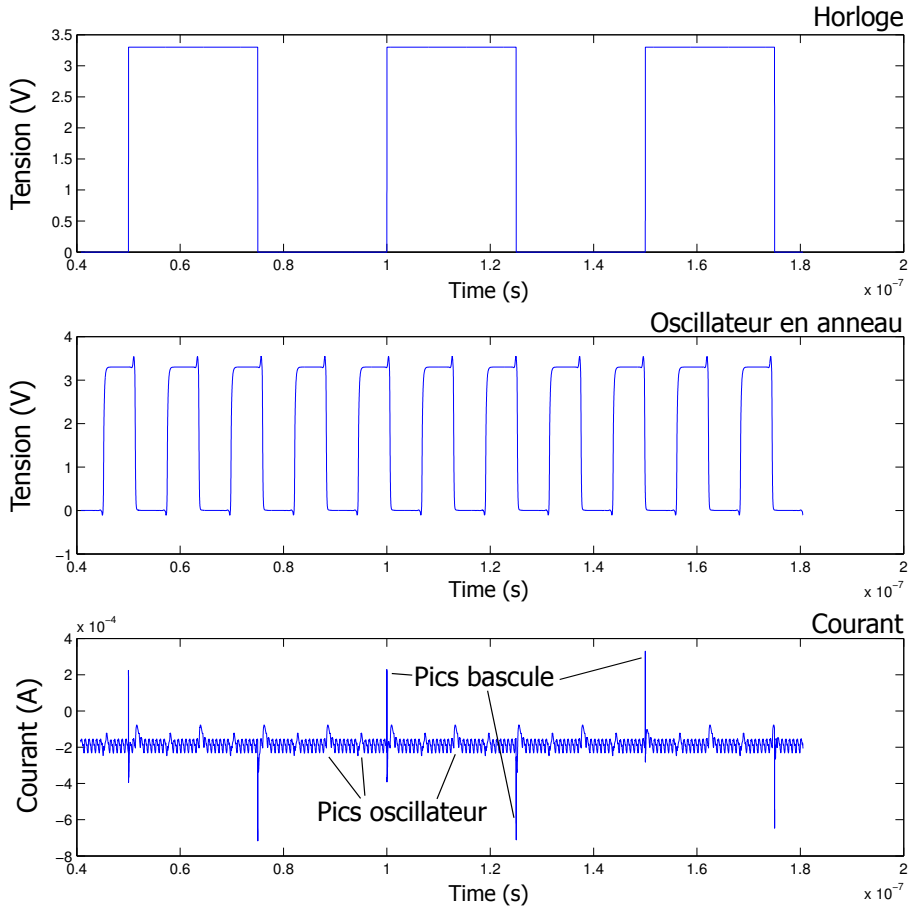

FIG. 2.8 – Résultats de simulation - de haut en bas : horloge utilisée pour échantillonner la bascule D, signal en sortie de l'oscillateur en anneau, courant fourni par l'alimentation.

circuit synchrone de taille importante dans le même circuit, et ce, en adaptant les techniques d'analyse et d'acquisition des traces électromagnétiques.

De plus, dans la communauté scientifique qui travaille sur la sécurité matérielle, il est fréquent que l'étude de la sécurité des générateurs soit délaissée au profit des autres blocs qui composent le système cryptographique, et notamment le chiffreur (ceci s'explique principalement car la majorité des personnes qui travaillent sur ces sujets sont pour la plupart concentrées sur l'étude des chiffreurs). Le chiffreur est certes une pièce maîtresse du système et requiert ainsi une attention particulière, mais il est également possible de corrompre l'intégrité totale du système cryptographique en attaquant le générateur (comme présenté dans le Chapitre 1). Nous présenterons dans le Chapitre 4 une attaque active utilisant le canal électromagnétique, qui offre comme possibilité le contrôle de la suite générée par le générateur.

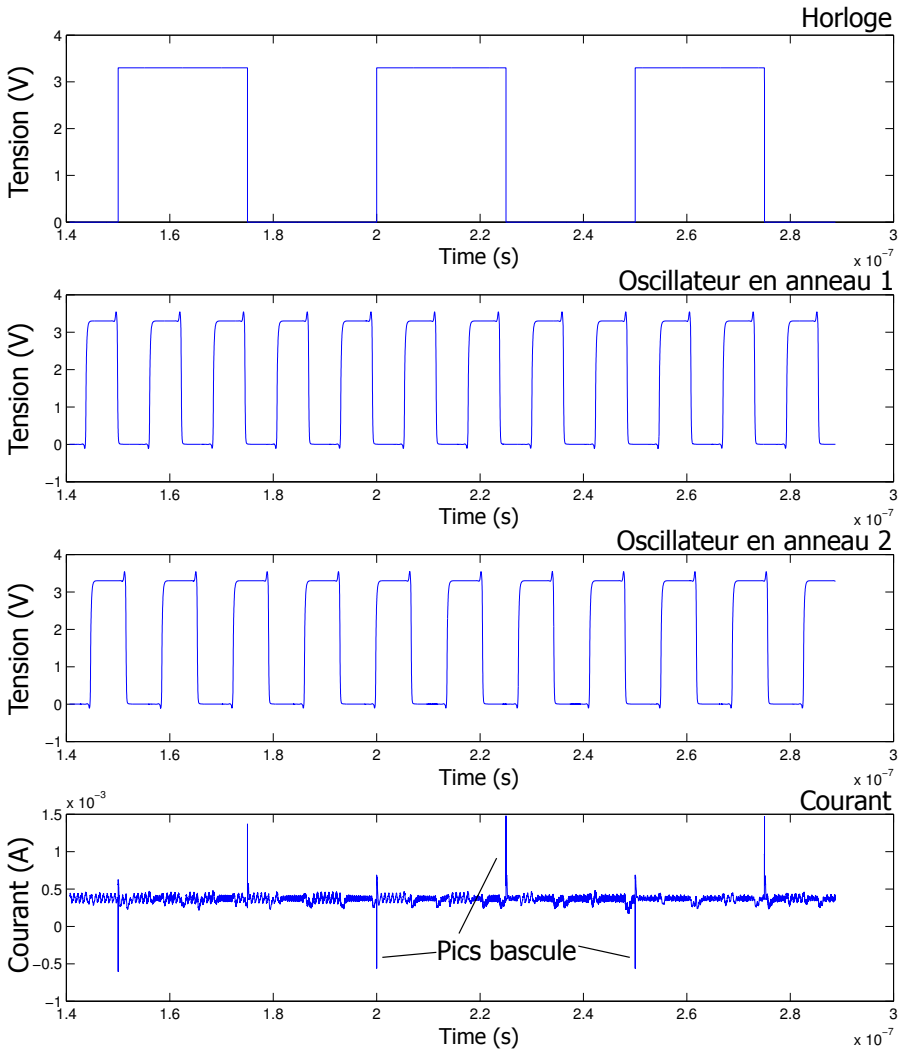

FIG. 2.9 – Résultats de simulation - de haut en bas : horloge utilisée pour échantillonner les deux bascules D, signal en sortie du premier oscillateur en anneau, signal en sortie du deuxième oscillateur en anneau, courant fourni par l'alimentation.

2.2 Bancs de tests électromagnétiques et circuits électroniques ciblés

Dans cette partie, nous allons décrire la composition des deux bancs de tests que nous avons utilisés pour réaliser les travaux présentés dans ce manuscrit. Nous présenterons également une étude de la sonde d'analyse utilisée pour réaliser ces travaux, et ensuite, les cartes électroniques qui ont subi les attaques électromagné-

tiques.

2.2.1 Banc d'analyse

Le banc d'analyse a été élaboré au tout début des travaux présentés dans ce manuscrit. Le choix des éléments constitutifs du banc a été fait en s'appuyant sur la connaissance pratique de partenaires du projet ANR EMAISeCi qui ont eux même des bancs similaires.

Le but principal de cette plateforme est d'acquérir des traces électromagnétiques de systèmes cryptographiques dont notamment les générateurs de nombres aléatoires. Il fut nécessaire de choisir le matériel (notamment par rapport aux fréquences mises en jeu dans les différents principes de génération d'aléa) adapté à ce type de structure.

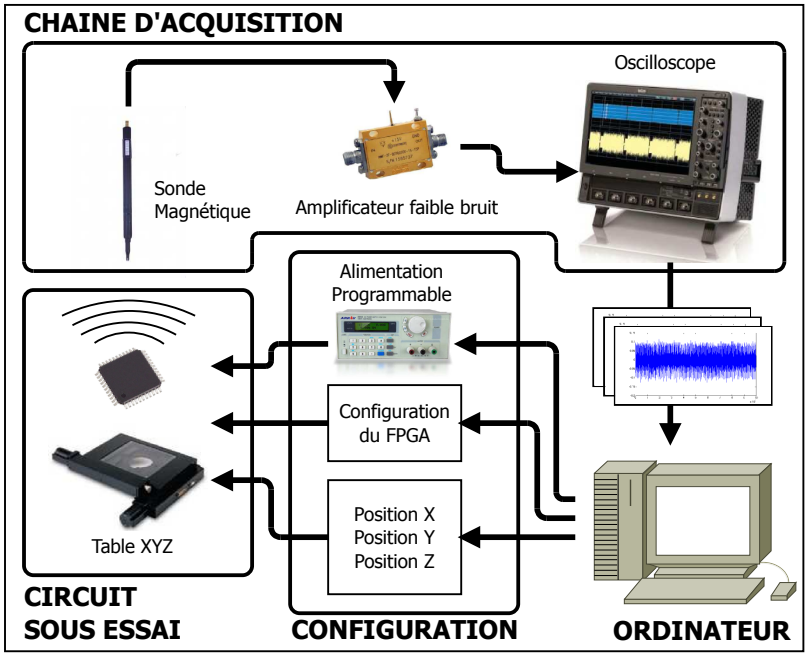

FIG. 2.10 – Schéma de principe du banc d'analyse électromagnétique.

Le banc d'analyse est décrit sur la Figure 2.10. Les principales caractéristiques des éléments qui le composent sont données ci dessous :

- une sonde magnétique LANGER RF-U 2.5-2 :
  - Bande passante : de 30 MHz à 3000 MHz.
  - Résolution spatiale : 500 μm.
- un amplificateur faible bruit MITEQ :
  - Bande passante : 100 MHz à 1 GHz.
  - Gain : 48 dB.
  - Figure de bruit : 0.7 dB.
- un oscilloscope Lecroy WaveRunner 640 Zi :

  - Fréquence d'échantillonnage jusqu'à 40 GS/s (sur deux canaux) et 20 GS/s (sur quatre canaux).
  - Codage sur 12 bits des valeurs acquises.
  - Bande passante jusqu'à 4 GHz.
  - Pilotable par ethernet.
- une alimentation programmable.
- une table XYZ Prior H101A + FB204 :
  - Résolution XY : 10 nm.
  - Répétabilité : $1\mu m$.
- un ordinateur pour contrôler les différents modules.

Ce banc d'analyse a été dupliqué par la société CASSIDIAN Cyber Security et le sera prochainement au laboratoire Lab-STICC.

La mise en œuvre du banc d'analyse a représenté une partie expérimentale très importante pour cette thèse. Un pourcentage significatif du travail nécessaire à la réalisation des travaux a été consacré à ces aspects expérimentaux.

2.2.2 Caractérisation de la sonde d'analyse

Un des éléments cruciaux (avec l'amplificateur faible bruit), du banc d'analyse électromagnétique est la sonde. La sonde choisie pour l'étude du rayonnement des générateurs, notamment pour des raisons pratiques, est une sonde commerciale LANGER RF-U 2.5-2. Cette sonde est seulement sensible aux champs magnétiques. Elle est censée avoir une topologie sensiblement proche d'une boucle. De manière à vérifier cela, nous avons réalisé une simple expérience qui consiste à prendre une piste sur un PCB, y faire traverser un courant sinusoïdal de fréquence f. Le schéma de l'expérience est représenté dans la Figure 2.11. De manière à caractériser la réponse de la sonde à la fois fréquentiellement et en déplacement (pour analyser comment le courant qui traverse la ligne sur le PCB est capté par la sonde suivant sa distance par rapport à la ligne), nous avons fait varier à la fois la fréquence de ce courant (de 50 MHz à 350 MHz) et le déplacement suivant l'axe x de la sonde d'analyse (quelques millimètres de part et d'autres de la ligne).

Le résultat est donc une carte de la ligne qui sur un axe (y) donne la réponse fréquentielle de la ligne et suivant l'axe x donne la réponse en déplacement pour cette fréquence. Le but ici est de vérifier, quelle que soit la fréquence du courant qui parcourt la ligne, la réponse de la sonde est plus ou moins identique. Nous essayerons de voir également les différences obtenues au niveau de la réponse de la sonde pour des orientations de la sonde différentes (0 ° - boucle ou bobinage parallèle à la ligne, 45 ° et 90 ° - boucle ou bobinage perpendiculaire à la ligne ; par exemple la sonde est représentée comme étant à 90 ° dans la Figure 2.11).

La Figure 2.12 montre une de ces cartes pour une orientation de sonde égale à 0 ° . On remarque tout d'abord que suivant la valeur des fréquences, la réponse en déplacement n'est pas la même (il y a un effet périodique qui apparait). En effet, notre installation expérimentale d'injection de courant dans la ligne présente un problème d'adaptation d'impédance. Pour certaines valeurs de fréquence, on

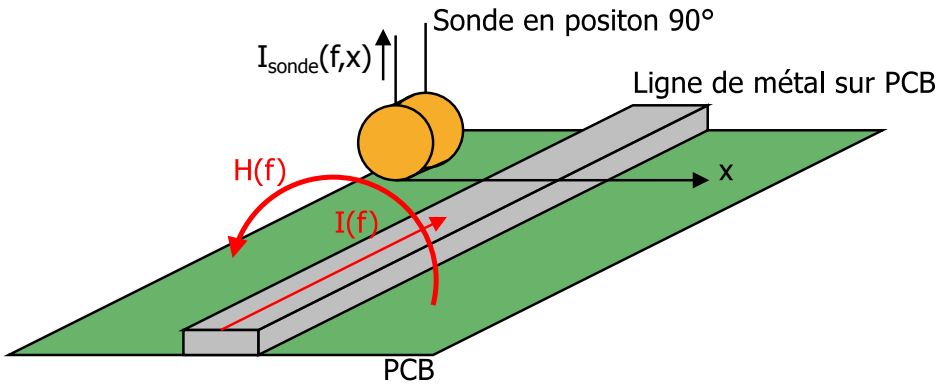

FIG. 2.11 – Schéma de principe de l'expérience de caractérisation de la sonde d'analyse.

remarque la présence de rebonds dans la ligne qui vont créer les zones sombres périodiques.

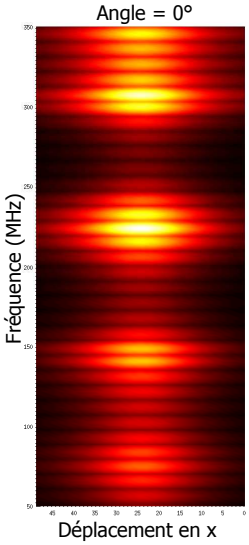

FIG. 2.12 – Carte de la réponse fréquentielle et locale de la sonde pour une ligne située sur un PCB et orientée à 0 °

Par l'application d'une correction de l'effet dû à une mauvaise adaptation d'impédance, nous obtenons les cartes montrées dans la Figure 2.13. Plus la zone sur la carte est claire, plus le champ mesuré est important (l'échelle de couleur est la même pour toutes les cartes). Pour des statistiques sur les valeurs de champs mesurées, voir la Tableau 2.3. On remarque que les orientations à 0 ° et à 45 ° sont relativement identiques. Seule l'amplitude du champ mesuré est différente (plus faible pour 45 °). Le champ généré par la ligne est représenté dans la Figure 2.11. La sonde va

être sensible au champ seulement si le champ entre dans la boucle ou le bobinage. L'orientation à 0 ° est donc évidement l'orientation la plus apte à capter correctement le rayonnement qui provient de cette ligne (cela est d'ailleurs confirmé par la Figure 2.13). On voit clairement que pour l'orientation à 90 ° , même s'il est (quand même) possible de discerner la ligne, le rayonnement capté par la sonde est très faible. Cette position n'est pas du tout adaptée à l'étude du rayonnement. Cependant, l'orientation à 90 ° est adaptée pour des lignes qui sont perpendiculaires à la ligne présentée dans Figure 2.11 (et donc par extension l'orientation à 0 ° est non adaptée à l'étude de ces lignes). Dans un circuit intégré comme présenté dans l'Annexe A, les lignes et les interconnexions vont être orientées dans les deux sens. Dans ce cas, deux solutions existent pour s'assurer de récolter tout le rayonnement et les contributions du circuit intégré :

- Effectuer, pour chaque analyse, une mesure pour une orientation de sonde à 0 ° et 90 ° .
- Effectuer simplement une mesure pour une orientation de sonde à 45 ° .

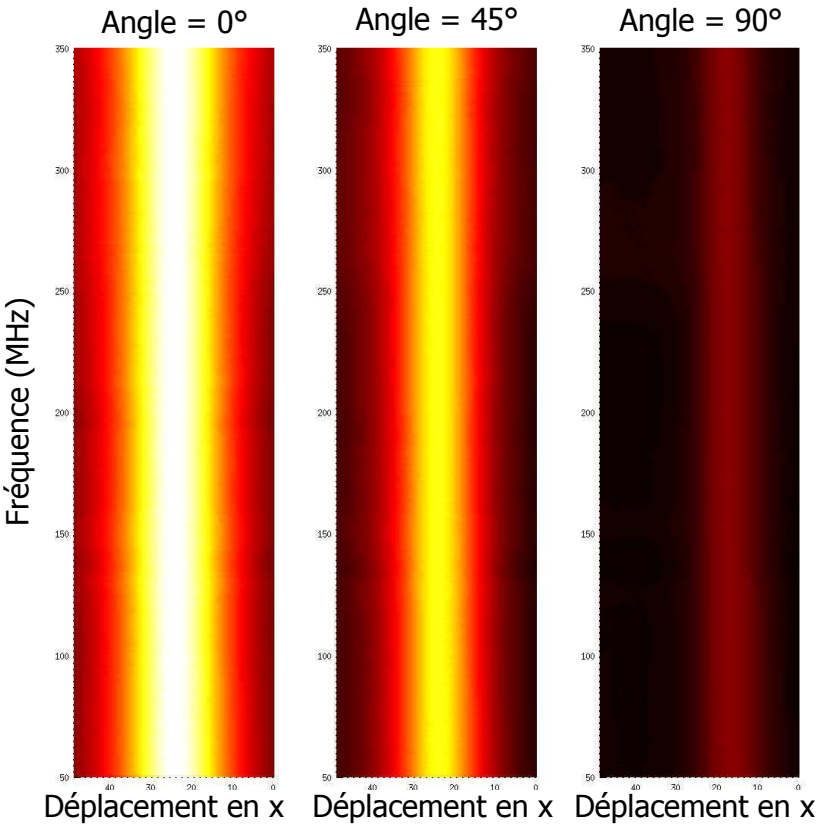

FIG. 2.13 – Cartes de la réponse fréquentielle et locale de la sonde pour une ligne située sur un PCB et orientée à 0 ° , 45 ° et 90 °

La deuxième solution semble être la plus raisonnable, la réponse de la sonde est

sensiblement la même pour 0 ° et 45 ° .

Note : la différence en déplacement pour l'orientation à 90 ° est due au fait que la pointe de la sonde n'est pas complètement symétrique par rapport à l'axe utilisé pour orienter la sonde.

TAB. 2.3 – Valeur de l'amplitude du champ mesurée à l'oscilloscope pour différentes orientations de sonde.

Angle	Amplitude maximum	Amplitude moyenne sur toute la surface
0 °	370 mV	90 mV
45 °	350 mV	68 mV
90 °	126 mV	17 mV

2.2.3 Banc d'injection harmonique

Le banc d'injection harmonique appartient au LIRMM (Laboratoire d'informatique, de robotique et de microélectronique de Montpellier) [Poucheret et al., 2011a] et [Poucheret et al., 2011b].

Le banc d'injection est décrit sur la Figure 2.14. Les principales caractéristiques des éléments qui le composent sont données ci dessous :

- une sonde d'émission : nous avons utilisé à la fois des sondes magnétiques et des sondes électriques.
- un amplificateur de puissance de 50 W.
- un générateur de signal RF.
- un coupleur qui permet la mesure de la puissance envoyée à la sonde et de la puissance retournée par la sonde.
- un puissance-mètre qui effectue cette mesure.
- une alimentation programmable.
- un oscillateur Lecroy WavePro 725Zi-A :
  - Fréquence d'échantillonnage jusqu'à 40 GS/s (sur deux canaux) et 20 GS/s (sur quatre canaux).
  - Codage sur 8 bits des valeurs acquises.
  - Bande passante jusqu'à 2.5 GHz.
  - Pilotable par ethernet.
- une table XYZ.
- une cage de Faraday qui protège l'utilisateur du rayonnement électromagnétique émis par la sonde (atténuation de 120dB).
- un ordinateur pour contrôler l'ensemble de la chaîne d'injection.

Le schéma de principe du banc peut être trouvé dans la Figure 2.14.

L'élément clé de cette plateforme est la sonde qui convertit l'énergie électrique en un champ électromagnétique. La plupart des sondes électromagnétiques utilisées pour caractériser la susceptibilité électromagnétique des composants (voir [Dubois et al., 2008]) sont inductives. Elles sont composées d'un bobinage dans lequel un fort courant est injecté. Le problème de ce type de sonde, est que pour réduire le

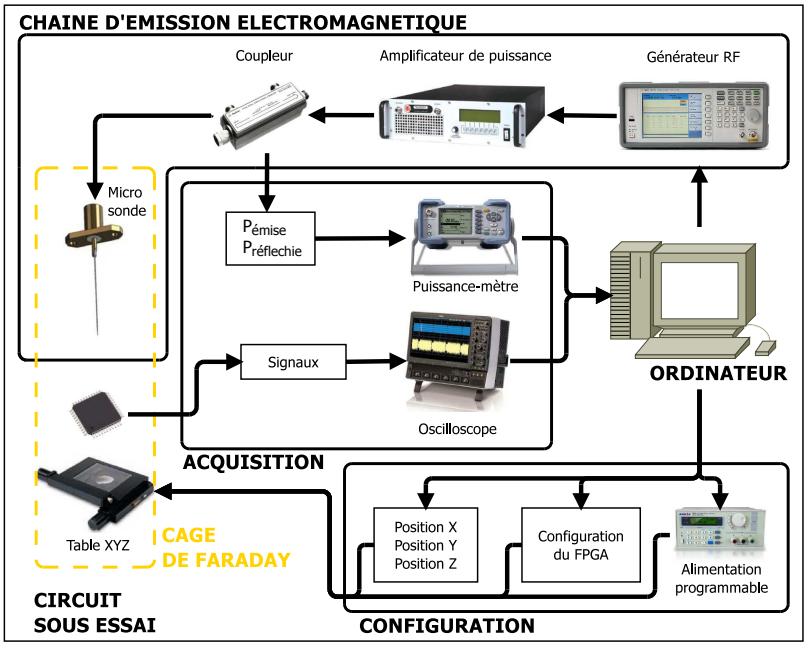

FIG. 2.14 – Schéma de principe du banc d'injection électromagnétique de signal harmonique.

diamètre du bobinage, il est nécessaire de réduire la section du fil utilisé. Il n'est donc plus possible d'injecter un fort courant pour des sondes micrométriques. En conséquence, il a été vérifié expérimentalement que la puissance injectée dans la sonde n'est plus suffisante pour perturber le comportement des portes logiques.

La sonde utilisée n'a donc pas la même topologie. Elle est issue d'un long prototypage, et le dernier modèle retenu est présenté dans la Figure 2.15. Cette sonde est faite d'un fin fil de tungstène de trois centimètres de long et qui a un diamètre de 200 μm d'un coté et de 10 μm de l'autre (coté pointe).

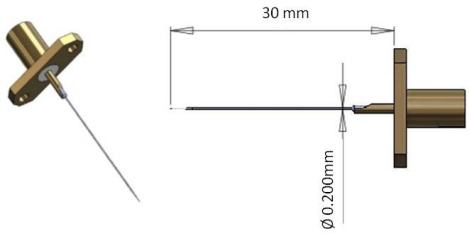

FIG. 2.15 – Micro-sonde uni-polaire.

Cette sonde produit principalement un champ électrique au bout de la pointe de cette dernière. C'est ce champ électrique qui perturbera par la suite le circuit intégré ciblé. Plus d'informations sur la plateforme et les effets de l'injection électromagnétique harmonique sont disponibles dans [Poucheret et al., 2011a] et [Poucheret et al., 2011b].

2.2.4 Cartes électroniques

Les cartes utilisées pour les travaux présentés dans la suite sont des cartes produites par la société Micronic. Le schéma de principe de ces cartes est présenté dans la Figure 2.16. Ces cartes sont adaptées à l'étude de la génération d'aléa. En effet, l'utilisation d'une alimentation linéaire propre permet une étude précise de l'aléa produit par le générateur. Comme il est possible de voir sur la Figure 2.16, une autre particularité de ces cartes réside dans leur construction. Elles sont composées d'une carte mère et d'une carte fille (voir la Figure 2.17 pour avoir un aperçu). La carte mère gère la connexion de la carte vers l'extérieur, c'est à dire, à la fois la communication (via l'USB), mais aussi l'alimentation (trois chemins d'alimentation différents configurables). La carte fille elle, contient le FPGA, l'alimentation du FPGA (cœur du FPGA et entrée/sortie) et un module de mémoire pour stocker des données.

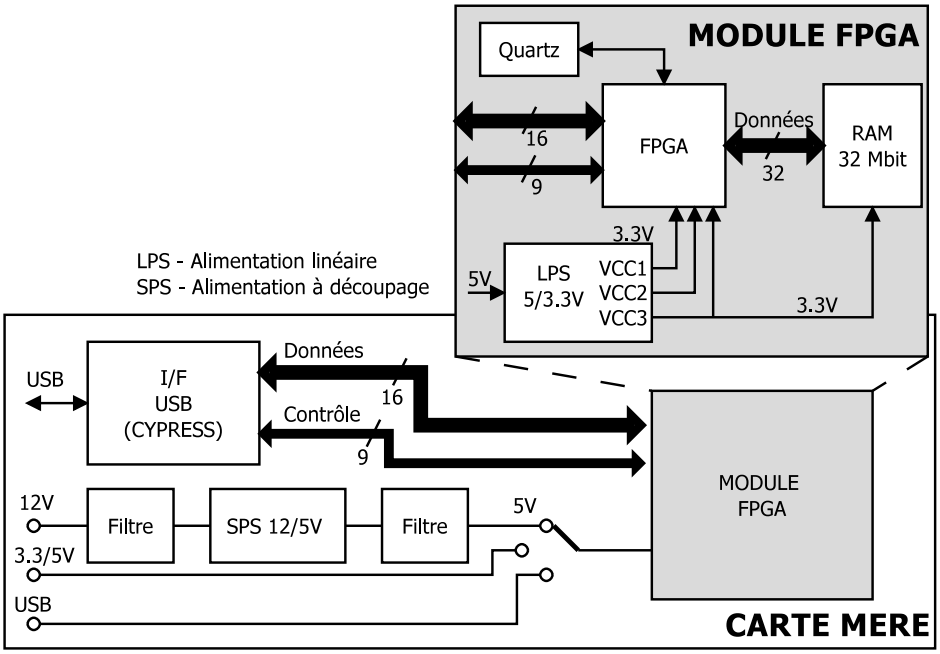

FIG. 2.16 – Schéma de principe des cartes utilisées.

Plusieurs cartes filles existent - chacune d'entres elles embarque un modèle différent de FPGA :

- Altera CycloneIII
- Altera CycloneIII (carte adaptée pour la réalisation d'attaque de type DPA).
- Altera Aria 2 GX
- Microsemi Fusion AFS700A
- Xilinx Spartan3AN
- Xilinx Virtex5

Pour obtenir plus d'informations sur ces cartes voir [EVARISTE, 2013].

L'idée de ces cartes est donc d'avoir une base similaire et adaptée à l'étude de

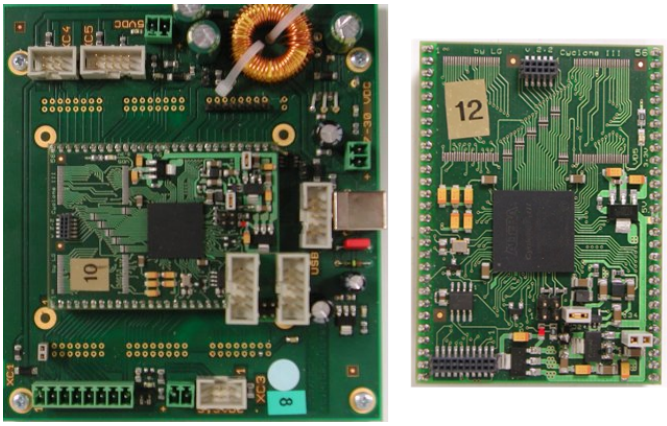

FIG. 2.17 – Photo de la carte mère et d'une carte fille à gauche. Photo d'une carte fille Altera Cyclone III à droite.

la génération d'aléa afin de pouvoir plus facilement comparer l'implantation des principes de générateurs d'aléa sur différentes familles de FPGA. Mis à part la carte fille Altera CycloneIII adaptée à la réalisation d'attaque de type DPA (que nous n'avons pas utilisé dans les études présentées ici), ces cartes ne sont donc pas adaptées à la réalisation d'attaques.

2.3 Conclusion

Nous avons pu voir dans ce chapitre une attaque dans l'état de l'art qui implique la perturbation d'un oscillateur en anneau à l'aide d'un champ électromagnétique harmonique ([Poucheret et al., 2011b]). On le rappelle, ce champ électromagnétique (réglé à une fréquence d'excitation de 1 GHz) est capable de modifier la fréquence de fonctionnement d'un oscillateur en anneau. Nous allons donc nous proposer d'étudier l'effet d'une telle injection électromagnétique sur plusieurs oscillateurs en anneau implantés dans un FPGA (et utilisés comme source d'aléa d'un générateur). Le but étant bien évidemment de perturber le plus d'oscillateurs possibles.

Au même titre, le canal caché électromagnétique est très riche quant à l'extraction d'information. Il est possible grâce à lui de récupérer des informations par rapport aux fréquences mises en jeu à l'intérieur du circuit et également récupérer des informations sur la position (dans le circuit) où ces fréquences sont particulièrement présentes. Il est donc potentiellement possible d'appliquer ce type d'analyse à un générateur de nombres aléatoires.

Nous nous proposons donc d'étudier le générateur présenté dans le chapitre précédent ([Wold and Tan, 2008]). Cependant, nous souhaitons réaliser l'attaque comme si nous n'avions aucune information préalable sur le circuit attaqué et sur le réglage du générateur d'aléa (fréquence des oscillateurs en anneau et position du générateur dans le circuit).

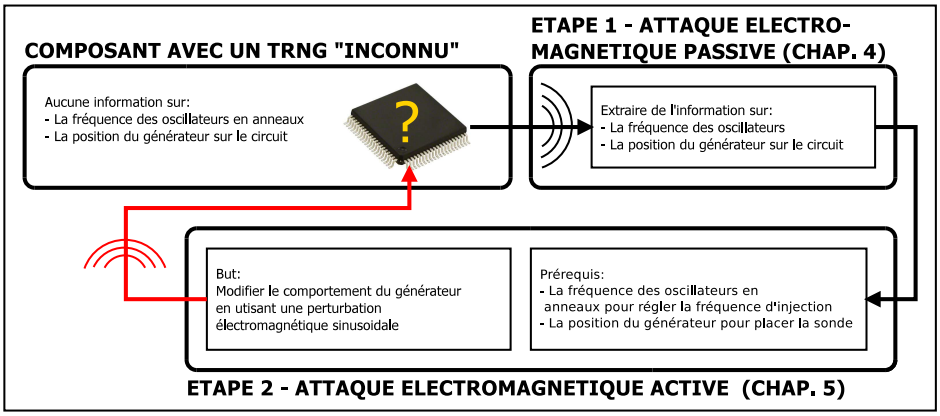

FIG. 2.18 – Présentation de l'attaque électromagnétique combinée.

Pour ce faire, nous proposons de suivre la méthodologie d'attaque électromagnétique combinée présentée dans la Figure 2.18. Cette attaque combinée consiste simplement à coupler une pré-analyse du champ électromagnétique à une attaque électromagnétique active dans le but de faciliter cette dernière qui nécessite des informations sur notamment la fréquence de fonctionnement du générateur (pour régler la fréquence du signal harmonique injecté) ou encore sa position (pour placer le plus efficacement la sonde d'injection au dessus de la partie que nous voulons influencer).

Nous allons donc dans les chapitres suivants présenter l'analyse du champ élec-

tromagnétique appliquée sur le générateur d'aléa, puis l'attaque électromagnétique active sur ce même générateur.

Chapitre 3

Utilisation du rayonnement électromagnétique des circuits intégrés comme source d'information sur les générateurs d'aléa

Dans ce chapitre nous présenterons le principe des différentes analyses cartographiques du rayonnement électromagnétique. Ensuite, nous expliquerons en détail la méthode retenue pour analyser les contributions des générateurs d'aléa à base d'oscillateurs en anneau.

Sommaire du chapitre

2.1 Utilisation du rayonnement électromagnétique comme canal d'attaque 20

2.1.1 Le canal électromagnétique comme moyen de récupération d'information 20

2.1.1.1 Découverte de la fuite d'information inopinée des circuits électriques 20

2.1.1.2 L'analyse du champ électromagnétique en champ proche 24

2.1.1.3 Étude comparative des fuites électromagnétiques . . 27

2.1.1.4 Localisation de blocs cryptographiques enfouis dans un circuit intégré 27

2.1.1.5 Matériel pour l'analyse en champ proche 29

2.1.1.6 Contremesures contre l'analyse en champ proche ? . 30

2.1.2 Le canal électromagnétique comme canal d'attaque active . . 33

2.1.2.1 Attaque impulsionnelle 33

2.1.2.2 Attaque harmonique 35

2.1.2.3 Comparatif 36

2.1.3 Le canal caché électromagnétique et la génération d'aléa ? . . 37

2.2 Bancs de tests électromagnétiques et circuits électroniques ciblés 40

2.2.1 Banc d'analyse 41

2.2.2 Caractérisation de la sonde d'analyse 42

2.2.3 Banc d'injection harmonique 45

2.2.4 Cartes électroniques 47
2.3 Conclusion 49

3.1 Objectif

Dans le cas des générateurs d'aléa, le but de l'analyse est de récupérer le plus d'information possible sur le générateur de manière à pouvoir par la suite réaliser une attaque active qui, elle, a pour but de perturber son fonctionnement.

En effet, le fonctionnement propre du générateur ne permet pas d'effectuer une analyse de type DPA sur ce type de structure, pour par exemple retrouver la suite de bits générée par le générateur (à chaque fois, les données créées par le générateur sont différentes).

Nous allons montrer dans ce chapitre qu'il est possible, en utilisant une propriété des oscillateurs en anneau, de retrouver les fréquences de fonctionnement des oscillateurs et leurs positions sur le circuit.

3.2 Différentes techniques de cartographie

Les différentes techniques de cartographie présentées précédemment (voir Chapitre 2), et dont nous allons détailler maintenant le principe d'analyse, ont toutes en commun le mode opératoire de création des cartes. La réalisation d'une carte nécessite en premier lieu de délimiter le circuit à étudier en zones (ou points) de même taille, comme cela est présenté dans la Figure 3.1. Ici le circuit est découpé en 225 zones (15x15). Pour chaque zone, une ou plusieurs traces du rayonnement électromagnétique sont acquises avec un oscilloscope. Le but final est d'obtenir une seule valeur pour chaque zone (pour le moment nous avons une trace du rayonnement électromagnétique qui est composée de plusieurs valeurs). C'est dans ce cadre que les analyses propres aux cartographies entrent en jeu (transformer les traces en une métrique unique). Nous allons présenter quatre analyses dans la suite, et, ensuite expliquer le type d'analyse que nous avons utilisé pour extraire l'information contenue dans le rayonnement électromagnétique des générateurs d'aléa.

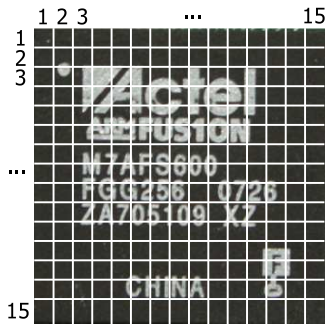

Fig. 3.1 – Principe de quadrillage d'un circuit intégré pour réaliser des cartes du rayonnement électromagnétique.

3.2.1 Cartographie temporelle

Cette analyse, présentée par les auteurs de [Sauvage et al., 2009] est la plus simple et la plus rapide à réaliser. En effet, comme son nom l'indique, elle opère une mesure sur la trace du rayonnement électromagnétique, ou encore trace « temporelle » (aucune transformation de la trace n'est nécessaire). Dans le cadre de l'étude menée par les auteurs de [Sauvage et al., 2009], la mesure effectuée sur la trace temporelle est un mesure du maximum de la valeur pic à pic de la trace.

Cette analyse, bien qu'elle soit rapide et facilement réalisable, n'apporte en général aucune information intéressante à l'attaquant. En effet, les zones qui rayonnent le plus sur un circuit sont les blocs analogiques (horloge, alimentation, ...) ou les connexions vers l'extérieur (pad, bounding, ...), en d'autres mots, tout ce qui n'est pas la partie intéressante de la puce pour un attaquant. Les contributions de ces blocs à la fuite d'information (provenant des blocs cryptographique ciblés) sont en général très faibles, voir inexistantes. Cette analyse donne en général une image de la consommation de courant du circuit (on le rappelle encore, le rayonnement électromagnétique est directement lié à la consommation de courant du circuit).

Nous confirmerons dans la suite l'inefficacité de cette analyse quant à son utilisation sur des générateurs d'aléas.

3.2.2 Cartographie à analyse fréquentielle

Cette technique de cartographie est également proposée par les auteurs de [Sauvage et al., 2009]. Le principe est décrit dans la Figure 3.2. Au dessus de chaque point du quadrillage, une mesure du rayonnement électromagnétique est réalisée et la densité spectrale de puissance correspondant à cette mesure est calculée à l'aide d'une transformée de Fourier. Par la suite l'attaquant sélectionne une fréquence (voir une bande de fréquences) et trace la carte de la valeur d'amplitude dans le spectre de cette fréquence (ou de cette bande de fréquences). Les cartes résultantes sont des images de la consommation de courant du circuit pour une fréquence donnée. A la différence de l'analyse précédente, cette analyse permet donc de masquer les contributions qui n'ont pas de rapport avec le système cryptographique ciblé.

Cette technique de cartographie est relativement rapide à réaliser (certes moins rapide que l'analyse temporelle). Elle peut même être faite à la volée pendant l'acquisition des traces du rayonnement électromagnétique. Cependant le gros du travail est de définir les fréquences mises en jeu par le système cryptographique. Si la cible des attaques est un chiffreur à clé privée (AES, DES, ...) qui est en général composé principalement de bascules, la fréquence d'horloge (ou ses harmoniques) de ces bascules est en général une bonne candidate. Cette fréquence d'horloge est en général relativement simple à identifier dans le spectre, car son amplitude sera l'une des plus importantes. Cette analyse est une bonne candidate pour l'analyse des systèmes contenant des générateurs de nombres aléatoires à base d'oscillateurs en anneau, car, si l'attaquant a la connaissance des fréquences des oscillateurs, il pourra potentiellement facilement retrouver la position des oscillateurs sur le circuit. Nous verrons

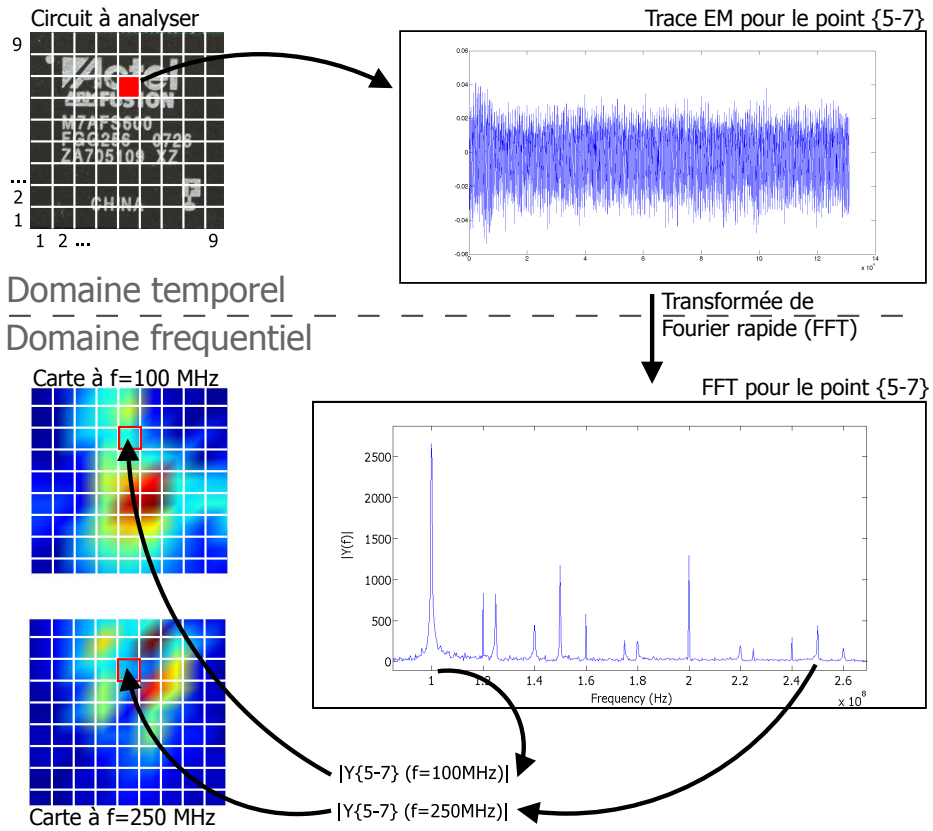

FIG. 3.2 – Principe de la technique de cartographie électromagnétique basée sur l'analyse fréquentielle

dans la suite qu'il n'est pas si aisé de retrouver les fréquences des oscillateurs dans un spectre fréquentiel et qu'il sera nécessaire de modifier en partie l'analyse pour la rendre plus efficace.

Les auteurs de [Sauvage et al., 2009], conseillent pour l'utilisation de cette analyse, de réaliser une moyenne de plusieurs traces pour chaque point. Pour notre cas d'étude, il n'est pas conseillé de réaliser cette opération, car effectuer une moyenne des traces temporelles du rayonnement électromagnétique diminue les contributions liées au générateur dans le spectre fréquentiel. Il est donc encore moins aisé de trouver les fréquences qui correspondent au générateur. Néanmoins il est conseillé de réaliser une moyenne des spectres fréquentiels.

3.2.3 WGMSI - Mesure d'incohérence dans la densité spectrale de puissance

Cette analyse présentée par les auteurs de [Dehbaoui et al., 2009] se base sur le principe que d'une mesure à l'autre, certaines portes logiques font toujours la même chose, (c'est à dire sont dans le même état), alors que d'autres ne manipulent pas forcement la même donnée (elles sont donc dans un état différent suivant la mesure).

Les auteurs créent donc un indicateur qui permet d'évaluer la cohérence (MSC) ou l'incohérence (MSI) du rayonnement électromagnétique :

$$MSC_{w_1,w_2}(f) = \frac{P_{w_1,w_2}(f)^2}{P_{w_1,w_1}(f)P_{w_2,w_2}(f)} \tag{3.1}$$

$$MSI_{w_1,w_2}(f) = 1 - MSC_{w_1,w_2}(f) \tag{3.2}$$

où :

- $w_1(t), w_2(t)$ sont les mesures effectuées à des instants différents,
- $P_{w_1,w_1}(f)$ est la densité spectrale de puissance pour la première mesure,
- $P_{w_1,w_2}(f)$ est la densité spectrale de puissance croisée pour les mesures 1 et 2.

Si pour une valeur de fréquence donnée, $MSI(f)$ (Magnitude Squared Incoherence) est égale à 1, la mesure est fortement incohérente pour cette fréquence. Au contraire, si elle est égale à 0, la mesure est fortement cohérente. Pour évaluer l'incohérence de la trace complète (donc sur tout le spectre de la trace et non seulement sur une valeur de fréquence), les auteurs ont introduit un autre évaluateur, à savoir :

$$WGMSI = \int_{f \in BP} \frac{MSI(f)}{nf} \frac{A_{w_2}(f)}{max(A_{w_2}(f))} df \tag{3.3}$$

où :

- $A_{w_2}(f)$ est l'amplitude de la densité spectrale de puissance pour la valeur de f,
- nf est le nombre de points dans la densité spectrale de puissance.

Au même titre que l'évaluateur précédent, si $WGMSI$ (Weighted Magnitude Squared Spectral Incoherence) tend vers 1, la mesure est complètement incohérente et donc dépendante des données (sur tout le spectre), alors que si $WGMSI$ tend vers 0, la mesure est cohérente et n'est pas dépendante des données.

Cet évaluateur permet donc de différencier sur un circuit les blocs qui manipulent des données différentes à chaque fois (chiffreur par exemple) et des blocs qui manipulent plutôt les mêmes données (source d'horloge - même si dans le cas de l'horloge il n'est pas forcement juste de parler de donnée, bloc analogique, etc ...).

Cependant la différence de valeur de l'évaluateur $WGMSI$ entre un bloc dépendant de la donnée et un bloc qui ne l'est pas, est relativement faible. En effet, seulement une partie des fréquences du spectre porte l'information de non cohérence.

Cette analyse requiert l'acquisition de plusieurs traces du rayonnement électromagnétique pour chaque point, avec des données manipulées différentes. Elle requiert également un calcul supplémentaire par rapport à une analyse fréquentielle simple, mais cette analyse présente l'avantage de ne pas avoir besoin de connaissance préalable sur l'algorithme attaqué. Il n'est en effet pas nécessaire d'avoir une information sur la fréquence de fonctionnement du circuit.

3.2.4 Cartographie de corrélation croisée

La dernière analyse ([Sauvage et al., 2010]) que nous présentons, se fonde sur le même type de principe. Cependant, contrairement à l'analyse proposée par les auteurs de [Dehbaoui et al., 2009], la mesure de cohérence s'effectue dans le domaine temporel plutôt que dans le domaine fréquentiel. L'analyse se base sur une évaluation de corrélation croisée entre deux traces en deux points différents du circuit. Cette évaluation de corrélation croisée est donnée par l'équation suivante :

$\Gamma_{A,B}(d) = \frac{cov(A,B_d)}{\sigma_A \sigma_B}$

où :

- A et B sont les traces récupérées aux points sélectionnés du circuit,
- *cov* est la mesure de covariance,
- d est le décalage temporel entre les deux traces A et B,
- σ_A et σ_B sont les déviations standard des traces A et B.

Le maximum de la valeur absolue de $\Gamma_{A,B}(d)$ donne l'évaluation de la cohérence entre les deux traces temporelles. Plus ce chiffre est proche de 1, plus les deux traces sont cohérentes (et donc correspondent au rayonnement électromagnétique du même bloc).

L'idée est donc, pour chaque point de la carte (qui agira comme point de référence), d'évaluer la corrélation croisée de la trace acquise en ce point avec les traces acquises pour tous les autres points de la carte. Cette carte représente le maximum de cohérence entre le point de référence et les autres points de la carte. Il en résulte donc N cartes (où N est le nombre de points qui constituent les cartes). Le problème est que manipuler N cartes (si N est important) n'est pas forcément très simple. Les auteurs proposent donc d'appliquer à ces N cartes un nouveau traitement qui permet de regrouper les cartes qui sont trop similaires en un seul groupe. En effet, pour des points situés sur le même bloc logique, leurs rayonnements sont fortement corrélés, les cartes produites pour ces points sont donc sensiblement similaires (ou encore corrélées). Pour regrouper ces cartes, les auteurs proposent un autre évaluateur basé sur une estimation de la corrélation (l'évaluation se fait en 2D cette fois ci). Chaque groupe de carte correspond alors à un bloc logique qui manipule les mêmes données.

L'avantage principal de cette technique de cartographie est que, même sans aucune connaissance du circuit ciblé, il est possible de discerner la position des blocs qui ne manipulent pas les mêmes données. Il reste encore après à discerner l'utilité de chaque bloc (en regardant les traces du rayonnement électromagnétique au dessus de chaque bloc par exemple).

Néanmoins, cette technique de cartographie demande beaucoup de calculs. Les calculs de corrélation sont longs à effectuer et il faut au total, pour une carte composée de M par M points, effectuer $\frac{M^2(M^2+1)}{2}$ calculs de corrélation pour concevoir toutes les cartes (donc sans compter les corrélations 2D pour regrouper les cartes les unes avec les autres).

Du point de vue de l'analyse des générateurs d'aléa, cette technique n'est pas forcement la plus adaptée. Comme pour l'analyse $WGMSI$, d'un moment à l'autre,

les données générées (donc manipulées) par le générateur d'aléa vont être différentes. De ce fait, la corrélation entre deux traces du rayonnement électromagnétique prises au dessus d'un générateur d'aléa en deux points différents est forcement faible. Pour l'analyse de corrélation, les deux points sont alors comptés comme n'étant pas du même bloc, alors qu'en réalité ils le sont.

3.3 Présentation de l'analyse électromagnétique appliquée aux générateurs d'aléa

Dans le cas d'application sur les générateurs de nombres aléatoires à base d'éléments oscillants (oscillateur en anneau ou autre), nous avons décidé de nous orienter vers une technique de cartographie à base d'analyse fréquentielle des traces du rayonnement électromagnétique ; ce type d'analyse nous semble être le plus adapté à notre cas d'étude.

Cependant, comme cela a été montré dans le chapitre précédent, la logique utilisée dans ces structures oscillantes consomme moins de courant que les autres blocs composant le système cryptographique (voir la section 3.1.5 et notamment la figure Figure 2.9). Le champ électromagnétique rayonné par un circuit électronique dépend directement de la consommation de courant locale (c'est à dire, le courant consommé par les blocs électroniques situés dans la zone « vue » par la sonde). La consommation du générateur, qui n'est en général pas composé de beaucoup de bascules, va donc être très faible par rapport aux autres blocs qui eux peuvent être composés de beaucoup de bascules (c'est notamment vrai pour un chiffreur à clé privée par exemple). Il est donc nécessaire, de façon à pouvoir discerner les fréquences mis en jeux par le générateur (qui auront une faible amplitude dans le spectre fréquentiel de la trace du rayonnement électromagnétique), de trouver une méthode pour faire ressortir facilement les contributions du générateur dans le spectre fréquentiel.

Comme cela a été dit précédemment, dans la présentation de l'analyse fréquentielle, la difficulté est de trouver les fréquences qui correspondent à notre cible. Pour un chiffreur, ceci est en général simple, il suffit de repérer les fréquences de l'horloge utilisée pour échantillonner les bascules qui composent le chiffreur. Sur la densité spectrale de puissance de la trace du rayonnement électromagnétique, c'est en général la fréquence qui a le pic d'amplitude la plus élevée. En ce qui concerne les générateurs d'aléa à base d'oscillateurs en anneau, nous avons déjà expliqué pourquoi leurs rayonnements sont faibles (et par extension, les contributions spectrales du générateur aux fréquences mises en jeu, c'est à dire les fréquences des oscillateurs, ont des amplitudes faibles). Il est donc difficile sans méthode particulière de trouver les fréquences qui correspondent aux oscillateurs.

Pour illustrer cela, la Figure 3.3 représente la densité spectrale de puissance d'une trace du rayonnement électromagnétique prise au dessus d'un générateur d'aléa. Sans connaître approximativement les valeurs de fréquence (il faut aussi également savoir à quel endroit du circuit regarder), il n'est pas possible de dire quelles fréquences correspondent au générateur. Il faut donc une méthode à partir des spectres pour

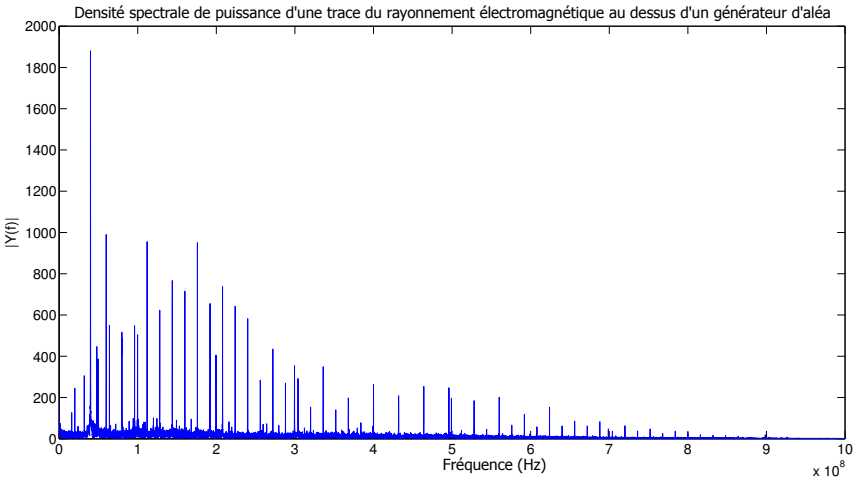

FIG. 3.3 – Densité spectrale de puissance d'une trace du rayonnement électromagnétique au dessus d'un générateur d'aléa (les contributions des oscillateurs se situent entre [325-331 MHz]).

discerner les fréquences utiles (celles des oscillateurs) des autres fréquences.

Les oscillateurs en anneau sont connus pour être sensibles, du point de vue de la fréquence de l'horloge produite, aux paramètres de fonctionnement du circuit (température, tension d'alimentation), mais aussi aux paramètres de fabrication du circuit. Ils sont d'ailleurs utilisés comme capteur de température dans les circuits intégrés [Arabi and Kaminska, 1997]. La méthode que nous proposons se base sur cette propriété des oscillateurs en anneau. Pour deux conditions de fonctionnement différentes, les fréquences des oscillateurs sont différentes. Les fréquences qui ne nous intéressent pas (qui sont principalement les sources d'horloges) ne devraient pas, elles, changer, ou du moins, pas dans les mêmes proportions. Donc en soustrayant le spectre fréquentiel pour une condition de fonctionnement et le spectre fréquentiel pour une autre condition, les contributions des oscillateurs devraient ressortir et être prépondérantes devant les autres contributions. La méthode est décrite dans la Figure 3.4. C'est cette technique d'analyse que nous allons étudier dans la suite de ce chapitre.

Nous avons choisi de modifier la tension d'alimentation du circuit dans la suite car cela est plus simple pour nous. Nous ne disposons d'aucun matériel qui permette de modifier la température d'un circuit suffisamment précisément et de façon stable sur un long temps (étuve ou four). Cependant, avec un chauffage d'appoint (environ 30 euros), il est tout de même possible d'obtenir des résultats satisfaisants.

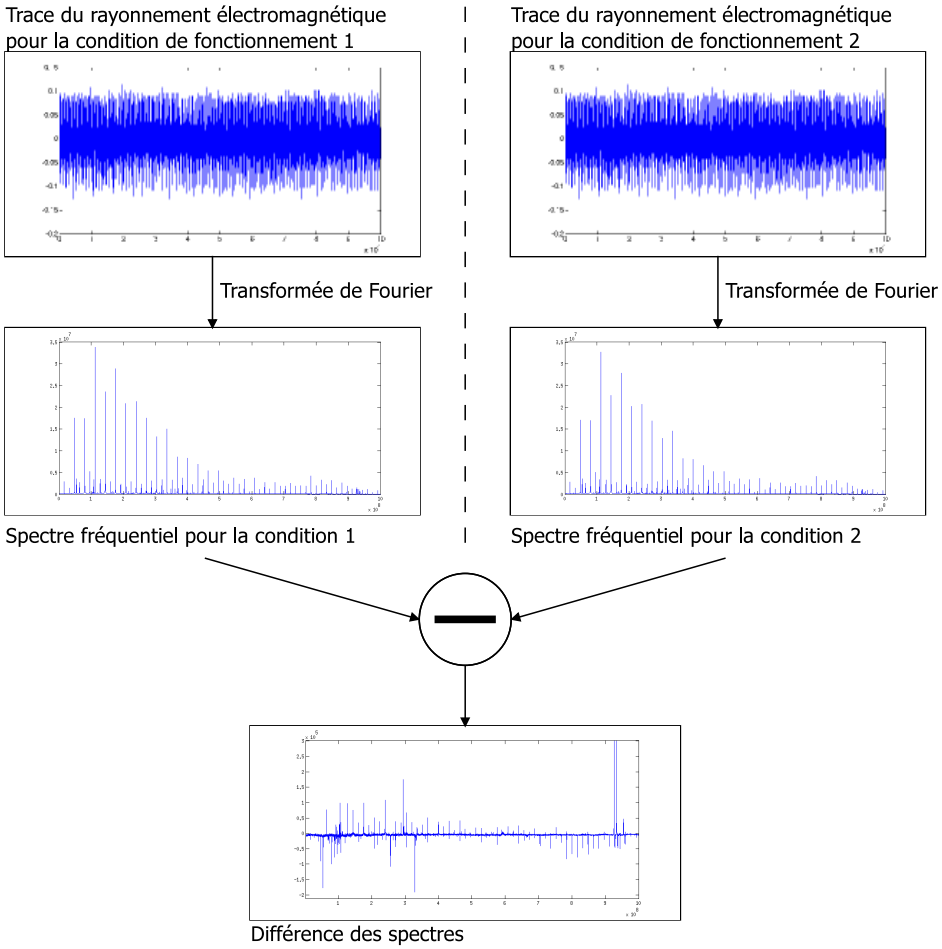

FIG. 3.4 – Principe de l'analyse différentielle adaptée à l'analyse du rayonnement électromagnétique des générateurs d'aléa.

3.4 Résultats de cartographie sur les générateurs à base d'oscillateurs en anneau

Dans cette section, nous allons présenter les différents résultats qui émanent de l'utilisation de la technique de cartographie présentée précédemment. Deux types de FPGA ont été ciblés dans cette partie, à savoir le module Altera CycloneIII et le module Actel Fusion.

3.4.1 Résultats de cartographie sur Altera CycloneIII

3.4.1.1 Présentation des expériences

La technique de cartographie proposée a été testée à l'aide de trois implantations différentes du générateurs à base d'oscillateurs en anneau. Les deux premières implantations ont pour but de montrer que la technique de cartographie permet de :

– facilement trouver les fréquences de fonctionnement des oscillateurs en anneau qui composent le générateur,
– déterminer la position du générateur sur la puce.

Ces deux premières implantations sont constituées du générateur seul, positionné en haut à gauche pour la première implantation (IMP#1) et en bas à droite pour la deuxième (IMP#2).

La troisième implantation a pour but de montrer que la technique de perturbation n'est pas sensible à d'autres blocs cryptographiques (ou autre) potentiellement présents sur la puce. Comme expliqué précédemment, le rayonnement d'un générateur d'aléa par rapport aux autres types de modules cryptographiques est faible. Nous avons sélectionné, comme source de forte consommation de courant, un chiffreur à clé privée (AES) classiquement utilisé dans nombreux systèmes cryptographiques. Durant toute la cartographie, le chiffreur effectue des chiffrements en utilisant toujours le même texte en clair et la même clé. Il est cadencé à une horloge de 20 MHz.

Pour cette implantation (IMP#3), le chiffreur est situé au milieu de la carte et le générateur en bas à droite.

Pour les trois implantations, le générateur utilisé est le même. Ce dernier est composé de cinquante oscillateurs en anneau de trois inverseurs chacun (ce qui donne une fréquence d'oscillation pour ce type de FPGA de l'ordre de 300 MHz).

Un récapitulatif de l'agencement utilisé pour les trois implantations se trouve dans la Figure 3.5.

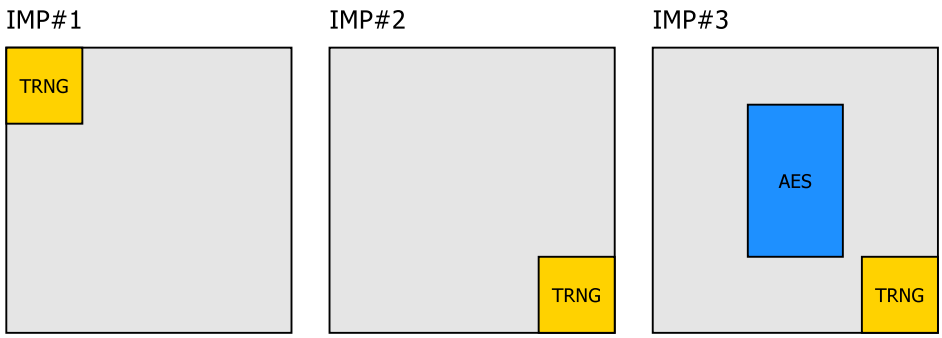

FIG. 3.5 – Schéma descriptif de l'agencement des blocs (floorplan) pour les trois implantations sur la cible Altera CycloneIII.

Pour les trois implantations, les cartes (composées de 90 points sur chaque axe) ont été réalisées sur toute la surface du circuit. Pour chaque point, dix traces ont été recueillies (chaque trace est composée de 400 000 échantillons) à une fréquence d'échantillonnage de 20 GS/s. Les dix traces ne sont pas moyennées temporellement ; ce sont les densités spectrales qui le sont.

Pour l'IMP#1 et #2, les tensions d'alimentation retenues sont 1.25 V et 1.38 V, et pour l'IMP#3, les tensions d'alimentation sont 1.24 V et 1.30 V.

3.4.1.2 Cartographie générateur d'aléa seul - IMP#1 & IMP#2

Le but de ces deux implantations est de retrouver la fréquence de fonctionnement des oscillateurs en anneau et la position du générateur d'aléa sur la puce.

La Figure 3.6 montre la consommation temporelle du circuit pour l'IMP#1 pour une tension d'alimentation du cœur à 1.25 V. Comme prévu, ce type d'analyse ne permet pas d'extraire d'information cruciale sur la cible. Seuls les points les plus rayonnants de la carte (située en périphérie de la puce), à savoir les pads et boundings d'alimentation, sont visibles et identifiables. Le rayonnement en provenance du DIE n'est donc pas directement exploitable. Il est nécessaire de venir appliquer une analyse fréquentielle à la trace du rayonnement électromagnétique.

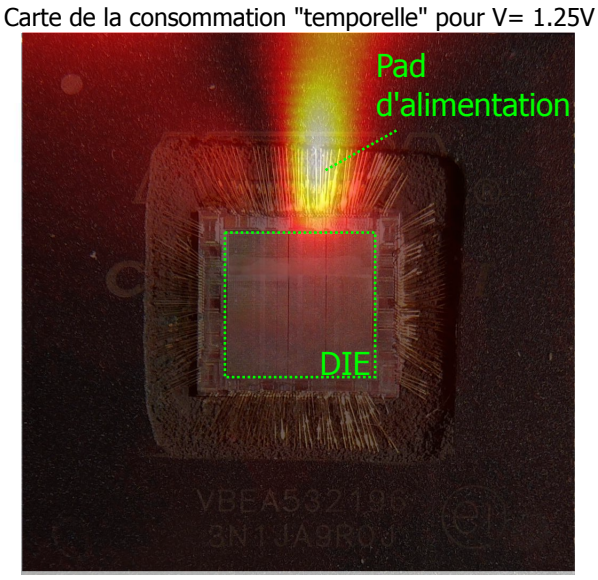

Fig. 3.6 – Carte résultante d'une analyse temporelle du rayonnement électromagnétique pour l'IMP#1 pour une tension d'alimentation de cœur à 1.25 V.

L'intérêt premier de l'analyse fréquentielle différentielle présentée précédemment réside dans la facilité, pour retrouver les informations sur le générateur dans le spectre fréquentiel, des traces du rayonnement électromagnétique. La Figure 3.7 montre la moyenne de tous les spectres du rayonnement électromagnétique pour les points qui sont dans la zone du DIE et pour un voltage de 1.25 V. Si on part du principe que l'attaquant n'a aucune information sur la localisation des différents blocs cryptographiques sur la puce, la stratégie qui consiste à regarder la moyenne du spectre sur toute la zone peut être considérée comme plutôt bonne (vouloir faire une recherche exhaustive sur tous les spectres un à un serait beaucoup plus long - par exemple, pour cette cartographie, cela reviendrait à regarder plus de 8000 spectres différents).

Le rectangle rouge représente la zone fréquentielle où les fréquences des oscillateurs en anneau sont présentes. Sans savoir que les fréquences des oscillateurs en anneau sont contenues dans cette bande fréquentielle il n'est pas possible de trouver (sauf recherche exhaustive, mais, qui là encore est longue et pénible à effectuer) cette information facilement.

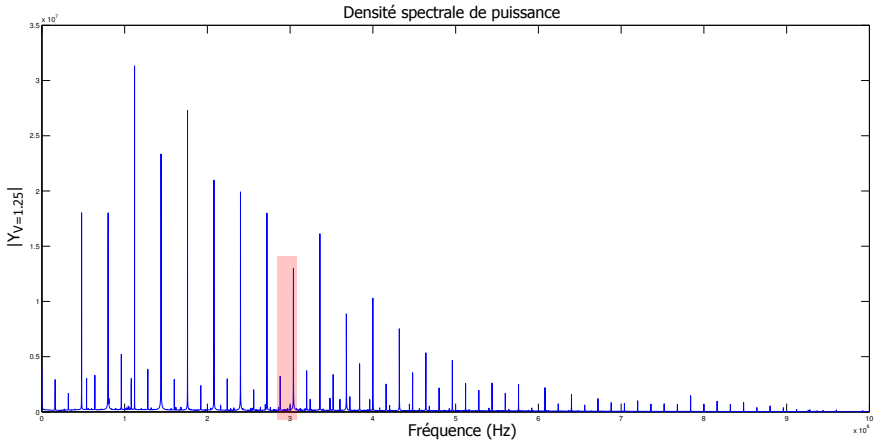

FIG. 3.7 – Moyenne des densités spectrales de puissance, sur tout le circuit, pour l'IMP#1 pour une tension d'alimentation de cœur à 1.25 V.

C'est dans ce cadre là que l'analyse proposée va faciliter l'extraction d'information. La Figure 3.8 présente la différence entre les spectres du rayonnement électromagnétique pour 1.25 V et 1.38 V (la partie supérieure correspond à 1.25 V et la partie inférieure à 1.38 V). Les fréquences des oscillateurs en anneau changent en fonction des conditions de fonctionnement - ici, les oscillateurs en anneau devraient osciller plus rapidement pour la tension d'alimentation de 1.38 V que pour la tension d'alimentation de 1.25 V. Il faut donc rechercher dans la Figure 3.8 un motif, dans la composante spectrale, présent à la fois dans la partie positive et dans la partie négative. C'est ce que l'on retrouve dans la zone en rouge. On peut clairement voir le même motif se répéter dans la différence des spectres à une distance de quelques dizaines de MHz due à la différence de tension d'alimentation entre les deux acquisitions. Il est possible également de voir dans la zone verte, la deuxième harmonique des fréquences correspondantes aux oscillateurs - cette information n'est pas cruciale dans le sens où elle n'est pas utile par la suite, mais permet de confirmer que les bandes de fréquences trouvées correspondent bien aux oscillateurs en anneau.

Par rapport aux résultats obtenus - nous ne supprimons pas toutes les fréquences « statiques » comme on peut le voir sur la Figure 3.8. En effet, même si ces fréquences ne changent pas avec la modification des conditions de fonctionnement du circuit, leur amplitude dans le spectre fréquentiel va varier avec le temps. Il se peut donc qu'entre les deux acquisitions, il y ait une différence d'amplitude pour ces fréquences là, ce qui crée des pics parasites lors de la différence des spectres. Plus le spectre est moyenné pour chaque point, plus ces pics parasites sont petits devant les pics qui

correspondent aux fréquences des oscillateurs en anneau.

D'après la Figure 3.9 qui est un zoom sur la zone rouge de la Figure 3.8, pour l'IMP#1, on trouve donc des oscillateurs en anneau avec des fréquences comprises :

- entre 290 MHz et 295 MHz pour une tension d'alimentation de 1.25 V.
- entre 325 MHz et 331 MHz pour une tension d'alimentation de 1.38 V.

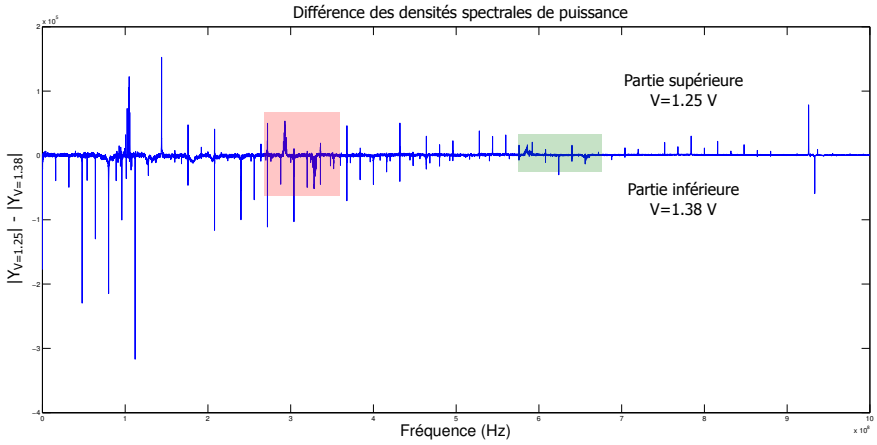

FIG. 3.8 – Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#1 pour une tension d'alimentation de cœur à 1.25 V et de 1.38 V.

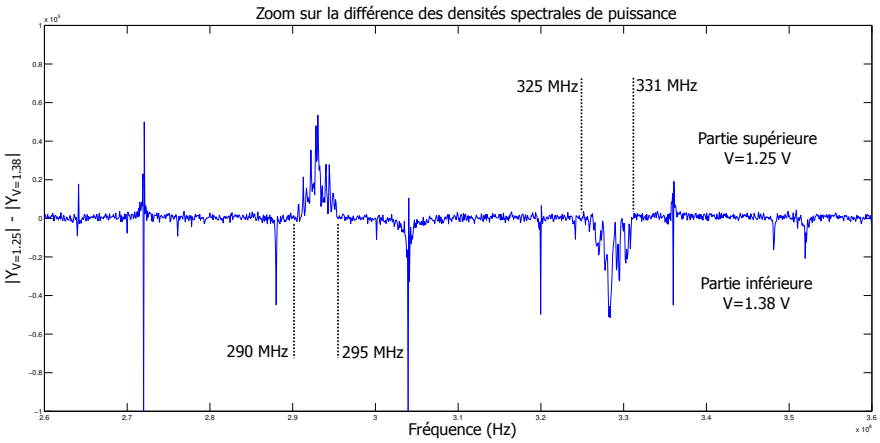

FIG. 3.9 – Zoom sur la différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#1 pour une tension d'alimentation de cœur à 1.25 V et de 1.38 V.

Nous avons maintenant l'information des fréquences de fonctionnement du générateur, nous pouvons alors réaliser des cartes fréquentielles dans le but de trouver la position du générateur d'aléa sur la puce. La Figure 3.10 présente quatre cartes dif-

férentes qui résultent de la technique de cartographie à base d'analyse fréquentielle. Les cartes présentées ont été réalisées avec les paramètres suivants :

- Carte a : tension d'alimentation à 1.25 V et bande fréquentielle choisie de [290 - 295 MHz].
- Carte b : tension d'alimentation à 1.38 V et bande fréquentielle choisie de [290 - 295 MHz].
- Carte c : tension d'alimentation à 1.25 V et bande fréquentielle choisie de [325 - 331 MHz].
- Carte d : tension d'alimentation à 1.38 V et bande fréquentielle choisie de [325 - 331 MHz].

D'après les informations extraites de la Figure 3.9, il est normalement seulement possible de trouver la position du générateur pour les cartes a et d (les deux autres cartes sont là pour prouver que c'est bien le rayonnement du générateur qui est affiché). Comme présenté dans la Figure 3.5, pour l'IMP#1, le générateur se situe en haut à gauche de la puce. Comme on peut le voir sur la Figure 3.10, on repère effectivement une zone rayonnante, sur les cartes a et d, en haut à gauche de la puce. Cette zone n'est pas présente sur les autres cartes (celles où on ne doit effectivement ne rien voir). Cette zone correspond donc au rayonnement du générateur d'aléa et se révèle donc être corrélée avec le floorplan du FPGA (Figure 3.5). On remarque que cette zone n'est pas la seule zone rayonnante sur les cartes a et d. En effet, on retrouve une zone qui correspond au plot (et bounding) d'alimentation. Une méthode pour supprimer ces rayonnements parasites est d'utiliser les cartes b et c. En effet, en réalisant l'opération (Carte a - Carte b) et (Carte d - Carte c), les rayonnements parasites seront gommés. Ces deux cartes sont visibles respectivement Figure 3.11 et Figure 3.12.

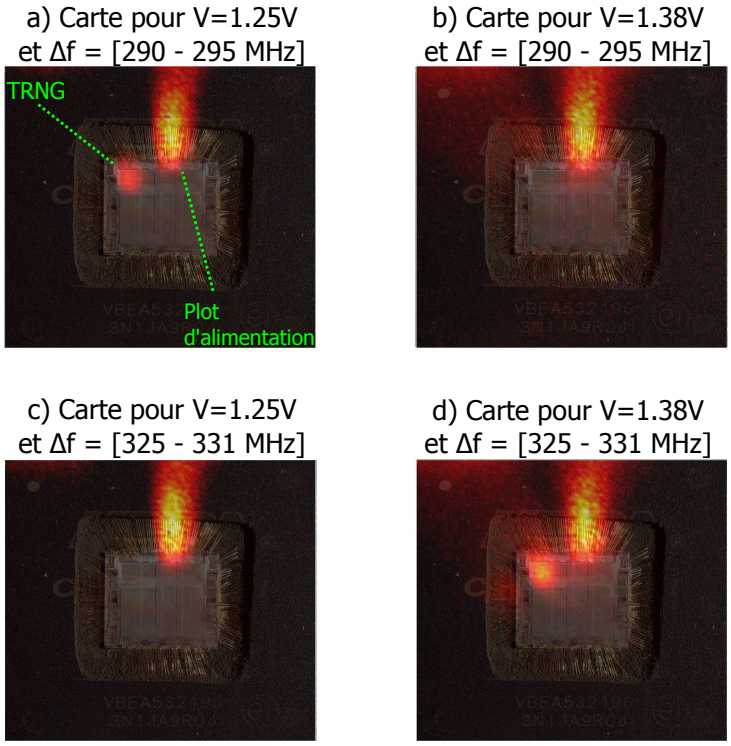

FIG. 3.10 – Cartes résultantes de l'analyse fréquentielle pour l'IMP#1 pour différents paramètres : a) V = 1.25 V et $\delta f = [290 - 295MHz]$ b) V = 1.38 V et $\delta f = [290 - 295MHz]$ c) V = 1.25 V et $\delta f = [325 - 331MHz]$ d) V = 1.38 V et $\delta f = [325 - 331MHz]$.

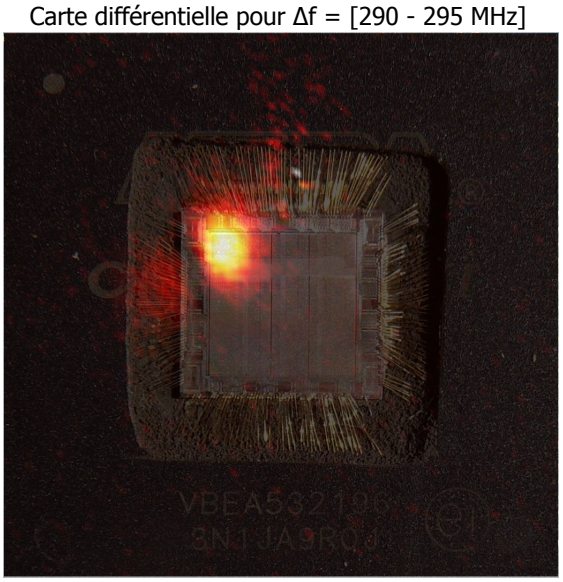

FIG. 3.11 – Carte résultante pour l'IMP#1 de la différence entre la carte a) et la carte b) de la Figure 3.10

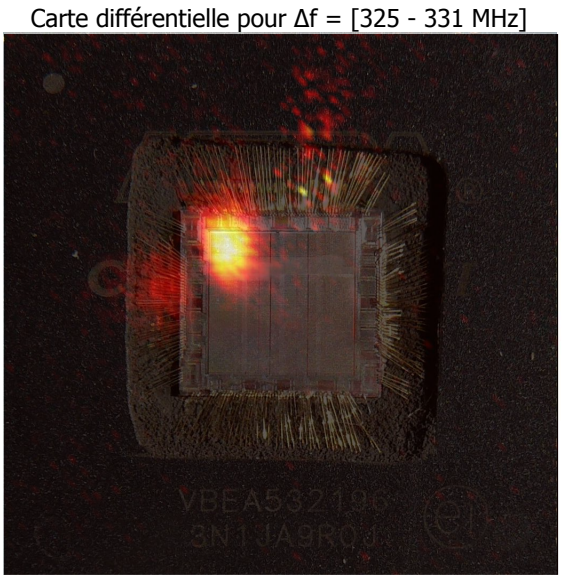

FIG. 3.12 – Carte résultante pour l'IMP#1 de la différence entre la carte c) et la carte d) de la Figure 3.10

La deuxième étape maintenant est de vérifier qu'en déplaçant le générateur sur la puce, le rayonnement associé trouvé grâce à notre méthode se déplace lui aussi sur les cartes résultantes de la méthode de cartographie. Nous allons donc maintenant nous intéresser à la deuxième implantation (IMP#2), où le générateur se situe en bas à droite de la puce.

En regardant la carte qui correspond à la consommation temporelle (Figure 3.13) pour IMP#2, il n'est pas toujours pas possible d'extraire de l'information. En effet, Figure 3.6 et Figure 3.13 sont semblables. Cela confirme les suppositions sur le non intérêt de ce type de carte.

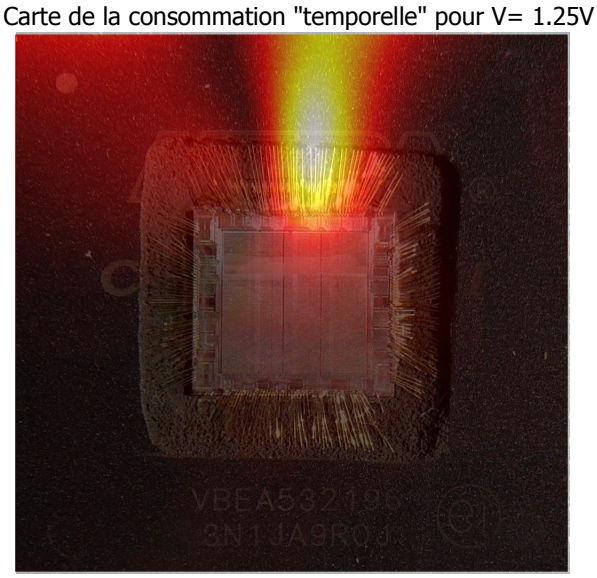

Fig. 3.13 – Carte résultante d'une analyse temporelle du rayonnement électromagnétique pour l'IMP#2 pour une tension d'alimentation de cœur à 1.25 V.

De la même façon que précédemment, nous allons utiliser notre analyse différentielle car il n'est pas possible de discerner les fréquences qui correspondent à nos oscillateurs en anneau sur le spectre du rayonnement électromagnétique (voir Figure 3.14). La Figure 3.15 présente la différence entre les spectres du rayonnement électromagnétique pour 1.25 V et 1.38 V (la partie supérieure correspond à 1.25 V et la partie inférieure à 1.38 V). De la même façon que pour la Figure 3.8, le motif que nous recherchons se trouve dans la zone rouge. Nous retrouvons également dans la zone verte les harmoniques de ces fréquences.

La Figure 3.16 qui est un zoom sur la zone rouge de la Figure 3.15. On a donc pour l'IMP#2 des oscillateurs en anneau avec des fréquences comprises :

- entre 293 MHz et 298 MHz pour une tension d'alimentation de 1.25 V.
- entre 328 MHz et 334 MHz pour une tension d'alimentation de 1.38 V.

Une petite remarque sur les valeurs des fréquences trouvées ici. Même si la topologie

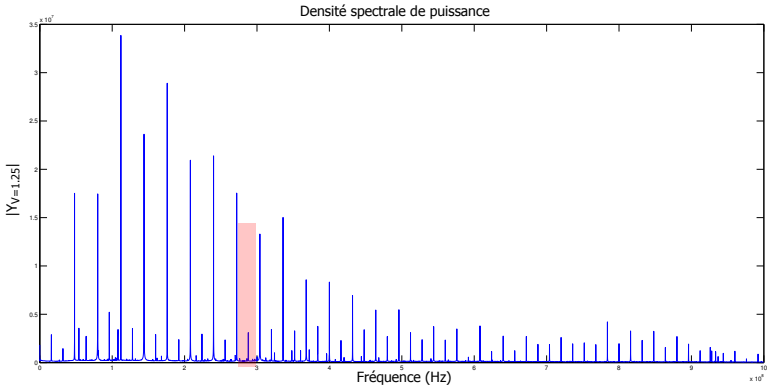

FIG. 3.14 – Moyenne des densités spectrales de puissance, sur tout le circuit, pour l'IMP#2 pour une tension d'alimentation de cœur à 1.25 V.

des oscillateurs est la même entre l'IMP#1 et l'IMP#2, du fait du déplacement des oscillateurs sur le circuit, les fréquences sont légèrement différentes. En effet, les portes logiques du FPGA n'ont pas des paramètres intrinsèques uniformes sur tout le circuit, et le routage peut être réalisé différemment par le logiciel.

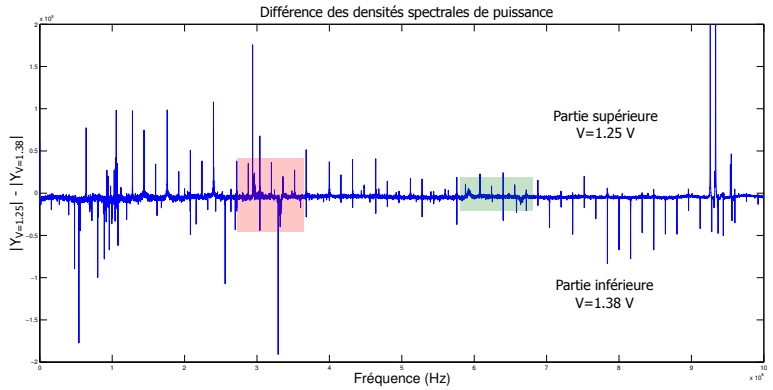

FIG. 3.15 – Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#2 pour une tension d'alimentation de cœur à 1.25 V et de 1.38 V.

Comme nous disposons des informations relatives aux fréquences de fonctionnement du générateur, il est maintenant possible de réaliser les cartes fréquentielles qui nous permettent de trouver la position du générateur sur le circuit. La Figure 3.17 présente les quatre cartes réalisées en accord avec les paramètres suivants :

- Carte a : tension d'alimentation à 1.25 V et bande fréquentielle choisie de [293 - 298 MHz].
- Carte b : tension d'alimentation à 1.38 V et bande fréquentielle choisie de [293 - 298 MHz].

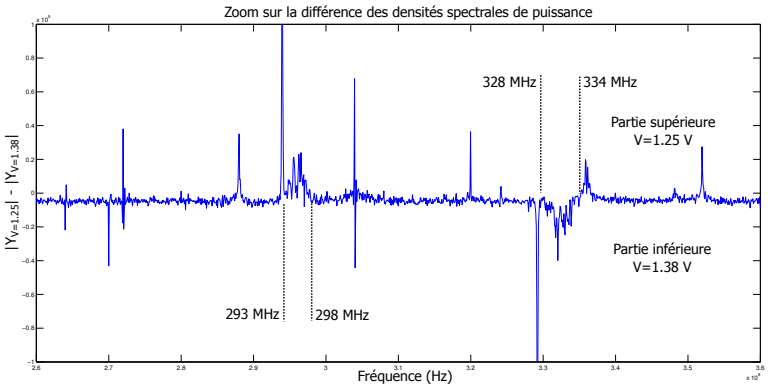

FIG. 3.16 – Zoom sur la différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#2 pour une tension d'alimentation de cœur à 1.25 V et de 1.38 V.

- Carte c : tension d'alimentation à 1.25 V et bande fréquentielle choisie de [328 - 334 MHz].
- Carte d : tension d'alimentation à 1.38 V et bande fréquentielle choisie de [328 - 334 MHz].

Il n'est possible de trouver un rayonnement électromagnétique qui corresponde au générateur que sur les cartes a et d. D'après Figure 3.5, le générateur d'aléa se situe en bas à droite de la puce pour l'IMP#2. Sur la Figure 3.17, on voit clairement, par rapport aux cartes de l'IMP#1 (Figure 3.10), que la position du générateur sur les cartes a changé et correspond bien au placement présenté dans la Figure 3.5 (c'est à dire en bas à droite de la puce).

Comme pour l'IMP#1, il est possible en réalisant l'opération (Carte a - Carte b) et (Carte d - Carte c) de supprimer les rayonnements parasites des cartes. La première carte sans rayonnement parasite est visible dans la Figure 3.18 et la deuxième dans la Figure 3.19.

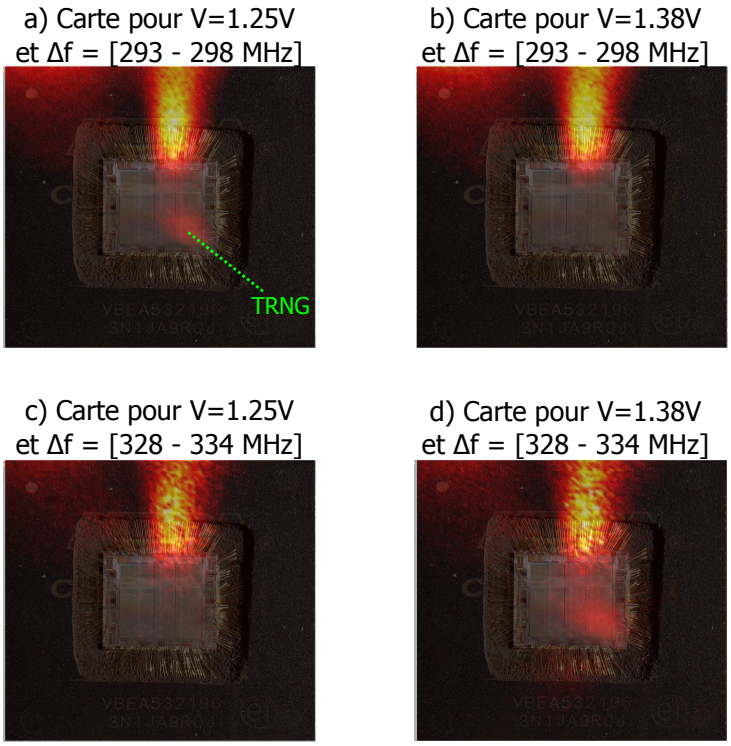

FIG. 3.17 – Cartes résultantes de l'analyse fréquentielle pour l'IMP#2 pour différents paramètres : a) V = 1.25 V et $\delta f = [293 - 298MHz]$ b) V = 1.38 V et $\delta f = [293 - 298MHz]$ c) V = 1.25 V et $\delta f = [328 - 334MHz]$ d) V = 1.38 V et $\delta f = [328 - 334MHz]$.

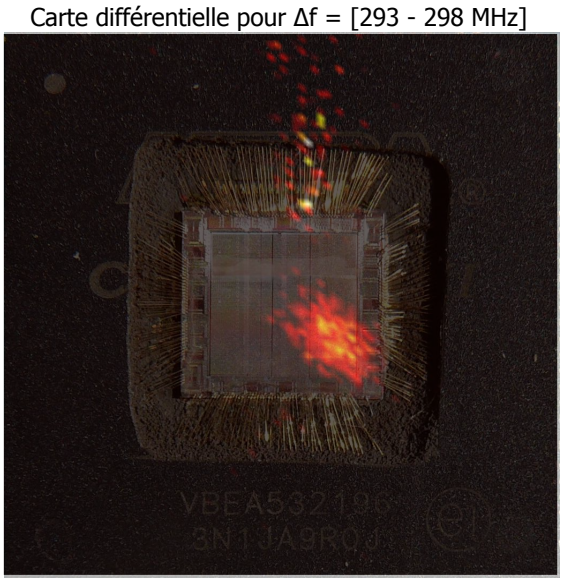

Fig. 3.18 – Carte résultante pour l'IMP#2 de la différence entre la carte a) et la carte b) de la Figure 3.17

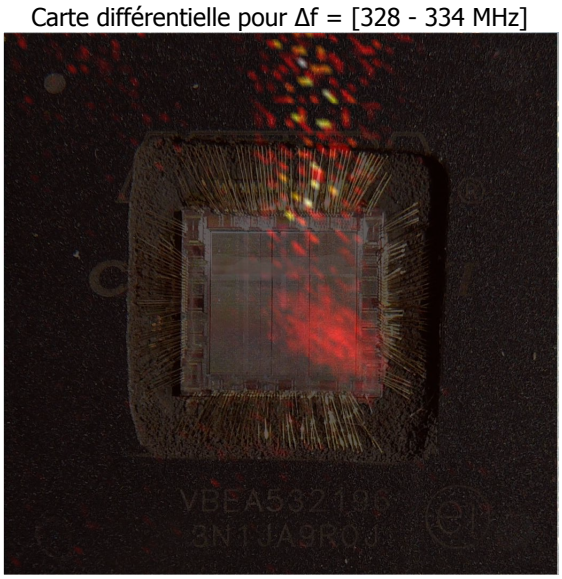

Fig. 3.19 – Carte résultante pour l'IMP#2 de la différence entre la carte c) et la carte d) de la Figure 3.17

3.4.1.3 Cartographie générateur et chiffreur - IMP#3

Maintenant, la dernière étape de l'étude de notre technique d'analyse est de vérifier que si le générateur est embarqué dans un système cryptographique (ici avec un chiffreur à clé privée qui va jouer un rôle de brouilleur), la technique est toujours efficace pour retrouver la fréquence et la position du générateur sur le circuit. Nous allons donc nous intéresser à l'IMP#3 présentée dans la Figure 3.5 où le générateur se situe en bas à droite et le chiffreur au centre.

La carte qui correspond à la consommation temporelle (Figure 3.20) pour l'IMP#3 ne porte toujours aucune information. La carte est encore semblable aux deux autres cartes, et ce même si l'implantation est différente des deux précédentes (Figure 3.6 et Figure 3.13).

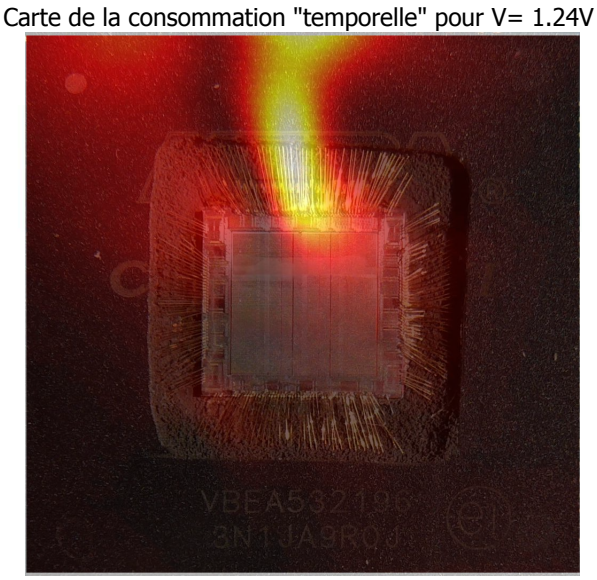

FIG. 3.20 – Carte résultante d'une analyse temporelle du rayonnement électromagnétique pour l'IMP#3 pour une tension d'alimentation de cœur à 1.24 V.

On ne peut toujours pas discerner dans la densité spectrale de puissance du rayonnement électromagnétique les contributions des oscillateurs en anneau (voir la Figure 3.21). La différence des spectres du rayonnement électromagnétique pour 1.24 V et 1.30 V (avec la partie supérieure qui correspond à 1.24 V et la partie inférieure à 1.30 V) est tracée dans la Figure 3.22. On retrouve le motif qui nous intéresse dans la zone rouge, et les harmoniques de ces fréquences dans la zone verte. On remarque la présence d'une perturbation, dans la zone bleue, pour l'acquisition à 1.30 V. Cette perturbation (d'amplitude relativement forte) autour de 800 MHz correspond à des tests d'antennes 4G effectués lors de l'acquisition des traces pour cette tension d'alimentation (Saint-Etienne était une ville test pour le développement de la 4G

en France).

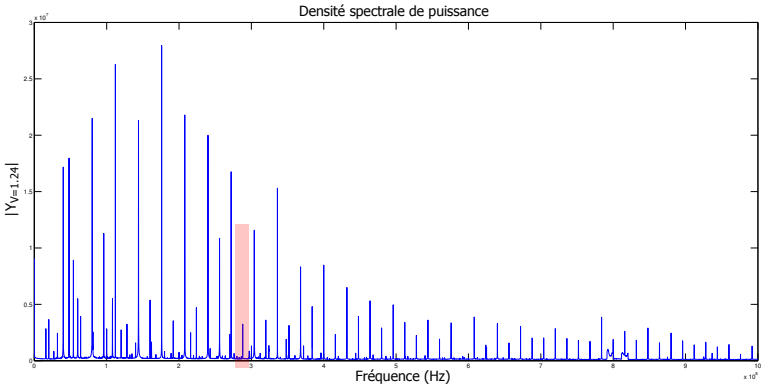

FIG. 3.21 – Moyenne des densités spectrales de puissance, sur tout le circuit, pour l'IMP#3 pour une tension d'alimentation de cœur à 1.24 V.

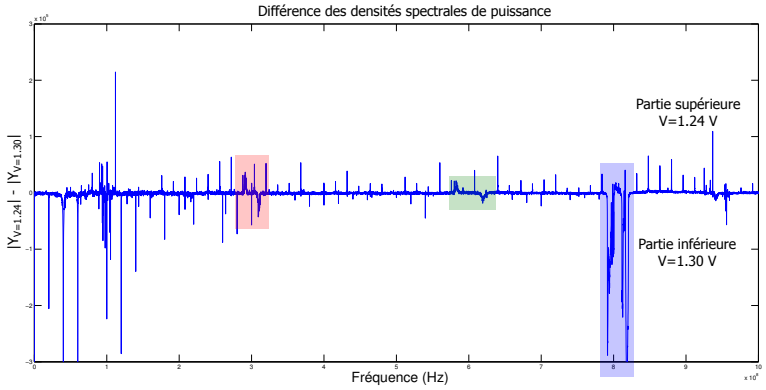

FIG. 3.22 – Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#3 pour une tension d'alimentation de cœur à 1.24 V et de 1.30 V.

La Figure 3.23 est le zoom sur la zone rouge de la Figure 3.22. On trouve, des fréquences d'oscillateurs pour cette implantation, comprises :

- entre 289 MHz et 294 MHz pour une tension d'alimentation de 1.24 V.
- entre 307 MHz et 312 MHz pour une tension d'alimentation de 1.30 V.

La Figure 3.17 présente les quatre cartes réalisées en accord avec les paramètres suivants :

- Carte a : tension d'alimentation à 1.24 V et bande fréquentielle choisie de [294 - 299 MHz].
- Carte b : tension d'alimentation à 1.30 V et bande fréquentielle choisie de [294 - 299 MHz].
- Carte c : tension d'alimentation à 1.24 V et bande fréquentielle choisie de [307

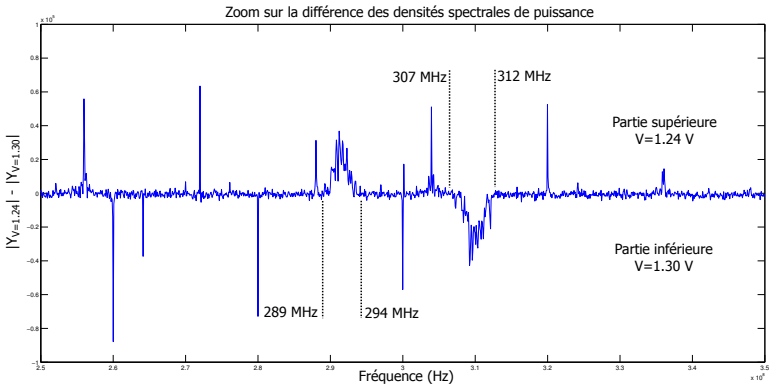

FIG. 3.23 – Zoom sur la différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#3 pour une tension d'alimentation de cœur à 1.24 V et de 1.30 V.

- 312 MHz].

– Carte d : tension d'alimentation à 1.30 V et bande fréquentielle choisie de [307 - 312 MHz].

On retrouve à la bonne position (en bas à droite) le générateur sur les cartes a et d. Sur les cartes b et c, comme précédemment, il n'y a pas de rayonnement à cette position.

Les cartes réalisées en effectuant l'opération (Carte a - Carte b) et (Carte d - Carte c) sont présentées, respectivement, dans la Figure 3.25 et dans la Figure 3.26.

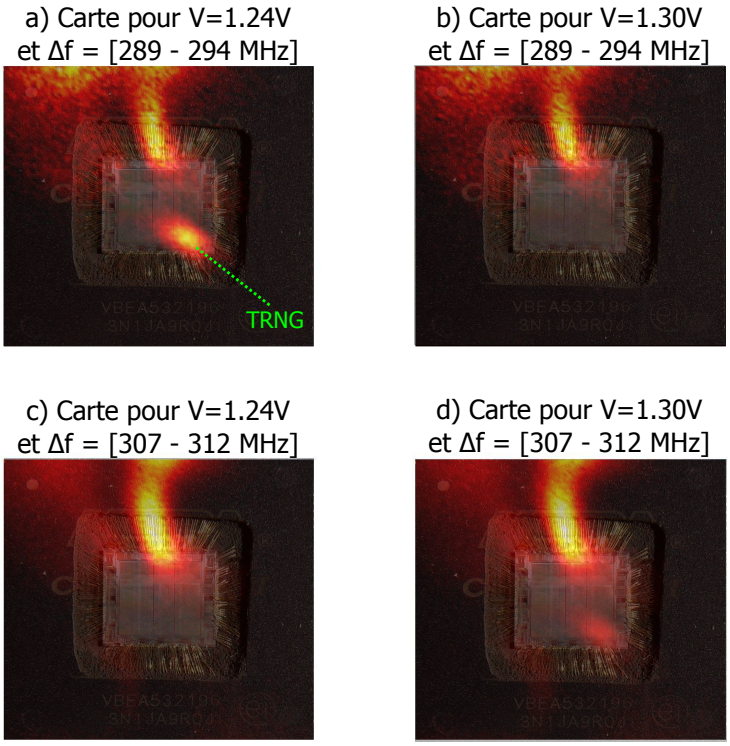

FIG. 3.24 – Cartes résultantes de l'analyse fréquentielle pour l'IMP#3 pour différents paramètres : a) V = 1.24 V et $\delta f = [294 - 299MHz]$ b) V = 1.30 V et $\delta f = [294 - 299MHz]$ c) V = 1.24 V et $\delta f = [307 - 312MHz]$ d) V = 1.30 V et $\delta f = [307 - 312MHz]$.

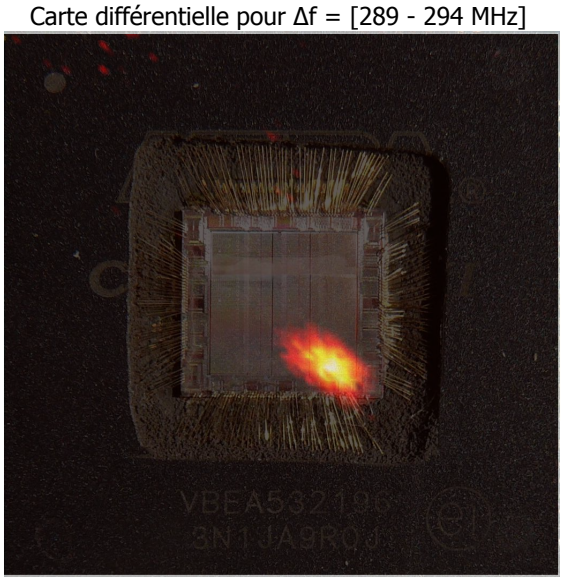

FIG. 3.25 – Carte résultante pour l'IMP#3 de la différence entre la carte a) et la carte b) de la Figure 3.24

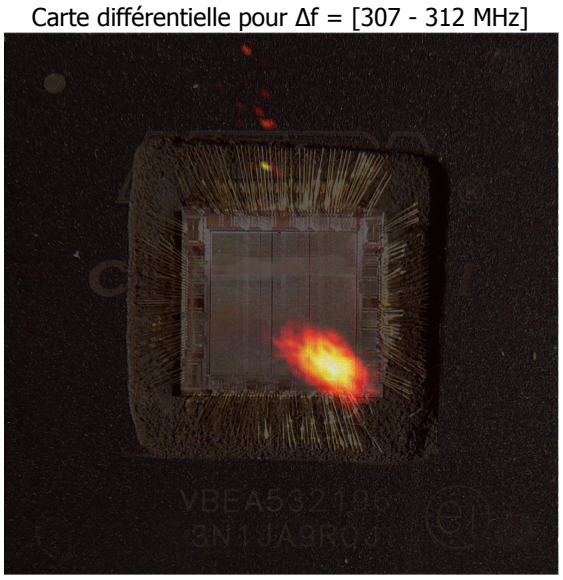

FIG. 3.26 – Carte résultante pour l'IMP#3 de la différence entre la carte c) et la carte d) de la Figure 3.24

3.4.2 Résultats de cartographie sur Microsemi Fusion

3.4.2.1 Présentation de l'expérience

Maintenant que la technique de cartographie a été approuvée sur Altera CycloneIII, nous allons vérifier le bon fonctionnement sur une autre technologie (Flash) de FPGA. Nous allons pour cette famille, n'utiliser qu'une seule implantation (équivalente à l'IMP#3 présentée précédemment). Cette implantation a pour but de montrer que la méthode d'analyse proposée permet de localiser le générateur dans le FPGA Microsemi Fusion et ce même en présence d'un bruit logique. Cette implantation sera appelée IMP#4. Elle est constituée d'un générateur et d'un chiffreur à clé privée (AES). Comme avant, le chiffreur effectue des chiffrements en utilisant toujours le même texte en clair et la même clé privée. L'horloge du chiffreur est encore de 20 MHz. Au niveau du placement, le chiffreur est situé au milieu de la carte et le générateur en haut à gauche. Le générateur est toujours composé de cinquante oscillateurs en anneau de trois inverseurs chacun (ce qui donne une fréquence d'oscillation pour cette technologie de l'ordre de 350 MHz).

Le schéma de principe du placement de l'implantation 4 est présentée Figure 3.27.

Nous avons gardé les mêmes paramètres d'acquisition que pour l'étude sur Altera CycloneIII à savoir :

- Les cartes sont composées de 90x90 points sur toute la surface du circuit.
- Dix traces de 400 000 échantillons sont recueillies pour chaque point à une fréquence d'échantillonnage de 20 GS/s.

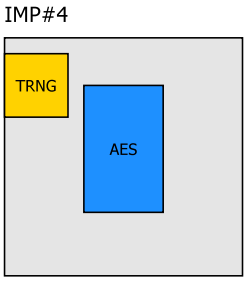

Fig. 3.27 – Schéma descriptif de l'agencement des blocs (floorplan) pour l'implantation sur la cible Microsemi Fusion.

Les tensions d'alimentation utilisées pour ce FPGA sont 1.5 V et 1.7 V.

3.4.2.2 Cartographie anneau et chiffreur

Au même titre que pour l'autre technologie de FPGA, la carte (voir la Figure 3.28) qui correspond à l'analyse temporelle n'apporte toujours aucune information sur le générateur.

La Figure 3.29 représente la moyenne des densités spectrales de puissance sur tout le circuit. Comme pour l'autre technologie il n'est toujours pas possible de repérer les fréquences qui correspondent aux oscillateurs. La différence des spectres

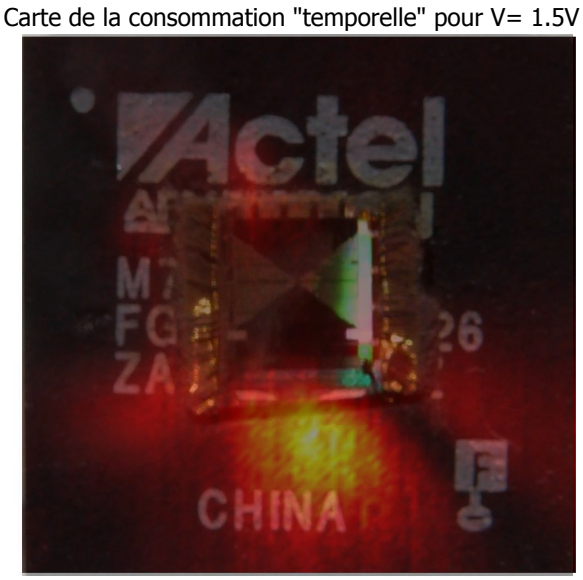

FIG. 3.28 – Carte résultante d'une analyse temporelle du rayonnement électromagnétique pour l'IMP#4 pour une tension d'alimentation de cœur à 1.5 V.

est visible dans la Figure 3.30. La partie supérieure correspond à 1.5 V et la partie inférieure à 1.7 V. Premier constat, par rapport au FPGA Altera CycloneIII, la différence de spectre est beaucoup plus bruitée (dans le sens où les fréquences non intéressantes ne sont pas complètement supprimées). Le motif que l'on recherche (situé dans la zone rouge) est certes toujours visible et repérable, cependant, la recherche n'est pas aussi simple.

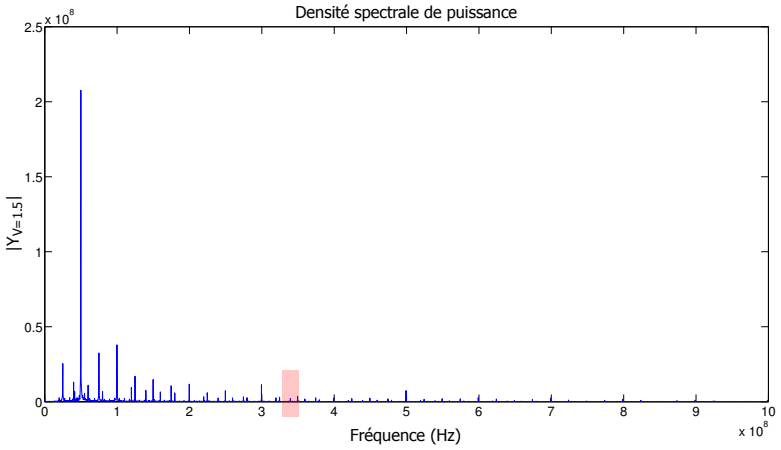

FIG. 3.29 – Moyenne des densités spectrales de puissance, sur tout le circuit, pour l'IMP#4 pour une tension d'alimentation de cœur à 1.5 V.

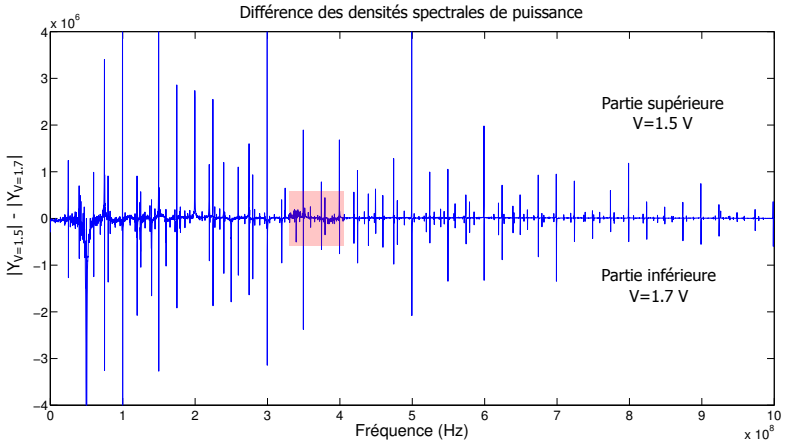

FIG. 3.30 – Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#4 pour une tension d'alimentation de cœur à 1.5 V et de 1.7 V.

La Figure 3.31 est le zoom sur la zone rouge de la Figure 3.22. On voit encore le caractère bruité de cette différence de spectre par rapport à ce qu'on avait pu voir pour l'autre technologie. On trouve, des fréquences d'oscillateurs pour cette implantation comprises :

- entre 331 MHz et 354 MHz pour une tension d'alimentation de 1.5 V.
- entre 376 MHz et 399 MHz pour une tension d'alimentation de 1.7 V.

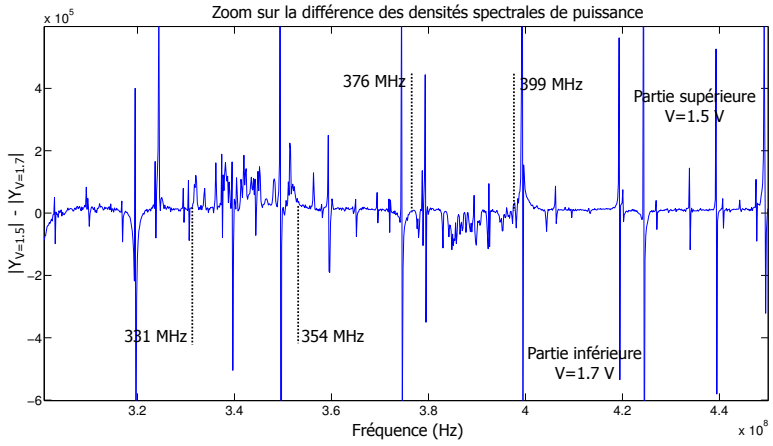

FIG. 3.31 – Zoom sur la différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#4 pour une tension d'alimentation de cœur à 1.5 V et de 1.7 V.

La Figure 3.32 présente les quatre cartes réalisées en accord avec les paramètres suivants :

- Carte a : tension d'alimentation à 1.5 V et bande fréquentielle choisie de [331 - 354 MHz].

- Carte b : tension d'alimentation à 1.7 V et bande fréquentielle choisie de [331 - 354 MHz].
- Carte c : tension d'alimentation à 1.5 V et bande fréquentielle choisie de [376 - 399 MHz].
- Carte d : tension d'alimentation à 1.7 V et bande fréquentielle choisie de [376 - 399 MHz].

On voit sur ces cartes qu'il est possible encore une fois grâce à notre analyse de localiser la position du générateur (ici en haut à gauche) sur le circuit. Il est plus difficile sur cette famille de FPGA de discerner le générateur que sur Altera CycloneIII.

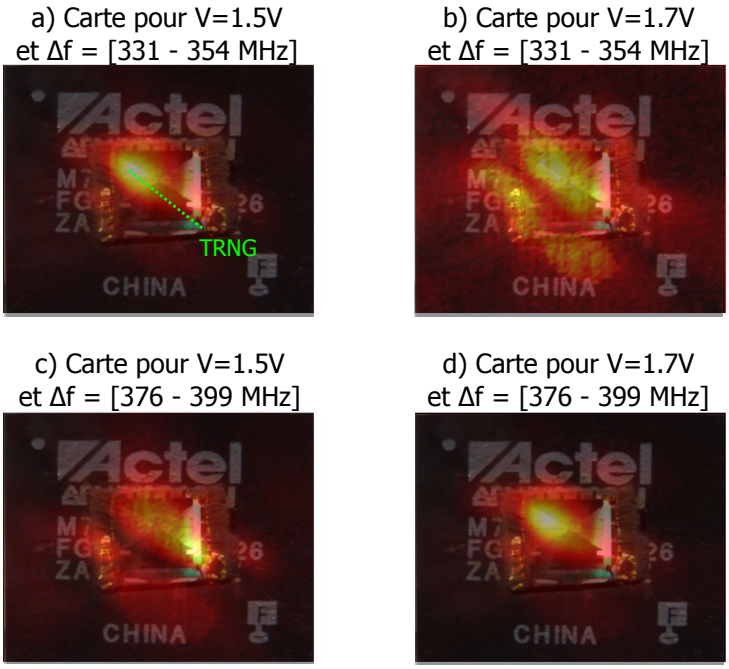

FIG. 3.32 – Cartes résultantes de l'analyse fréquentielle pour l'IMP#4 pour différents paramètres : a) V = 1.5 V et $\delta f = [331 - 354MHz]$ b) V = 1.7 V et $\delta f = [331 - 354MHz]$ c) V = 1.5 V et $\delta f = [376 - 399MHz]$ d) V = 1.7 V et $\delta f = [376 - 399MHz]$.

Cependant, les cartes réalisées en effectuant l'opération (Carte a - Carte b) et (Carte d - Carte c) présentées, respectivement, dans la Figure 3.33 et dans la Figure 3.34, permettent de trouver la position du générateur aussi facilement que pour les études présentées pour le FPGA Altera CycloneIII.

Les résultats sont identiques sur les deux types de technologies de FPGA. La méthode est donc fonctionnelle et permet facilement de retrouver les valeurs des fréquences des oscillateurs et leurs positions sur le circuit.

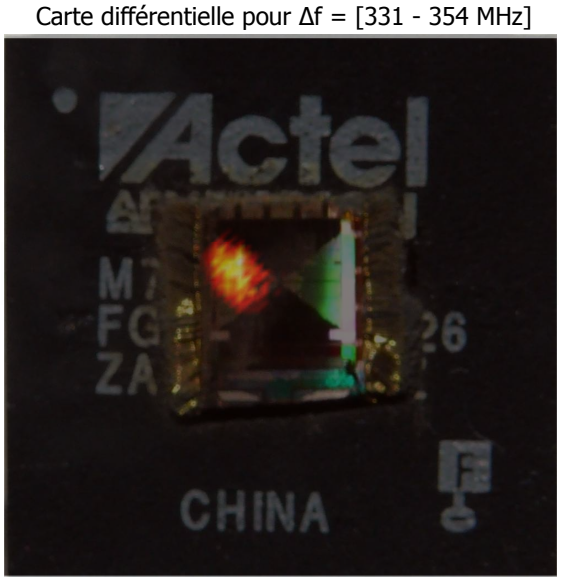

FIG. 3.33 – Carte résultante pour l'IMP#4 de la différence entre la carte a) et la carte b) de la Figure 3.32

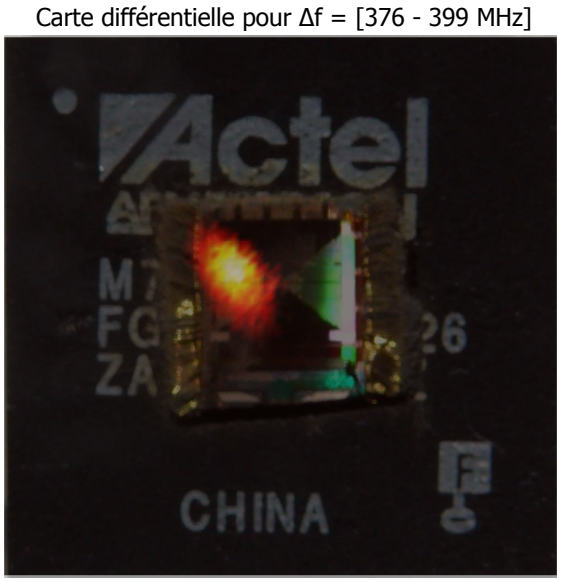

FIG. 3.34 – Carte résultante pour l'IMP#4 de la différence entre la carte d) et la carte c) de la Figure 3.32

3.5 Différence analyse locale et globale

L'analyse présentée se révèle être efficace pour retrouver de l'information sur les générateurs de nombres aléatoires, cependant, elle s'avère également avoir des défauts importants. En effet, tout d'abord, il est nécessaire de modifier la carte sur laquelle se trouve le circuit ciblé de manière à pouvoir changer la tension d'alimentation du circuit (ou de disposer d'une étuve si on souhaite plutôt modifier la température du circuit, qui entraîne un surcoût du banc d'analyse). Il est également nécessaire, pour chaque implantation étudiée d'effectuer deux séries d'acquisitions de traces ce qui double le temps total d'acquisition et d'analyse du circuit. Pour les paramètres d'acquisition utilisés, il faut environ six heures pour une acquisition d'une série de traces. Il faut donc au minimum douze heures, pour une implantation donnée, pour effectuer l'acquisition complète. Néanmoins, nous proposons ici, une solution pour effectuer cette analyse en une seule acquisition. L'analyse et la recherche d'information peuvent même être effectuées exhaustivement à l'aide d'un oscilloscope.

3.5.1 Principe

Comme présenté dans le Chapitre 2, le rayonnement électromagnétique d'un générateur d'aléa est très faible du fait de sa petite taille et sa faible consommation de courant. Le rayonnement du générateur est donc visible seulement localement. En utilisant une sonde qui va capter le rayonnement de tout le circuit (donc le rayonnement global), il n'est pas possible de trouver dans sa densité spectrale de puissance, les contributions fréquentielles qui correspondent au générateur.

Le principe de notre méthode d'analyse est de supprimer les contributions qui ne correspondent pas au rayonnement électromagnétique du générateur (différentes horloges et leurs harmoniques, bruit ambiant électromagnétique, ...). Ces contributions vont se retrouver que ce soit dans le rayonnement local (c'est d'ailleurs ici que nous souhaitons les supprimer) ou global du circuit. L'idée est donc d'acquérir en même temps le rayonnement électromagnétique local pour un point de la cartographie, calculer sa densité spectrale, et de lui soustraire la densité spectrale du rayonnement électromagnétique global du circuit. Le schéma de principe de la méthode est présenté Figure 3.36. La première sonde (sonde qui mesure le rayonnement local) est la même sonde que celle utilisée précédemment. La deuxième sonde (mesure du rayonnement global) est une sonde LANGER RF-R 400-1 (voir la Figure 3.35 - nous avons choisi d'utiliser une sonde commerciale,principalement car nous avions cette sonde à disposition). Il est également possible d'utiliser une sonde "faite maison" (par exemple un simple bobinage de diamètre proche du circuit). Nous avons également un étage d'amplification pour la sonde globale (mais de moins bonne qualité que celui de la sonde locale). L'amplificateur utilisé est un amplificateur LANGER PA 203.

Deux choix peuvent être fait à ce moment :

- Acquérir les traces du rayonnement électromagnétique pour les deux sondes et

FIG. 3.35 – Sonde LANGER RF-R400-1 utilisée pour la mesure à deux sondes.

réaliser l'analyse (analyse fréquentielle) sur un ordinateur comme précédemment.

– Réaliser les transformées de Fourier et la différence des spectres sur l'oscilloscope et acquérir cette différence.

C'est cette deuxième méthode que nous avons choisi d'illustrer dans la suite. En effet, elle permet de montrer l'efficacité de cette méthode à deux sondes pour effectuer une analyse à la volée du circuit avec un oscilloscope.

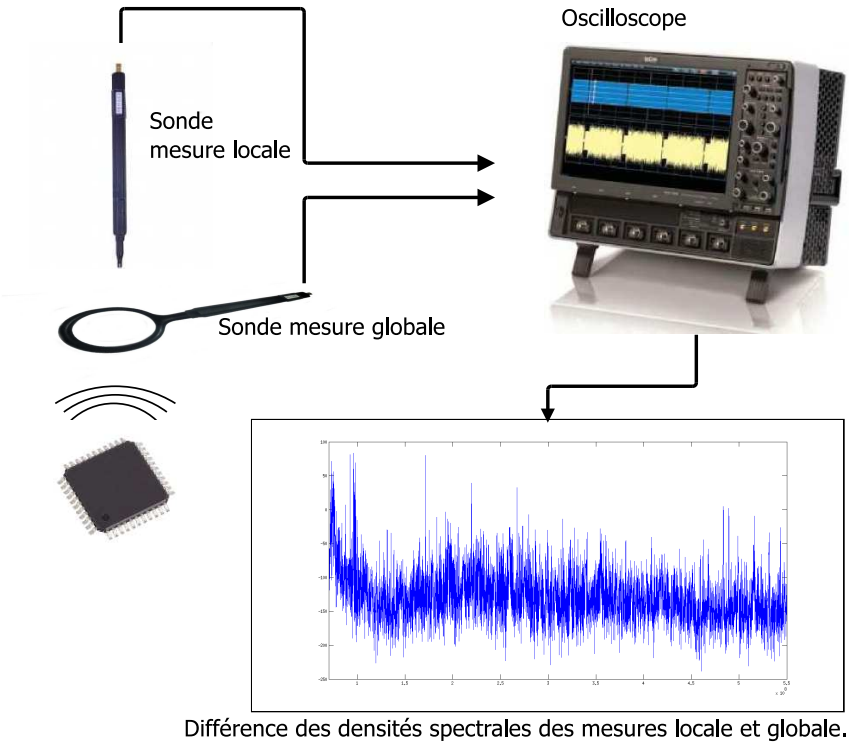

FIG. 3.36 – Principe d'analyse à base d'une sonde qui mesure le rayonnement électromagnétique local et d'une sonde qui mesure le rayonnement électromagnétique global.

3.5.2 Résultat sur l'IMP#3 (Altera Cyclone III)

La différence des moyennes des densités spectrales de puissance sur tout le circuit est représentée dans la Figure 3.37. Nous ne cherchons plus maintenant un motif qui se répète à la fois sur la partie inférieure et la partie supérieure du spectre, mais seulement un pic sur la partie qui correspond au rayonnement local. Comme on peut le voir sur la Figure 3.37, la zone qui correspond aux oscillateurs est située dans la zone rouge. C'est en effet le seul regroupement de fréquences dans la partie qui correspond au rayonnement local (les autres pics dans la partie inférieure sont du bruit).

Les fréquences des oscillateurs en anneau sont comprises entre 315 MHz et 318 MHz. Nous ne retrouvons pas tout à fait les résultats obtenus pour l'IMP#3, ceci est dû au fait que pour cette acquisition, nous avons utilisé le régulateur présent sur la carte pour alimenter le cœur du FPGA, la tension d'alimentation est donc différente (et les fréquences aussi).

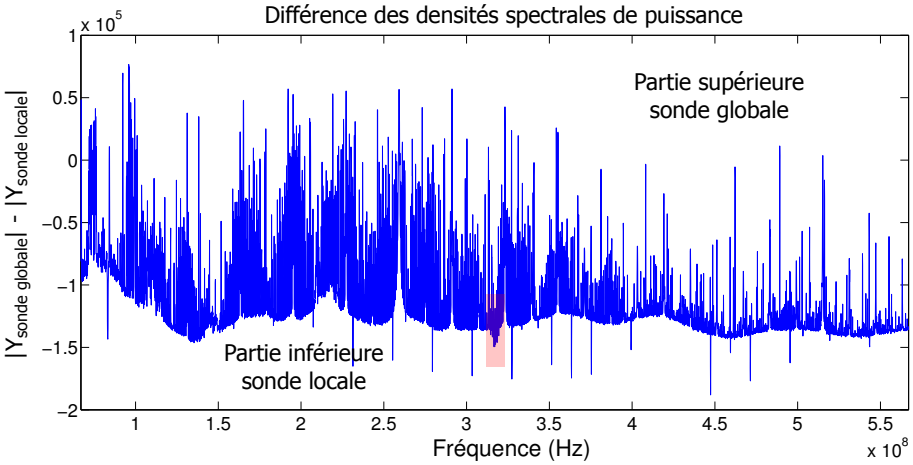

FIG. 3.37 – Différence des moyennes des densités spectrales de puissance, sur tout le circuit, pour l'IMP#3 pour la méthode de mesure à deux sondes.

La carte obtenue, en prenant comme plage de fréquence 315 MHz jusqu'à 318 MHz, est affichée dans la Figure 3.38.

Nous obtenons avec cette méthode quasiment les mêmes résultats que ceux obtenus avec la méthode initiale. L'avantage premier de cette méthode réside dans son temps d'acquisition (il est dans le pire des cas deux fois plus court). L'autre gros avantage est qu'il est relativement facile d'effectuer directement avec un oscilloscope (si ce dernier dispose d'un module de calcul de densité spectrale de puissance) la recherche du générateur sur le circuit sans passer par la réalisation d'une carte. On peut noter cependant que les cartes résultantes sont moins précises que celles obtenues avec l'autre méthode.

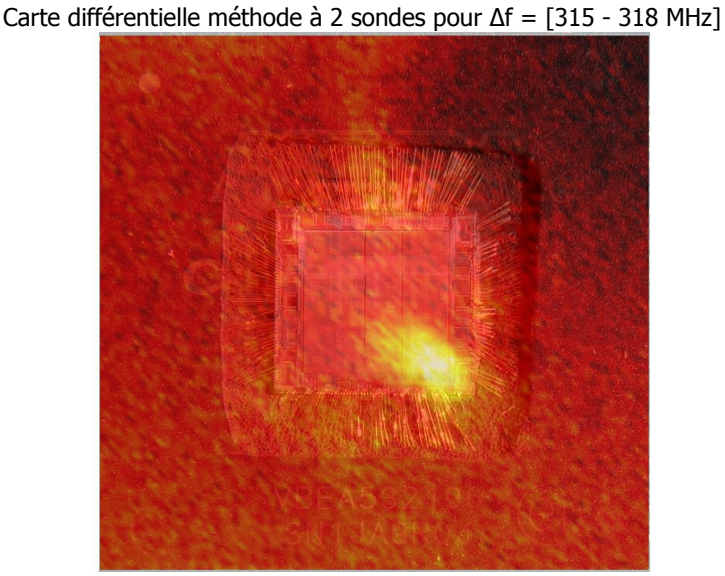

FIG. 3.38 – Carte résultante de la méthode à deux sondes.

3.6 Conclusion

Nous avons présenté ici une méthode d'analyse du rayonnement électromagnétique adaptée aux générateurs d'aléa à base d'oscillateur en anneau. Cette méthode se base sur une analyse fréquentielle déjà existante ([Sauvage et al., 2009]) mais a été adaptée, en exploitant une propriété des oscillateurs en anneau, à l'étude des générateurs d'aléa qui utilisent ces derniers comme source d'aléa. En effet, en récupérant deux spectres du rayonnement électromagnétique du circuit pour des tensions d'alimentation différentes, il est possible en effectuant une différence entre les deux spectres, de mettre en avant les fréquences qui correspondent aux oscillateurs.

Nous avons montré ici, quelle que soit la technologie de FPGA (Flash ou SRAM), quelle que soit la composition de l'implantation (c'est à dire même en présence d'un système cryptographique presque complet), que nous sommes capables de récupérer des informations cruciales sur le générateur, à savoir, la fréquence de fonctionnement des oscillateurs, mais également leurs positions dans le circuit.

Nous avons également proposé une méthode d'analyse qui se base sur la différence entre une mesure globale et une mesure locale du champ qui est émis par le circuit sous test. Cette méthode ne nécessite pas de modifier les conditions de fonctionnement de la carte, et peut être également facilement réalisable à la volée avec un oscilloscope qui dispose de module de calcul mathématique (transformée de Fourier). Cependant cette méthode nécessite une sonde supplémentaire mesurant le champ électromagnétique globale et un amplificateur pour cette sonde.

Cette analyse représente la première étape de notre attaque combinée. Main-

tenant que nous disposons de suffisamment d'informations sur le générateur, il est possible d'utiliser le canal caché électromagnétique pour venir perturber la génération d'aléa. C'est ce que nous proposons d'étudier dans le prochain chapitre.

Chapitre 4

Attaque en faute sur générateur d'aléa par injection électromagnétique harmonique

Dans ce chapitre, nous allons présenter une attaque active qui utilise un rayonnement électromagnétique harmonique. Cette attaque suit directement l'attaque passive présentée dans le chapitre précédent (comme cela a déjà été expliqué par la Figure 2.18). Nous commencerons par présenter les expérimentations effectuées. Ensuite nous étudierons les effets de l'onde électromagnétique, d'un point de vue expérimental, sur les oscillateurs en anneau et sur le générateur complet. Puis nous étudierons plus en détail le phénomène de verrouillage des oscillateurs. Enfin, nous discuterons d'une modélisation électrique et mathématique de l'effet de l'attaque sur l'extracteur d'entropie du générateur.

Les travaux expérimentaux présentés dans ce chapitre ont été réalisés en collaboration avec François Poucheret et Philippe Maurinne du LIRMM (Laboratoire d'information, robotique et micro-électronique de Montpellier), dans le cadre du projet ANR EMAISeCi.

Sommaire du chapitre

3.1 Objectif **53**

3.2 Différentes techniques de cartographie **53**

3.2.1 Cartographie temporelle 54

3.2.2 Cartographie à analyse fréquentielle 54

3.2.3 WGMSI - Mesure d'incohérence dans la densité spectrale de puissance 55

3.2.4 Cartographie de corrélation croisée 57

3.3 Présentation de l'analyse électromagnétique appliquée aux générateurs d'aléa **58**

3.4 Résultats de cartographie sur les TRNGs **60**

3.4.1 Résultats de cartographie sur Altera CycloneIII 60

3.4.1.1 Présentation des expériences 60

3.4.1.2 Cartographie générateur d'aléa seul - IMP#1 & IMP#2 62

3.4.1.3 Cartographie générateur et chiffreur - IMP#3 . . . 73

3.4.2 Résultats de cartographie sur Microsemi Fusion 78

3.4.2.1 Présentation de l'expérience 78

3.4.2.2 Cartographie anneau et chiffreur 78

3.5 Différence analyse locale et globale 83
3.5.1 Principe 83
3.5.2 Résultat sur l'IMP#3 (Altera Cyclone III) 85
3.6 Conclusion 86

4.1 Présentation de l'attaque

4.1.1 Les cibles

L'intuition de départ, quant à l'influence de l'injection harmonique électromagnétique sur les générateurs à base d'oscillateurs en anneau, était que nous allions pouvoir verrouiller (ici verrouiller a le même sens que pour une boucle à verrouillage de phase) les oscillateurs sur une fréquence qui n'est pas leur fréquence d'origine. Ce phénomène de verrouillage peut apparaître sans que cela résulte d'une attaque. En effet deux oscillateurs peuvent naturellement s'influencer l'un avec l'autre si ces derniers sont situés relativement proches l'un de l'autre dans le circuit. Ce phénomène a été mis en lumière par le biais d'études expérimentales dans notre équipe [Bochard et al., 2010].

Pour cette attaque, nous avons choisi de présenter seulement les résultats sur le module FPGA Microsemi Fusion. Cependant, l'attaque est également effective sur les modules Altera Cyclone III et Xilinx Spartan3.

Les expérimentations ont été effectuées sur deux implantations différentes :

- La première étude a été réalisée sur les oscillateurs en anneau seuls. La première implantation, décrite dans la Figure 4.1 est composée de quatre oscillateurs en anneau, eux mêmes composés de 3 inverseurs (les mêmes oscillateurs en anneau qui ont été utilisés précédemment). Nous savons, d'après les résultats d'analyse du Chapitre 3 que ces oscillateurs ont une fréquence de fonctionnement proche de 320 MHz pour une tension de fonctionnement qui correspond à la tension nominale du FPGA (1.5 V). Cette implantation est appelée dans la suite Cible#1.

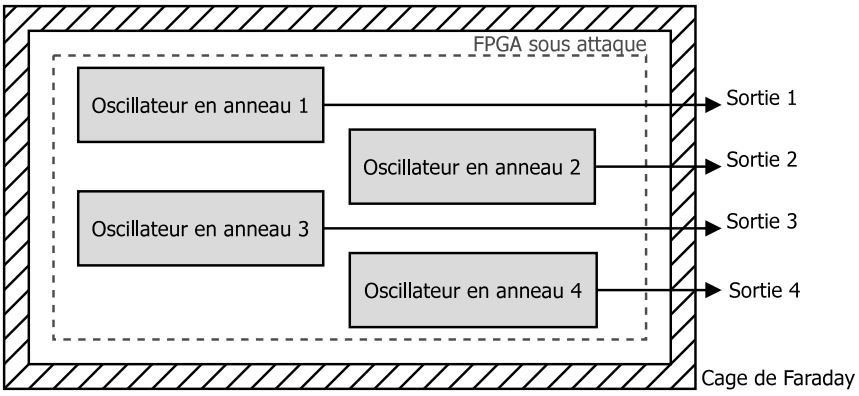

FIG. 4.1 – Implantation des oscillateurs en anneau pour la Cible#1 (cette figure ne représente pas un floorplan précis de l'implantation).

- La deuxième étude a été réalisée sur un générateur d'aléa et le module de communication associé. La seconde implantation, décrite dans la Figure 4.2 est séparée sur deux FPGAs. La première carte, qui est installée dans la cage de Faraday, et donc sous l'influence du rayonnement électromagnétique, incorpore seulement le cœur du générateur d'aléa (voir la Figure 1.4). En effet, pour

s'assurer que la communication USB (module USB, parallélisation des données, mémoire FIFO) avec l'ordinateur n'est pas impactée par la perturbation électromagnétique, cette partie là, a été implantée dans le FPGA d'une carte située en dehors de la cage de Faraday (et donc par conséquent, non soumise aux perturbations électromagnétiques). La vitesse de transfert du module de communication (jusqu'à 20 MB/s) est largement suffisante pour assurer un transfert correct du flot de bits produit par le générateur. La mémoire FIFO quant à elle assure qu'aucune donnée n'est perdue lors du transfert. On remarque sur la Figure 4.2 que deux signaux sont échangés entre les deux cartes. Le premier signal correspond à l'horloge utilisée par les bascules D du générateur. Ce signal est généré par une PLL dans la carte qui gère la communication avec l'ordinateur. Le deuxième signal correspond au bit aléatoire généré par le générateur à chaque front montant du signal d'horloge. Les câbles qui permettent de transmettre ces deux signaux sont blindés de manière à assurer que la perturbation électromagnétique ne soit pas conduite par les câbles. Pendant l'attaque, ces deux signaux sont également surveillés par le biais d'un oscilloscope de manière à être certain que leurs intégrités ne soient pas affectées. Cette implantation est appelée dans la suite Cible#2.

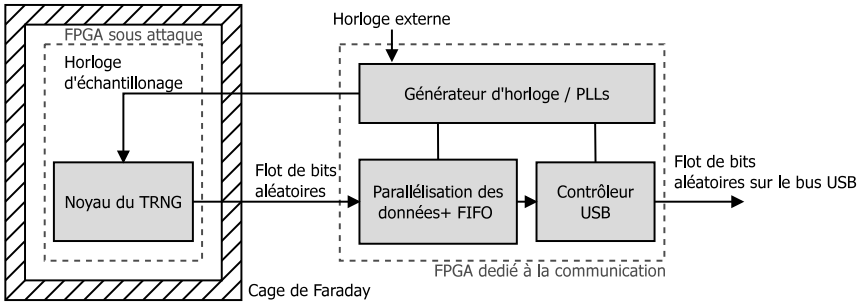

FIG. 4.2 – Architecture de test du générateur de nombre aléatoires - Cible#2

Dans les deux implantations, nous avons particulièrement porté attention à ce qu'aucun oscillateur en anneau ne soit initialement verrouillé sur un autre (certains placement-routages font que deux oscillateurs peuvent être initialement verrouillés l'un avec l'autre, notamment lorsque ces oscillateurs sont proches).

Dans les deux cas, les oscillateurs en anneau sont composés de trois inverseurs, ce qui correspond, comme dit précédemment, à une fréquence de fonctionnement proche de 320 MHz. Pour la Cible#2, le générateur est composé de 50 oscillateurs en anneau, et utilise une horloge d'échantillonnage de 24 kHz. Cette fréquence d'échantillonnage (relativement faible par rapport aux valeurs trouvées généralement dans la littérature - [Wold and Tan, 2008] ou [Sunar et al., 2007]) a été choisie de manière à être sûr que le flot de bits produit par le générateur puisse passer les tests statistiques NIST. De manière générale, réduire la fréquence d'échantillonnage améliore les propriétés statistiques du flot de bits produit par le générateur (en effet, le temps d'accumulation de l'incertitude temporelle est plus long). Au contraire, augmenter

cette fréquence peut potentiellement entraîner une réduction de l'entropie extraite par le générateur.

A noter que le générateur utilisé est composé de deux fois plus d'oscillateurs en anneau que ce qui est préconisé par les auteurs de [Wold and Tan, 2008], ce qui le rend ainsi moins sensible à la possible dépendance entre les oscillateurs.

4.1.2 Paramètres de l'attaque

Comme montré à la fois dans la Figure 4.1, la Figure 4.2, mais aussi dans le Chapitre 2, le circuit sous test est placé dans une cage de Faraday. La sonde d'injection utilisée est placée au dessus de la position du générateur (cette position a été trouvée grâce à l'analyse présentée dans le Chapitre 3) et au plus proche du capot en plastique du circuit (ndlr : ce capot n'a pas été altéré de manière à rendre l'attaque plus facile), c'est à dire à une distance de l'ordre de la centaine de μm.

- Le premier jeu d'expérimentations réalisées sur la Cible#1, a pour but l'analyse de l'influence de l'attaque électromagnétique harmonique sur les oscillateurs en anneau. La puissance du signal harmonique transmise à la sonde ($P_{\text{transmise}}$) est fixée successivement à [34 nW ; 340 μW ; 1 mW ; 3 mW], et sa fréquence balaye une plage comprise entre 300 MHz et 325 MHz. Cette plage de fréquence a été choisie par rapport aux résultats présentés dans le Chapitre 3. Pour cette analyse, nous avons acquis successivement dix traces pour chacune des quatre voies de l'oscilloscope, avec une fréquence d'échantillonnage de l'oscilloscope réglée à 20 MS/s, dans le but de récupérer :
  - V_1 qui est le signal qui provient de l'oscillateur#1 et qui est également utilisé comme signal de déclenchement de l'oscilloscope.
  - V_2, V_3, V_4 qui sont les signaux qui proviennent respectivement des oscillateurs #2, #3 et #4.
- Le second jeu d'expérimentations, vise à l'étude de l'effet de l'attaque électromagnétique harmonique sur le comportement d'un générateur de nombres aléatoires complet (Cible#2). Une sauvegarde du flot de bits produit par le générateur sans attaque a été réalisée comme référence. Par la suite pour chaque paramètre d'injection, un flot de bits a été acquis. Nous verrons dans la suite que la fréquence du signal harmonique injecté a été choisie et fixée à 309.7 MHz.

4.2 Influence de l'injection électromagnétique harmonique sur les oscillateurs en anneau

4.2.1 Choix de la fréquence d'injection

Le choix de la fréquence d'injection est crucial. Cette fréquence détermine si l'attaque est un succès. Le but premier est d'induire une dépendance forte entre les oscillateurs en anneau et cette fréquence d'injection, il apparaît donc nécessaire que

la fréquence d'injection soit relativement proche des fréquences des oscillateurs en anneau.

Grâce aux travaux présentés dans le Chapitre 3, nous savons que la fréquence des oscillateurs en anneau qui constituent notre générateur est de l'ordre de 325 MHz. Nous allons donc chercher une fréquence d'injection dans une bande de fréquence proche de 320 MHz. En effet, nous souhaitons, si possible, impacter, avec notre perturbation électromagnétique harmonique, le plus d'oscillateurs à la fois avec la plus faible puissance d'injection possible.

La première étape de l'étude est de trouver une fréquence qui permette de perturber le plus d'oscillateurs. C'est pour cette raison, que l'attaque électromagnétique harmonique a été réalisée pour différentes valeurs de fréquence. Plus précisément, nous avons balayé une plage de fréquence comprise entre 300 MHz et 325 MHz (avec un pas de 50 kHz). Pendant ce balayage de fréquence, nous avons particulièrement étudié le rapport entre l'amplitude de la fréquence d'injection ($Y_{f_{inj}}$) et l'amplitude de la fréquence du i-ème oscillateur en anneau ($Y_{f_{RO_i}}$), dans le spectre fréquentiel du signal de sortie du i-ème oscillateur en anneau : $DFTR(i) = Y_{f_{inj}}/Y_{f_{RO_i}}$ (RO_i fait référence au i-ème oscillateur en anneau).

La Figure 4.3 représente le ratio $DFTR$ pour chaque oscillateur sur la plage de fréquence sélectionnée. On peut voir que ce ratio est maximum pour chaque oscillateur sur une plage qui s'étend de 307 MHz à 313 MHz. Nous avons choisi sur cette plage de fréquence, la fréquence de 309.7 MHz comme fréquence d'injection. Cette fréquence est la fréquence d'injection utilisée dans toute la suite des expérimentations.

La Figure 4.4 représente les spectres fréquentiels des signaux de sortie des oscillateurs 1 et 3 sous deux conditions différentes d'injection harmonique. La Figure 4.4.a correspond à un cas où il n'y a pas attaque, alors que la Figure 4.4.b correspond à une attaque électromagnétique harmonique avec une fréquence d'injection de 309.7 MHz et une puissance transmise ($P_{transmise}$) égale à 3 mW. Quand il n'y a pas présence d'attaque, on ne voit dans le spectre que des contributions aux fréquences qui correspondent à celles des deux oscillateurs (327 MHz pour l'oscillateur 3 et 331 MHz pour l'oscillateur 1 avec une différence de fréquence ΔF entre elle). Lors de l'attaque, on remarque, dans le spectre, l'apparition d'une contribution à la fréquence d'injection. Les fréquences qui correspondent aux oscillateurs ne sont pas supprimées, mais la fréquence d'injection prédomine (son amplitude est 15 fois plus importante que les amplitudes qui correspondent aux fréquences des oscillateurs). Les oscillateurs oscillent donc, sous l'effet de la perturbation électromagnétique, à la fréquence d'injection. On peut dire en un sens que les oscillateurs (au moins les oscillateurs 1 et 3) sont mutuellement verrouillés sur le signal d'injection.

4.2.2 Étude de l'évolution de l'information mutuelle lors de l'attaque

Pour vérifier que les quatre oscillateurs en anneau sont effectivement tous dépendants du signal d'injection, nous avons analysé l'évolution de l'information mutuelle

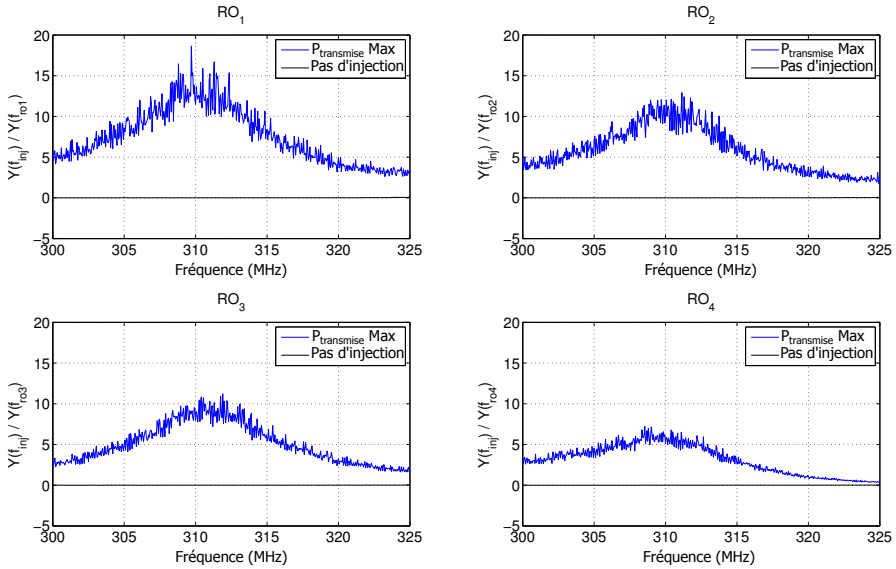

FIG. 4.3 – Rapport $DFTRi = Y_{f_{inj}}/Y_{f_{RO_i}}$ en fonction de la fréquence d'injection pour les signaux de sorties de chaque oscillateur en anneau (RO_1 à RO_4).

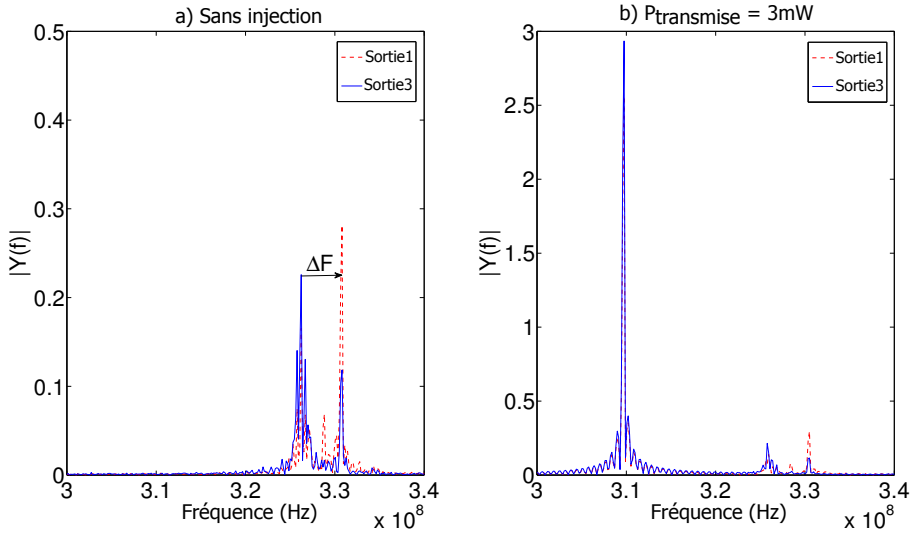

FIG. 4.4 – Transformée de Fourier des signaux V_1 et V_3 sous : a) des conditions normales de fonctionnement b) une perturbation électromagnétique harmonique avec une fréquence égale à 309.7 MHz et avec $P_{transmise} = 3$ mW.

(IM) entre les signaux de sortie des quatre oscillateurs ($V_i(t)$,$V_j(t)$). L'information mutuelle est un évaluateur qui permet de vérifier la dépendance entre deux variables aléatoires. Il est également souvent utilisé comme évaluateur lors d'analyses qui exploitent les canaux cachés [Batina et al., 2011] pour l'attaque de bloc de chiffrement.

Pour nos expérimentations, nous nous attendions à observer :

- Une valeur faible de l'information mutuelle entre $V_i(t)$ et $V_j(t)$ quand $P_{transmise}$ = 340 nW, ce qui montre que les oscillateurs ne sont pas verrouillés,
- Une valeur de l'information mutuelle qui augmente progressivement avec l'augmentation de $P_{transmise}$, ce qui montre l'effet de verrouillage progressif des oscillateurs avec le signal d'injection.

Le tableau Tableau 4.1 montre les valeurs de l'information mutuelle pour différentes puissances d'injection. Comme attendu, les valeurs de l'information mutuelle sont faibles (0.02 bit) quand $P_{transmise}$ = 340 nW. De même, lorsque la puissance augmente (et atteint 3 mW), la valeur moyenne de l'information mutuelle augmente jusqu'à 0.99 bits. Cela montre clairement le verrouillage des oscillateurs sur une même fréquence.

Par la suite, dans le but de rendre l'affichage des résultats plus léger, nous avons choisi seulement un couple d'oscillateurs. Ce seront donc les oscillateurs 1 et 3 qui seront par la suite étudiés (comme cela est déjà le cas pour Figure 4.4).

TAB. 4.1 – Valeurs de l'information mutuelle, obtenues pour différentes puissances d'injection, pour les différents couples d'oscillateurs en anneau.

$P_{transmise}$ @ 309.7 MHz	340 nW	34 μW	1 mW	3 mW
IM(RO#1,RO#2)	0.0267	0.1746	0.5478	1.5729
IM(RO#1,RO#3)	0.0305	0.7697	0.7889	1.1029
IM(RO#1,RO#4)	0.0135	0.2838	0.6747	0.8221
IM(RO#2,RO#3)	0.1055	0.1086	0.3872	0.8379
IM(RO#2,RO#4)	0.0245	0.1332	0.2247	0.6477
IM(RO#3,RO#4)	0.0383	0.3196	0.8053	0.9382
IM moyenne	**0.0398**	**0.2983**	**0.5715**	**0.9870**

4.2.3 Visualisation de l'effet à l'oscilloscope

Cette dépendance est également visible directement sur l'oscilloscope grâce à l'utilisation du mode d'affichage en persistance. Figure 4.5 montre les signaux V_1 et V_3 obtenus sans (Figure 4.5.a) et avec (Figure 4.5.b) injection. Comme il est directement visible sur les figures, sans attaque, les deux sorties des oscillateurs ne sont pas du tout synchronisées, alors que lors de l'injection électromagnétique, les oscillateurs se synchronisent.

4.2.4 Réduction de la phase entre les deux oscillateurs

Sous des conditions normales de fonctionnement, les oscillateurs en anneau, de même topologie, ont des fréquences de fonctionnement différentes (ceci est dû aux délais d'interconnexion qui sont différents et aux variations du processus de fabrication). La différence de fréquence $\Delta F = f_{RO_1} - f_{RO_3}$ produit un glissement linéaire

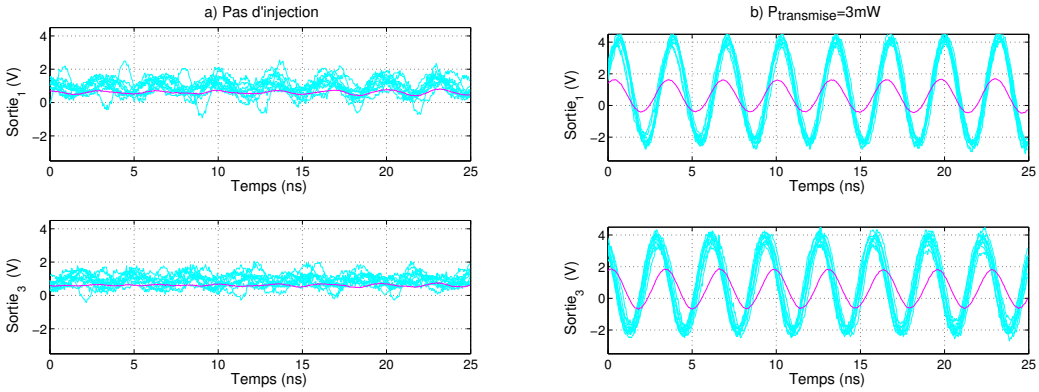

FIG. 4.5 – Superposition en persistance de traces acquises successivement (trait gras) et traces moyennes (trait fin) de V_1 et V_3 pendant : a) des conditions de fonctionnement normales et b) une attaque électromagnétique harmonique avec $P_{transmise}$ = 3 mW et f_{inj} = 309.7 MHz.

entre les fronts montants des signaux qui proviennent des deux oscillateurs (les positions temporelles des fronts dépendent également de l'incertitude temporelle, mais comparativement à ΔF, l'impact de cette incertitude temporelle est faible et ne peut se voir que sur une accumulation sur plusieurs périodes).

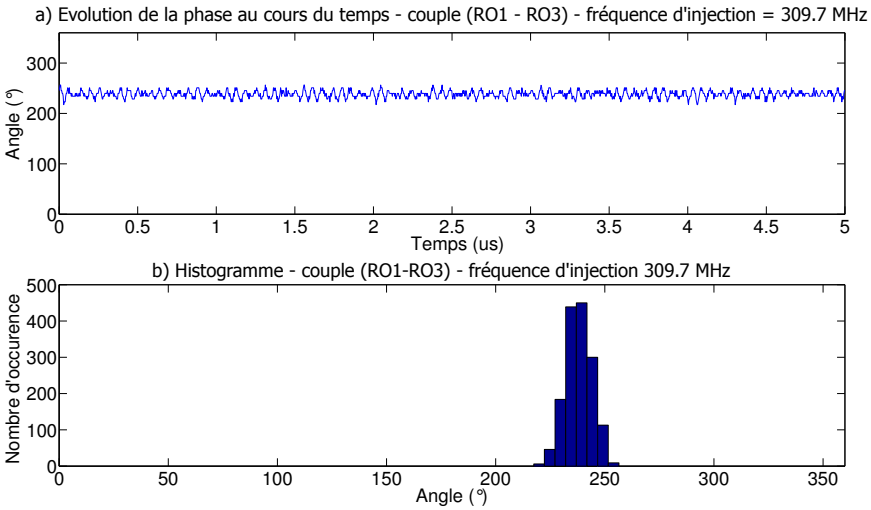

FIG. 4.6 – a) Différence de phase entre V_1 et V_3 au cours du temps b) Histogramme des phases.

Dans le cas d'un forte injection électromagnétique harmonique, les deux oscillateurs sont verrouillés sur la fréquence d'injection. Ce phénomène s'observe facilement sur la Figure 4.4, où l'harmonique de plus forte amplitude du signal de sortie des oscillateurs correspond à la fréquence du signal perturbateur. Ainsi, les deux oscillateurs ont la même fréquence ; nous nous proposons donc d'évaluer la diffé-

rence de phase entre les signaux des oscillateurs. Sur la Figure 4.6, nous avons tracé l'évolution de la différence de phase entre les signaux V_1 et V_3. En accord avec l'histogramme (situé également sur la Figure 4.6, on peut voir que, la phase est distribuée entre 222 ° et 252 ° , et elle est centrée autour de 237 ° , ce qui donne une plage de variation de la phase de 30 ° . Si on regarde de plus près l'évolution de la différence de phase au cours du temps, elle semble suivre une tendance sinusoïdale. Comme dit précédemment, pendant l'injection harmonique, V_1 et V_3 sont composées de deux fréquences, l'une qui correspond à la fréquence d'injection (f_{inj}) et l'autre qui correspond aux fréquences propres à chaque oscillateur (f_{RO_1} and f_{RO_3}). La présence de ces deux fréquences (proches l'une de l'autre) dans le spectre produit un phénomène de battement (comme on l'entend en acoustique). Ce phénomène de battement explique cette tendance sinusoïdale.

4.3 Une maîtrise complète du flot de bits produit par le générateur

Après avoir étudié l'effet de l'attaque électromagnétique harmonique sur les oscillateurs en anneau, c'est à dire sur la source d'entropie de notre générateur, nous allons maintenant nous intéresser à l'étude de l'effet sur le générateur complet. Nous nous attendons bien évidemment à retrouver un impact de l'effet de verrouillage des oscillateurs sur le flot de bits aléatoires produit par le générateur (au même titre que les résultats présentés dans [Markettos and Moore, 2009]).

4.3.1 Effet de la dépendance des oscillateurs sur le flot de sortie du générateur de nombres aléatoires

Les flots de bits produits par le générateur de nombres aléatoires, pour différents niveaux de puissance d'injection électromagnétique sont présentés dans la Figure 4.7. Chaque flot de bits présenté est composé de 120 lignes de 32-bits (tous les bits sont acquis successivement). Sur cette figure, les carrés noirs correspondent à un niveau binaire de 1 et les blancs à un niveau binaire de 0. Il est bon de rappeler que, sous des conditions normales de fonctionnement (Figure 4.7.a), le flot de bits produit par le générateur de nombres aléatoires passe les tests statistiques de la suite NIST, avec un niveau de confiance α de 0.001, appliqués à 1000 séquences de 1 Mbit. De manière à accélérer l'étude, nous avons, pour les flots de bits acquis pendant les attaques, seulement utilisé le test de fréquence (ou encore test de biais). Ce test évalue l'équilibre entre le nombre de 1 et de 0 dans le flot de bits. Si les données générées ne passent pas ce test, il n'est pas nécessaire de continuer l'étude avec les autres tests (plus complexes, et plus longs à appliquer).

Dans le Tableau 4.2, le biais est défini comme $Biais = abs(0.5 - P(0)) = abs(0.5 - P(1))$, où P(x) est la probabilité d'obtenir l'élément x en sortie du générateur. Le biais peut varier entre 0 et 0.5. Nous utilisons un affichage du biais en %, qui est obtenu en extrapolant les valeurs de biais entre 0% et 100% qui cor-

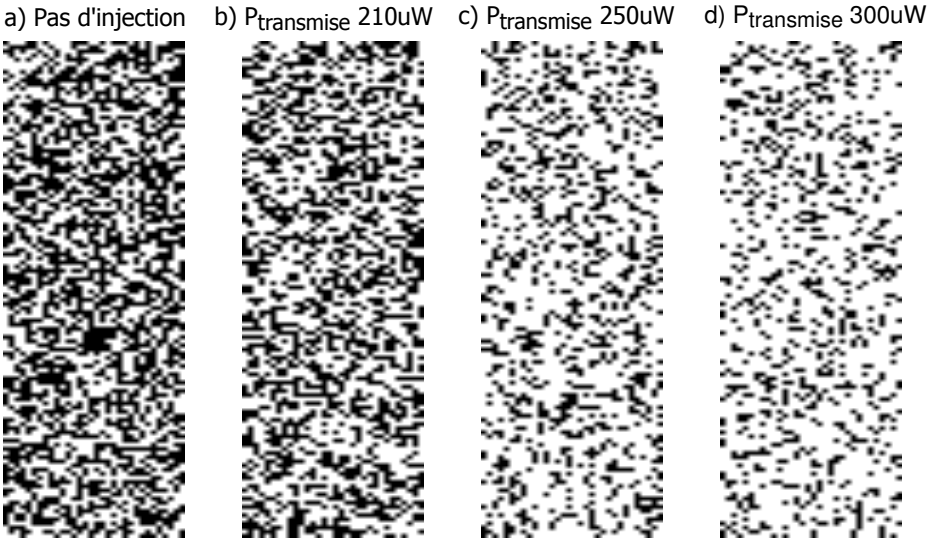

FIG. 4.7 – Flots de bits (120x32) produits par le générateur de nombres aléatoires sous des puissances différentes d'injection et une fréquence d'injection de 309.7 MHz - De la gauche vers la droite : a) Pas d'injection b) $P_{tranmise}$ = 210 μW c) $P_{tranmise}$ = 260 μW d) $P_{tranmise}$ = 300 μW

TAB. 4.2 – Paramètres statistiques du flot de bits de sortie du générateur.

$P_{tranmise}$	Pas d'injection	210 μW	260 μW	300 μW
Biais%	0.1%	15.87%	51.57%	55%
Tests NIST	SUCCES	ECHEC	ECHEC	ECHEC

respondent respectivement aux valeurs de biais de 0 et 0.5. Un bon générateur de nombres aléatoires doit avoir un biais très proche de 0%.

En accord à la fois avec la Figure 4.7 et le Tableau 4.2, l'effet de l'injection électromagnétique sur le biais de la suite de bits produite par le générateur est clair. Par exemple, pour une puissance d'injection de 210 μW (Figure 4.7.b) le biais atteint une valeur de 15% (par exemple, pour 100 bits produits par le générateur, 15 bits seront impactés par l'injection électromagnétique). En augmentant la puissance du signal harmonique jusqu'à 260 μW, le biais augmente jusqu'à 50% (Figure 4.7.c et Figure 4.7.d).

4.3.2 Contrôle dynamique du biais

L'expérience précédente confirme qu'il est possible de modifier le comportement du générateur de nombres aléatoires (notamment de modifier le biais de la suite de bits produite). Dans l'expérience qui suit, nous voulons observer le comportement dynamique du générateur sous l'effet de l'attaque : en d'autres mots, savoir lors du début (ou de l'arrêt) de l'application de la perturbation, combien de temps met la suite de bits produite par le générateur avant d'être (ou respectivement de ne plus

être) impactée. Pour cela, nous avons rajouté dans la chaîne d'injection (voir la Figure 2.14), un modulateur d'amplitude (AM) entre le générateur RF et l'entrée de l'amplificateur de puissance. Ce montage permet d'effectuer une multiplication analogique entre le signal d'injection (un signal sinusoïdal avec une fréquence de 309.7 MHz et un signal carré de fréquence 1 Hz). Ce dernier nous permet de contrôler avec précision, le début et la fin de l'injection électromagnétique. Ce signal de contrôle est fourni par un générateur de signal classique. La Figure 4.8.a représente l'évolution du signal en entrée de l'amplificateur de puissance (donc après multiplication du signal sinusoïdal et du signal carré). La Figure 4.8.b montre le flot de bits produit par le générateur. Et enfin la Figure 4.8.c représente l'évolution du biais de la suite générée dans le temps. Ce biais a été calculé en utilisant une fenêtre glissante de 10 000 bits et un pas de glissement de 32 bits.

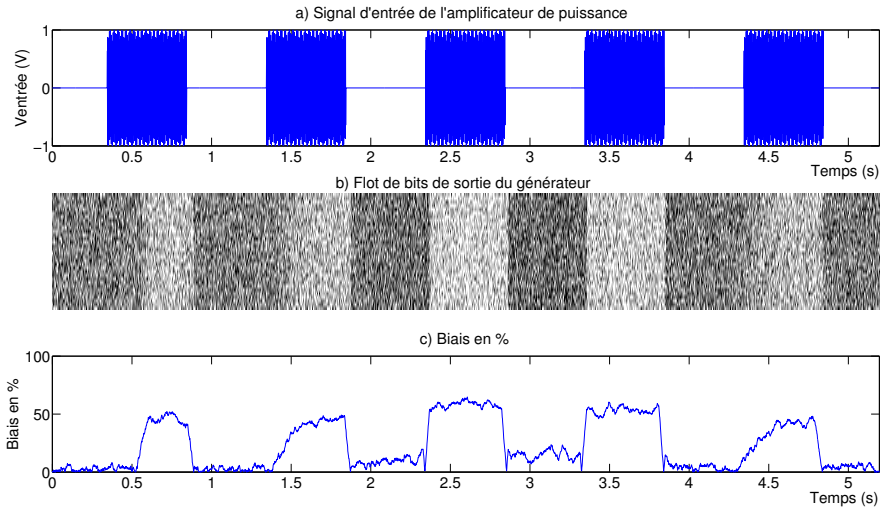

FIG. 4.8 – a) Signal modulé en amplitude en entrée de l'amplificateur de puissance - b) Flot de bit en sortie du générateur (à lire de bas en haut et de gauche à droite) - c) Biais en % de la suite de bits génerée.

En regardant le flot de bits (Figure 4.8.b) ou l'évolution du biais (Figure 4.8.c), il est évident que le comportement du générateur est rapidement impacté par la perturbation électromagnétique (de l'ordre d'une milliseconde), et qu'il retourne également dans son état initial avec la même rapidité. En effet, nous pouvons observer ici, que le biais évolue en accord avec les paramètres dynamiques (temps de montée et de descente) de l'étage d'amplification de puissance du banc d'injection. Pour le banc utilisé, les différents modules qui constituent cet étage ont en effet un temps de réponse de l'ordre de la milliseconde. La différence de valeur pour l'évaluation du biais entre deux périodes d'attaques successives est due au fait que l'amplificateur de puissance n'est pas adapté à être utilisé avec une entrée qui est modulée en amplitude. De ce fait, la puissance en sortie du générateur n'est pas fixe d'une période à l'autre.

Cette expérience montre clairement qu'il est possible de manipuler de manière dynamique le générateur de nombres aléatoires, et ce même s'il est composé d'un grand nombre d'oscillateurs en anneau. Ce contrôle dynamique de l'injection électromagnétique harmonique est d'une grande importance du point de vue de l'attaquant. En effet, cela lui permet, en cas de présence de tests statistiques embarqués qui évaluent la suite générée de manière périodique, de pouvoir impacter le générateur lorsque ces tests ne fonctionnent pas.

4.4 Une étude du comportement des oscillateurs en anneau sous injection électromagnétique harmonique

Dans cette partie, nous allons étudier par simulation l'effet de l'attaque par injection harmonique sur les oscillateurs en anneau. Le but de cette étude est de fournir un modèle permettant de décrire les phénomènes électriques mis en jeu. Nous avons parlé, dans les parties précédentes, de la notion de verrouillage ou d'interdépendance des oscillateurs en anneau. Nous allons ici, utiliser un modèle électrique de ce phénomène et nous allons voir si ce modèle peut s'appliquer à notre cas en réalisant plusieurs simulations sur des oscillateurs en anneau. Nous comparerons leur comportement en simulation avec ce que nous avons obtenu en expérimentation.

4.4.1 Le modèle d'Adler et sa généralisation aux oscillateurs numériques

La première observation notable de l'effet de verrouillage de deux oscillateurs (au sens large du terme) entre eux a été réalisée par Christian Huygens au XVIIe siècle ([Huygens, 1893]). En effet, ce dernier s'est rendu compte, que les balanciers de deux horloges étaient capables de synchroniser leurs mouvements entre eux, si ces horloges étaient accrochées au mur suffisamment proches l'une de l'autre. Huygens explique ce phénomène par un transfert de vibration, par l'intermédiaire du mur, d'une horloge à l'autre, ce qui force la synchronisation des oscillateurs. C'est le même type de phénomène qui s'applique aux oscillateurs électriques.

Par la suite, des travaux sur l'étude du verrouillage des oscillateurs électriques analogiques (RC, LC) ont été réalisés par Adler en 1973 (voir [Adler, 1973]). Dans ses travaux, il modélise cet effet de verrouillage comme une source de courant perturbatrice ajoutée entre la sortie de l'oscillateur et la masse (voir Figure 4.9). Il fournit également, en plus du modèle électrique, une modélisation mathématique qui permet de calculer les plages de verrouillage possibles en fonction des paramètres technologiques de l'oscillateur, de la fréquence de la source perturbatrice, et de l'intensité du courant perturbateur généré par cette source. Par la suite ces travaux ont été approfondis par les auteurs de [Bhansali and Roychowdhury, 2009]. On retrouve notamment une généralisation à des oscillateurs numériques (dont les oscillateurs en anneau).

Cependant, nous n'allons pas étudier en détail les modèles mathématiques qui

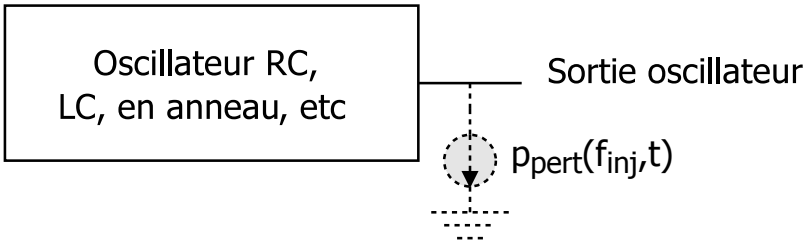

FIG. 4.9 – Modélisation électrique proposée par Adler du phénomène de verrouillage des oscillateurs.

correspondent à l'effet de verrouillage pour les oscillateurs en anneau. En effet, nous ne disposons d'aucun paramètre technologique propre aux différentes portes logiques utilisées dans le FPGA.

4.4.2 Analyse du comportement des oscillateurs en anneau en simulation

Pour étudier le phénomène de verrouillage induit par la perturbation électromagnétique harmonique, nous allons utiliser le même modèle électrique que celui proposé par Adler (voir la Figure 4.9).

4.4.2.1 Circuit et paramètres de simulation

Le circuit utilisé pour modéliser l'effet de la perturbation est présenté dans la Figure 4.10. Nous avons, dans ce circuit, placé deux oscillateurs en anneau de fréquences proches, mais différentes. La modélisation de l'effet de l'injection électromagnétique harmonique est donc réalisée par le biais des deux sources de courant (virtuelles) identiques positionnées entre la sortie des oscillateurs et la masse.

Les variables suivantes seront utilisées dans la suite :

- $f_{inj} = f_{pert}$ est la fréquence du signal sinusoïdal perturbateur,
- V_{inj} est l'amplitude du signal sinusoïdal perturbateur avant d'entrer dans le canal électromagnétique. Cette amplitude est directement dépendante du gain de l'amplificateur RF,
- I_{pert} est l'intensité du courant sinusoïdal perturbateur p_{pert}. Cette intensité est directement dépendante du canal électromagnétique et de V_{inj},
- (X, Y, Z) est la position de la sonde au dessus du circuit,
- t est le temps,
- $C_{sonde,circuit}$ représente l'efficacité du couplage entre la sonde et le circuit. Une valeur égale à 1 correspond à une transmission complète de toute la puissance, et une valeur égale à 0 correspond à une non transmission de puissance. Nous utiliserons l'écriture $C_{s,c}$ dans les équations suivantes.

Le signal perturbateur S_{inj} appliqué au circuit par le biais du canal électromagnétique est modélisé par l'Equation 4.1. Le but des travaux de cette thèse n'est pas de modéliser l'interaction entre la sonde et le circuit, nous allons donc considérer que

le canal électromagnétique peut être vu comme une fonction de transfert H. Cette fonction de transfert dépend de la position de la sonde, de sa topologie, du couplage entre la sonde et le circuit (cependant, nous expliquerons un peu plus en détails dans la section suivante de ce chapitre, l'interaction entre la sonde et le circuit), mais aussi de la fréquence d'injection f_{inj}. On peut donc modéliser les sources de courant par l'Equation 4.2 et la valeur de leur intensité par l'Equation 4.3

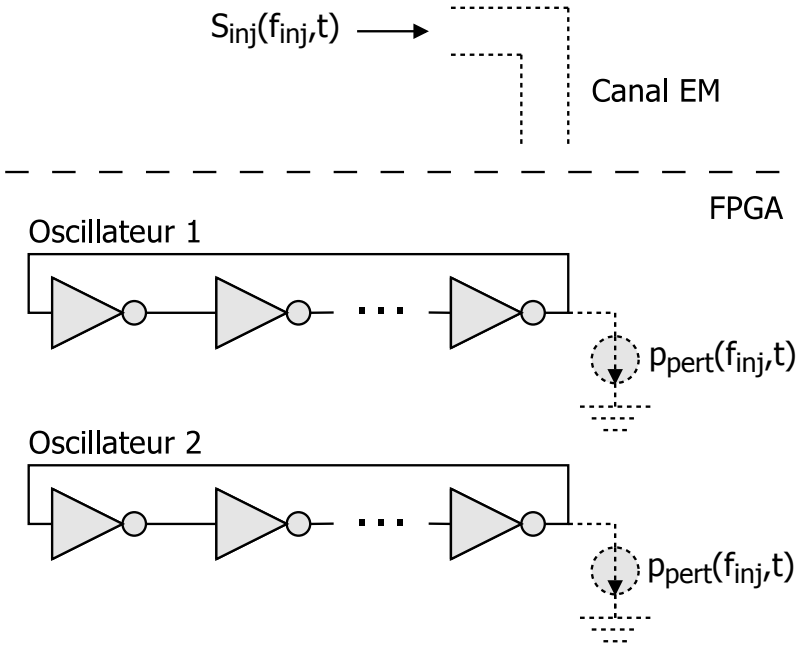

FIG. 4.10 – Circuit utilisé en simulation pour étudier le phénomène de verrouillage.

$$S_{inj}(f_{inj}, t) = V_{inj}(f_{inj}, t) sin(2\pi f_{inj} t) \tag{4.1}$$

$$p_{pert}(f_{pert}, t, (X, Y, Z), C_{s,c}) = I_{pert}(f_{pert}, t, (X, Y, Z), C_{s,c}) sin(2\pi f_{pert} t) \tag{4.2}$$

$$I_{pert}(f_{pert}, t, (X, Y, Z), C_{s,c}) = V_{inj}(f_{inj}, t) H((X, Y, Z), C_{s,c}, f_{inj}) \tag{4.3}$$

Pour simplifier les calculs, comme nous allons nous placer dans un cas de simulation électrique (et comme l'interaction sonde/circuit ne nous intéresse pas ici), nous allons considérer que l'intensité du courant n'est pas dépendante de la position de la sonde et de l'interaction sonde/circuit. Le modèle mathématique de la source de courant est alors décrit par l'Equation 4.4.

$$p_{pert}(f_{inj}, t) = I_{pert}(f_{inj}, t) sin(2\pi f_{inj} t) \tag{4.4}$$

Les simulations qui vont suivre ont été réalisées avec un simulateur Spice utilisant des modèles de transistor CMOS BSIM4.7.0. Une première simulation sans injection

a été réalisée de manière à déterminer les fréquences de fonctionnement des oscillateurs. Les spectres de sortie des oscillateurs sont représentés dans la Figure 4.11, avec en rouge le spectre du premier oscillateur et en bleu le spectre du deuxième oscillateur. La fréquence de fonctionnement du premier oscillateur est d'environ 316 MHz, et celle du deuxième d'environ 336 MHz.

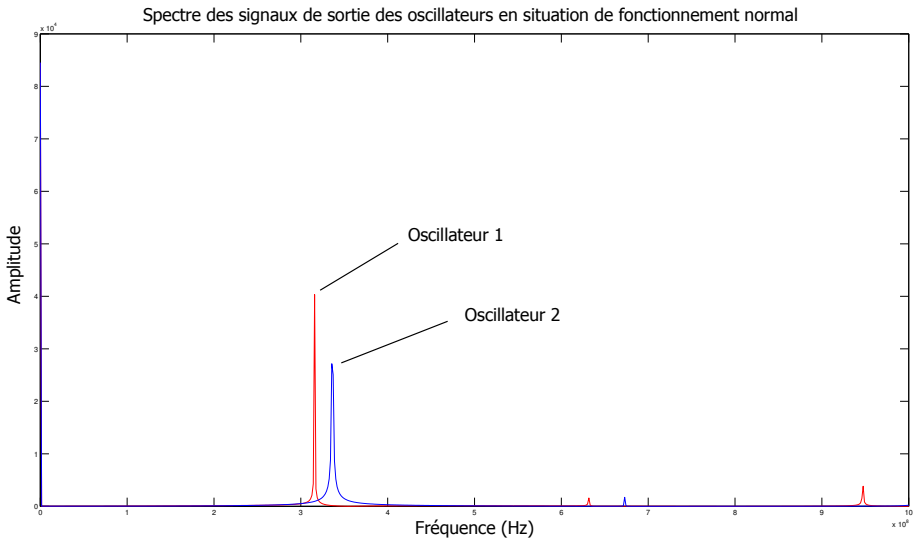

FIG. 4.11 – Spectres fréquentiels des sorties des deux oscillateurs pour des conditions normales de fonctionnement.

Par la suite nous avons balayé plusieurs fréquences d'injection (de 300 MHz à 350 MHz avec un pas d'un MHz) et plusieurs intensités du courant d'injection (de 0 μA à 20 μA avec un pas de 500 nA) de façon à déterminer pour quels couples (fréquence, intensité du courant), les oscillateurs en anneau sont impactés par la perturbation. Pour chaque couple, une simulation de 1 μs a été réalisée avec un pas de simulation de 10 ps.

4.4.2.2 Résultats

Dans la suite, l'état de verrouillage correspond à un état où la fréquence d'un oscillateur suit une autre fréquence que sa fréquence de fonctionnement nominale. Par exemple, si la fréquence nominale d'un oscillateur est normalement 320 MHz, et que du fait de notre injection électromagnétique (à 310 MHz par exemple), la contribution fréquentielle principale du signal de sortie de l'oscillateur est à 310 MHz, nous dirons que l'oscillateur est complètement verrouillé sur la fréquence d'injection.

La Figure 4.12 représente donc la plage de verrouillage (c'est à dire les couples (fréquence, intensité du courant) pour lesquels la fréquence de l'oscillateur correspond à la fréquence d'injection) pour le premier oscillateur (celui qui a une fréquence de fonctionnement de 316 MHz). La zone en blanc correspond aux couples pour lesquels l'oscillateur n'est pas complètement verrouillé (voir pas du tout), alors que la

zone en rouge correspond aux couples pour lesquels l'oscillateur est complètement verrouillé sur la fréquence d'injection.

Premièrement, en accord avec ce qui apparait sur la Figure 4.12, il ne faut aucune puissance pour verrouiller un oscillateur sur sa fréquence nominale, ce qui semble tout à fait logique. Deuxièmement, plus la différence entre la fréquence d'injection et la fréquence nominale de l'oscillateur est importante, plus le courant pour verrouiller l'oscillateur est important. La relation entre le courant et la différence de fréquence est d'ailleurs linéaire (et symétrique suivant que la différence est positive ou négative). On trouve donc une forme en V, en accord avec les équations présentées dans [Adler, 1973] et [Bhansali and Roychowdhury, 2009].

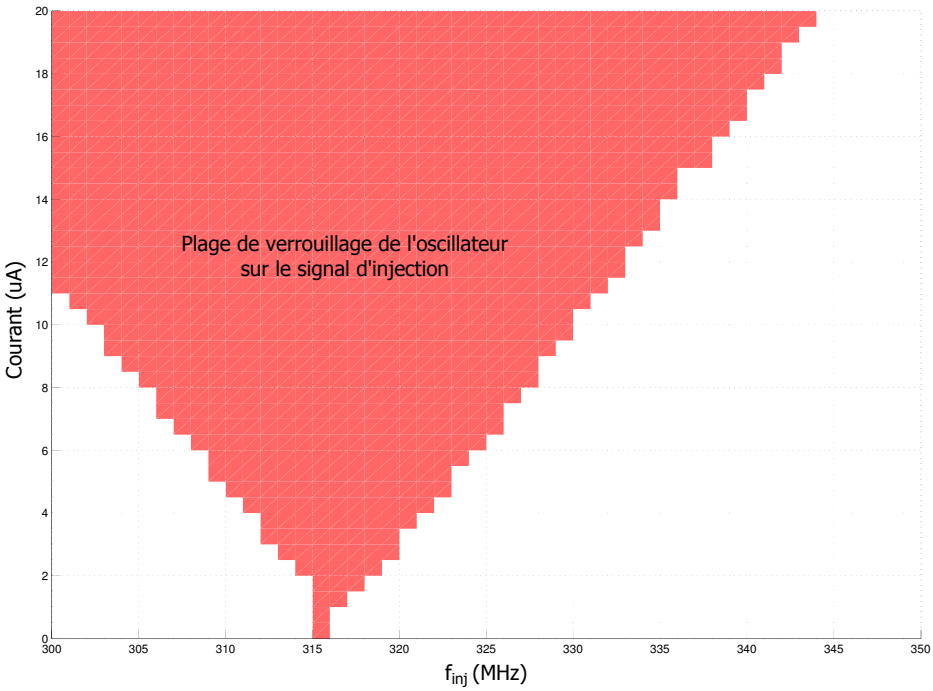

FIG. 4.12 – Zone de verrouillage pour le premier oscillateur.

Si on rajoute à cette figure, la même étude pour le deuxième oscillateur, on obtient la Figure 4.13. Les zones en jaune correspondent aux zones de verrouillage pour le premier ou le deuxième oscillateur seul. La zone rouge correspond à l'intersection des zones de verrouillage des deux oscillateurs (c'est à dire pour les couples de paramètres d'injection qui entrainent le verrouillage des deux oscillateurs sur le signal injecté). Si le générateur de nombres aléatoires ciblé dispose de plus de deux oscillateurs, il faut ajouter une zone de verrouillage pour chaque oscillateur supplémentaire. Plus les fréquences des oscillateurs sont écartées dans le spectre, plus le courant nécessaire pour verrouiller tous les oscillateurs sur la même fréquence est important. La fréquence la plus efficace pour le signal d'injection, quel que soit le

nombre d'oscillateurs est la moyenne de toutes les fréquences nominales des oscillateurs (voir point A sur la Figure 4.13). En effet, c'est la fréquence pour laquelle, le courant nécessaire pour être dans la zone de verrouillage commune est le plus faible. Dans le cas des deux oscillateurs présentés à la Figure 4.13, c'est 326 MHz la valeur de fréquence d'injection la plus efficace.

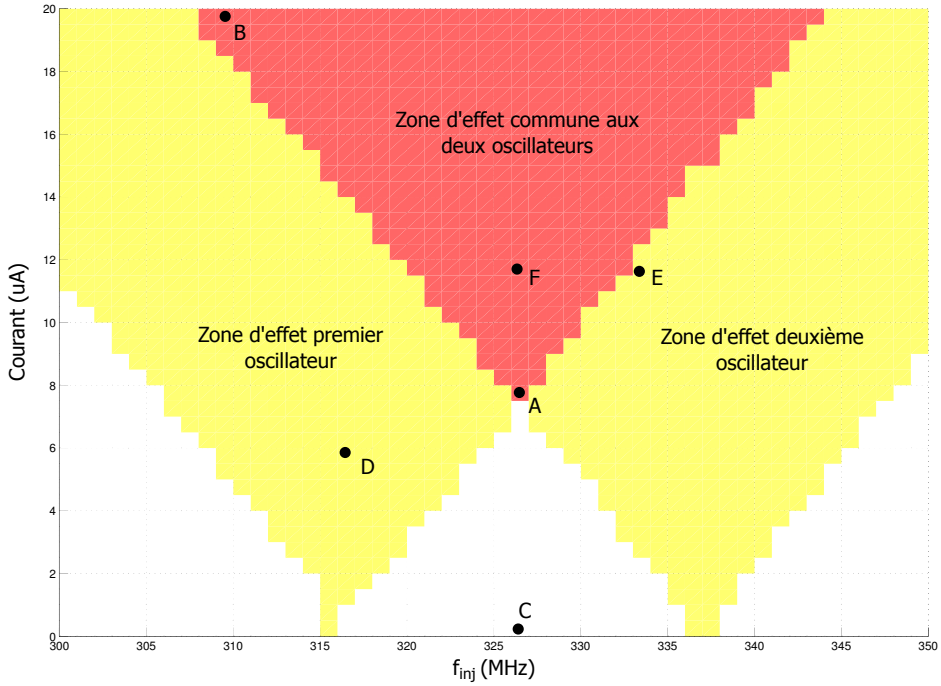

FIG. 4.13 – Zones de verrouillage pour deux oscillateurs.

La Figure 4.14 représente les spectres des sorties des deux oscillateurs lors d'un injection harmonique avec une fréquence d'injection égale à 309 MHz et avec une intensité du courant égale à 20 μA (on se place dans la zone commune de verrouillage des deux oscillateurs - voir point B sur la Figure 4.13). On remarque que dans cette situation, les seules fréquences existantes dans les spectres sont la fréquence d'injection et ses harmoniques. Les fréquences nominales des deux oscillateurs ne sont plus visibles.

A noter que pour chaque oscillateur la zone de verrouillage est la zone où l'oscillateur est complètement influencé par l'injection. Dans la zone blanche, l'oscillateur est progressivement influencé par l'injection sans pour autant être complètement verrouillé (c'est à dire que la fréquence de l'oscillateur est égale à la fréquence d'injection) ; sa fréquence est modifiée sans pour autant être égale à la fréquence d'injection (la fréquence moyenne du signal est à la fois différente de la fréquence d'injection et de sa fréquence nominale - elle se situe entre les deux).

La Figure 4.15 montre l'évolution, en fonction de l'intensité du courant, de l'am-

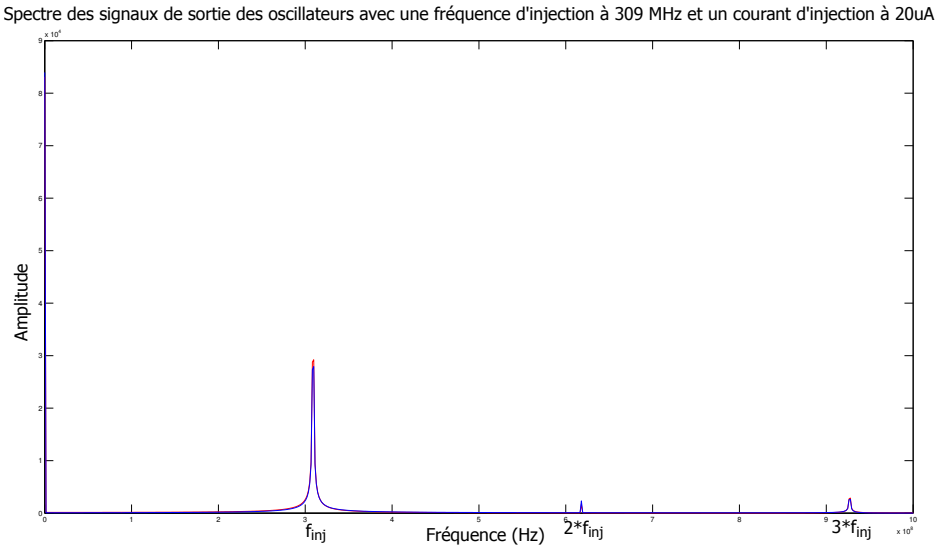

FIG. 4.14 – Spectres fréquentiels des sorties des deux oscillateurs pour une fréquence d'injection de 309 MHz et pour un courant de 20 μA (point B sur la Figure 4.13)

plitude de la fréquence nominale du premier oscillateur dans son spectre pour différentes valeurs de fréquence d'injection (300 MHz pour la trace rouge, 319 MHz pour la trace bleue, 334 MHz pour la trace verte et enfin 350 MHz pour la trace noire). La Figure 4.16 montre quant à elle l'évolution, en fonction de la valeur du courant, de l'amplitude de la fréquence d'injection dans le spectre de sortie du premier oscillateur. On voit clairement, grâce à ces deux figures qu'un transfert de puissance d'une fréquence à l'autre s'opère. Lorsque l'intensité du courant d'injection devient très importante, l'oscillateur est complètement verrouillé par l'injection harmonique. Les Figure 4.15 et Figure 4.16 montrent également que pour un oscillateur, plus la fréquence d'injection est proche de sa fréquence nominale, plus l'injection est efficace.

La Figure 4.17 représente l'évolution de la durée entre les fronts montants des deux oscillateurs pour plusieurs jeux de paramètres d'injection différents :

- Point C : (326 MHz - 0 A) - aucun oscillateur n'est verrouillé,
- Point D : (316 MHz - 6 μA) - l'oscillateur 1 est verrouillé, oscillateur 2 n'est pas verrouillé et très peu influencé,
- Point E : (334 MHz - 11.5 μA) - l'oscillateur 1 n'est pas verrouillé, l'oscillateur 2 est verrouillé,
- Point F : (326 MHz - 11.5 μA) - les deux oscillateurs sont verrouillées.

Les points peuvent être retrouvés dans la Figure 4.13. Sur la Figure 4.17, pour le point C, aucun des oscillateurs n'est verrouillé, on peut donc clairement voir un décalage de la durée entre chaque front successif du fait de la différence de fréquence des deux oscillateurs. Les discontinuités dans les différentes traces sont dues au fait qu'un des deux oscillateurs est plus rapide que l'autre, et remet donc ainsi à 0 la durée. Pour le point D, l'oscillateur 1 est complètement verrouillé et l'oscillateur 2

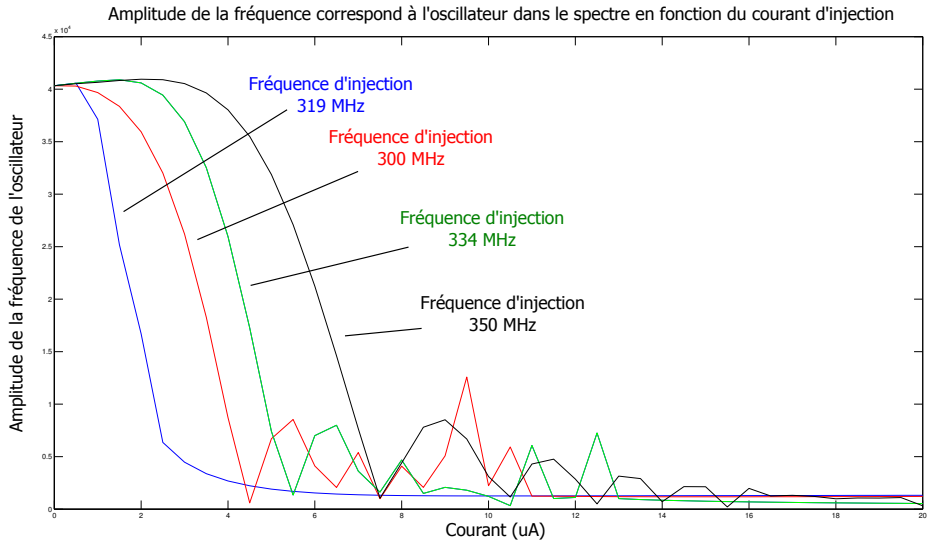

FIG. 4.15 – Amplitude de la fréquence nominale du premier oscillateur dans le spectre fréquentiel de la sortie de l'oscillateur en fonction du courant d'injection pour plusieurs fréquences d'injection différentes.

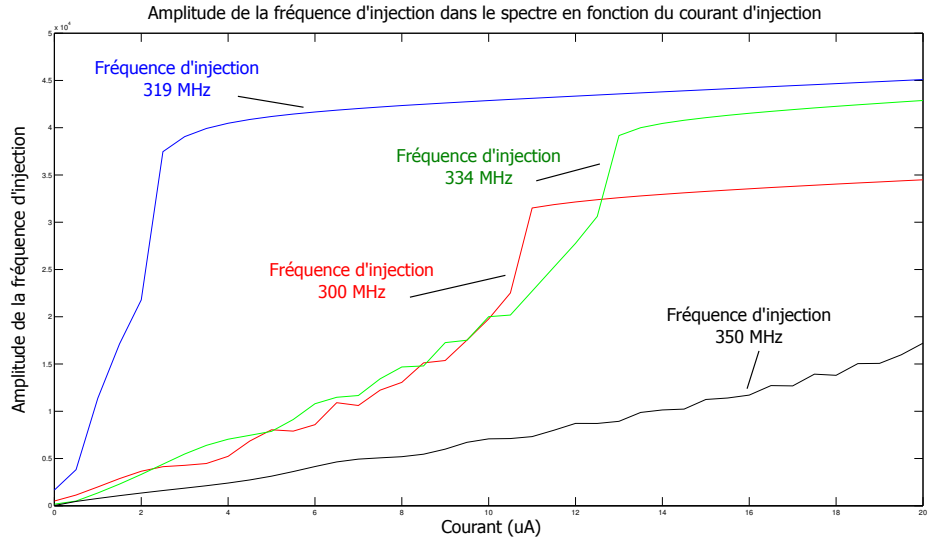

FIG. 4.16 – Amplitude de la fréquence d'injection dans le spectre fréquentiel de sa sortie en fonction du courant d'injection pour plusieurs fréquences d'injection.

est faiblement influencé par l'injection. On se retrouve donc dans un cas proche du cas obtenu pour le point C. On peut cependant remarquer une légère modification de la forme de la durée entre les deux fronts, la pente n'est plus complètement linéaire. Pour le point E, où l'oscillateur 2 est complètement verrouillé et l'oscillateur 1 est

fortement influencé (car la fréquence et le courant sélectionnés font que ce point se situe proche de la frontière de sa zone de verrouillage). On se retrouve donc dans un cas où, en moyenne, la fréquence de l'oscillateur 1 n'est plus sa fréquence nominale, mais n'est pas non plus la fréquence de verrouillage. On voit clairement que la durée n'évolue plus du tout linéairement. Si nous tracions l'histogramme de durée entre les fronts pour ce jeu de paramètres, nous verrions un pic apparaitre entre 2 ns et 2.5 ns. Finalement, pour le point F, pour lequel les deux oscillateurs sont verrouillés sur la même fréquence, la durée entre les deux fronts est constante. Les oscillateurs sont donc complètement dépendants l'un de l'autre.

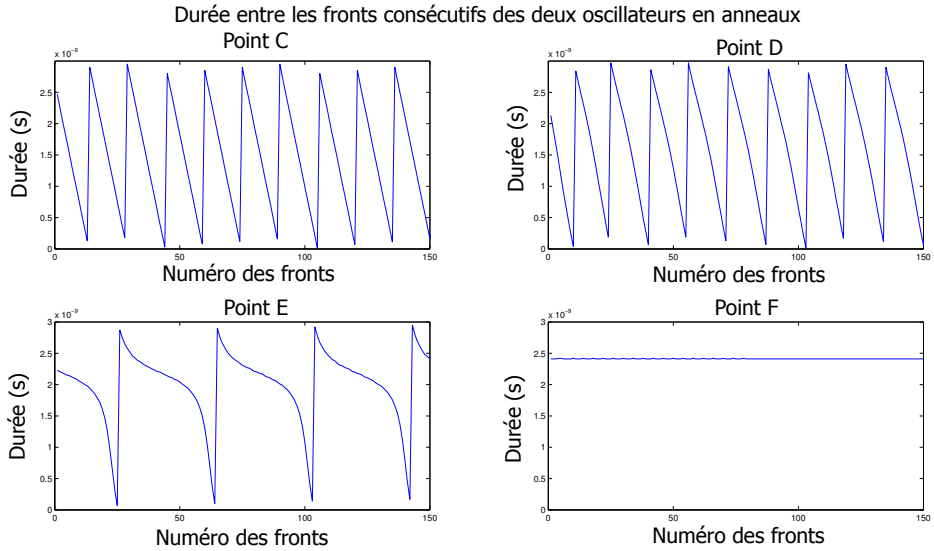

FIG. 4.17 – Durée entre les fronts consécutifs des deux oscillateurs pour plusieurs paramètres d'injection.

4.4.2.3 Verrouillage d'un oscillateur avec une harmonique du signal injecté

Nous avons précédemment étudié la zone de verrouillage d'un oscillateur autour de sa fréquence nominale (voir Figure 4.12). Une question demeure, jusqu'où s'arrête cette zone de verrouillage ? Est-il par exemple possible de verrouiller un oscillateur avec une fréquence d'injection proche d'une des harmoniques de la fréquence de l'oscillateur ? Nous avons étendu donc l'étude de la zone de verrouillage, pour le premier oscillateur (comme dans la Figure 4.12) à une plage de fréquence qui va de 250 MHz à 1 GHz. Pour rappel, cet oscillateur a une fréquence nominale de 316 MHz. Le résultat de cette étude étendue est présentée dans la Figure 4.18. Les simulations ont été réalisées en utilisant un pas de simulation de 50 ps (au lieu de 10 ps précédemment).

Premièrement, on retrouve notre forme en entonnoir centrée sur la fréquence nominale de l'oscillateur. La zone bleue correspond à la zone où l'oscillateur est ver-

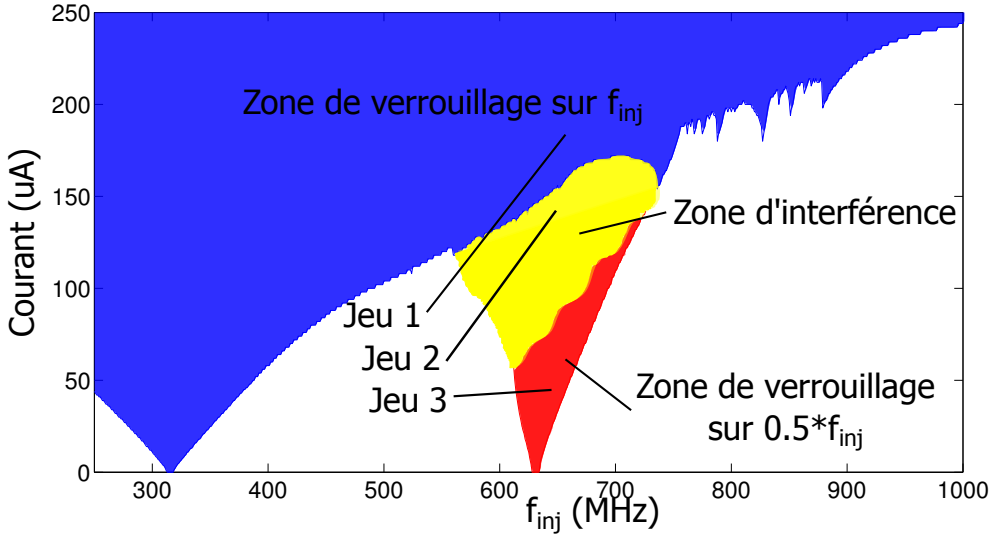

FIG. 4.18 – Zone de verrouillage pour le premier oscillateur pour une plage fréquentielle de 250 MHz à 1 GHz.

rouillé sur la fréquence d'injection. On observe que cette zone s'étend sur une large plage. Cependant, pour des fréquences d'injection très éloignées de la fréquence nominale de l'oscillateur, il sera nécessaire de fournir un très fort courant (qui peut être au delà de la limite supportable par les transistors sur un circuit réel). On remarque la présence de deux autres zones, dont la zone rouge, qui est centrée autour de la deuxième harmonique de la fréquence nominale de l'oscillateur (632 MHz). Dans cette zone l'oscillateur est verrouillé sur une fréquence égale à la moitié de la fréquence d'injection. Par exemple pour une fréquence d'injection de 650 MHz, en choisissant un courant de manière à être dans la zone rouge, la fréquence de l'oscillateur est verrouillée sur une fréquence de 325 MHz au lieu de 316 MHz. Ce phénomène est très intéressant pour attaquer une large gamme de circuits avec le même banc d'injection. Effectivement si le banc (principalement l'antenne et l'amplificateur de puissance) est dimensionné pour une fréquence bien plus grande que la fréquence nominale de l'oscillateur, il est possible à faible courant de verrouiller l'oscillateur à partir d'une harmonique de la fréquence nominale. Finalement, la dernière zone, située entre la zone rouge et la zone bleue, est en fait une zone de transition (ou encore d'interférence). En effet dans cette zone, le signal de sortie de l'oscillateur n'est pas composé d'une seule fréquence, mais correspond à l'addition de deux sinusoïdales de fréquences différentes.

Nous avons sélectionné trois jeux de paramètres pour illustrer le comportement de la sortie de l'oscillateur dans ces trois zones :

- Jeu 1 : f_{inj} = 640 MHz et I_{pert} = 180 μA (zone bleue).
- Jeu 2 : f_{inj} = 640 MHz et I_{pert} = 50 μA (zone rouge).
- Jeu 3 : f_{inj} = 640 MHz et I_{pert} = 145 μA (zone jaune).

Pour le premier jeu de paramètres, la sortie de l'oscillateur et le spectre fré-

quentiel de ce signal sont représentés dans la Figure 4.19. La sortie de l'oscillateur est une sinusoïde de fréquence 640 MHz (la fréquence d'injection). Sur le spectre aucune contribution à la fréquence nominale de l'oscillateur n'apparait. On a donc, avec l'application d'un courant de forte intensité réussi à doubler la fréquence de fonctionnement de l'oscillateur.

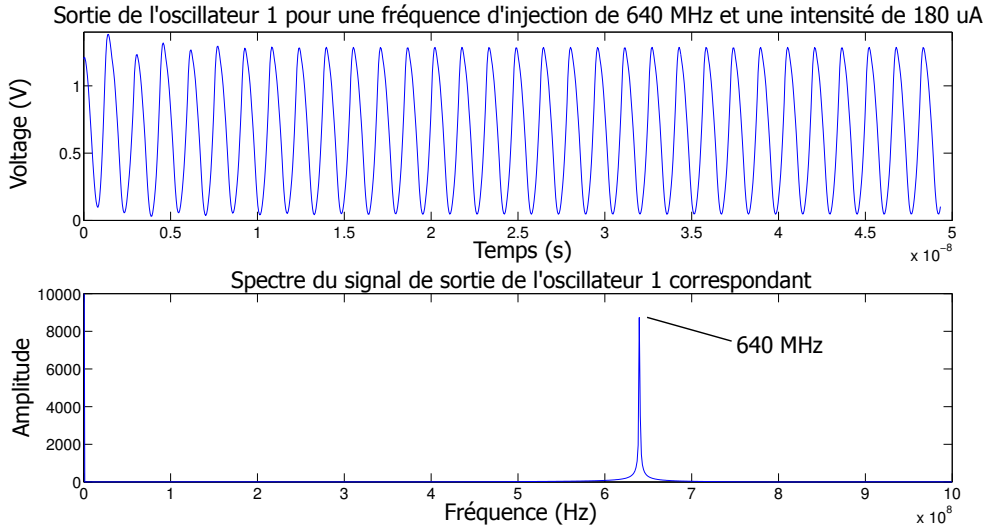

FIG. 4.19 – Signal de sortie, et son spectre fréquentiel, du premier oscillateur pour une fréquence d'injection de 640 MHz et une intensité de 180 μA (jeu 1).

Pour le deuxième jeu de paramètres (voir la Figure 4.20), on remarque au niveau du spectre fréquentiel de la sortie de l'oscillateur que la fréquence de l'oscillateur est effectivement bien égale à la valeur de la fréquence d'injection divisée par deux (320 MHz). On peut penser à juste titre que pour cette valeur de fréquence d'injection et cette intensité du courant, l'injection électromagnétique harmonique n'est pas assez forte pour que tous les fronts du signal perturbateur puissent impacter l'oscillateur. On se retrouve dans un cas de figure où seulement un front sur deux du signal perturbateur vient influencer l'oscillateur (c'est à dire, la fréquence du signal perturbateur est divisée par deux).

Enfin, la Figure 4.21 correspond à la sortie de l'oscillateur et son spectre fréquentiel pour le troisième jeu de paramètres. Le signal de sortie de l'oscillateur comporte deux sinusoïdes non synchrones. Le signal est donc déformé et en l'état est difficilement exploitable comme signal d'horloge. En regardant le spectre de plus près, on remarque la présence d'une contribution à la fréquence d'injection de 640 MHz, mais également d'une contribution à 335 MHz. Cette fréquence ne correspond à aucune fréquence mise en jeu précédemment.

Pour comprendre un peu plus pourquoi cette fréquence (nous l'appellerons fréquence d'interférence) est égale à 335 MHz, nous allons tracer l'évolution de la valeur de cette fréquence et l'évolution de l'amplitude de cette fréquence dans le spectre fréquentiel de la sortie de l'oscillateur, en fonction de la valeur du courant d'injection.

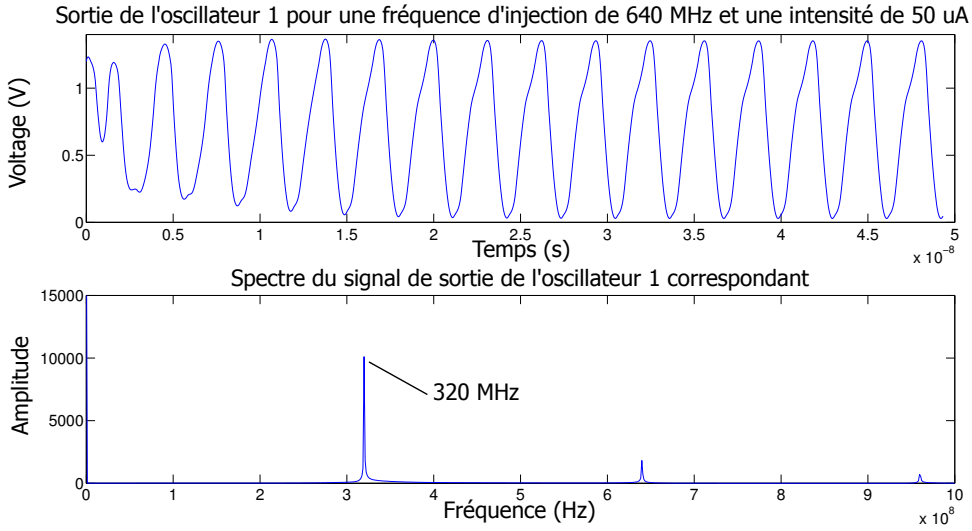

FIG. 4.20 – Signal de sortie, et son spectre fréquentiel, du premier oscillateur pour une fréquence d'injection de 640 MHz et une intensité de 50 μA (jeu 2).

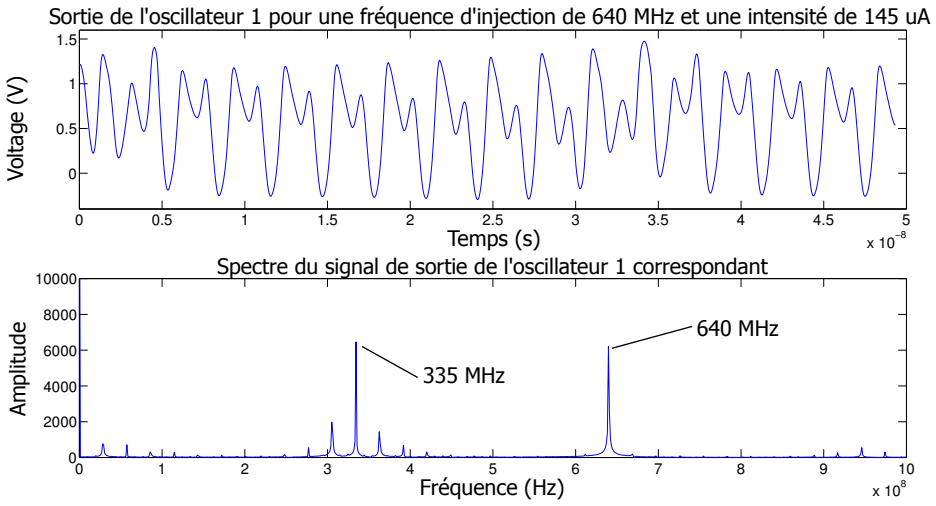

FIG. 4.21 – Signal de sortie, et son spectre fréquentiel, du premier oscillateur pour une fréquence d'injection de 640 MHz et une intensité de 145 μA.

Ces graphiques sont représentés dans la Figure 4.22. Les grandeurs en regard de la fréquence d'interférence sont représentées en bleu, alors que les grandeurs en regard de la fréquence d'injection sont représentées en rouge (pour le deuxième graphique, la fréquence d'injection n'est pas représentée car elle ne change pas en fonction du courant). Le phénomène est le suivant : progressivement quand l'intensité du courant augmente (à partir du moment où l'on est dans la zone d'interférence), la valeur de la fréquence d'interférence (on peut difficilement parler de fréquence d'interférence

avant d'avoir une puissance d'injection égale à 140 μA - zone rouge) augmente et son amplitude dans le spectre décroît. Au même moment, l'amplitude qui correspond à la fréquence d'injection augmente, il y a transfert de puissance entre ces deux fréquences. A partir de 155 μA, la valeur de la fréquence d'interférence se met subitement à décroître tandis que son amplitude tend vers 0. Pour un courant supérieur à 160 μA, la fréquence d'interférence n'existe presque plus car nous sommes rentrés dans la zone bleue.

En réalité, cet effet d'interférence existe à toutes les frontières entre la zone blanche (où le verrouillage n'est pas complet) et la zone bleue par exemple. En effet, ce phénomène de dépendance entre la fréquence de l'oscillateur et la fréquence d'injection n'est pas binaire, et passe par une phase où deux fréquences coexistent et créent un signal composite (quand les fréquences sont proches, ce phénomène est beaucoup moins visible).

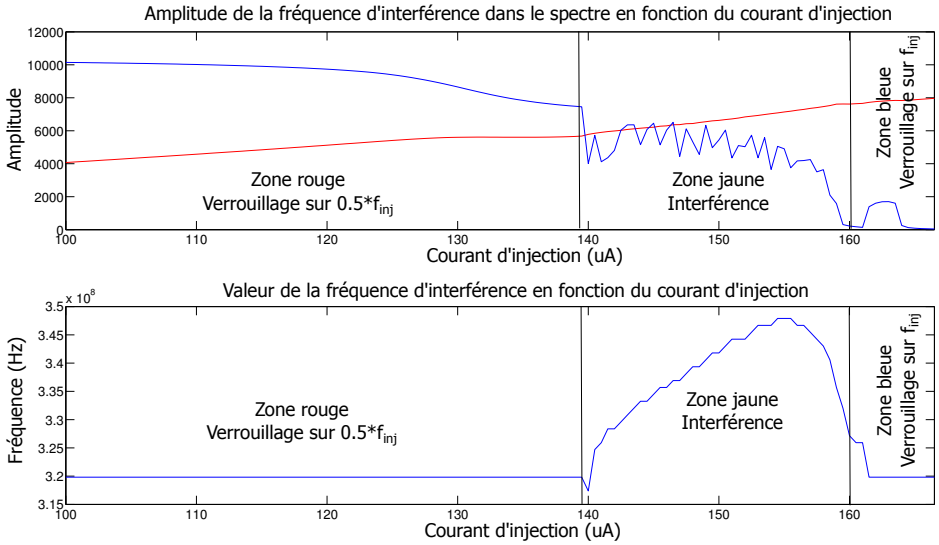

FIG. 4.22 – Evolution de la fréquence d'interférence

Au final, même s'il est possible de verrouiller l'oscillateur à partir des harmoniques de sa fréquence nominale, l'attaque sur le générateur d'aléa complet peut s'avérer plus délicate. Effectivement la zone de verrouillage commune à tous les oscillateurs ne sera effective qu'à partir d'un courant injecté de forte intensité. Par la suite, nous allons étudier l'effet du verrouillage sur la sortie binaire du générateur, pour des fréquences d'injection proches de la fréquence de fonctionnement des oscillateurs.

4.4.3 Effet du verrouillage des oscillateurs sur la sortie du générateur

Finalement, la dernière étape est consiste à étudier l'effet du verrouillage des oscillateurs sur la sortie du générateur de nombres aléatoires. Nous avons gardé les deux oscillateurs et nous avons rajouté la partie d'extraction d'entropie (bascules et porte Ou-exclusive). Le schéma du générateur utilisé est présenté dans la Figure 4.23. Les fréquences de fonctionnement des deux oscillateurs ont légèrement changé, du fait de l'ajout de l'extraction d'entropie (elles sont maintenant de 275 MHz et 293 MHz). Nous avons donc ajusté également la fréquence d'injection. Elle est pour cette expérience fixée à 285 MHz. Nous avons récupéré pour 3 intensités différentes (0 A, 5 μA et 15 μA), la sortie du générateur. Nous n'avons pas ajouté de bruit (donc les horloges n'avaient aucune incertitude temporelle) à cette simulation, seule la contribution pseudo-aléatoire du générateur est présente dans sa sortie. Nous rappelons que le flot aléatoire de ce générateur est composé à la fois d'une composante pseudo-aléatoire (due aux différences de fréquences entre les oscillateurs) et d'une composante aléatoire (due aux incertitudes temporelles des horloges produites par les oscillateurs).

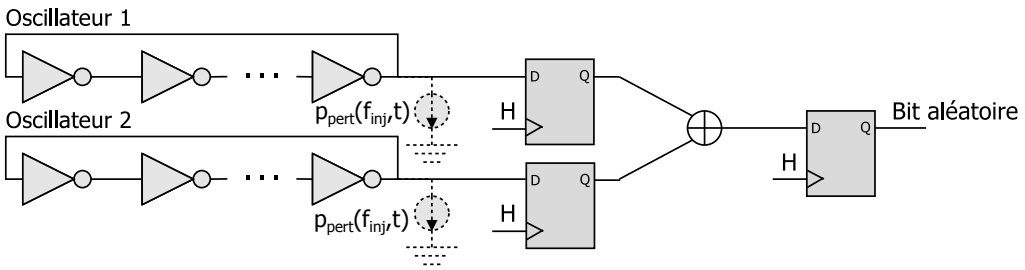

FIG. 4.23 – Circuit utilisé pour étudier l'effet du verrouillage des oscillateurs sur la sortie du générateur.

La Figure 4.24 montre les trois traces de sortie du générateur sous différentes conditions d'injection. L'horloge utilisée pendant la simulation est également présente dans la figure comme référence. On peut voir que la sortie du générateur, sous des conditions de fonctionnement normales (intensité nulle du courant d'injection), présente la composante pseudo-aléatoire due à la différence de fréquence entre les deux oscillateurs. En effet, on ne peut pas retrouver sur cette trace un motif qui se répète (certes, cette sortie est pseudo-aléatoire, il est donc possible de retrouver un motif, mais dans ce cas là, la durée de ce motif est importante par rapport à la période de l'horloge d'échantillonnage utilisée).

Lors d'une injection (que ce soit à 5 μA ou 15 μA), on voit clairement, dans la sortie du générateur, l'apparition d'un motif qui se reboucle en moins de 20 périodes d'horloge. La composante pseudo-aléatoire est effectivement complètement supprimée de la suite binaire produite par le générateur. En effet, la différence de fréquence entre les deux oscillateurs est maintenant nulle (comme on l'a vu précédemment, lors du verrouillage les deux oscillateurs fonctionnent à la fréquence d'injection). De

plus, si la différence de phase entre les deux oscillateurs, sous effet de l'injection, n'est pas proche de 0 ° (ce qui est plus que probable), l'horloge n'échantillonne jamais sur les incertitudes de deux oscillateurs en même temps. Si deux oscillateurs sont verrouillés sur la même fréquence, cela revient à n'avoir qu'un seul oscillateur.

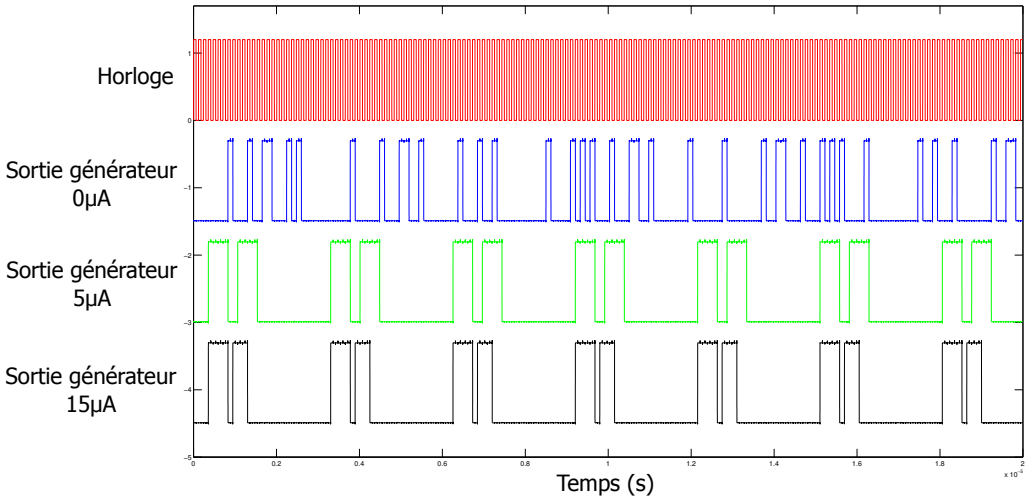

FIG. 4.24 – Résultats de simulation pour différents paramètres d'injection. De haut en bas : Horloge, sortie pour f_{inj} = 285 MHz et I_{pert}= 0 μA, sortie pour f_{inj} = 285 MHz et I_{pert}= 5 μA et sortie pour f_{inj} = 285 MHz et I_{pert}= 15 μA.

Au final, le verrouillage des oscillateurs pour ce type de générateur de nombres aléatoires est équivalent à supprimer un oscillateur pour chaque paire d'oscillateurs verrouillée. Si par exemple, 25 oscillateurs constituent le générateur et que sur ces 25 oscillateurs, 10 sont verrouillés sur une fréquence, le générateur, d'un point de vue de l'entropie de la suite binaire générée, sera équivalent à un générateur composé de 16 oscillateurs.

Dans la suite, nous étudierons l'effet de l'injection électromagnétique harmonique sur le reste des éléments qui composent le générateur de nombres aléatoires.

4.5 Un modèle électrique et mathématique de l'effet de l'attaque sur l'extracteur d'entropie

Nous avons montré que l'injection harmonique électromagnétique a des effets sur la dépendance des oscillateurs en anneau. Cependant, les oscillateurs ne sont pas les seuls composants qui constituent le générateur. On retrouve également un arbre de portes OU-exclusif, et des bascules D utilisées pour réaliser l'opération d'extraction d'entropie. Nous allons montrer dans la suite que l'injection harmonique a également un effet sur l'extraction d'entropie. Nous allons aussi fournir un modèle électrique et mathématique de cet effet qui permet d'évaluer, en fonction des paramètres d'in-

jection, si l'attaque a une chance de perturber l'extraction d'entropie.

4.5.1 Étude du comportement de l'extraction d'entropie sous injection électromagnétique

Pour pouvoir facilement étudier le comportement de l'extraction d'entropie, nous avons utilisé une version simplifiée du générateur. Comme il est possible de le voir sur la Figure 4.25, cette version est seulement composée de deux oscillateurs en anneau suivis de deux bascules D (FF1 et FF2 dans Figure 4.25), d'une porte OU exclusif et enfin d'une dernière bascule D (FF3) qui échantillonne le bit aléatoire. La fréquence d'échantillonnage et le nombre de portes inverseuses qui composent les oscillateurs restent inchangés par rapport aux premières expérimentations (voir le détail de Cible#2). Cette réduction du nombre d'éléments qui composent le générateur a été effectuée dans le but de pouvoir mesurer avec un oscilloscope les différents signaux intermédiaires de production du bit aléatoire. Ce sont les signaux S_{FF1}, S_{FF2}, S_{XOR} et S_{FF3} de la Figure 4.25.

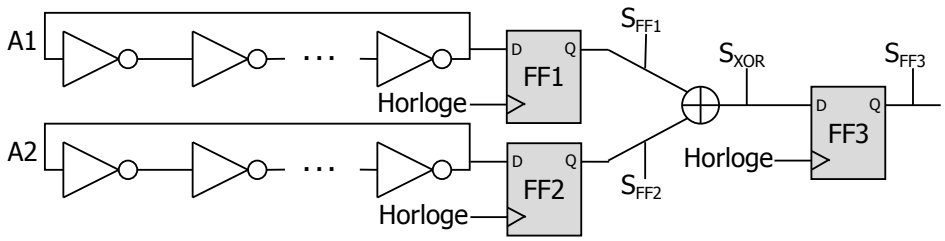

FIG. 4.25 – Schéma de principe du circuit utilisé pour étudier l'effet de l'injection électromagnétique sur l'extraction d'entropie.

4.5.1.1 Effet sur les bascules FF1 et FF2

Malheureusement, il n'est pas possible de s'assurer du bon fonctionnement, sous l'effet de l'injection électromagnétique, des deux premières bascules (FF1 et FF2). Les signaux à l'entrée de ces bascules proviennent d'oscillateurs en anneau (ces signaux ont des fréquences proches de 320 MHz). Il sera donc difficile de déterminer, avec une mesure externe, si ces bascules échantillonnent correctement. Effectivement les signaux produits par les oscillateurs sont asynchrones par rapport à l'horloge utilisée pour échantillonner (de plus la mesure externe ajoute une incertitude temporelle qui ne permet pas de déterminer facilement le moment où l'échantillon est collecté). Par la suite nous montrerons tout de même que ces bascules ont un comportement anormal durant l'injection.

4.5.1.2 Effet sur la porte OU exclusif

Pour vérifier le bon fonctionnement de la porte OU exclusif, nous avons observé à l'aide d'un oscilloscope les signaux en entrée de la porte (S_{FF1} et S_{FF2}) et le signal de

sortie de cette porte (S_{XOR}). La Figure 4.26 est une reconstruction de l'acquisition faite à l'aide d'un oscilloscope (pour faciliter la lecture des chronogrammes) des signaux S_{XOR}, S_{FF1} et S_{FF2}, sous effet de la perturbation électromagnétique.

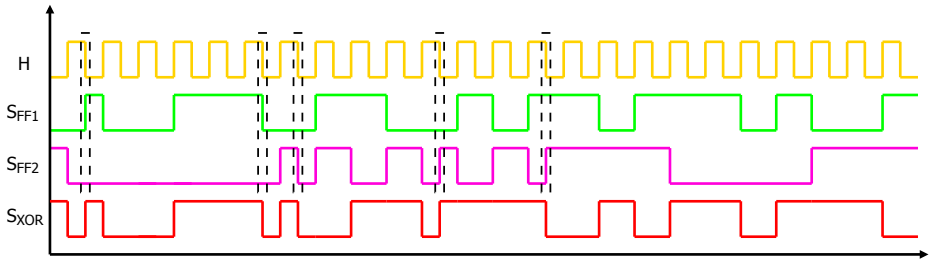

FIG. 4.26 – Observation des signaux S_{FF1}, S_{FF2}, S_{XOR} et H pour étudier l'effet de la perturbation électromagnétique sur la porte OU exclusif.

En ce qui concerne la porte OU exclusif, on peut voir sur la Figure 4.26, grâce aux signaux S_{FF1}, S_{FF2} et S_{XOR}, que la perturbation électromagnétique n'a aucun effet sur le résultat en sortie la porte.

Comme dit précédemment, on ne peut pas étudier précisément l'effet de la perturbation sur les bascules FF1 et FF2. Cependant, la Figure 4.26 représente également le signal qui correspond à l'horloge (H) utilisée pour l'échantillonnage des oscillateurs en anneau (et donc comme horloge de référence des bascules FF1 et FF2). On voit, en regardant soit S_{FF1} ou S_{FF2} que ces deux signaux sont modifiés sur des fronts descendants de l'horloge. On peut conclure que, sous l'effet de l'injection électromagnétique, les bascules D échantillonnent des valeurs sur des fronts descendants de l'horloge (ces bascules sont réglées pour fonctionner uniquement sur le front montant de l'horloge). Cet effet indésirable est mis en avant sur la Figure 4.26 par les rectangles en lignes discontinues.

4.5.1.3 Effet sur la bascule FF3

La Figure 4.27 représente les signaux S_{XOR} et S_{FF3} sous l'effet de la perturbation électromagnétique. Le signal $S_{FF3normal}$ quant à lui, est une reconstruction de ce que devrait être la sortie de la bascule, sous des conditions normales de fonctionnement, et en accord avec l'entrée S_{XOR}. Sur la Figure 4.27, il est facile de voir la différence entre le vrai signal de sortie (S_{FF3}) sous perturbation, et le signal ($S_{FF3normal}$). L'injection harmonique électromagnétique a donc un effet sur le comportement de la bascule FF3. Ici, on remarque encore des échantillonnages de la part de la bascule sur des fronts descendants de l'horloge (voir les rectangles en ligne discontinue sur la Figure 4.27). Cependant, tous les fronts descendants n'entraînent pas un échantillonnage (fronts marqués d'une flèche dans la Figure 4.27). A noter qu'il reste des fronts descendants soit non entourés d'un rectangle en ligne discontinue, soit non marqués d'une flèche, qui correspondent à des fronts où la valeur précédemment sauvegardée par la bascule est la même que celle qui aurait dû être échantillonnée. On ne peut donc pas savoir si la bascule a été réactive sur

ces fronts. Nous pensons que l'échantillonnage sur quelques fronts descendants de l'horloge est due à la superposition d'un signal sinusoïdal (de même fréquence bien évidemment que le signal utilisé pour alimenter la sonde d'injection) avec le signal d'horloge, qui peut entrainer la création de faux fronts montants en parasitant les fronts descendants de l'horloge.

Un dernier effet présent dans la Figure 4.27 est visible dans le rectangle en ligne pleine. Cet effet correspond à une valeur échantillonnée par la bascule, sur un front montant, qui se retrouve être fausse.

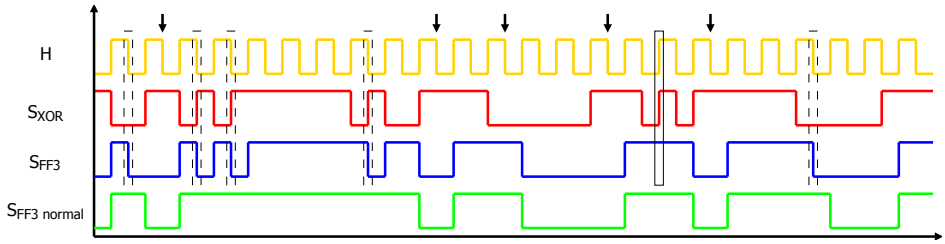

FIG. 4.27 – Observation des signaux H, S_{XOR} et S_{FF3} pour vérifier le comportement de la bascule FF3 sous l'effet de la perturbation électromagnétique. Le signal $S_{FF3normal}$ est une reconstruction du signal que l'on devrait obtenir en sortie de la bascule FF3 sans perturbation électromagnétique.

Pour résumer l'effet de la perturbation électromagnétique sur le comportement des bascules D :

- Les bascules ont tendance à échantillonner sur certains fronts descendants du signal d'horloge.
- Quelques valeurs échantillonnées sur le front montant de l'horloge ne sont pas correctes. Plusieurs raisons peuvent expliquer ce comportement :
  - la bascule n'a pas prélevé d'échantillon sur ce front montant,
  - la valeur échantillonnée a été corrompue,
  - l'instant d'échantillonnage est décalé (par exemple, à cause d'un ajout d'une incertitude temporelle sur l'horloge).

A noter que le deuxième effet se produit beaucoup moins souvent que le premier effet.

4.5.1.4 Effet sur l'extraction d'entropie

Nous avons donc mis en lumière par, une étude expérimentale, les effets de l'injection électromagnétique harmonique sur les bascules du générateur. Dans la suite de cette partie, nous allons développer un modèle afin de valider, par simulation, les résultats expérimentaux.

4.5.2 Modélisation électrique

Pour vérifier si notre hypothèse, à propos des échantillonnages des bascules D sur front descendant, est correcte, nous avons réalisé un modèle électrique de l'injection

électromagnétique harmonique. Ce modèle nous permet d'effectuer des simulations électriques avec le logiciel Cadence (et donc le simulateur électrique Spectre).

4.5.2.1 Les modèles

Deux modèles ont été créés et étudiés. Le premier, présenté à la Figure 4.28, modélise l'injection harmonique électromagnétique comme un générateur de signal sinusoïdal connecté au réseau d'horloge. Le deuxième quant à lui, présenté à la Figure 4.29, modélise l'injection harmonique électromagnétique comme deux générateurs de signaux sinusoïdaux connectés aux deux lignes d'alimentation (un entre le potentiel positif de l'alimentation (Vdd) et le potentiel positif de la bascule, et l'autre sur le potentiel négatif de l'alimentation (masse) et le potentiel négatif de la bascule).

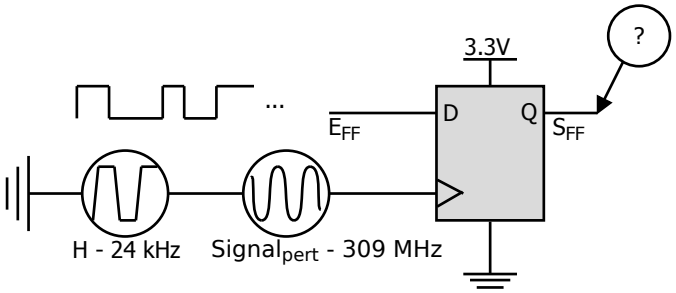

FIG. 4.28 – Premier modèle de l'effet de l'injection électromagnétique harmonique sur les bascules D - superposition d'un générateur de signal sinusoïdal sur l'arbre d'horloge.

4.5.2.2 Simulation électrique

Pour les deux modèles, nous avons utilisé comme signal d'entrée de la bascule D, le même signal que le signal d'entrée (S_{XOR}) présenté à la Figure 4.27.

Les paramètres de simulation utilisés, pour les deux modèles, sont les suivants :
- Tension d'alimentation : 3.3 V,
- Amplitude du signal sinusoïdal : 500 mV,
- Fréquence du signal sinusoïdal : 310 MHz,
- Durée des fronts montants et descendants de l'horloge : 20 ns (horloge externe dont les performances ne sont pas améliorées par une PLL interne).

Les résultats de simulation (Figure 4.30 pour le premier modèle et Figure 4.31 pour le second modèle) montrent que les deux modèles, pour des paramètres de simulation identique (c'est à dire pour la même attaque électromagnétique), nous permettent d'obtenir des sorties de bascule identiques. Cependant, sur la Figure 4.30 et la Figure 4.31, à contrario de ce que l'on a réellement sur la Figure 4.27, la bascule échantillonne sur chaque front descendant de l'horloge. Ceci est dû aux paramètres de simulation relativement arrangeants du point de vue du succès de l'attaque (nous

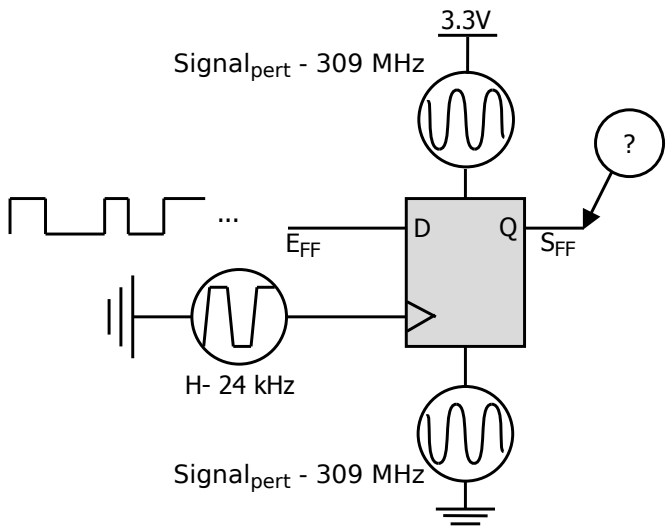

FIG. 4.29 – Second modèle de l'effet de l'injection électromagnétique harmonique sur les bascules D - superposition de générateurs de signaux sinusoïdaux sur les deux rails d'alimentation.

montrerons plus tard que si nous réduisons l'amplitude ou la fréquence du signal sinusoïdal, il est possible de retrouver un comportement similaire à ce que nous avons sur la Figure 4.27). Un autre point important, la Figure 4.27 correspond à une acquisition sur du matériel réel, il est possible et même certain que la puissance transmise par l'amplificateur RF à la sonde émettrice pendant l'attaque ne reste pas constante au cours du temps (l'amplitude du signal sinusoïdal est donc une variable dépendant du temps).

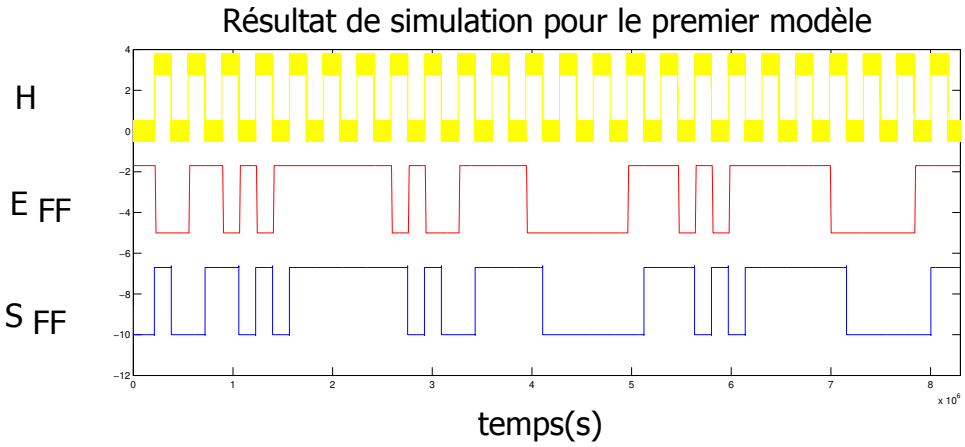

FIG. 4.30 – Résultat de simulation pour le premier modèle.

D'après les résultats de simulation, les deux modèles électriques peuvent être utilisés pour décrire les effets de l'injection électromagnétique harmonique sur l'extracteur d'entropie du générateur d'aléa. Nous allons voir dans la suite que chaque

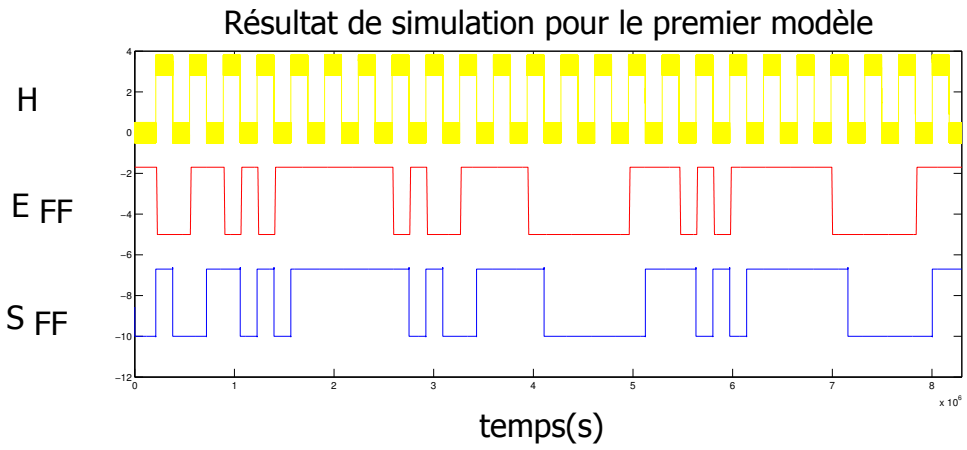

FIG. 4.31 – Résultat de simulation pour le second modèle.

modèle correspond à une attaque bien précise.

4.5.2.3 Choix du modèle électrique

Chaque sonde, ou antenne dans notre cas, utilisée pour transmettre ou recevoir une onde électromagnétique, est plus ou moins sensible à un type de champ, que ce soit magnétique ou électrique. Cette sensibilité dépend principalement du type d'antenne utilisée (forme, composition, etc...). Cependant certaines antennes avec des topologies complexes, vont pouvoir être sensibles aux deux champs. Pour rester dans des cas simples, ce sont ceux que nous avons étudiés au cours de cette thèse, nous n'aborderons pas l'utilisation de ce type de sondes. Deux exemples d'antennes facilement réalisables sont la bobine (ou boucle) et la pointe. Les bobines (ou boucles) vont pouvoir émettre ou capter un champ magnétique alors que les pointes ont tendance à émettre ou capter un champ électrique.

Pendant une attaque active, comme c'est le cas de l'attaque présentée dans ce chapitre, la sonde joue le rôle d'antenne émettrice et le circuit intégré, le rôle d'antenne réceptrice. Le succès de l'attaque est lié à la puissance transmise au circuit qui dépend du couplage entre les deux antennes.

Un FPGA moderne, de technologie SRAM ou Flash (tel que ceux utilisés lors de nos expérimentations), est constitué de plusieurs réseaux d'interconnexions complexes dont notamment (voir la Figure 4.32) :

- Un réseau d'alimentation composé de nombreuses boucles (qui peut être vu comme une grille en général).
- Un arbre d'horloge qui est principalement composé de longues lignes qui va de part et d'autre du circuit (de manière à fournir à chaque point du circuit une horloge avec le même décalage temporel).

En accord avec ce qui est dit en Annexe A, le réseau d'alimentation (qui est principalement formé de boucles) est donc très réceptif aux champs magnétiques, alors que l'arbre d'horloge (qui est principalement constitué de longues lignes) sera

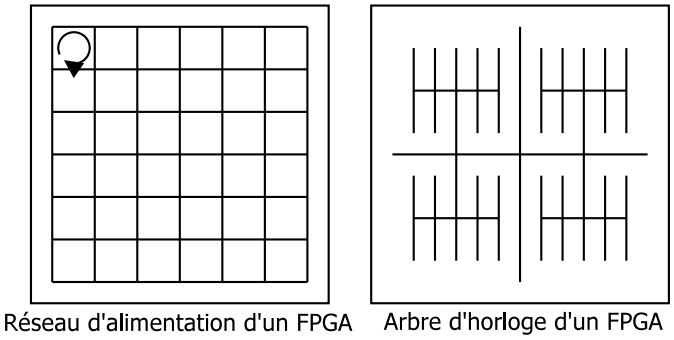

FIG. 4.32 – Topologie classique du réseau d'alimentation et de l'arbre d'horloge d'un FPGA

lui réceptif aux champs électriques. En conséquence, le premier modèle (Figure 4.28) sera donc plutôt adapté pour décrire une attaque qui utilise une sonde qui émet principalement un champ électrique, alors que le second modèle (Figure 4.29) sera plutôt propice à la description des attaques utilisant des sondes qui émettent un champ magnétique.

Dans ce chapitre, nous avons décrit une attaque, sur un générateur de nombres aléatoires, qui utilise une sonde électrique (voir la Figure 2.15), nous allons donc nous concentrer sur l'étude du modèle mathématique lié au premier modèle électrique proposé qui modélise la perturbation sur l'arbre d'horloge du circuit (voir Figure 4.28). Ce modèle mathématique, qui sera présenté dans la suite, donne, en fonction des paramètres du signal sinusoïdal perturbateur (amplitude et fréquence) les chances de réussite de l'attaque. La différence entre le premier et le second modèle est relativement faible, le modèle mathématique lié au second modèle électrique (Figure 4.29), devrait être relativement proche du modèle que nous allons proposer. En effet, le principe est le même, au lieu d'être appliquée sur les fronts de l'horloge, la perturbation est appliquée sur le seuil de basculement de la bascule.

4.5.3 Modèle mathématique

4.5.3.1 Étude des faux fronts montants

La Figure 4.33 décrit trois fronts descendants du signal d'horloge (en bleu) avec pour chacun une superposition d'un signal sinusoïdal perturbateur qui a des paramètres différents (fréquence et amplitude). Sur la gauche de la Figure 4.33, on peut voir que la perturbation sinusoïdale, de faible amplitude, ne crée pas de faux fronts montants. En effet, la pente du front descendant de l'horloge est plus importante que la pente positive du signal sinusoïdal. La pente de l'horloge perturbée (horloge plus signal sinusoïdal, en rouge sur la Figure 4.33) reste négative quel que soit le temps. Pour le deuxième jeu de paramètres (partie centrale de la Figure 4.33), nous avons sélectionné la même fréquence que précédemment, mais nous avons augmenté l'amplitude. On remarque la création de faux fronts montants, mais malheureuse-

ment, d'un point de vue de l'attaque, l'horloge perturbée ne croise pas le seuil de la bascule avec une pente positive, et donc n'entraine pas l'échantillonnage. Bien évidemment, il est possible, par modification de la phase de la perturbation sinusoïdale de positionner un faux front montant de manière à avoir un échantillonnage sur ce front descendant de l'horloge. Cependant, il n'y a aucune certitude que le même effet se reproduira sur le prochain front descendant de l'horloge. Enfin, pour le dernier jeu de paramètres (droite de la Figure 4.33), nous avons augmenté la fréquence du signal sinusoïdal tout en gardant la même amplitude que précédemment. On voit que dans ce cas là, un faux front montant est créé (et sera créé sur les prochains fronts descendants de l'horloge) quelle que soit la phase du signal sinusoïdal. C'est dans ce dernier cas de figure où nous nous trouvions lors de nos simulations (création d'un faux front montant à chaque front descendant de l'horloge), alors que lors des expérimentations présentées dans Figure 4.27, nous nous situions plutôt dans un cas proche de celui du deuxième jeu de paramètres.

En général, plus grande est la valeur de l'amplitude et plus grande est la fréquence de la perturbation sinusoïdale, plus grandes sont les chances d'obtenir au moins un faux front montant lors des fronts descendants de l'horloge.

Dans la suite nous allons proposer des expressions mathématiques qui permettront de déterminer en fonction des paramètres de l'horloge et des paramètres relatifs à l'injection, si l'attaque sur l'extracteur d'entropie est réalisable.

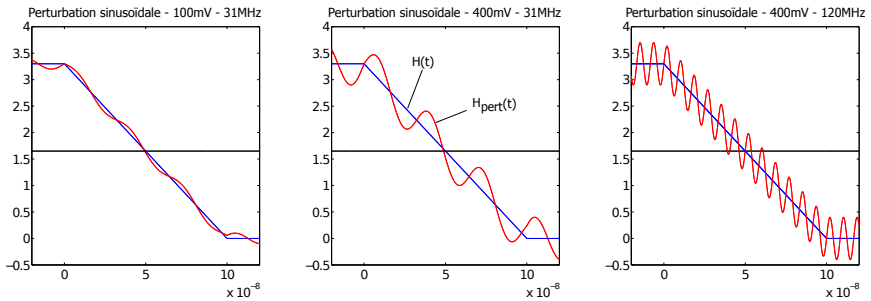

FIG. 4.33 – Front descendant du signal d'horloge pour différents réglages de la perturbation sinusoïdale.

4.5.3.2 Construction du modèle

Pour simplifier les calculs, nous considérerons dans la suite que le seuil des bascules D est une tension qui correspond à la moitié de la valeur de la tension d'alimentation du circuit (Vdd).

Les variables suivantes seront utilisées dans la suite des calculs :

- $f_{inj} = f_{pert} = \frac{1}{T_{pert}}$ est la fréquence du signal sinusoïdal perturbateur,
- V_{inj} est l'amplitude du signal sinusoïdal perturbateur avant d'entrer dans le canal électromagnétique. Cette amplitude est directement dépendante du gain de l'amplificateur RF,

- V_{pert} est l'amplitude du signal sinusoïdal perturbateur après être passé par le canal électromagnétique. Cette amplitude est directement dépendante du canal électromagnétique et de V_{inj},
- T est la période de l'horloge utilisée comme signal d'échantillonnage des bascules D,
- T_R and T_F sont respectivement les durées du front montant et du front descendant de ce signal d'horloge,
- (X, Y, Z) est la position de la sonde au dessus du circuit,
- t est le temps,
- $C_{sonde,circuit}$ représente l'efficacité du couplage entre la sonde et le circuit. Une valeur égale à 1 correspond à une transmission complète de toute la puissance, et une valeur égale à 0 correspond à une non transmission de puissance.

La représentation mathématique du signal d'horloge ($H(t)$) est donnée par l'Equation 4.5, et celle de la perturbation sinusoïdale ($S_{inj}(t)$) par l'Equation 4.6.

$$H(t) = \begin{cases} 0 & \text{pour } 0 + kT \leq t \leq \frac{T}{2} - T_R + kT \\ \frac{Vdd}{T_R}(t - (\frac{T}{2} - T_R)) & \text{pour } \frac{T}{2} - T_R + kT \leq t \leq \frac{T}{2} + kT \\ Vdd & \text{pour } \frac{T}{2} + kT \leq t \leq T - T_F + kT \\ -\frac{Vdd}{T_F}(t - T) & \text{pour } T - T_F + kT \leq t \leq T + kT \end{cases} \tag{4.5}$$

où k est le numéro de la période.

$$S_{inj}(f_{inj}, t) = V_{inj}(f_{inj}, t) sin(2\pi f_{inj} t + \phi_{inj}(f_{inj}, t) \tag{4.6}$$

La Figure 4.34 représente le processus relatif à l'attaque électromagnétique harmonique. Premièrement, le signal S_{inj} (qui provient de l'amplificateur RF) entre dans le canal électromagnétique et produit le signal S_{pert}. Ce signal est en fait le même signal sinusoïdal, mais avec une amplitude plus faible du fait de son passage par le canal électromagnétique. Le canal électromagnétique tend à réduire l'amplitude du signal perturbateur car le couplage entre la sonde et le circuit n'est et ne sera jamais maximal (si on veut obtenir un rendement de 1, il faudrait que la sonde soit en contact avec une piste du circuit - en d'autres termes, ce ne serait plus une attaque électromagnétique). Il est possible de modéliser l'influence de ce canal électromagnétique sur les amplitudes des signaux perturbateurs en utilisant une fonction de transfert. Nous appellerons cette fonction de transfert G, mais nous ne donnerons pas de formule pour cette fonction (le but du travail proposé ici n'est pas de travailler sur l'interaction entre la sonde et le circuit). Cette fonction dépend de plusieurs paramètres, comme la topologie de l'antenne émettrice (forme,

taille, type, ...), le couplage entre l'antenne et le circuit, la position de l'antenne sur le circuit, etc. Nous supposerons que cette fonction de transfert est linéaire. La formule qui lie l'amplitude V_{inj} du signal perturbateur avant passage dans le canal électromagnétique et l'amplitude V_{pert} du signal perturbateur après passage dans le canal électromagnétique est présentée dans l'Equation 4.7.

Dans le but de simplifier le modèle mathématique, nous allons considérer que lors d'une attaque, la position de la sonde reste constante, la puissance transmise par l'amplificateur RF à la sonde est constante au cours du temps, et enfin le couplage entre la sonde et le circuit ne change pas. La fréquence du signal sinusoïdal perturbateur est aussi un paramètre fixe lors d'une attaque, ce qui rend ainsi la valeur de V_{pert} constante également. Nous considérerons enfin que la phase du signal sinusoïdal est nulle. L'expression finale du signal de perturbation (S_{pert}) est donnée par l'Equation 4.8.

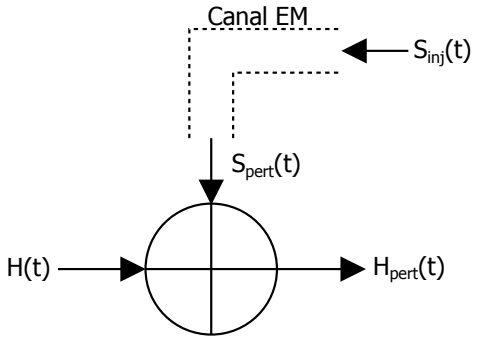

FIG. 4.34 – Représentation du canal électromagnétique et du processus relatif à l'attaque.

$$V_{pert}(f_{pert}, t, (X, Y, Z), C_{sonde,circuit}) = V_{inj}(f_{inj}, t)G((X, Y, Z), C_{sonde,circuit}) \quad (4.7)$$

$$S_{pert}(t) = V_{pert} sin(2\pi f_{pert} t) \quad (4.8)$$

Nous souhaitons trouver les paramètres d'injection qui vont nous assurer la création d'un faux front montant sur le front descendant du signal d'horloge. Nous allons donc nous concentrer sur l'étude du front descendant du signal d'horloge.

D'après la Figure 4.34, l'horloge perturbée (H_{pert}) est définie comme l'addition du signal d'horloge sans perturbation (voir l'Equation 4.5) et du signal sinusoïdal (voir l'Equation 4.8). L'expression mathématique correspond à H_{pert} peut être trouvée dans l'Equation 4.9.

$$H_{pert}(t) = \frac{Vdd}{T_F}(T - t) + V_{pert} sin(2\pi f_{pert} t) \quad (4.9)$$

Pour obtenir un faux front montant sur H_{pert}, nous devons trouver une valeur de t qui respecte le jeu de conditions présenté dans l'Equation 4.10 et l'Equation 4.11.

$$H_{pert}(t) = V_{seuil} \tag{4.10}$$

$$\frac{dH_{pert}(t)}{dt} = cos(2\pi f_{pert}t) - \frac{Vdd}{2\pi f_{pert}V_{pert}T_F} \quad \geq \quad 0 \tag{4.11}$$

En accord avec ce que nous avons pu présenter avant à l'aide de la Figure 4.33, nous pouvons dénombrer trois cas différents :

- Premier cas : la pente de l'horloge perturbée (H_{pert}) n'est jamais positive pendant son front descendant - l'Equation 4.11 n'est pas respectée (correspond à la partie gauche sur la Figure 4.33).
- Deuxième cas : la pente de l'horloge perturbée est positive pendant son front descendant, mais il n'est pas possible de garantir qu'il existe une valeur de t qui respecte l'Equation 4.10 (partie centrale de la Figure 4.33).
- Troisième cas : il est certain de pouvoir trouver une valeur de t qui respecte à la fois l'Equation 4.10 et l'Equation 4.11 (partie droite de Figure 4.33).

Pour respecter l'Equation 4.11, il est nécessaire de respecter l'Equation 4.12. Dans cette équation, la valeur maximale du cosinus est un. Il est alors possible de simplifier cette expression (voir l'Equation 4.13).

$$cos(2\pi f_{pert}t) \geq \frac{Vdd}{2\pi f_{pert}V_{pert}T_F} \tag{4.12}$$

$$f_{pert}V_{pert} \geq \frac{Vdd}{2\pi T_F} \tag{4.13}$$

Si l'Equation 4.13 n'est pas respectée, on peut d'ores et déjà dire que l'attaque échouera. Si elle est respectée, l'attaque peut éventuellement réussir, mais rien n'est encore garanti ; on peut être à la fois dans la deuxième ou le troisième cas.

Pour garantir le succès complet de l'attaque, il est nécessaire de respecter également l'Equation 4.10. Il faut donc trouver au moins une valeur de t pour laquelle la dérivée sera nulle. Cette condition est exprimée par l'Equation 4.14 et la solution de cette équation est présentée dans l'Equation 4.15 (avec $k \in \mathbb{Z}$).

$$cos(2\pi f_{pert}t) \quad = \quad \frac{Vdd}{2\pi f_{pert}V_{pert}T_F} \tag{4.14}$$

$$\begin{aligned} T_0 \quad &= \quad -\frac{1}{2\pi f_{pert}}Arccos(\frac{Vdd}{2\pi f_{pert}V_{pert}T_F}) + kT_{pert} \\ T_1 \quad &= -T_0 = \quad \frac{1}{2\pi f_{pert}}Arccos(\frac{Vdd}{2\pi f_{pert}V_{pert}T_F}) + kT_{pert} \end{aligned} \tag{4.15}$$

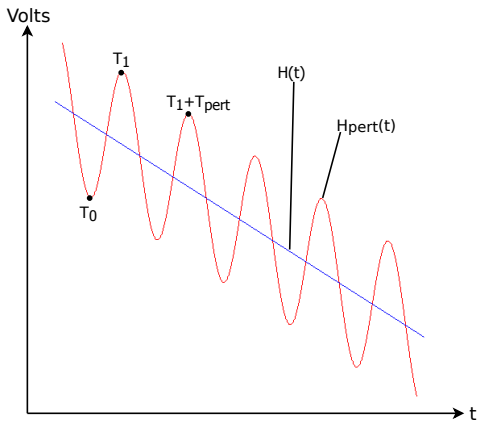

FIG. 4.35 – Zoom sur un front descendant de l'horloge perturbée (H_{pert}) dans le but d'expliquer le choix pour la construction des inégalitées.

$$H_{pert}(T_1 + T_{pert}) \geq H_{pert}(T_0) \tag{4.16}$$

Pour k=0 :

$$\begin{aligned}
& H_{pert}(T_1 + T_{pert}) && \geq && H_{pert}(T_0) = H_{pert}(-T_1) \\
& \tfrac{Vdd}{T_F}(T - (T_1 + T_{pert})) && \geq && \tfrac{Vdd}{T_F}(T + T_1) \\
& +V_{pert} sin(2\pi f_{pert}(T_1 + T_{pert})) && && +V_{pert} sin(-2\pi f_{pert} T_1) \\
& \tfrac{Vdd}{T_F}(-(2T_1 + T_{pert})) + 2V_{pert} sin(2\pi f_{pert} T_1) && \geq && 0 \\
& -\tfrac{Vdd}{T_F}(\tfrac{1}{\pi f_{pert}} Arccos(\tfrac{Vdd}{2\pi f_{pert} V_{pert} T_F}) + T_{pert}) && && \\
& +2V_{pert} sin(Arccos(\tfrac{Vdd}{2\pi f_{pert} V_{pert} T_F})) && \geq && 0 \\
& -\tfrac{Vdd}{2\pi V_{pert} f_{pert} T_F}(Arccos(\tfrac{Vdd}{2\pi f_{pert} V_{pert} T_F}) + \pi) && && \\
& +sin(Arccos(\tfrac{Vdd}{2\pi f_{pert} V_{pert} T_F})) && \geq && 0 \\
& f(\tfrac{Vdd}{2\pi f_{pert} V_{pert} T_F}) && \geq && 0
\end{aligned} \tag{4.17}$$

En regardant la Figure 4.35, pour s'assurer d'être dans le troisième cas (donc que l'attaque réussisse), nous devons vérifier que l'Equation 4.16 est respectée.

Le détail du calcul qui permet d'obtenir la solution de l'Equation 4.16 est présenté dans l'Equation 4.17. La forme finale de l'Equation 4.17 n'est pas calculable algébriquement. Nous allons donc faire appel à une fonction $f(x) = -x(Arccos(x)+$

$\pi) + sin(Arccos(x))$ avec $x = \frac{Vdd}{2\pi f_{pert} V_{pert} T_F}$. Cette fonction f représente la partie de gauche de la forme finale de l'Equation 4.17. La Figure 4.36 est le graphique de la fonction $f(x)$ pour x allant de -1 à 1. On peut voir que cette fonction est exclusivement décroissante et qu'elle admet une racine x_0 qui peut être évaluée numériquement. On a dans notre cas, avec les mêmes paramètres d'attaque que ceux présentés dans les simulations précédemment (voir Figure 4.30 ou Figure 4.31), $x_0 \approx 0.217$. Pour les valeurs de $x \leq x_0$ nous aurons, $f(x) \geq 0$. Nous pouvons alors maintenant définir une relation entre les paramètres du signal sinusoïdal perturbateur et les propriétés du signal horloge. Cette relation est décrite dans l'Equation 4.18.

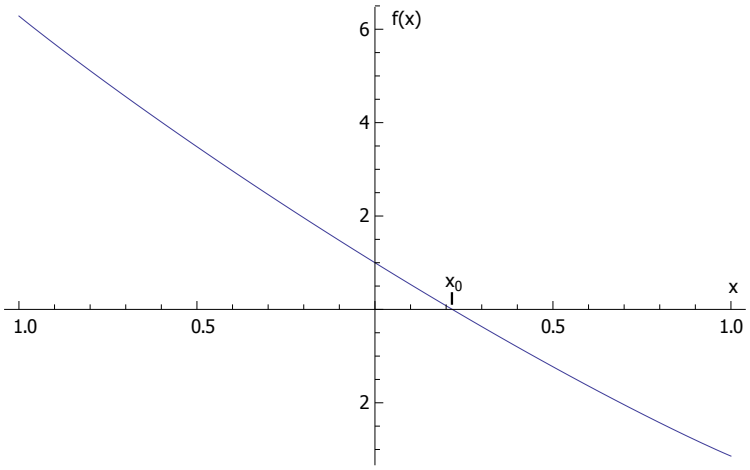

FIG. 4.36 – Graphique de la fonction $f(x)$ qui représente l'inéquation finale de l'Equation 4.17, pour x allant de -1 à 1.

$$f_{pert} V_{pert} \geq \frac{Vdd}{2\pi T_F x_0} \tag{4.18}$$

En utilisant à la fois l'Equation 4.13 et l'Equation 4.18, il est possible de construire un graphique qui donne les chances de succès de l'attaque en fonction de la fréquence et de l'amplitude de la perturbation sinusoïdale. Ce graphique est présenté dans la Figure 4.37. Le graphique a été construit en utilisant les paramètres d'horloge et de tension d'alimentation précédemment utilisés (Vdd = 3.3 V et T_F = 20 ns). On distingue clairement les trois zones différentes (comme présenté précédemment) :

- La zone noire qui correspond aux jeux de paramètres qui mènent à un échec de l'attaque.
- La zone grise qui correspond aux jeux de paramètres qui ne permettent pas de certifier que l'attaque sera effective sur tous les fronts descendants de l'horloge.
- La zone blanche qui correspond aux jeux de paramètres qui assurent la réussite de l'attaque.

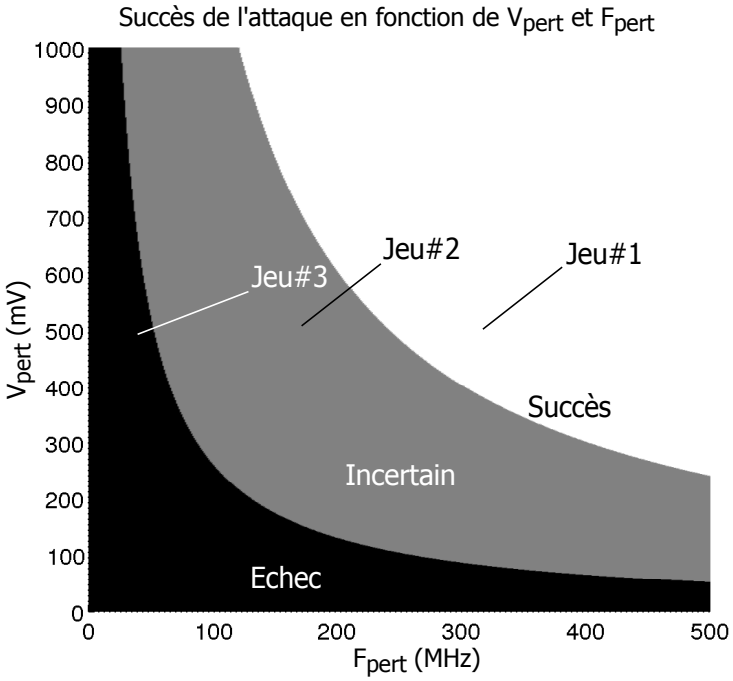

FIG. 4.37 – Graphique qui donne la probabilité de succès de l'attaque en fonction des paramètres de l'attaque avec Vdd = 3.3 V et T_F = 20 ns.

4.5.3.3 Vérification du modèle mathématique avec une simulation électrique.

Avec l'aide de la Figure 4.37, nous avons sélectionné trois jeux de paramètres (un dans chaque zone) :

- f_{pert} = 310 MHz - V_{pert} = 500 mV : la bascule doit échantillonner sur chaque front descendant de l'horloge - correspond à la sortie $S_{FF-310MHz}$
- f_{pert} = 185 MHz - V_{pert} = 500 mV : la bascule doit échantillonner sur quelques fronts descendants de l'horloge - correspond à la sortie $S_{FF-185MHz}$
- f_{pert} = 45 MHz - V_{pert} = 500 mV : la bascule ne doit jamais échantillonner sur un front descendant de l'horloge - correspond à la sortie $S_{FF-45MHz}$

Le but de cette étude est de vérifier si le modèle mathématique construit précédemment est en accord avec les simulations électriques. Nous avons donc réalisé trois nouvelles simulations, avec des paramètres d'attaque qui correspondent à ceux donnés juste avant.

On peut voir, grâce à la Figure 4.38 que pour chaque jeu de paramètres (qui ont été sélectionnés à l'aide du modèle mathématique), le résultat est bien celui qui était attendu. Le premier jeu de paramètres (sortie $S_{FF-310MHz}$ est le même que celui utilisé pour la Figure 4.30. Comme dit précédemment, avec ce jeu de paramètres, l'échantillonnage s'effectue pour chaque front descendant de l'horloge, comme attendu. Pour le deuxième jeu de paramètre, on voit que l'échantillonnage se

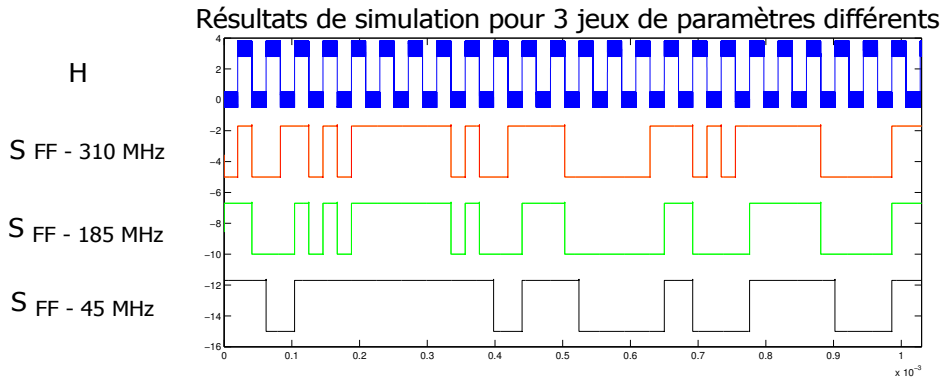

FIG. 4.38 – Résultats de simulation électrique pour les trois jeux de paramètres. De haut en bas : signal d'horloge H, sortie de la bascule pour le premier jeu ($S_{FF-310MHz}$), le second jeu $S_{FF-185MHz}$ et le troisième jeu $S_{FF-45MHz}$ de paramètres d'injection.

produit seulement pour certains fronts descendants (comme ce qu'on avait dans la Figure 4.27). Enfin, pour le dernier jeu de paramètres, la bascule D n'échantillonne sur aucun front descendant.

Le modèle mathématique proposé ici permet ainsi, avant même d'entreprendre une attaque pratique, de savoir, si les paramètres d'attaque utilisés sont bien réglés de manière à permettre à l'attaque d'être réussie (à condition, bien évidemment de connaître certains détails sur les propriétés de l'horloge utilisée pour échantillonner les bascules D du générateur).

4.5.4 Discussion sur l'impact de la perturbation sur l'extracteur d'entropie

Comme présenté dans le Chapitre 1, le générateur de nombres aléatoires à base d'oscillateurs en anneau utilisé dispose de plusieurs paramètres qui peuvent être réglés de manière à modifier la quantité d'entropie produite par le générateur, mais également modifier sa vitesse de production de bits. Ces paramètres sont :

- Le nombre d'oscillateurs en anneau qui composent le générateur.
- Le nombre d'éléments inverseurs qui composent les oscillateurs en anneau (ou en d'autres mots, la fréquence de ces oscillateurs).
- La fréquence d'échantillonnage des bascules D.

Par exemple, en augmentant le nombre d'oscillateurs en anneau ou leurs fréquences, le concepteur du générateur peut augmenter la quantité d'entropie présente dans la suite générée par le générateur. D'un autre coté, augmenter la fréquence d'échantillonnage (c'est à dire la vitesse de production des bits) du générateur peut entrainer une baisse d'entropie dans la suite générée (le temps d'accumulation de l'incertitude temporelle n'est plus assez long). Les auteurs de [Wold and Tan, 2008] conseillent l'utilisation d'un générateur composé de 25 oscillateurs en anneau

(chaque oscillateur a une fréquence de l'ordre de 300 MHz). Pour ces réglages là, les auteurs affirment que la fréquence d'échantillonnage maximum est de l'ordre d'un MHz. Une fréquence inférieure à cette fréquence ne causera aucune perte d'entropie au niveau de la suite générée (au contraire même), alors qu'une fréquence supérieure peut potentiellement entraîner une diminution de l'entropie de la suite (et donc un défaut de sécurité). Si on souhaite réduire le nombre d'oscillateurs en anneau (tout en gardant des oscillateurs avec une fréquence de fonctionnement proche de 300 MHz) de 25 à 2 par exemple (12.5 fois moins d'oscillateurs), il est nécessaire, pour que le générateur produise une suite qui contient sensiblement la même quantité d'entropie, de diviser la fréquence d'échantillonnage d'environ 40 fois (passage de 1 MHz à 25 kHz). La fréquence d'échantillonnage a donc un fort impact sur la génération de l'aléa pour ce type de générateur.

Ici, pour notre cas d'étude, le nombre d'oscillateurs en anneau est fixe (même si leurs fréquences sont légèrement modifiées à cause de la perturbation électromagnétique, comme vu dans la section 5.2.1). Une bascule D qui échantillonne à la fois sur le front montant et le front descendant du signal d'horloge est équivalent à doubler la fréquence d'échantillonnage d'une bascule classique. Si la fréquence d'échantillonnage utilisée par les bascules qui composent le générateur de nombres aléatoires est réglée de manière à obtenir le meilleur ratio vitesse de production des bits et de bonnes propriétés statistiques de la suite générée, il est certain qu'en doublant la fréquence d'échantillonnage, l'entropie contenue dans la suite produite par le générateur sera réduite (sans compter l'effet de dépendance entre les oscillateurs en anneau induite par l'attaque, qui réduit elle aussi l'entropie en sortie). Nous pouvons conclure que si on choisit correctement les paramètres du signal perturbateur (amplitude et fréquence), l'attaquant pourra encore augmenter l'efficacité de son attaque.

La principale faiblesse de l'implantation utilisée pour réaliser cette étude, d'un point de vue de l'extracteur d'entropie, est l'utilisation d'une horloge externe comme horloge d'échantillonnage des bascules D du générateur de nombres aléatoires. En effet, cette horloge a l'inconvénient d'avoir des temps de montée et descente relativement longs par rapport à une horloge générée par une boucle à verrouillage de phase par exemple, ce qui rend plus facile la création de faux fronts montants. Nous pensons que l'utilisation d'une boucle à verrouillage de phase pour générer une horloge qui a de bonnes propriétés est la meilleure solution pour se prémunir des effets indésirables de la perturbation électromagnétique harmonique. Cependant, supprimer cet effet sur l'extracteur d'entropie, n'est pas suffisant, comme vu précédemment, le phénomène d'interdépendance des oscillateurs en anneau (ou verrouillage) reste encore possible, et nécessite de créer un circuit de détection de l'attaque.

4.6 Conclusion

Nous avons montré dans ce chapitre, d'un point de vue expérimental premièrement, qu'il était possible de perturber en même temps, par le biais de l'injection d'un champ électromagnétique harmonique, le fonctionnement de plusieurs oscillateurs en anneau, en les verrouillant sur un signal de fréquence différente. Il est alors possible, pour un générateur d'aléa à base d'oscillateurs en anneau, de contrôler dynamiquement le biais de la suite de bits produite par ce dernier (pour une puissance d'injection suffisamment grande, le biais peut atteindre une valeur de 50%).

Ensuite, nous nous sommes intéressés à modéliser les interactions de l'injection électromagnétique harmonique sur les oscillateurs, mais aussi sur l'extracteur d'entropie du générateur d'aléa. Nous avons dans les deux cas construit un modèle électrique représentant l'injection électromagnétique de façon à mieux comprendre les effets de cette dernière.

Pour résumer, on constate deux effets de l'injection électromagnétique harmonique :

- Le verrouillage des oscillateurs sur la fréquence d'injection - si N oscillateurs sont verrouillés, cela est équivalent à n'avoir plus qu'un oscillateur.
- La fréquence d'échantillonnage des bits aléatoires peut doubler si l'horloge n'est pas assez robuste (et donc le temps d'accumulation de l'incertitude temporelle pour chaque oscillateur est divisé par deux).

Prenons la place d'un concepteur de générateur d'aléa. Imaginons utiliser le même générateur que nous avons utilisé pour les expériences présentées dans ce chapitre (cinquante oscillateurs composés de trois portes inverseuses). Maintenant, imaginons que, pour le système cryptographique dans lequel ce générateur sera implanté, la fréquence d'échantillonnage doit être au moins égale à 2 MHz (pour des conditions normales de fonctionnement, cette configuration du générateur sera capable de fournir des suites de bits de qualité à cette fréquence d'échantillonnage). Imaginons maintenant que cette fréquence (2 MHz) soit proche de la fréquence maximum d'échantillonnage pour garder une qualité des bits produits suffisante. Imaginons enfin qu'un attaquant soit capable de verrouiller une dizaine d'oscillateurs à l'aide d'un champ électromagnétique harmonique. Alors, le générateur va produire une suite de bits équivalente à un générateur de quarante et un oscillateurs (pour la même fréquence de fonctionnement). En règle générale, moins le générateur est composé d'oscillateurs plus petite est la fréquence d'échantillonnage maximale. La fréquence d'échantillonnage étant réglée proche de la fréquence limite (pour un générateur composé de cinquante oscillateurs), en supprimant (par verrouillage ici) neuf oscillateurs, il est sûr que le générateur ne sera plus capable de fournir une suite de bits avec des propriétés statistiques acceptables. De plus nous n'avons pas tenu compte du possible doublement de la fréquence d'échantillonnage induit par l'injection électromagnétique harmonique, qui ne ferait qu'aggraver la situation.

Il est donc évident que ce type d'attaque est extrêmement dangereuse pour les générateurs à base d'oscillateurs en anneau. Il est également important, pour s'en prémunir, de ne pas concevoir des générateurs d'aléa dont les paramètres sont réglés

à la limite (pour limiter les coûts de fabrication). Il faut en effet laisser une marge de manœuvre, notamment sur la fréquence d'échantillonnage - par exemple utiliser une fréquence d'échantillonnage au moins deux fois plus petite que la fréquence limite théorique - pour s'assurer du bon fonctionnement du générateur en cas d'attaque.

Chapitre 5

Résumé des contributions et perspectives

Nous avons montré tout au long de ce manuscrit l'importance de la sécurité des générateurs d'aléa. En effet, les travaux présentés ici, montrent la faiblesse d'un des principes de génération d'aléa le plus répandu. Nous avons montré, qu'en utilisant le canal caché électromagnétique, il est possible de réaliser une attaque complète (récupération d'information et perturbation) sur un générateur d'aléa. Cela était l'objectif principal de notre équipe au sein du projet EMAISeCi. Il est maintenant important, pour les concepteurs de générateur d'aléa, de prendre en compte ce type de vulnérabilité dans l'établissement du cahier des charges.

Principales contributions

Les principales contributions présentées dans ce manuscrit sont :

- Développement d'un banc d'analyse du rayonnement électromagnétique. Le matériel qui compose ce banc est particulièrement adapté à l'étude du rayonnement électromagnétique des générateurs d'aléa. Ce banc a déjà été dupliqué par la société CASSIDIAN Cyber Security et prochainement par le laboratoire Lab-STICC.
- Développement d'une analyse du rayonnement électromagnétique adaptée au générateur d'aléa à base d'oscillateurs en anneau. Cette analyse permet de retrouver la position et la fréquence des oscillateurs qui composent le générateur.
- Mise en évidence de la possibilité d'attaquer les générateurs à base d'oscillateurs en anneau en injectant un champ électromagnétique harmonique.
- Réalisation d'un modèle électrique du phénomène de verrouillage des oscillateurs en anneau induit par le champ électromagnétique harmonique.
- Réalisation d'un modèle électrique et mathématique de l'effet du champ électromagnétique harmonique sur les bascules D qui composent le générateur d'aléa.

Perspectives

Premièrement nous avions choisi délibérément de cibler un seul et unique principe de générateur d'aléa à base d'oscillateurs en anneau. Ce choix était principalement dû à l'importante utilisation de ce type d'oscillateurs dans les différents

principes de génération d'aléa. Nous pensons que les différents travaux présentés ici sont applicables à d'autres principes de génération d'aléa basés également sur des oscillateurs en anneau, cependant, il conviendrait de le vérifier expérimentalement.

Une extension de ces travaux aux fonctions physiques non clonables (Physical Unclonnable Function - PUF) qui exploitent les oscillateurs en anneau est également possible et peut mettre en évidence des problèmes de robustesse aux attaques de ces principes.

Il serait également intéressant d'étudier les attaques électromagnétiques sur des principes de génération d'aléa basés sur des éléments autres que les oscillateurs en anneau, comme par exemple les boucles à verrouillage de phase ([Fischer and Drutarovsky, 2003] par exemple) ou encore des générateurs basés sur la métastabilité des bascules ([Danger et al., 2007] par exemple).

Ensuite il serait important de quantifier l'impact de la réduction des propriétés statistiques de la suite produite par le générateur d'aléa. Par exemple dans le cas de l'utilisation des bits aléatoires produits par le générateur dans des techniques de masquages de la consommation de courant du chiffreur, chiffrer la réduction du nombre de traces de consommation de courant nécessaire si on applique un biais sur la suite de bits aléatoires.

Ensuite, l'étude fine de l'interaction entre la sonde d'émission et le circuit est d'une grande importance. En effet, de manière à réellement comprendre l'effet de l'injection électromagnétique sur les transistors qui composent le circuit, il est nécessaire de réaliser ce type d'étude. De la même façon, pouvoir quantifier la puissance réellement transmise au circuit (nous l'avons vu dans les modèles électriques proposés). Néanmoins, ce type d'étude ne relève pas réellement du domaine de la cryptographie matérielle.

Enfin, il est maintenant important, au même titre que les autres blocs composants les systèmes cryptographiques, d'intégrer à l'étude de la génération d'aléa, une étude sécuritaire de ce bloc. Nous l'avons montré, il est en effet, possible d'attaquer ce type de module, il est donc également nécessaire de le protéger.

Liste des publications

Publication dans un journal international

1. (Soumis en septembre 2013) Bayon, P. ; Bossuet, L. ; Aubert, A. ; Fischer, V. ; Poucheret, F. ; Robisson, B. ; Maurine, P., ***From analysis to attack : a methodology for performing electromagnetic attacks on ring oscillator-based true random number generators***, Journal of Cryptographic Engineering

Publication dans des conférences internationales

2. Bayon, P. ; Bossuet, L. ; Aubert, A. ; Fischer, V. ; Poucheret, F. ; Robisson, B. ; Maurine, P., ***Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator***, Proceedings of Third International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2012
3. Bayon, P. ; Bossuet, L. ; Aubert, A. ; Fischer, V., ***Electromagnetic analysis on ring oscillator-based true random number generators***, 2013 IEEE International Symposium on Circuits and Systems (ISCAS), pp.1954,1957, 19-23 May 2013
4. Bayon, P. ; Bossuet, L. ; Aubert, A. ; Fischer, V., ***EM radiation analysis on true random number generators : Frequency and localization retrieval method***, Proceedings of the IEEE Asia-Pacific International Symposium and Exhibition on Electromagnetic Compatibility, APEMC 2013

Communications non actées

5. Bayon, P. ; Bossuet, L. ; Aubert, A., ***La génération d'aléa : une cible potentielle des attaques par analyse du rayonnement électromagnétique ?***, Journées sécurité numérique du GdR SoC-SiP
6. Bayon, P. ; Bossuet, L. ; Aubert, A., ***Random Number Generation : a potential target of electromagnetic emanation analysis ?***, Cryptographic Architectures Embedded in Reconfigurable Devices, Cryptarchi 2011
7. Bayon, P. ; Bossuet, L. ; Aubert, A. ; Fischer, V. ; Poucheret, F. ; Robisson, B. ; Maurine, P., ***Contacless Electromagnetic Fault injection on Ring Oscillator Based TRNG***, PHISIC 2011
8. Bayon, P. ; Bossuet, L. ; Aubert, A. ; Fischer, V. ; Poucheret, F. ; Robisson, B. ; Maurine, P., ***Electromagnetic Attacks on Ring Oscillator-Based True Random Number Generator***, Cryptographic architectures embedded in reconfigurable devices - Cryptarchi 2012

Bibliographie

R. Adler. A study of locking phenomena in oscillators. *Proceedings of the IEEE*, 61 (10) :1380–1385, 1973.

D. Agrawal, B. Archambeault, J.R. Rao, and P. Rohatgi. The em side-channel(s). In *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '02, pages 29–45, London, UK, UK, 2003. Springer-Verlag.

M.-L. Akkar and C. Giraud. An implementation of des and aes, secure against some attacks. In CetinK. Koc, David Naccache, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 309–318. Springer Berlin Heidelberg, 2001.

Australian National University ANU. `http://150.203.48.55/index.php`, 2011.

K. Arabi and B. Kaminska. Built-in temperature sensors for on-line thermal monitoring of microelectronic structures. In *Computer Design : VLSI in Computers and Processors, 1997. ICCD '97. Proceedings., 1997 IEEE International Conference on*, pages 462–467, 1997.

L. Batina, B. Gierlichs, E. Prouff, M. Rivain, F.-X. Standaert, and N. Veyrat-Charvillon. Mutual information analysis : a comprehensive study. *Journal of Cryptology*, 24(2) :269–291, 2011.

P. Bhansali and J. Roychowdhury. Gen-adler : The generalized adler's equation for injection locking analysis in oscillators. In *Design Automation Conference, 2009. ASP-DAC 2009. Asia and South Pacific*, pages 522–527, 2009.

N. Bochard, F. Bernard, V. Fischer, and B. Valtchanov. True-randomness and pseudo-randomness in ring oscillator-based true random number generators. *Int. J. Reconfig. Comp.*, 2010, 2010.

E. Brier, C. Clavier, and F. Olivier. Correlation power analysis with a leakage model. In *CHES*, pages 16–29, 2004.

J.-S. Coron and L. Goubin. On boolean and arithmetic masking against differential power analysis. In *Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '00, pages 231–237, London, UK, UK, 2000. Springer-Verlag.

O. Cret, A. Suciu, and T. Gyorfi. Practical issues in implementing trngs in fpgas based on the ring oscillator sampling method. In *SYNASC '08 : Proceedings of the 2008 10th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 433–438, Washington, DC, USA, 2008. IEEE Computer Society.

J.L. Danger, S. Guilley, and P. Hoogvorst. Fast true random generator in fpgas. In *Circuits and Systems, 2007. NEWCAS 2007. IEEE Northeast Workshop on*, pages 506–509, 2007.

J.L. Danger, S. Guilley, and P. Hoogvorst. High speed true random number generator based on open loop structures in fpgas. 2009.

A. Dehbaoui, V. Lomne, P. Maurine, L. Torres, and M. Robert. Enhancing electromagnetic attacks using spectral coherence based cartography. In *Very Large Scale Integration (VLSI-SoC), 2009 17th IFIP International Conference on*, pages 11–16, 2009.

A. Dehbaoui, J.-M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria. Injection of transient faults using electromagnetic pulses -practical results on a cryptographic system-. *IACR Cryptology ePrint Archive*, 2012 :123, 2012a.

A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria. Electromagnetic transient faults injection on a hardware and a software implementations of aes. In *FDTC*, pages 7–15, 2012b.

J. Di-Battista, J.-C. Courrege, B. Rouzeyre, L. Torres, and P. Perdu. When failure analysis meets side-channel attacks. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 188–202. Springer Berlin Heidelberg, 2010.

M. Dichtl and J.D. Golic. High-speed true random number generation with logic gates only. *Lecture notes in computer science*, 4727 :45, 2007.

M. Dichtl and N. Janssen. A high quality physical random number generator. In *Proc. Sophia Antipolis Forum Microelectronics (SAME 2000)*, pages 48–53, 2000.

T. Dubois, S. Jarrix, A. Penarier, P. Nouvel, D. Gasquet, L. Chusseau, and B. Azais. Near-field electromagnetic characterization and perturbation of logic circuits. *Instrumentation and Measurement, IEEE Transactions on*, 57(11) :2398–2404, 2008.

M. Epstein, L. Hars, R. Krasinski, M. Rosner, and H. Zheng. Design and implementation of a true random number generator based on digital circuit artifacts. *Lecture notes in computer science*, pages 152–165, 2003.

EVARISTE. `http://evariste.univ-st-etienne.fr/` and `http://labh-curien.univ-st-etienne.fr/wiki-evariste-ii/index.php/Main_P%age`, 2013.

R. C. Fairfield, R. L. Mortenson, and K. B. Coulthart. An lsi random number generator (rng). In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 203–230, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

J. Ferrigno and M. Hlavac. When aes blinks : introducing optical side channel. *Information Security, IET*, 2(3) :94–98, 2008.

Security Requirements For Cryptographic Modules FIPS. `http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf`, 2001.

V. Fischer and M. Drutarovsky. True random number generator embedded in reconfigurable hardware. *Lecture notes in computer science*, pages 415–430, 2003.

T. Fukunaga and J. Takahashi. Practical fault attack on a cryptographic lsi with iso/iec 18033-3 block ciphers. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*, pages 84–92, 2009.

K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis : Concrete results. In *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '01, pages 251–261, London, UK, UK, 2001. Springer-Verlag.

J.D.J. Golic. New methods for digital generation and postprocessing of random data. *IEEE Transactions on Computers*, 55(10) :1217–1229, 2006.

S. Guilley, L. Sauvage, J.-L. Danger, N. Selmane, and R. Pacalet. Silicon-level solutions to counteract passive and active attacks. In *Fault Diagnosis and Tolerance in Cryptography, 2008. FDTC '08. 5th Workshop on*, pages 3–17, 2008.

T. Gyorfi, O. Cret, and A. Suciu. High performance true random number generator based on fpga block rams. In *Proceedings of the 2009 IEEE International Symposium on Parallel&Distributed Processing-Volume 00*, pages 1–8. IEEE Computer Society, 2009.

Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone. Transient iemi threats for cryptographic devices. *Electromagnetic Compatibility, IEEE Transactions on*, 55(1) :140–148, 2013.

C. Huygens. *Oeuvres complètes de Christiaan Huygens : Correspondance, 1664-1665.* Number vol. 5. Martinus Nijhoff, 1893.

H. Istvan, A. Suciu, and O. Cret. Fpga based trng using automatic calibration. In *IEEE 5th International Conference on Intelligent Computer Communication and Processing, 2009. ICCP 2009.*, pages 373 – 376, 2009.

C. Klein, O. Cret, and A. Suciu. Design and implementation of a high quality trng in fpga. In *Intelligent Computer Communication and Processing, 2008. ICCP 2008. 4th International Conference on*, pages 311–314, 2008.

P. C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '96, pages 104–113, London, UK, UK, 1996. Springer-Verlag.

P. C. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 388–397, London, UK, UK, 1999. Springer-Verlag.

P. Kohlbrenner and K. Gaj. An embedded true random number generator for fpgas. In *Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays*, pages 71–78. ACM, 2004.

S.H.M. Kwok and E.Y. Lam. Fpga-based high-speed true random number generator for cryptographic applications. In *2006 IEEE Region 10 Conference TENCON 2006*, pages 1–4, 2006.

A. T. Markettos and S. W. Moore. The frequency injection attack on ring-oscillator-based true random number generators. In *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '09, pages 317–331, Berlin, Heidelberg, 2009. Springer-Verlag.

G. Marsaglia. The marsaglia random number cdrom including the diehard battery of tests of randomness. `http://www.stat.fsu.edu/pub/diehard/`, 1995.

B. Mounier, A.-L. Ribotta, J. Fournier, M. Agoyan, and A. Tria. Em probes characterisation for security analysis. In *Cryptography and Security*, pages 248–264, 2012.

NSA. Tempest : A signal problem ? Technical report, National Security Agency, 2007.

E. Peeters, F.-X. Standaert, and J.-J. Quisquater. Power and electromagnetic analysis : improved model, consequences and comparisons. *Integr. VLSI J.*, 40(1) : 52–60, January 2007.

G. Piret and J.-J. Quisquater. A differential fault attack technique against spn structures, with application to the aes. In *AES and KHAZAD". CHES 2003, LNCS 2779*, pages 77–88. Springer-Verlag, 2003.

F. Poucheret, L. Chusseau, B. Robisson, and P. Maurine. Local electromagnetic coupling with cmos integrated circuits. In *Electromagnetic Compatibility of Integrated Circuits (EMC Compo), 2011 8th Workshop on*, pages 137–141, 2011a.

F. Poucheret, K. Tobich, M. Lisart, L. Chusseau, B. Robisson, and P. Maurine. Local and direct em injection of power into cmos integrated circuits. In *FDTC*, pages 100–104, 2011b.

QUANTIS. `http://www.idquantique.com/index.php?option=com_content\&view=article\&%id=9`, 2006.

J.-J. Quisquater and D. Samyde. Electromagnetic analysis (ema) : Measures and counter-measures for smart cards. In *Proceedings of the International Conference*

on Research in Smart Cards : Smart Card Programming and Security, E-SMART '01, pages 200–210, London, UK, UK, 2001. Springer-Verlag.

J.-J. Quisquater and D. Samyde. Eddy current for magnetic analysis with active sensor. In *Esmart 2002, Nice, France*, 9 2002.

D. Real, F. Valette, and M. Drissi. Enhancing correlation electromagnetic attack using planar near-field cartography. In *Design, Automation Test in Europe Conference Exhibition, 2009. DATE '09.*, pages 628–633, 2009.

A. Rukhin, J. Soto, J. Nechvatal, E. Barker, S. Leigh, M. Levenson, D. Banks, A. Heckert, J. Dray, S. Vo, M. Smid, M. Vangel, and L.E. Bassham. A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2001.

R. Santoro, O. Sentieys, and S. Roy. On-the-fly evaluation of fpga-based true random number generator. In *Proceedings of the 2009 IEEE Computer Society Annual Symposium on VLSI*, ISVLSI '09, pages 55–60, Washington, DC, USA, 2009. IEEE Computer Society.

L. Sauvage, S. Guilley, and Y. Mathieu. Electromagnetic radiations of fpgas : High spatial resolution cartography and attack on a cryptographic module. *ACM Trans. Reconfigurable Technol. Syst.*, 2(1) :4 :1–4 :24, March 2009.

L. Sauvage, S. Guilley, F. Flament, J.-L. Danger, and Y. Mathieu. Cross-correlation cartography. In *Proceedings of the 2010 International Conference on Reconfigurable Computing and FPGAs*, RECONFIG '10, pages 268–273, Washington, DC, USA, 2010. IEEE Computer Society.

P. Schaumont and K. Tiri. Masking and dualrail logic don't add up. In *In Cryptographic Hardware and Embedded Systems – CHES 2007, 9th International Workshop*, pages 10–13, 2007.

D. Schellekens, B. Preneel, and I. Verbauwhede. Fpga vendor agnostic true random number generator. In *Proceedings of the International Conference on Field Programmable Logic and Applications (FPL'06)*, pages 1–6. Citeseer, 2006.

J. Schmidt and C. Herbst. A practical fault attack on square and multiply. In *Fault Diagnosis and Tolerance in Cryptography, 2008. FDTC '08. 5th Workshop on*, pages 53–58, 2008.

J.-M. Schmidt and M. Hutter. Optical and em fault-attacks on crt-based rsa : Concrete results. In Johannes Wolkerstorfer Karl C. Posch, editor, *Austrochip 2007, 15th Austrian Workhop on Microelectronics, 11 October 2007, Graz, Austria, Proceedings*, pages 61 – 67. Verlag der Technischen Universität Graz, 2007.

A. Shamir and E. Tromer. Acoustic cryptanalysis. *presentation available from http ://www. wisdom. weizmann. ac. il/ tromer*, 2004.

M. Simka, M. Drutarovský, and V. Fischer. Testing of pll-based true random number generator in changing working conditions. *RADIOENGINEERING,*, 20 :94–101, April 2011.

S.P. Skorobogatov. Semi-invasive attacks – a new approach to hardware security analysis. Technical Report UCAM-CL-TR-630, University of Cambridge, Computer Laboratory, April 2005.

S.P. Skorobogatov. Using optical emission analysis for estimating contribution to power analysis. In *Proceedings of the 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography*, FDTC '09, pages 111–119, Washington, DC, USA, 2009. IEEE Computer Society.

S.P. Skorobogatov and R.J. Anderson. Optical fault induction attacks. In *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '02, pages 2–12, London, UK, UK, 2002. Springer-Verlag.

B. Sunar, W.J. Martin, and D.R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on Computers*, 56(1) :109, 2007.

T. Symul, S. M. Assad, and P. K. Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*, 98(23), 2011.

M. Thamrin, I. Ahmad, and M.K. Hani. A true random number generator for crypto embedded systems. In *Regional Postgraduate Conference on Engineering and Science*, pages 253–256. School of Postgraduate Studies, UTM, 2006.

K. Tiri and I. Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. pages 246–251, 2004.

T.E. Tkacik. A hardware random number generator. In Burton S. Kaliski Jr., Çetin Kaya Koç, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002*, volume 2523 of *LNCS*, pages 450–453. Springer, 2003.

K.H. Tsoi, K.H. Leung, and P.H.W. Leong. Compact fpga-based true and pseudo random number generators. In *Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM), California USA*, pages 51–61. Citeseer, 2003.

K.H. Tsoi, K.H. Leung, and P.H.W. Leong. High performance physical random number generator. *IEEE Proc. Computers & Digital Techniques*, 1(4) :349–352, 2007.

B. Valtchanov, V. Fischer, and A. Aubert. Enhanced trng based on the coherent sampling. In *Proceedings of 2009 International Conference on Signals, Circuits ans Systems 2009 International Conference on Signals, Circuits ans Systems*, 11 2009.

W. van Eck. Electromagnetic radiation from video display units : an eavesdropping risk ? *Comput. Secur.*, 4(4) :269–286, December 1985.

M. Varchola and M. Drutarovsky. New high entropy element for fpga based true random number generators. In *Proceedings of the 12th international conference on Cryptographic hardware and embedded systems*, CHES'10, pages 351–365, Berlin, Heidelberg, 2010. Springer-Verlag.

F. Vargas, D. L. Cavalcante, E. Gatti, D. Prestes, and D. Lupi. On the proposition of an emi-based fault injection approach. In *On-Line Testing Symposium, 2005. IOLTS 2005. 11th IEEE International*, pages 207–208, 2005.

I. Vasyltsov, E. Hambardzumyan, Y.S. Kim, and B. Karpinskyy. Fast digital trng based on metastable ring oscillator. *Lecture notes in computer science*, 5154 : 164–180, 2008.

M. Vuagnoux and S. Pasini. Compromising electromagnetic emanations of wired and wireless keyboards. In *Proceedings of the 18th conference on USENIX security symposium*, SSYM'09, pages 1–16, Berkeley, CA, USA, 2009. USENIX Association.

K. Wold and C.H. Tan. Analysis and enhancement of random number generator in fpga based on oscillator rings. In *Proceedings of the International Conference on Reconfigurable Computing and FPGAs (ReConFig/'08)*, pages 385–390, 2008.

S.-K. Yoo, B. Sunar, D. Karakoyunlu, and B. Birand. A robust and practical random number generator. 2007.

S.-K. Yoo, D. Karakoyunlu, B. Birand, and B. Sunar. Improving the robustness of ring oscillator trngs. *ACM Trans. Reconfigurable Technol. Syst.*, 3(2) :9 :1–9 :30, May 2010.

Annexe A : Notion d'électromagnétisme

Dans cette annexe nous allons présenter les propriétés de l'électromagnétisme sur lesquels les différents travaux d'analyse du champ électromagnétique se basent. Le but n'est pas de réaliser un modèle du champ électromagnétique rayonné par un circuit intégré mais de définir quelles sont les sources de ce rayonnement. Cette maitrise des sources permet d'effectuer correctement les mesures du champ électromagnétique et ainsi exploiter au maximum ses possibilités.

A.1 Modèle théorique : les équations de Maxwell

Les premières expérimentations prouvant l'existence de forces « électriques » et « magnétiques » remontent aux civilisations antiques. Ce n'est qu'au XIXe siècle que les premiers travaux théoriques de modélisation et de compréhension de ces phénomènes sont apparus. Ces travaux ont été unifiés par James Maxwell, qui en s'appuyant sur les travaux précédents de plusieurs physiciens (notamment Ampère et Faraday), a construit un modèle théorique des ondes électromagnétiques présenté dans « A Treatise on Electricity and Magnetism ». Outre le modèle apporté, il explique que les forces électrique et magnétique sont liées et ne forment qu'une seule et unique force dite électromagnétique. Il démontre également que la lumière est une onde électromagnétique qui se propage à vitesse constante.

Le modèle théorique introduit par Maxwell se base sur quatre équations qui régissent le comportement des ondes électromagnétiques. Deux modèles existent, un, microscopique, l'autre, macroscopique. Le premier, définit le comportement des ondes électromagnétiques dans le vide, alors que le second définit le comportement des ondes électromagnétiques quel que soit le milieu, à partir du moment où ce dernier peut être considéré comme continu. Un milieu continu est un milieu où les paramètres utilisés pour construire le modèle peuvent être considérés comme continus. Pour des raisons pratiques évidentes, nous allons nous intéresser au modèle macroscopique.

Le modèle macroscopique nécessite l'utilisation de quatre vecteurs pour représenter une onde électromagnétique :

- $\vec{E}$ est le champ électrique ($V.m^{-1}$).
- $\vec{H}$ est le champ magnétique ($A.m^{-1}$).
- $\vec{D}$ est l'induction électrique ($C.m^{-2}$).
- $\vec{B}$ est l'induction magnétique ($V.s.m^{-2}$).

Les paramètres utilisés pour décrire les équations de Maxwell sont les suivants :

- μ est la perméabilité magnétique du milieu continu ($H.m^{-1}$).
- $\vec{j}$ est la densité de courant ($A.m^{-2}$).
- ρ_e est la densité de charge ($C.m^{-3}$).

Deux relations existent entre, respectivement, le champ électrique et l'induction électrique, et le champ magnétique et l'induction magnétique :

$$\vec{D} = \epsilon \vec{E} \tag{A.1}$$

$$\vec{B} = \mu \vec{H} \tag{A.2}$$

Dans un milieu continu les équations de Maxwell sont les suivantes :

- Maxwell-Gauss :

$$div\vec{D} = \rho_e \tag{A.3}$$

- Maxwell-Thomson :

$$div\vec{B} = 0 \tag{A.4}$$

- Maxwell-Faraday :

$$rot\vec{E} = -\frac{\delta \vec{H}}{\delta t} \tag{A.5}$$

- Maxwell-Ampère :

$$rot\vec{H} = \frac{\delta \vec{D}}{\delta t} + \vec{j} \tag{A.6}$$

A.2 Zone de rayonnement ?

Quand on souhaite étudier le rayonnement électromagnétique d'une antenne (typiquement l'antenne est pour nous le circuit qui peut être vu comme un réseau d'antennes, à savoir les interconnexions et les transistors du circuit), il est bon de savoir dans quelle zone de champ de l'antenne notre système de mesure se situe.

La Figure A.1 décrit les différentes zones de champ autour d'une antenne classiquement utilisée en radio-télécommunication. Elles sont au nombre de quatre :

- La zone de champ réactif : cette zone existe jusqu'à une distance de $\frac{\lambda}{2\pi}$ à partir de l'antenne. Dans cette zone l'onde est dite évanescente (en d'autres mots l'onde est plane et son amplitude décroit exponentiellement avec la distance). Dans cette zone, le champ électromagnétique est principalement composé d'un champ magnétique en présence de courant élevé, et d'un champ électrique en présence d'une tension élevée.
- La zone de Rayleigh : zone située entre $\frac{\lambda}{2\pi}$ et $\frac{D^2}{2\lambda}$. Dans cette zone l'amplitude du champ varie peu (en fonction de la distance avec l'antenne).
- La zone de Fresnel : zone de champ proche situé entre $\frac{D^2}{2\lambda}$ et $\frac{2D^2}{\lambda}$. Présence d'interférence dans cette zone du à la transition entre champ proche et lointain, ce qui rend le calcul des champs, mis en jeu dans cette zone, difficile.
- La zone de Fraunhoffer : zone de champ lointain, où l'onde se propage de $\frac{2D^2}{\lambda}$ jusqu'à l'infini. L'onde n'est plus contenue dans un tube de diamètre égal à la largeur de l'antenne. L'onde ici est encore considérée comme plane et son amplitude décroit inversement proportionnellement avec la distance.

Dans la liste précédente, λ correspond à la longueur d'onde de l'onde rayonnée (cette grandeur est exprimée dans l'Equation A.7) et D correspond à la largeur de l'antenne.

L'onde plane est un concept introduit par l'étude de la propagation des ondes. Une onde plane est définie comme une onde dont les fronts d'onde sont compris dans des plans infinis perpendiculaires à la direction de propagation. Dans un référentiel classique, si l'onde se propage suivant l'axe des z, quelle que soit la position d'observation de l'onde en x ou y, l'onde sera considérée comme identique. Seul le déplacement suivant l'axe des z entraine une modification de l'apparence de l'onde (amplitude, phase, etc).

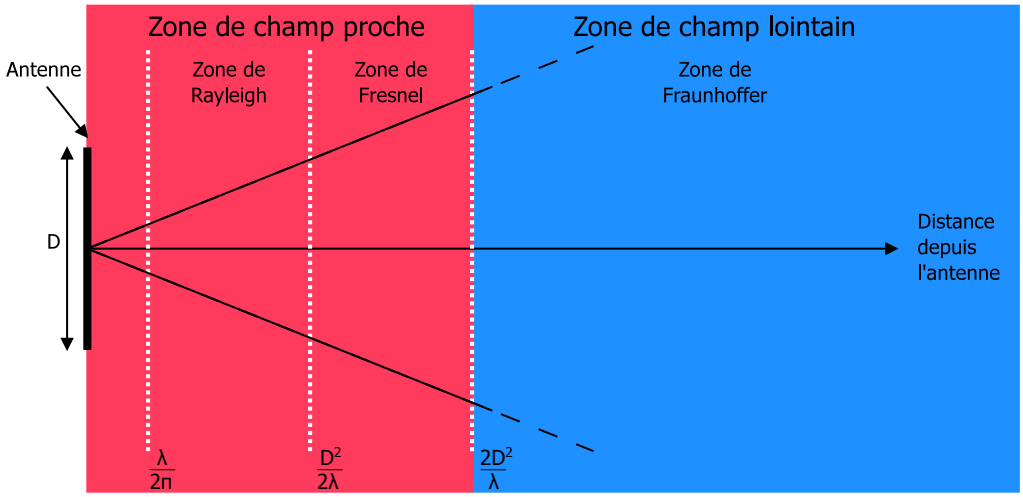

FIG. A.1 – Répartition des zones de champ en fonction de la distance avec l'antenne.

Il est bon maintenant de savoir quelles vont être les limites entre la zone de champ proche et lointain pour notre cas d'étude.

En pratique, on prend le rapport $\frac{\lambda}{2\pi}$ comme limite entre le champ proche et le champ lointain du fait de la taille des antennes émettrices (comme dit précédemment les antennes sont les interconnexions et les transistors composant le circuit - donc que les tailles mises en jeu ici sont relativement petites et dépendent fortement du design et de la technologie du circuit étudié). Les zones de Rayleigh et de Fresnel n'existent donc pas pour ce type d'antennes (ce sont des zones en général seulement considérées dans le cas des antennes à fort gain et de grande taille). Cette limite est donc dépendante des longueurs d'onde et par conséquence des fréquences de l'onde émise (voir l'l'Equation A.7). Il est donc bon de savoir, pour un circuit intégré moderne, quelle est la distance maximum à laquelle on peut encore considérer le champ comme proche.

Pour une circuit intégré moderne classique (ASIC ou FPGA), les fréquences mises en jeu vont du MHz au GHz pour les circuits les plus performants.

La longueur d'onde est reliée à la fréquence par la formule suivante :

$$\lambda = \frac{c}{2\pi f} \tag{A.7}$$

où c est la vitesse de propagation de l'onde dans le milieu considéré et f la fréquence de cette onde. On prend habituellement comme valeur pour c la vitesse de la lumière dans le vide, soit 2.9 $m.s^{-1}$.

Fréquence (MHz)	Longueur d'onde	Taille de la zone de champ proche
1	300 m	$\tilde{4}$9 m
100	3 m	$\tilde{4}$7 cm
500	60 cm	$\tilde{9}$.5 cm
1000	30 cm	$\tilde{4}$.7 cm
3000	10 cm	$\tilde{1}$.5 cm

Tab. A.1 – Taille de la zone de champ proche en fonction de la fréquence de la source.

D'après le Tableau A.1, même pour des fréquences relativement élevées, en mettant la sonde de mesure presque en contact avec la surface du circuit électronique (qui se situe à quelques millimètres des lignes de métal, en fonction de l'épaisseur du capot), la mesure est faite dans la zone de champ proche. C'est donc évidemment dans cette zone, à quelques centimètres, voir millimètres de la surface du circuit, de manière à maximiser l'amplitude du champ électromagnétique collecté - comme dit précédemment, dans la zone de champ proche l'amplitude du champ décroit exponentiellement avec la distance par rapport à l'antenne émettrice - que nous effectuerons notre analyse du champ électromagnétique rayonné par le circuit.

A.3 Circuit intégré et électromagnétisme ?

Le but de cette partie n'est pas de construire un modèle précis fil par fil - transistor par transistor du rayonnement d'un circuit intégré, mais de fournir une analyse sur la provenance du rayonnement électromagnétique des circuits.

A partir de l'Equation A.6, il est possible d'en déduire le modèle de rayonnement d'un fil infini. Cependant, il est nécessaire, pour construire ce modèle d'être certain d'être le cadre de l'approximation des régimes quasi stationnaires (ARQS). Cette approximation revient à négliger le temps de propagation de l'onde devant la période de cette dernière. En d'autres mots, si l'antenne de réception est située à une distance D de l'antenne émettrice, il est nécessaire de s'assurer que $\lambda \gg D$ pour être dans le cadre de l'ARQS. Les longueurs d'ondes mises en jeu dans nos études sont comprises entre 300 mètres et 60 centimètres. La distance entre l'antenne émettrice et l'antenne réceptrice est en général de l'ordre du millimètres (qui peut dans certains cas aller au maximum jusqu'au centimètre). De ce fait, pour ce type de longueur d'ondes, nous pouvons nous placer dans le cadre de l'ARQS.

Ainsi, l'Equation A.6 peut être simplifiée en l'Equation A.8. Cette représentation est une forme locale, nous avons besoin, dans le cas du fil infini d'une représenta-

tion intégrale. Cette forme intégrale est en fait plus communément appelée théorème d'Ampère. Ici le théorème d'Ampère, dans le cadre de l'ARQS est donné par l'Equation A.9. En l'appliquant au cas du fil infini (voir la Figure A.2, on obtient comme expression pour le champ magnétique généré par le courant traversant le fil l'Equation A.10.

Les différentes définitions mathématiques et physiques pour ces calculs sont les suivantes :

- $\oint$ est l'intégrale curviligne sur le contour fermé τ,
- τ est un cercle,
- S est la surface s'appuyant sur le contour τ
- $\vec{dl} = rd\theta\vec{u_\theta}$,
- $\sum I_{traversant}$ est la somme des intensités des courants traversant le contour τ.

$$rot\vec{H} = \vec{j} \tag{A.8}$$

$$\oint_\tau \vec{H}.\vec{dl} = \int\int_S \vec{j}.\vec{dS} = \sum I_{traversant} \tag{A.9}$$

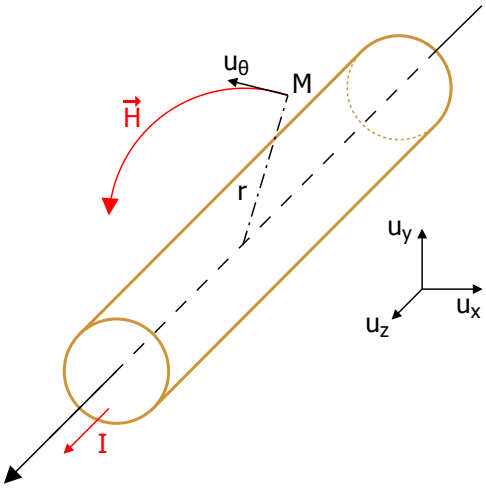

FIG. A.2 – Modèle de rayonnement magnétique d'un fil considéré infini.

$$\vec{H}(r) = \frac{I\vec{u_\theta}}{2\pi r} \tag{A.10}$$

Même si ce modèle du fil infini n'est pas forcement le plus précis pour modéliser le rayonnement d'un circuit intégré, il est tout de même utile. En effet, l'idée ici n'est pas de modéliser correctement l'amplitude du champ magnétique produit par le circuit, mais de surtout connaître son orientation par rapport aux éléments qui constituent le circuit.

La Figure A.2 montre une vue en coupe d'un circuit quelconque composé de trois niveaux de métallisation. Un circuit intégré classique (FPGA / ASIC) est composé :

- De transistors.

– De grilles et plans d'alimentation.
– D'un arbre d'horloge.
– De divers interconnexions entre les transistors.

Comme signifié dans [Gandolfi et al., 2001], le rayonnement électromagnétique d'une puce dépend de sa consommation de courant. Cela est en effet confirmé par l'Equation A.10.

Comme présenté dans la figure Figure A.3, pour chaque piste qui compose le circuit, le champ généré autour de cette dernière est directement dépendant du courant circulant dedans.

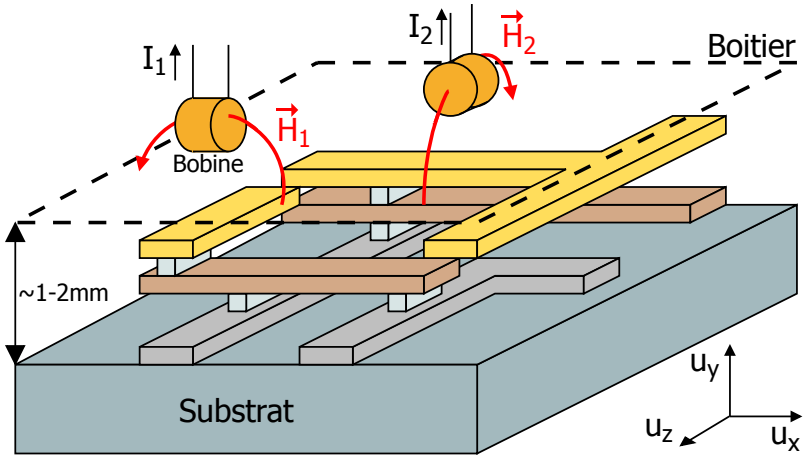

FIG. A.3 – Vue en coupe d'une portion d'un circuit intégré.

On remarque également, suivant l'orientation de la sonde (qui est ici une boucle ou une bobine), le champ magnétique capté par cette dernière n'est pas le même. En effet, la bobine qui capte le champ magnétique $\vec{H_1}$ (bobine à 0 °) n'est pas capable de capturer le champ magnétique $\vec{H_2}$ et inversement. L'orientation de la sonde par rapport au circuit a donc une forte influence sur le résultat de l'analyse. Intuitivement, l'orientation optimale ne correspond à aucune de celles présentées dans la Figure A.3, mais plutôt une orientation à 45 ° de la sonde par rapport au circuit. Nous confirmerons dans le Chapitre 3 cette affirmation.

Pour le type de circuit utilisé pour réaliser nos expériences (et en général pour tout les circuits électroniques), le champ électromagnétique rayonné peut être considéré comme un champ purement magnétique orthogonal à la surface du circuit. Les sondes utilisées dans l'analyse du rayonnement électromagnétique d'un circuit intégré sont donc construites de manière à être fortement sensibles au champ magnétique (bobinage par exemple).