Rétro-conception matérielle partielle appliquée à l'injection ciblée de fautes laser et à la détection efficace de Chevaux de Troie Matériels

Franck Courbon

NNT : *2015 EMSE 0788*

THÈSE

présentée par

Franck COURBON

pour obtenir le grade de
Docteur de l'École Nationale Supérieure des Mines de Saint-Étienne

Spécialité : Microélectronique

RETRO-CONCEPTION MATERIELLE PARTIELLE APPLIQUEE A L'INJECTION CIBLEE DE FAUTES LASER ET A LA DETECTION EFFICACE DE CHEVAUX DE TROIE MATERIELS

soutenue à Gardanne, le 03 Septembre 2015

Membres du jury

Président :	Jean-Luc DANGER	HDR, Pr, Télécom ParisTech
Rapporteurs :	Bruno ROUZEYRE	HDR, Pr, Université de Montpellier
	Régis LEVEUGLE	HDR, Pr, Université de Grenoble
Examinateurs :	Jean-Michel PORTAL	HDR, Pr, Université Aix-Marseille
	Christian TOULEMONT	Serma Technologies, Pessac
	Philippe LOUBET-MOUNDI	Gemalto, La Ciotat
	Jacques FOURNIER	HDR, CEA-Tech, Gardanne
Directeur de thèse :	Assia TRIA	HDR, CEA-Tech, Gardanne

Spécialités doctorales	Responsables :	Spécialités doctorales	Responsables
SCIENCES ET GENIE DES MATERIAUX	K. Wolski Directeur de recherche	MATHEMATIQUES APPLIQUEES	O. Roustant, Maître-assistant
MECANIQUE ET INGENIERIE	S. Drapier, professeur	INFORMATIQUE	O. Boissier, Professeur
GENIE DES PROCEDES	F. Gruy, Maître de recherche	IMAGE, VISION, SIGNAL	JC. Pinoli, Professeur
SCIENCES DE LA TERRE	B. Guy, Directeur de recherche	GENIE INDUSTRIEL	A. Dolgui, Professeur
SCIENCES ET GENIE DE L'ENVIRONNEMENT	D. Graillot, Directeur de recherche	MICROELECTRONIQUE	S. Dauzere Peres, Professeur

EMSE : Enseignants-chercheurs et chercheurs autorisés à diriger des thèses de doctorat (titulaires d'un doctorat d'État ou d'une HDR)

ABSI	Nabil	CR	Génie industriel	CMP
AVRIL	Stéphane	PR2	Mécanique et ingénierie	CIS
BALBO	Flavien	PR2	Informatique	FAYOL
BASSEREAU	Jean-François	PR	Sciences et génie des matériaux	SMS
BATTAIA-GUSCHINSKAYA	Olga	CR		FAYOL
BATTON-HUBERT	Mireille	PR2	Sciences et génie de l'environnement	FAYOL
BERGER DOUCE	Sandrine	PR2	Sciences de gestion	FAYOL
BIGOT	Jean Pierre	MR(DR2)	Génie des Procédés	SPIN
BILAL	Essaid	DR	Sciences de la Terre	SPIN
BLAYAC	Sylvain	MA(MDC)	Microélectronique	CMP
BOISSIER	Olivier	PR1	Informatique	FAYOL
BONNEFOY	Olivier	MA(MDC)	Génie des Procédés	SPIN
BORBELY	Andras	MR(DR2)	Sciences et génie des matériaux	SMS
BOUCHER	Xavier	PR2	Génie Industriel	FAYOL
BRODHAG	Christian	DR	Sciences et génie de l'environnement	FAYOL
BRUCHON	Julien	MA(MDC)	Mécanique et ingénierie	SMS
BURLAT	Patrick	PR1	Génie Industriel	FAYOL
COURNIL	Michel	PR0	Génie des Procédés	DIR
DARRIEULAT	Michel	IGM	Sciences et génie des matériaux	SMS
DAUZERE-PERES	Stéphane	PR1	Génie Industriel	CMP
DEBAYLE	Johan	CR	Image Vision Signal	CIS
DELAFOSSE	David	PR0	Sciences et génie des matériaux	SMS
DELORME	Xavier	MA(MDC)		FAYOL
DESRAYAUD	Christophe	PR1	Mécanique et ingénierie	SMS
DOLGUI	Alexandre	PR0	Génie Industriel	FAYOL
DRAPIER	Sylvain	PR1	Mécanique et ingénierie	SMS
FAVERGEON	Loïc	CR	Génie des Procédés	SPIN
FEILLET	Dominique	PR1	Génie Industriel	CMP
FRACZKIEWICZ	Anna	DR	Sciences et génie des matériaux	SMS
GARCIA	Daniel	MR(DR2)	Génie des Procédés	SPIN
GAVET	Yann	MA(MDC)	Image Vision Signal	CIS
GERINGER	Jean	MA(MDC)	Sciences et génie des matériaux	CIS
GOEURIOT	Dominique	DR	Sciences et génie des matériaux	SMS
GRAILLOT	Didier	DR	Sciences et génie de l'environnement	SPIN
GROSSEAU	Philippe	DR	Génie des Procédés	SPIN
GRUY	Frédéric	PR1	Génie des Procédés	SPIN
GUY	Bernard	DR	Sciences de la Terre	SPIN
HAN	Woo-Suck	MR	Mécanique et ingénierie	SMS
HERRI	Jean Michel	PR1	Génie des Procédés	SPIN
KERMOUCHE	Guillaume	PR2	Mécanique et Ingénierie	SMS
KLOCKER	Helmut	DR	Sciences et génie des matériaux	SMS
LAFOREST	Valérie	MR(DR2)	Sciences et génie de l'environnement	FAYOL
LERICHE	Rodolphe	CR	Mécanique et ingénierie	FAYOL
LI	Jean-Michel		Microélectronique	CMP
MALLIARAS	Georges	PR1	Microélectronique	CMP
MAURINE	Philippe	Ingénieur de recherche		CMP
MOLIMARD	Jérôme	PR2	Mécanique et ingénierie	CIS
MONTHEILLET	Frank	DR	Sciences et génie des matériaux	SMS
MOUTTE	Jacques	CR	Génie des Procédés	SPIN
NEUBERT	Gilles	PR		FAYOL
NIKOLOVSKI	Jean-Pierre	Ingénieur de recherche		CMP
NORTIER	Patrice	PR1		SPIN
OWENS	Rosin	MA(MDC)		CMP
PICARD	Gauthier	MA(MDC)		FAYOL
PIJOLAT	Christophe	PR0	Génie des Procédés	SPIN
PIJOLAT	Michèle	PR1	Génie des Procédés	SPIN
PINOLI	Jean Charles	PR0	Image Vision Signal	CIS
POURCHEZ	Jérémy	MR	Génie des Procédés	CIS
ROBISSON	Bruno	Ingénieur de recherche		CMP
ROUSSY	Agnès	MA(MDC)	Génie industriel	CMP
ROUSTANT	Olivier	MA(MDC)	Mathématiques appliquées	FAYOL
ROUX	Christian	PR	Image Vision Signal	CIS
STOLARZ	Jacques	CR	Sciences et génie des matériaux	SMS
TRIA	Assia	Ingénieur de recherche	Microélectronique	CMP
VALDIVIESO	François	PR2	Sciences et génie des matériaux	SMS
VIRICELLE	Jean Paul	DR	Génie des Procédés	SPIN
WOLSKI	Krzystof	DR	Sciences et génie des matériaux	SMS
XIE	Xiaolan	PR1	Génie industriel	CIS
YUGMA	Gallian	CR	Génie industriel	CMP

ENISE : Enseignants-chercheurs et chercheurs autorisés à diriger des thèses de doctorat (titulaires d'un doctorat d'État ou d'une HDR)

BERGHEAU	Jean-Michel	PU	Mécanique et Ingénierie	ENISE
BERTRAND	Philippe	MCF	Génie des procédés	ENISE
DUBUJET	Philippe	PU	Mécanique et Ingénierie	ENISE
FEULVARCH	Eric	MCF	Mécanique et Ingénierie	ENISE
FORTUNIER	Roland	PR	Sciences et Génie des matériaux	ENISE
GUSSAROV	Andrey	Enseignant contractuel	Génie des procédés	ENISE
HAMDI	Hédi	MCF	Mécanique et Ingénierie	ENISE
LYONNET	Patrick	PU	Mécanique et Ingénierie	ENISE
RECH	Joël	PU	Mécanique et Ingénierie	ENISE
SMUROV	Igor	PU	Mécanique et Ingénierie	ENISE
TOSCANO	Rosario	PU	Mécanique et Ingénierie	ENISE
ZAHOUANI	Hassan	PU	Mécanique et Ingénierie	ENISE

Mise à jour : 11/05/2015

Remerciements

Chers lecteurs, merci à vous d'avoir eu la curiosité d'obtenir un exemplaire de mon travail de thèse. En espérant que chaque page vous entraîne à lire la suivante. Cette section est dédiée à tous ceux qui m'ont permis d'avoir l'opportunité de mener à terme ce doctorat et de finir très tardivement mes études. Petit expert de la rétro-conception je vais commencer par un rétro-planning en remerciant Monsieur Bruno Rouzeyre et Monsieur Régis Leveugle de m'avoir autorisé à présenter mes travaux. Je remercie également Messieurs Jean-Michel Portal, Christian Toulemont et Jean-Luc Danger d'avoir été examinateurs de mon travail. Vos remarques m'ont permis de clôturer de la meilleure des manières mes travaux. C'est un vrai honneur d'avoir des personnes autant renommées qui ont consacrées de leur temps à évaluer mes travaux. Antérieure à cette soutenance nos chemins se sont déjà croisés pour certains, Jean-Luc tes remarques alliées à tes connaissances ont toujours été d'intérêt. Et toi Bruno, tu auras été un exemple professionnel à suivre avec ton style, ta simplicité, tes connaissances et tes différents projets.

Ensuite viennent d'autres membres du jury un peu plus familiers, je tiens à remercier mon encadrant académique Jacques Jean-Alain Fournier pour sa franchise, son expérience, son expertise, sa générosité, sa contribution pour les articles avec toujours la bonne vision et une rapidité hors du commun et ainsi de suite. Au plaisir de se recroiser dans un futur proche avec Maurice ou non.

Je remercie également mon encadrant industriel, Philippe Loubet-Moundi, pour la mission confiée (vraiment merci pour cette chance unique), la partie de ses connaissances partagées, sa patience, son professionnalisme, son partage de bureau, ses questionnements sur une éventuelle blessure à mon retour du foot et enfin ses chemises colorées. Cet arc-en-ciel de couleurs s'est retrouvé dans notre éventail de résultats.

Je tiens à remercier ensuite ma directrice de thèse, Assia Tria, pour sa franchise et sa grande aide apportée lors de la rédaction de ce manuscrit. Un réel plaisir d'avoir pu partager ensemble la fin de rédaction et d'avoir pu corriger des fautes de français inimaginables.

Obtenir ce doctorat n'aurait pu être possible sans école. Ainsi, je remercie grandement l'Ecole des Mines de Saint-Etienne de m'avoir accepté. Né à Saint-Etienne 26 ans et demi plus tôt, c'est un vrai honneur d'être diplômé du fleuron local. Pas autant locales que les attaques en fautes laser il est vrai de part ma présence sur le site de l'Ecole des Mines de Saint-Etienne dédié à la micro-électronique, le campus Georges Charpak Provence situé à Gardanne. Je tiens à remercier tous les acteurs de ce site, depuis le personnel de la salle blanche (j'en profites pour remercier ceux que j'ai pu croiser dans un autre type de salle blanche), le personnel de la vie de l'école (ou encore de son accès), les membres des différents labos jusqu'à ceux qui vous piquent l'amphithéâtre la veille de votre soutenance. Je remercie ensuite notre équipe SAS, Systèmes et Architectures Sécurisés, pour les aspects techniques bien entendu mais aussi pour toutes les autres discussions qui n'étaient pas exactement centrées sur la sécurité des circuits intégrés. Et bien entendu mes anciens et présents collègues de l'espace doctorant. Ce fut toujours un plaisir de venir sur le site et vraiment agréable de passer des petits moments avec vous tous.

Un financement m'a donné l'opportunité de faire une thèse. Je remercie ainsi Gemalto dans son ensemble pour avoir misé sur moi. Au final, il résulte un pari gagnant avec un parcours de sportif digne de l'ASSE des années 70. Merci donc à ceux ayant donné leur accord pour que je continue mes travaux de stage dans le cadre d'une thèse CIFRE. Je vous remercie encore de

m'avoir confié les missions très intéressantes que j'ai pu prendre en main et faire évoluer. Ce fut une grande opportunité d'appartenir au Security Labs et tout particulièrement à l'équipe d'évaluation. Chez vous, je n'ai pas détecté des Chevaux de Troie mais une réelle passion et c'est celle-ci qui me pousse aujourd'hui à apprendre toujours et encore et à rester dans ce domaine où il y a encore matière à innover et de grandes choses à poursuivre. Merci à l'équipe des 5 mousquetaires pour tous les moments sympathiques passés avec vous. Merci Mr Pascal M. (mécano agréé toute discipline), Francis O. (une encyclopédie vivante captivante), Eric B. (attaquant combinant rigueur et bonne humeur) et enfin merci au connu et reconnu Jean-Claude M. qui est un exemple à suivre (sans aucune parenthèse).

Je tiens également à remercier les petits contacts avec les « gens du couloir » et tout particulièrement Karine V. (la perfection professionnelle et humaine), Carine B. (la gentillesse incarnée), Olivier P. (la classe incarnée), Lionel A. (mon anti-stéphanois préféré), et enfin une citation de plus pour le plus lointain Dr Alexandre B. (pas de copie possible de ses volées). Je remercie également tous ceux que j'ai pu côtoyer au sein de Gemalto dans les bouchons entre La Ciotat et Marseille, pendant des cours de langues étrangères, au cours de séances de bluff ou d'apprentissage du maniement de petites balles jaunes ou d'un ballon rond en salle ou à l'extérieur. Merci à ceux avec qui j'ai pris le grand large, mordu l'asphalte, resté aux bords des quais, vu le lion rouge ou encore partagé des spécialités de Naples ou des spécialités de l'autre côté de la Méditerranée. Remerciements également aux personnes ayant aujourd'hui désertées le 'msn' interne.

Je remercie également tous ceux que j'ai pu rencontrer en conférences, dans le cadre de différents projets externes ou encore pendant divers entretiens. Merci d'avoir posé des questions, d'avoir été intéressé par mes travaux et d'avoir partagé ensemble de superbes instants dans différents pays et villes.

A tous ceux du sud, au plaisir de retravailler avec vous, d'échanger sur tant de sujets différents, de partager la boisson locale anisée ou encore de pratiquer les sports locaux se jouant en doublette/triplette, à 5 contre 5 ou encore à 11 contre 11. Un grand merci au Dr David H. (un 'vrai' Docteur) d'avoir remis mon pouce en place le jour de soumission d'un article, une opération n'aurait pas vraiment été la bienvenue.

Etre en thèse n'aurait pas pu être possible sans avoir de master, je tiens à remercier tous ceux qui m'ont permis de grandir et de réussir trois différents masters, les enseignants, les correspondants, les administratifs et les différents collègues étudiants. Un merci tout particulier à Mr Jean-Jacques D., ce premier qui m'a fait découvrir l'électronique, Mme Isabelle P-S., Mme Virginie F., Mr Marc S., Mr Stéphane R., Mr Viktor F., Mr Abdelkader S., Mr Ian O'C., Mr Pierre B. et enfin Mr Lilian B. ce dernier qui m'a fait découvrir le monde de la sécurité. Merci aux villes de Saint-Etienne, de Lyon et de Glasgow de m'avoir aussi bien traîté.

Merci à toutes les personnes qui m'ont permis d'effectuer mes précédents stages, notamment Dominic B., Ion K., Susan P., David S. sans qui non plus je ne serais pas là. Je n'oublie pas non plus toutes les personnes rencontrées lors de mes différents jobs étudiants qui m'ont vu repartir avec de riches enseignements.

Je remercie tous les minots des Bouches du Rhône notamment David N. et tous les autres adeptes du peuchère. Je remercie ensuite Florent G. et tous les autres garagnats de la Loire, avec qui beausseigne le contact n'avait pas forcément trop pu être cassé. Merci également à ceux de

Glasgow que j'ai pu recroiser lors de mes récents déplacements et une pensée particulière pour mes différents voisins des villes du nord. Ravi d'avoir pu accueillir certains en villégiature à La Ciotat entre autre Maxime R., Mikael B., Florent G., Adrien S. et ses deux patronnes, Mr & Mme M. Amaury et Fanny pour finir avec Olivier L. et le jeune.

Je finirais cette petite liste (non exhaustive pour ne froisser personne) par les personnes à mes yeux les plus chères. Merci aux personnes de ma famille qui m'ont apportés éducation et m'ont permis de faire les bons choix. Un grand merci notamment à ceux ayant pu faire le déplacement le jour de ma soutenance, Jean-François A., Marie-Andrée A., Jean-François B., Thérèse B., Christophe C., Jean-Jacques C., Florine G., mon grand frère qui reste mon premier modèle et enfin ma maman que j'admire pour sa persévérance et son courage. Ce succès est également le tien.

Un sincère merci à vous tous.

A la mémoire de celui qui m'a tout appris

Sommaire

Table des figures

Liste des tableaux

Bibliographie personnelle

Article de journal

[Courbon 2015b] Franck Courbon, Jacques J.A. Fournier, Philippe Loubet-Moundi and Assia Tria, *Combining image processing and laser fault injections for characterizing a hardware AES.* Published in the IEEE Transactions on Computer-Aided Design (TCAD) of Integrated Circuits and Systems, Special Issue on Hardware Security and Trust, January 2015.

Brevet

[Loubet-Moundi 2013a] Philippe Loubet-Moundi and Franck Courbon, *Method for spreading elementary cells in integrated circuit.* European Patent Application EP2874081 Filled date : 11/15/2013 Publication date : 05/20/2015.

Conférences internationales avec actes

[Courbon 2015d] Franck Courbon, Philippe Loubet-Moundi, Jacques J.A. Fournier and Assia Tria, *SEMBA : A SEM Based Acquisition technique for fast invasive Hardware Trojan detection.* In the proceedings of the 22nd European Conference on Circuit Theory and Design (ECCTD), August 2015.

[Courbon 2015c] Franck Courbon, Philippe Loubet-Moundi, Jacques J.A. Fournier and Assia Tria, *A high efficiency Hardware Trojan detection technique based on fast SEM imaging.* In the proceedings of Design, Automation and Test in Europe Conference and Exhibition (DATE), March 2015.

[Courbon 2014b] Franck Courbon, Philippe Loubet-Moundi, Jacques J.A. Fournier and Assia Tria, *Increasing the efficiency of laser fault injections using fast gate level reverse engineering.* In the proceedings of Hardware Oriented Security and Trust (HOST), May 2014.

[Courbon 2014a] Franck Courbon, Philippe Loubet-Moundi, Jacques J.A. Fournier and Assia Tria, *Adjusting laser injections for fully controlled faults.* In the proceedings of Constructive Side-Channel Analysis and Secure Design (COSADE), April 2014.

Workshops

[Courbon 2015a] Franck Courbon, Philippe Loubet-Moundi, Jacques J.A. Fournier and Assia Tria, *Combining 'fine-grained' laser fault attacks partial hardware reverse engineering.* Journée Sécurité Numérique du GDR SoC-SiP : 10ème édition – Vendredi 26 Juin 2015 . L'injection de fautes dans les circuits intégrés : attaques et émulation de phénomènes naturels.

[Courbon 2014c] Franck Courbon, Philippe Loubet-Moundi, Jacques J.A. Fournier and Assia Tria, *Retrieving flip-flop localization and controlling them with lasers ; Methodologies and practical results.* TRUDEVICE–MEDIAN Open Forum, Amsterdam, Netherlands, September 2014.

[Courbon 2013b] Franck Courbon, Philippe Loubet-Moundi, Jacques J.A. Fournier and Assia Tria, *Imaging techniques for the Detection of Hardware Trojans.* TRUDEVICE workshop, Freiburg, Germany, December 2013.

Glossaire

AES : Advanced Encryption Standard
ASIC : Application Specific Integrated Circuit
BICS : Built-in Current sensors
CAD/CAO : Computer-Aided Design / Conception Assisté par Ordinateur
CBC : Cipher Block Chaining / Mode de chainage
CALISSON : CAractérisation, ModéLIsation et Spécifications Sécuritaires de circuits prOtotypes iNtégrés
CIs : Circuit Intégrés
CMOS : Complementary Metal-Oxyde Semiconductor
CTMs/HTs : Chevaux de Troie Matériels/Hardware Trojans
DES : Data Encryption Standard
DFF : Flip-Flop de type D
DFA : Differential Fault Analysis
DUT : Device Under Test
ECB : Electronic Code Book / Dictionnaire de codes
ECC : Elliptic Curve Cryptography / Cryptographie sur les courbes elliptiques
FBBI : Forward Body Biasing Injection
FIB : Focused Ion Beam
FIRE : Fault Injection Reverse Engineering
FPGA : Field Programmable Gate Arrays
GE : Gate Equivalent
HF : HydroFluoric
HOMERE : Hardware trOjans : Menaces et robustEsse des ciRcuits intEgrés
LASER : Light Amplification by Stimulated Emission of Radiation
MEB/SEM : Microscope Electronique à Balayage/Scanning Electron Microscope
MOSFET : Metal Oxyde Semiconductor Field Effect Transistor
MPU : Memory Protection Unit
Noeud technologique : Caractérise la taille de l'élément le plus petit sur un circuit intégré
PANDORE : Protection Against New kinD of Reverse Engineering
SRAM : Static Random Access Memory
RE : Reverse Engineering
RSA : Rivest Shamir Adleman
SCARE : Side Channel Analysis for Reverse Engineering
SOI : Silicon On Insulator
YAG : Yttrium Aluminium Garnet/ Grenat d'Yttrium et d'Aluminium
ZCE : Zone de Charge d'Espace

Introduction générale

Dans un monde où de plus en plus de produits électroniques font partie intégrante de notre quotidien pour communiquer, s'identifier ou pour payer, les tâches effectuées par ceux-ci s'avèrent cruciales. Les besoins en termes de sécurité se font de plus en plus ressentir.

Ces différents produits se matérialisent notamment par des cartes à puce dotées d'une structure relativement comparable à un ordinateur mais avec des zones mémoires et des fonctionnalités moins importantes. C'est le dispositif le plus répandu utilisant des algorithmes cryptographiques. Même si ces derniers sont mathématiquement sûrs, leurs mises en oeuvre requièrent des architectures matérielles qui sont ainsi amenées à manipuler ou stocker des informations sensibles. Ces architectures matérielles sont composées de plusieurs millions de transistors, éléments de base de l'électronique numérique. De part leurs implémentations physiques, ces architectures matérielles sont des points de vulnérabilités qui peuvent être exploiter pour attaquer ces algorithmes cryptographiques "mathématiquement sûrs".

En effet, différentes microscopies invasives ou non-invasives peuvent permettre de distinguer ces transistors. D'autre part, des grandeurs physiques peuvent être mesurées par le biais de canaux dits 'auxiliaires' : leur consommation de courant, leur activité électromagnétique, leur temps de traitement, leur échauffement local ou encore leur émission de lumière localisée. Le fonctionnement de ces circuits influe sur ces grandeurs, ces circuits sont également sensibles à des perturbations par variations d'horloge ou d'alimentation, par injections de pulsations électromagnétiques ou de lumière. Ces perturbations sont appelées attaques par fautes dans le domaine de la sécurité des systèmes embarqués.

Parmi la grande variété d'attaques possibles, l'injection de fautes apparaît être une grande menace au vu des précisions spatiales et temporelles atteignables avec un faisceau de lumière focalisé (laser). Afin de rendre ces attaques plus rapides, plus précises spatialement et plus contrôlées électriquement, nous proposons une approche invasive permettant de récupérer des zones spatiales d'intérêt, en l'occurence des cellules sensibles en matière de sécurité. Une image, dite de base, couvrant la totalité d'une seule couche (ou niveau) du circuit est obtenue par des techniques de préparation d'échantillons, de microscopies et d'alignement. Cette image de base est ensuite traitée pour localiser les différentes occurences de cellules de base présentes dans le circuit intégré. Ainsi, une fois cette image de base obtenue et traitée, les zones/cellules d'intérêt à attaquer sont localisées afin d'être perturber par injection de fautes laser finement contrôlées.

Notre approche invasive est également appelée rétro-conception matérielle partielle car elle réduit drastiquement l'expertise et le coût requis. Outre l'application de cette approche pour l'injection de fautes laser finement localisées, nous utilisons la même approche d'imagerie afin de vérifier l'intégrité des circuits intégrés contre notamment l'insertion de modifications malicieuses appe-

lées également Chevaux de Troie Matériels (CTMs). L'image de base récupérée est comparée à une référence qui peut être un circuit de référence ou des éléments extraits des fichiers de conception du circuit.

Le chapitre 1 traite des caractéristiques des circuits intégrés, des différents types d'attaques réalisables et des circuits de test utilisés. Nous détaillons tout particulièrement les méthodes/attaques invasives de type rétro-conception, et les méthodes/attaques par fautes de type laser. Il apparaît ainsi nécessaire d'améliorer le positionnement spatial des attaques et avantageux de combiner une méthode invasive avec d'autres types d'attaques (en l'occurrence par fautes).

Obtention d'informations spatiales au niveau transistor

Dans un premier temps, nous avons choisi de travailler sur l'obtention d'informations de localisation de cellules de bases. Ce travail est basé sur la proposition d'une méthode invasive appliquée à la couche matérielle des circuits intégrés. Afin de satisfaire les besoins industriels, nous cherchons à obtenir une méthode standard, pratique et reproductible. Nous proposons ainsi une méthodologie composée de 3 étapes. Cette méthodologie est appelée par la suite SEMBA pour "Scanning Electron Microscope Based Analysis". Elle se compose d'une préparation d'échantillon afin d'obtenir une seule couche d'un circuit intégré, d'acquisitions et de traitements d'images. Ces trois étapes sont détaillées dans le chapitre 2 et sa mise en oeuvre a été appliquée à différents circuits intégrés et à différentes fins. Ces travaux sont notamment utilisés dans le cadre du projet PANDORE - Protection Against New kinD of Reverse Engineering.

Amélioration industrielle de la caractérisation de circuits intégrés

Dans le chapitre 3, l'image de base récupérée par la mise en oeuvre de notre méthode invasive est utilisée comme base de positionnement pour un faisceau laser. Avant leur mise sur le marché, les dispositifs sécurisés sont notamment caractérisés vis-à-vis de leur sensibilité aux injections laser. La capacité de distinguer des points d'intérêts (cf chapitre 2) est combinée à la possibilité de contrôler finement l'effet du laser permettant ainsi d'accélérer significativement le temps de caractérisation. Ainsi, nous verrons également dans ce même chapitre 3 l'influence des paramètres laser sur la création de fautes. Au final, nous validons en pratique un modèle de fautes précis sur une cellule de base critique en matière de sécurité (cellule de stockage flip-flop) d'un circuit de technologie identique à celle des circuits du marché 'carte à puce' actuel (90nm). Ces travaux ont été notamment validés par une mise en oeuvre sur un circuit de type carte à puce. Ils font partie des résultats du projet CALISSON2 - CAractérisation, ModéLIsation et Spécifications Sécuritaires de circuits.

Développement et application pratique d'une méthode industrialisable de détection de Chevaux de Troie Matériels

Dans le chapitre 4, la capacité d'obtenir des informations de localisation de cellules de base via la méthodologie SEMBA proposée est utilisée à des fins de détection de Chevaux de Troie Matériels. L'image de base obtenue est comparée à une référence du circuit. Nous évaluons la pertinence de notre approche d'un point de vue industriel mais aussi ses avantages et inconvénients. La définition de notre technique de détection est donc abordée et est également accentuée par la détection semi-automatisée d'un Cheval de Troie Matériel présent dans un cas réel de circuits infectés. La majorité des travaux liés à cet aspect a été réalisée dans le cadre du projet HOMERE - Hardware trOjans : Menaces et robustEsse des ciRcuits intEgrés.

Chapitre 1

Circuits intégrés, bases de rétro-conception et de corruption malveillante

Dans ce chapitre, les Circuits Intégrés (CIs) sont décrits depuis la matière qui les constitue jusqu'à leur organisation globale. Vis-à-vis de ces propriétés matérielles, nous décrierons la sécurité des circuits intégrés et les différents types d'attaques ayant pour but de récupérer des informations sensibles. Nous aborderons tout particulièrement l'état de l'art des techniques de rétro-conception matérielle, de l'injection de fautes laser et de la détection de Chevaux de Troie Matériels.

Sommaire

1.1 Les Circuits Intégrés

Dans cette section, nous nous intéressons au silicium qui est l'élément de base du Circuit Intégré et à ses propriétés de conduction électrique. La réalisation d'un transistor est décrite et l'association de plusieurs transistors permettant la réalisation de cellules de base est exposée. Nous verrons, succinctement, comment les circuits intègrent ces cellules de bases et comment un produit final, de type carte à puce, fonctionne.

1.1.1 Les semi-conducteurs dont le silicium

Le silicium Celui-ci existe à l'état naturel sous forme de sable, cf figure 1.1 : c'est l'élément chimique le plus répandu sur notre Terre. Le sable brut est traité puis purifié afin d'obtenir du silicium polycristallin contenant moins d'un milliardième d'impureté.

FIGURE 1.1: Matière de base : le sable

Le silicium est déposé dans un creuset en graphite et liquéfié à très haute température (point de fusion du silicium à 1414 degrés Celsius). A partir d'un germe, on effectue un tirage progressif du lingot sous couvert de conditions particulières (température, vitesse de rotation, déplacement...) on obtient ainsi des lingots de différents diamètres suivant la vitesse de tirage. Cette méthode est appelée technique de Czochralski [36]. Le barreau de silicium ainsi obtenu, cf figure 1.2, est équeuté puis découpé en tranches de quelques centaines de μm d'épaisseur appelées plaquettes ou plus communément 'wafers'.

FIGURE 1.2: Barreau de silicium

Le diamètre de ces 'wafers' est généralement exprimé en pouce, et varie selon l'unité de fabrication d'origine entre 6, 8 ou 12 pouces soit 150mm, 200mm ou 300mm. Le diamètre du wafer permet d'intégrer un nombre de puces plus importants à nombre d'étapes équivalentes. Une fois découpés, les wafers sont polis pour obtenir une surface sans aucune aspérité. L'épaisseur des plaquettes ainsi obtenue est généralement de $380\mu m$ permettant ainsi la réalisation des différentes étapes de fabrication tout en limitant les contraintes mécaniques qui pourraient survenir. A la fin du processus de fabrication, les plaquettes sont testées. Une opération d'amincissement appelée 'backlap' peut être réalisée : l'épaisseur pouvant atteindre jusqu'à $50\mu m$ permettant l'insertion

de telles puces dans des supports papiers telles que pour le passeport électronique. Un wafer est généralement de 300mm de diamètre pour une épaisseur de quelques $300\mu m$. Le silicium polycristallin dispose de 4 électrons sur sa couche de valence, cf figure 1.3.

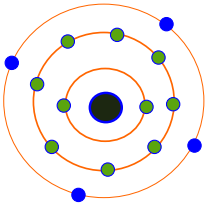


FIGURE 1.3: Répartition électronique autour de l'atome de Silicium

Ces wafers n'ont pas les propriétés électriques idéales pour la réalisation de transistors, qui sont la base des systèmes intégrés. Mais ce qui rend les semi-conducteurs intéressant, comme le Silicium, est la possibilité de contrôler leurs caractéristiques électriques au niveau local.

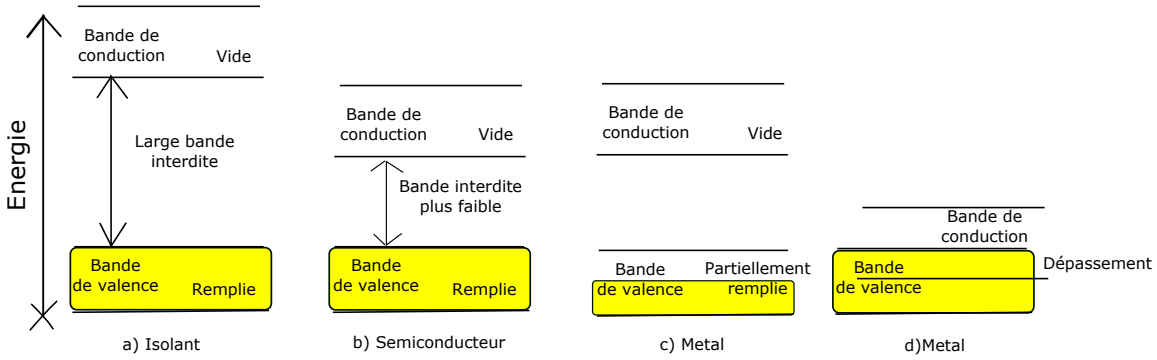


FIGURE 1.4: Niveau d'énergie pour les bandes de valence et de conduction

Les semi-conducteurs Les matériaux solides peuvent être classés en trois groupes : les isolants, les semi-conducteurs et les conducteurs. Ils disposent de bandes d'énergies (appelées 'gap' également) indiquant à quel niveau des électrons peuvent exister, on parle alors de bande de conduction et de bande de valence, cf figure 1.4. La séparation entre celles-ci est appelée bande interdite et représente l'énergie nécessaire pour transférer un électron d'une bande à l'autre. Les propriétés électriques d'un matériau sont fonctions des populations électroniques des différentes bandes. La conduction électrique résulte du déplacement des électrons à l'intérieur de chaque bande. Un électron ne peut se déplacer que s'il existe une place libre appelée 'trou' dans sa bande d'énergie.

Un matériau dont la bande de conduction est vide est appelé isolant. Dans ce cas l'énergie de 'gap' est supérieur à 9eV (l'électron-volt est une unité de mesure d'énergie) ne permettant pas le passage des électrons de la bande de valence à la bande de conduction, les bandes d'énergies sont toutes vides ou toutes pleines. Pour un conducteur, il n'existe pas d'énergie de gap, la bande de conduction est partiellement pleine, la conduction est particulièrement élevée. De leur côté, les semi-conducteurs ont un 'gap' moins large, les électrons ne peuvent pas franchir la bande interdite, la conduction est faible et varie fortement avec la température. Mais des excitations thermiques ou électriques permettent à certains électrons de passer de la bande de valence à

la bande de conduction. Lorsque l'on dope un semi-conducteur avec des atomes d'impuretés convenablement choisis on modifie ainsi ses propriétés de conductivité.

Le silicium possède 4 électrons sur sa couche périphérique.

- Si on introduit un atome ayant 5 électrons sur sa couche de valence (par ex. Phosphore), 4 de ses électrons participeront aux liaisons dites covalentes (liaison chimique permettant de lier deux atomes), le cinquième restera disponible. Cet atome appelé "donneur" peut facilement passer dans la bande de conduction et augmente la conductivité électrique. A température ambiante, toutes les impuretés sont ionisées et la conductivité devient de type N lorsque l'on augmente le dopage.
- Si on introduit un atome ayant 3 électrons sur sa couche de valence (par ex. Bore), celui-ci ne peut saturer que 3 des 4 liaisons. Il manque donc une liaison par atome d'impureté à un niveau d'énergie situé juste au dessus de la bande de valence, appelé niveau accepteur. A 0 Kelvin, ces niveaux accepteurs sont vides, lorsque la température augmente ils peuvent être occupés par des électrons provenant de la bande de valence. Les niveaux vides de la bande de valence engendrent des trous, la conductivité devient de type P lorsque l'on augmente le dopage.

Une fois ces deux types de semi-conducteurs juxtaposés (formant donc une jonction PN), une partie des trous contenus dans la zone P et une partie des électrons de la zone N diffusent instantanément de part et d'autre, cf figure 1.5.

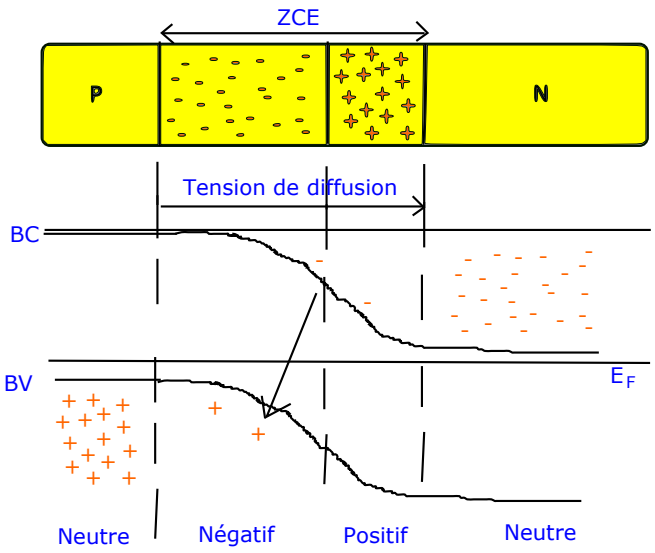


FIGURE 1.5: Jonction PN et bandes de conduction

Aux alentours de la jonction, les porteurs de charge se neutralisent. On dit qu'à l'équilibre une zone sans charge mobile existe, elle est appelée zone de charge d'espace (ZCE). Un champ électrique orienté de N vers P maintient la séparation entre les trous et les électrons qui participent à la conductivité électrique. Il faut moins d'énergie pour déplacer un électron qu'un trou dans le réseau cristallin, de ce fait les électrons ont donc une plus grande mobilité.

1.1.2 Le transistor, l'inverseur et les cellules de base

Le transistor De telles jonctions sont la base des composants électroniques actifs, dont les propriétés sont directement utilisées pour la réalisation de transistors NMOS et PMOS. Ces transistors se décomposent en trois éléments, la source, le drain et la grille, cf figure 1.6. Dans le

cas d'un transistor NMOS, le substrat est de type P, la source et le drain sont deux électrodes de type N insérées dans le substrat. Pour un transistor PMOS, une zone n-well est implantée (ce type de zone permettant la réalisation de zone active pour le transistor PMOS) dans le même substrat P pour ensuite pouvoir concevoir le drain et la source de ce transistor PMOS avec deux électrodes de type P.

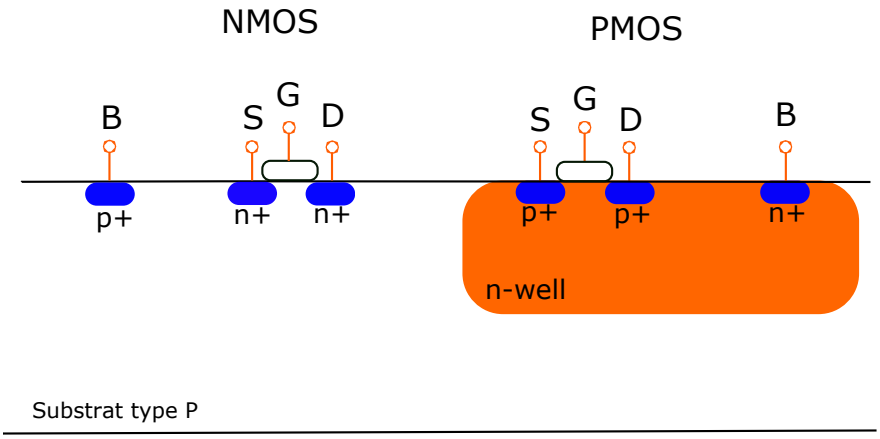


FIGURE 1.6: Transistors PMOS et NMOS

La structure physique est alors équivalente à un ensemble NPN. On a donc deux jonctions tête-bêche qui ne permettent pas en l'état la conduction de courant. La distance séparant la source du drain est appelée longueur de grille. Cette zone est recouverte d'une fine couche d'isolant puis d'une couche de polysilicium constituant la grille. Sur un circuit intégré, la longueur de grille (L_G) du transistor le plus petit, cf figure 1.7, correspond à la valeur du noeud technologique qui caractérise la taille de l'élément le plus petit sur un circuit intégré.

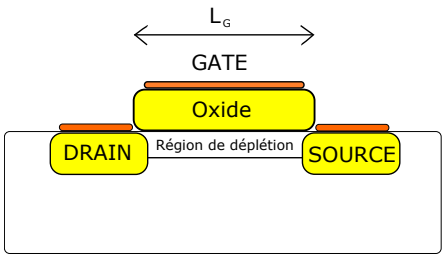


FIGURE 1.7: Transistor au niveau implant

Si la tension appliquée sur la grille est positive par rapport à celle du substrat, les électrons présents dans le substrat au voisinage de l'isolant transitent à travers celui-ci et forment un canal de diffusion entre la source et le drain. La tension alors appliquée sur la grille permet de faire varier la conductivité du canal, modulant ainsi le courant entre la source et le drain. Ce fonctionnement basé sur l'action appliquée à un canal unique s'appelle 'à effet de champ' (Field Effect) et son implémentation physique, grille isolée du substrat avec un di-électrique, porte le nom de Metal Oxyde Semiconductor (MOS). On parle ainsi de transistors MOSFET (Metal Oxyde Semiconductor Field Effect Transistor). A contrario, la tension de grille doit être négative pour un transistor PMOS. Il résulte ainsi la possibilité de controller l'état des transistors, bloqués ou passants.

L'inverseur L'inverseur est constitué de deux transistors, cf figure 1.8, PMOS et NMOS. Un seul des transistors est conducteur à la fois, lorsque l'entrée est à l'état haut, seul le transistor NMOS est passant. La tension appliquée à sa source, un niveau de tension bas, se retrouve sur le drain qui est également la sortie de l'élément inverseur. Inversement, lorsque l'entrée est à l'état bas, seul le transistor PMOS est passant. La tension appliquée à sa source, un niveau de tension haut, se retrouve sur le drain qui est également la sortie de l'élément inverseur.

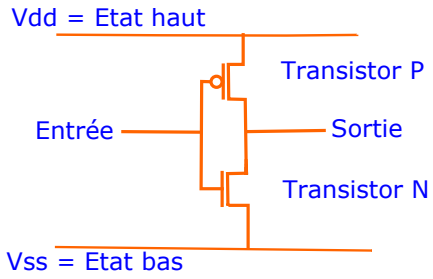


FIGURE 1.8: Schéma électrique d'un inverseur

De part leur caractéristique de fonctionnement inversée, on dit qu'ils sont complémentaires. D'où le nom de 'Complementary Metal Oxide Semi-conductor' (CMOS) qui est la technologie de fabrication de circuits intégrés (basée donc sur l'utilisation de transistors MOSFET).

Les cellules de base Les états bloqués ou passants des transistors permettent la création de toutes les fonctions booléennes. L'association de plusieurs transistors permet la création de fonctions appelées cellules de base [24]. Ces cellules de base permettent la réalisation d'opérateurs logiques (OU, NON-ET, OU-EXCLUSIF...) communément appelées 'cellules' ou 'cellules logiques'. L'utilisation de ce couple de transistors MOSFET P et N se retrouve à la sortie de chaque cellule de base imbriquée dans le circuit. Il faut ainsi au minimum 2 transistors pour créer la plus petite cellule de base (l'inverseur) et de l'ordre d'une vingtaine pour réaliser des blocs plus complexes tels que les bascules bistables flip-flop [48]. La figure 1.9 donne le schéma logique d'une porte NON-ET et la réalisation d'une porte OU-EXCLUSIF à partir de 4 portes NON-ET. Toute porte logique peut être réalisée à partir de portes NON-ET.

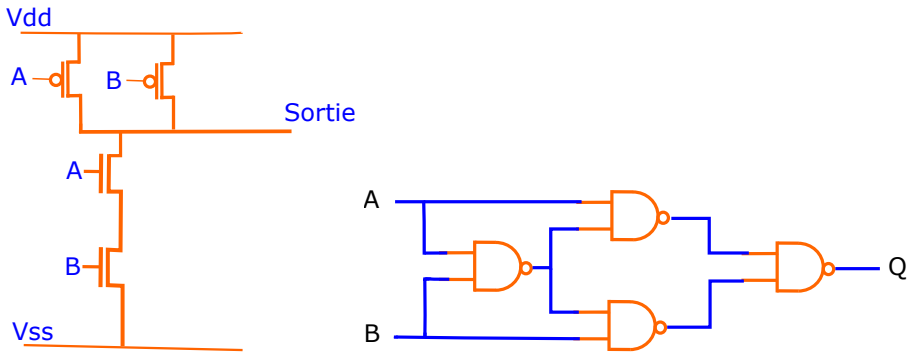


FIGURE 1.9: Schémas logiques de porte NON-ET et OU-EXCLUSIF à partir de portes NON-ET

Cependant, pour satisfaire les besoins de coût notamment, chaque cellule est optimisée. L'implémentation de ces différentes cellules varie selon les fabricants de circuits (appelés fondeurs), les optimisations des outils de Conception Assistée par Ordinateur (CAO) et le noeud technologique.

Ces cellules sont tout d'abord différentes afin de réaliser différentes fonctions en respectant les contraintes technologiques telles que la surface silicium utilisée, la consommation de puissance ou encore le temps d'accès. Pour une même fonction, la cellule diffère également vis-à-vis de la présence de signaux ou d'entrées supplémentaires (par exemple de remise à zéro, de 2, 3, 4 entrées ou encore adaptée vis-à-vis du courant dit de 'drive' (courant permettant le bon fonctionnement des portes suivantes)) . Ainsi chaque cellule est conçue pour réaliser une fonction donnée, l'ensemble de ces fonctions constitue une librairie, que l'on appelle 'kit de design'. Quand le fondeur conçoit sa propre librairie, elle est dite 'propriétaire'. Les outils de CAO chargent donc ces librairies pour associer les différentes cellules afin de concevoir numériquement un circuit intégré et ainsi créer différents blocs fonctionnels.

Ces cellules de base sont associées dans un ensemble appelé 'Logique Synthétisée' qui inclut notamment l'unité de traitement central (CPU), les possibles co-processeurs et des mémoires internes. Les cellules de base ne sont pas organisées par ligne et par colonne mais des prises au substrat pour les tensions d'alimentations et de masse des transistors sont présentes sous forme de colonne avec un espacement fixe. La logique est généralement dite mélangée (scrambling). Dans le paragraphe suivant nous abordons la nécessité de concevoir le circuit couche par couche. Nous axons les descriptions faites pour un circuit standard de type carte à puce.

1.1.3 De la conception à l'encartage

Utilisation des différentes couches d'un CI Les zones spécifiques, appelées caissons, sont dopées (par implantation ionique de Bore ou de Phosphore) pour réaliser les zones N et P. La grille des transistors est constituée de silicium polycristallin. Ensuite, une succession de dépôt d'isolant et de couches métalliques est effectuée. Par définition le premier niveau métal en partant de la grille est appelé niveau 'metal1'. Les connexions entres couches sont possibles grâce à la présence de vias, et on parle notamment de plots (en tungstène) pour la connexion entre la grille et le niveau 'metal1'. Les niveaux 'metal' supérieurs sont appelés 'Metal2', 'Metal3', 'MetalX'... Généralement les cellules de bases sont conçues jusqu'au niveau 'Metal1' voire 'Metal2'. Les niveaux 'Metal2' et supérieurs contiennent les connexions entre les cellules de base. Les deux derniers niveaux sont affectés pour les lignes d'alimentation et d'horloge. Sur la figure 1.10, la même zone d'un circuit intégré est photographiée sur plusieurs niveaux d'un circuit. Nous notons tout particulièrement le niveau substrat où des informations au niveau transistor sont présentes.

La conception des circuits intégrés Outre la logique synthétisée, les circuits intègrent des parties analogiques et des espaces mémoires organisés en colonnes et lignes d'éléments identiques stockant chacun un bit de donnée. Cette configuration est visible sur la figure 1.11. Il existe différents types de mémoire, les mémoires volatiles ou non dont la densité impacte les choix d'implémentation des fabricants de cartes à puce. En effet, un bit de donnée de ROM nécessite 1 transistor par cellule alors que pour la RAM, il en faut 6. C'est pour cela que les circuits carte à puce sont très contraints en mémoire RAM. Avec la complexité des circuits actuels, plusieurs intervenants peuvent être amenés à travailler sur le même circuit. On parlera d'IP propriétaires pour les briques provenant de tierces personnes.

Les outils de conception permettent le cheminement des étapes suivantes :

- la définition de chaque bloc du circuit intégré,
- le placement de chaque élément,
- la synthèse de l'arbre d'horloge,
- le routage de chaque élément,

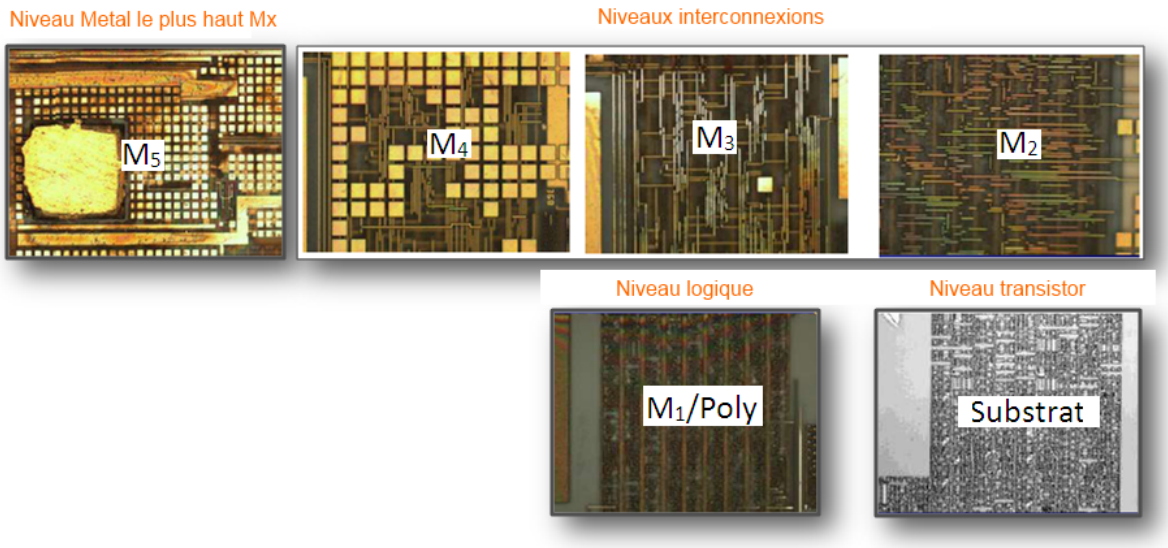


FIGURE 1.10: Différentes couches d'un circuit intégré, figure extraite de Nohl *et al.* [63]

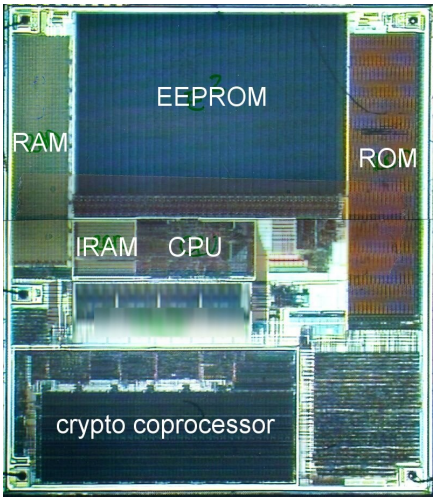


FIGURE 1.11: Différentes parties d'un circuit intégré de type carte à puce

- les vérifications physiques LVS (Layout vs. Schematic) et DRC (Design Route Checking)
- la génération finale de fichiers (dont le GDSII) permettant la fabrication de différents masques de fabrication (utilisés pour les différentes étapes de lithographie).

Fabrication du masque et de circuits Un des fichiers de sortie de ces outils est le GDSII (Graphical Database System), c'est un fichier binaire donné au fondeur de CIs, nécessaire à la réalisation physique du circuit intégré. Un exemple de ce type de fichier est donné figure 1.12. Une fois ce type de fichier chargé par un outil de conception, les polygones des schémas d'implantation des différents éléments du circuit sont visibles. Ces éléments peuvent être visibles niveaux par niveaux. Ce fichier GDSII englobe notamment les formes géométriques des éléments à fabriquer sur chaque niveau du circuit.

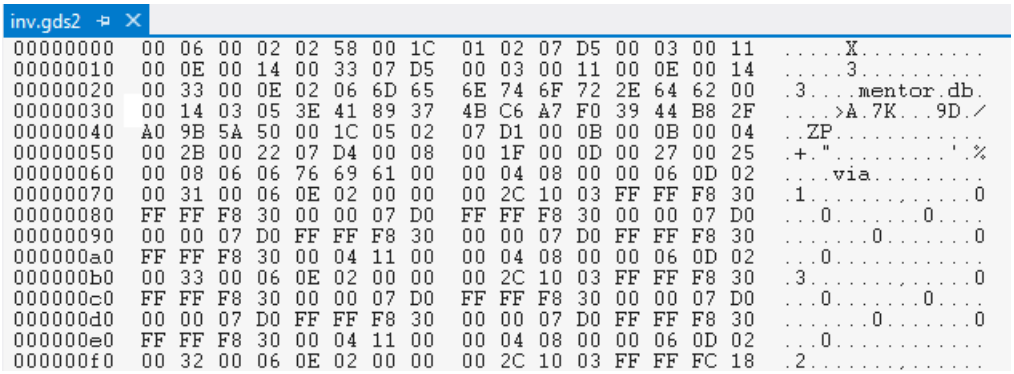


FIGURE 1.12: Exemple d'un fichier GDSII

Le GDSII notamment va ainsi permettre au fabricant de circuits intégrés de réaliser les opérations physico-chimiques sur le substrat pour réaliser le circuit attendu. Tout d'abord des masques pour les différentes étapes de fabrication sont créés à l'aide des fichiers de design. Une fois ces masques créés, ils sont utilisés pour pouvoir implémenter matériellement les fonctions conçues. Les circuits sont ainsi fabriqués sur les wafers tels que présentés en tout début de ce manuscrit. En fonction de la taille du circuit intégré, jusqu'à plusieurs milliers de circuits intégrés peuvent ainsi être fabriqués sur le même wafer. Le nombre de circuits intégrés fabriqués en parallèle est dépendant du 'stepper' utilisé (équipement insolant un nombre de champs par pas successifs). Une fois les circuits intégrés fabriqués, ils sont sciés et subissent des tests de fonctionnalité.

Un autre type de fichier sortant d'un logiciel de CAO est un fichier de type DEF (Design Exchange Format). Dans un tel fichier, on retrouve le nom de chaque cellule utilisée, son orientation tout comme sa localisation spatiale en μm vis-à-vis d'une origine prise sur le circuit, cf figure 1.13. Le verilog est de son côté un langage de description matériel de circuits logiques utilisé pour la conception de circuits intégrés spécifiques appelés ASICs. L'ASIC (Application Specific Integrated Circuit) est un circuit CMOS dédié à une application spécifique, non reconfigurable à contrario des FPGAs (Field Programmable Gate Arrays)). Similairement au fichier de type DEF, on peut y repérer le nom des instances utilisées dans le circuit, cf figure 1.13.

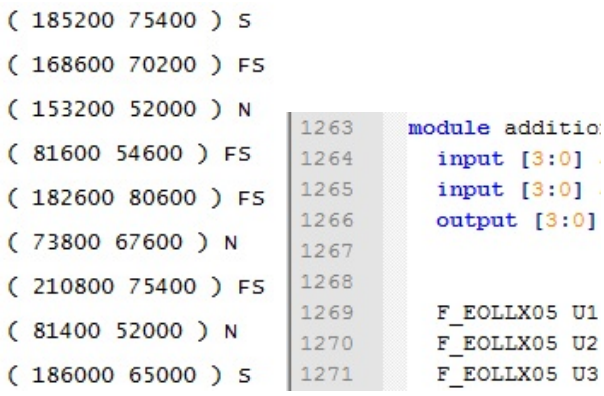


FIGURE 1.13: a) Partie d'une description verilog d'un circuit (à gauche), b) Partie d'une description de type DEF d'un circuit (à droite)

Encartage du composant Un circuit de type carte à puce est présent dans un corps de carte plastique sous une broche de contacts d'aspect dorée appelée également module. Cette broche de contacts est divisée en 8 parties et permet le dialogue avec un lecteur (ou terminal) par liaison électrique. A l'intérieur de la carte, une antenne interne peut également être présente pour une communication dite sans contact, cf figure 1.14. Le dialogue entre le terminal et la carte s'effectue par le biais de trames de données appelées APDU (Application Protocol Data Unit) et est définit dans la norme ISO7618-4.

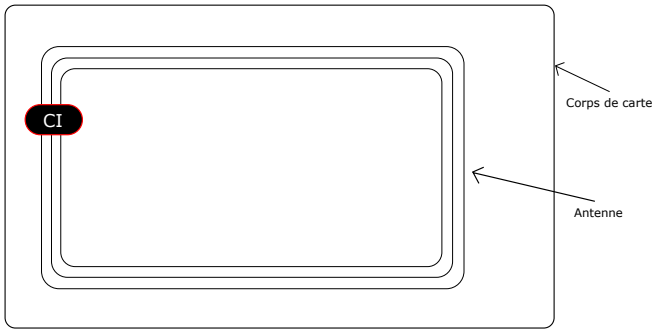


FIGURE 1.14: Vue globale d'une carte à puce

Sous ce module, on retrouve la puce elle-même de quelques mm^2, cette dernière comporte des fils de connection partant du niveau métallique le plus haut vers l'arrière de la broche de contacts dorée. Généralement pour la carte à puce, on peut s'apercevoir que le recto de la carte plastique ne correspond pas avec la face avant (active) du circuit intégré, cf figure 1.15.

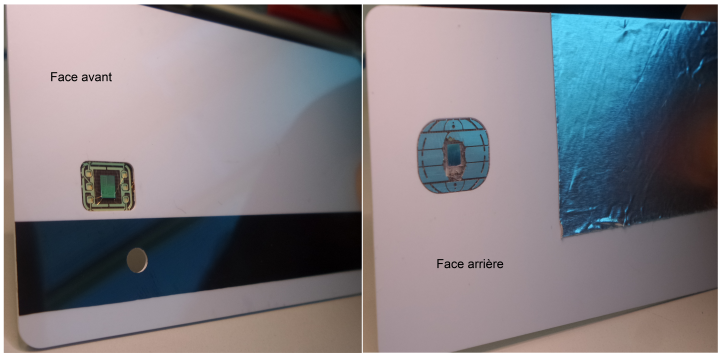


FIGURE 1.15: a) Vue face avant d'un circuit intégré (à gauche), b) Vue face arrière d'un circuit intégré (à droite)

1.1.4 Une base physique pour un besoin de communication sécurisée

La communication des circuits intégrés décrits précédemment repose sur un protocole mais aussi sur l'utilisation d'algorithmes de chiffrement afin d'encrypter des données. Ces algorithmes permettent l'échange d'informations chiffrées même sur un canal de communication non sécurisé et peuvent être implémentés soit matériellement soit de manière logicielle. Ces algorithmes répondent aux propriétés de confidentialité, d'intégrité, d'authentification et de non répudiation. Ils sont classés en deux catégories, les algorithmes de chiffrement asymétriques et symétriques.

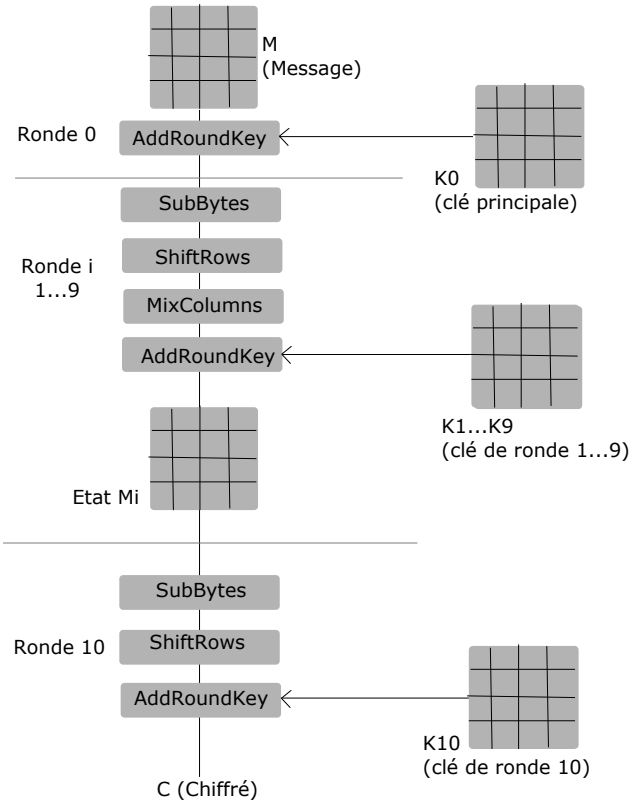


FIGURE 1.16: Détail de l'algorithme de chiffrement AES

Les algorithmes de chiffrement asymétriques utilisent deux clés liées entre elles mathématiquement. L'une appelée clé publique est utilisée pour le chiffrement, elle est connue de tous. La seconde dite clé secrète permet de déchiffrer un message et n'est connue que du propriétaire. Les principaux algorithmes asymétriques implémentés dans les produits carte à puce sont le RSA (Rivest, Shamir, Adleman) [64] et les courbes elliptiques [60] (ECC : Elliptic Curves Cryptography).

Pour les algorithmes de chiffrement symétriques, la même clé appelée clé secrète est utilisée par l'expéditeur et le destinataire, elle sert aussi bien pour le chiffrement que le déchiffrement de données. A l'inverse du chiffrement asymétrique, aucune clé n'est publiée, il faut donc se mettre d'accord sur un protocole d'échange entre les protagonistes. Le chiffrement symétrique peut être organisé soit par flot soit par bloc où les données sont organisées en blocs de n bits. A l'issu du chiffrement par bloc, le chainage de ces données doit être effectué (modes ECB, CBC...)

Parmi les algorithmes de chiffrement symétriques par bloc embarqué dans les produits carte à puce on trouve le DES (Data Encryption Standard) et son successeur désigné AES (Advanced Encryption Standard). Ces algorithmes de chiffrement sont standardisés par le NIST [74] et sont largement présents dans nombreux systèmes embarqués. Dans ce travail nous nous sommes notamment intéressés à des échantillons de tests qui implémentent un AES 128bits et dont l'algorithme est présenté dans la figure 1.16.

L'AES est basé sur une permutation par réseau réalisée en 4 transformations successives plus une étape où une sous-clé est recalculée, cf figure 1.16.

- SubBytes : fonction non-linéaire interchangeant chaque bloc de données avec une valeur stockée dans une table dite de substitution.
- ShiftRows : fonction qui opère un décalage d'1, 2 ou 3 rangs des octets
- MixColumns : opération de transformation appliquée à chaque colonne
- KeyScheduling : opération de dérivation de la sous-clé de ronde
- AddRoundKey : combinaison de la sous-clé de ronde utilisée par une opération XOR bit à bit

Lors du dernier tour, l'itération ne comporte pas d'opération MixColumns. Cette propriété sera utilisée dans le reste du manuscrit. Cet algorithme est largement utilisé dans les systèmes embarqués.

1.2 Sécurité et intégrité des Circuits Intégrés

Dans la section précédente, nous avons présenté les caractéristiques physiques des CIs, celles-ci sont susceptibles de permettre la fuite d'information de part leur implémentation physique et logique. Ces fuites ou émanations peuvent apparaître sous certaines conditions tandis qu'à contrario ces CIs sont sensibles à des perturbations externes basées sur les mêmes grandeurs physiques. Sur cette base matérielle repose des processus prouvés sûrs mathématiquement, mais le risque de fuites d'informations peut être préjudiciable selon les conditions d'utilisation. Ainsi, des produits répondant à différents critères de sécurité permettent de se prémunir d'éventuelles menaces.

1.2.1 Les familles d'attaques

De multiples attaques sont décrites dans la littérature, on les classe généralement en 4 catégories [50]. Tout d'abord, les attaques logiques qui exploitent une faille au niveau de l'implémentation logicielle [17]. Les attaques logiques ne seront pas abordées dans ce manuscrit car les implémentations logiques sont notamment vues comme de plus en plus fiables. La deuxième catégorie est les attaques par canaux auxiliaires (side-channel) où les variations de temps d'exécution, de consommation de puissance ou d'émissions électromagnétiques permettent d'obtenir des informations sur les données manipulées (SPA [57], DPA [49], CPA [22]). Les attaques invasives où le composant est modifié ou analysé [6] afin d'en extraire par exemple le design à des fins de clonage voire d'extraire des secrets. Enfin, les attaques par fautes où une perturbation externe est utilisée pour modifier une donnée ou changer le déroulement d'une exécution normale d'une tâche [8]. L'utilisation conjointe de 2 types d'attaques est appelée attaque combinée. Le tableau 1.1 répertorie les différentes grandeurs physiques observables sur tout circuit intégré.

Attaques par canaux auxiliaires

Un circuit intégré possède une ou plusieurs interfaces ou canaux de communication standard pour échanger des informations, avec ou sans contact comme vu dans la partie 1.1.3. Cependant, des canaux auxiliaires peuvent permettre de récupérer également des informations sur le CI. Sa consommation, son rayonnement électromagnétique, son temps de traitement, sa chaleur ou encore sa lumière localement émise font partie de ces grandeurs physiques permettant de retrouver des informations d'intérêt. Ces fuites proviennent du basculement d'état des transistors ou du courant traversant les lignes d'alimentation. Ce type d'attaque est non invasif et permet ainsi d'analyser un circuit sans aucune préparation dans certains cas. Par exemple, Guilley *et al.* [42] explique que les transitions entre un état logique et son complémentaire peut entraîner un léger

Tableau 1.1: Les différentes grandeurs physiques observables

Grandeur physique	Attaque passive	Attaque active
Alimentation	Analyse du courant consommé	Perturbation de la tension d'alimentation
Temps d'exécution (horloge)	Mesure du temps d'exécution	Perturbation du signal d'horloge et violation des contraintes temporelles
Rayonnement électromagnétique	Analyse des émissions électromagnétiques	Injection électromagnétique
Lumière	Analyse de la lumière émise par le circuit	Injection de lumière
Température	Analyse de la chaleur émise par le circuit	Chauffage du circuit
Tension de substrat	NA	Modification locale de la tension du substrat
Ondes acoustiques	Analyse du bruit émis par le circuit	NA
Implémentation physique	Rétro-conception (inspection visuelle)	Attaque par probing, Modification du circuit

pic sur la consommation de courant à cause des courants de charge et de court-circuit. Ce basculement serait ainsi repérable par un attaquant.

La chronologie pour effectuer les attaques par canaux auxiliaires peut se généraliser de manière simplifiée par les étapes suivantes :

- Mise en place d'un banc de mesure,
- mise en marche du circuit à analyser (avec boucle de fonctionnement si besoin),
- acquisition du signal contenant l'information,
- visualisation des courbes,
- re-synchronisation temporelle du signal,
- traitement des données statistiques,
- hypothèse et extraction de secrets.

Ainsi pour chaque étape listée, il existe une grande variété de techniques pour mesurer et traiter les différentes mesures temporelles, de consommation instantanée, d'ondes électromagnétiques ou de photons émis [33].

Attaques par fautes

Les attaques par fautes reposent sur l'idée que si un résultat fauté est obtenu, alors un attaquant peut utiliser cette information pour récupérer des informations sensibles voire secrètes. Dans la littérature, il est dit que ces fautes peuvent être soit temporaires, soit permanentes jusqu'à la prochaine mise hors tension du CI, soit encore permanentes mais irréversibles. Il existe différentes sources d'injections de fautes, on peut répertorier :

- Les violations de l'alimentation (glitch de tension) ou de l'arbre d'horloge (glitch d'horloge),
- les injections d'ondes électromagnétique (attaques par fautes EM),
- les injections de lumière (attaques par fautes optiques).

Glitch tension/fréquence :

Un changement ponctuel de tension [9] ou de fréquence [5] peut faire basculer plus aisément l'état d'un transistor et ainsi faire en sorte que le signal arrivant sur une cellule se retrouve non pris en compte. On peut par ce biais "fauter" un calcul en cours ou passer outre une condition d'accès. Cette technique a l'avantage de présenter un faible coût (de l'ordre de la centaine d'euros) et une facilité de mise en oeuvre.

ElectroMagnétique (EM) :

Une bobine constituée d'une ou plusieurs spires est utilisée pour l'injection d'ondes EM. Les courbures d'ondes ainsi créées sont dirigées vers le circuit intégré permettant sous certaines conditions la génération de fautes. Un banc d'injection EM est constitué d'un générateur de nano-impulsions associé, d'un module électronique de déclenchement et d'une sonde EM.

Forward Body Biaising Injection (FBBI) :

Notamment connue par les concepteurs de circuits intégrés, une tension de quelques mV peut être appliquée au substrat d'un circuit intégré pour moduler les tensions de seuil des transistors MOS. Dans le cas des attaques par fautes, il est également possible de créer des fautes avec cette approche en appliquant une tension de plusieurs Volts. Un générateur d'impulsions relié à une pointe permet d'appliquer cette tension au substrat. Ces impulsions locales de tension vont perturber le fonctionnement de certaines cellules du circuit.

Fautes optiques :

Un faisceau de lumière appliqué au voisinage d'une jonction PN vient créer un photocourant [43] moyennant des conditions spécifiques d'énergie et de localisation. Ce courant peut faire basculer l'état d'un transistor. Ce basculement d'état d'un ou plusieurs transistors peut lui-même amener un changement d'état au niveau de la sortie d'une cellule de base. Enfin ce changement d'état peut permettre de contourner un mécanisme de sécurité, de perturber une opération de calcul ou bien de modifier une donnée manipulée. Une des premières attaques a été réalisée à l'aide d'un flash lumineux (de type appareil photo) [73] et a permis de mettre en évidence la possibilité de modifier une valeur stockée dans une cellule mémoire. De nos jours, des faisceaux de lumière focalisée (laser) sont préférés. La mise en oeuvre de ces modifications nécessite une certaine précision spatiale (quelques μm) et temporelle (quelques ns) dépendant du cas d'étude.

Attaques invasives

Les attaques invasives, quant à elles, nécessitent l'accès au circuit et peuvent dans certains cas le modifier de manière irréversible. Cette catégorie comprend notamment :

- Les attaques par sondage (ou probing),
- la modification de circuit,
- la rétro-conception.

Attaques par probing :

Les attaques par probing nécessitent de placer des pointes (appelées également sondes et pouvant atteindre des tailles de quelques dixièmes de μm) sur des pistes d'intérêt. La sonde permet soit de récupérer le signal présent sur la piste soit d'injecter un signal donné. Le circuit doit bien entendu être fonctionnel. Il existe ainsi des stations de probing composées de pointes de différentes tailles. Le déplacement doit permettre de finement placer et maintenir la pointe afin de permettre la récupération/injection du signal et de l'effectuer avec une certaine reproductibilité. On parle également de micro-probing pour des résolutions micrométriques.

Modification de circuit :

La modification de circuit nécessite l'utilisation d'équipements permettant de modifier physiquement un circuit intégré. On pense notamment aux lasers permettant de couper des pistes métalliques mais également à un équipement spécifique tel que le 'Focused Ion Beam' (FIB). Il est possible de faire de l'imagerie avec ce type d'équipements (fonctionnement globalement similaire à un Microscope Electronique à Balayage (MEB, abordé dans la partie 1.3.2) à part qu'un faisceau d'ions est utilisé au lieu d'un faisceau d'électrons. Avec un FIB, il est possible d'ajouter ou d'enlever de la matière en combinant le faisceau d'ions avec un gaz. Des pistes métalliques peuvent par exemple être déconnectées (désactivation d'un générateur d'aléas), reliées à de nouvelles portes logiques (modifications de fonctions) ou ajoutées (création de nouvelles fonctions). Il est également possible de contrôler le retrait d'une certaine épaisseur de silicium pour, par exemple, accéder à la couche active des transistors [44]. Le FIB est notamment utilisé pour préparer des échantillons minces, les résolutions possibles sont de l'ordre du nm avec ce type d'équipement.

Rétro-conception :

La rétro-conception (ou reverse-engineering) est une succession d'opérations qui consiste à retrouver les éléments de conception du circuit pour en extraire tout ou partie de celui-ci. La rétro-conception nécessite généralement un retrait successif de chaque niveau du composant. L'utilisation de microscopes optiques ou électroniques à balayage associée à un traitement d'image permet de remonter tout d'abord au schéma électrique du composant puis dans certains cas de remonter à une description de type VHDL. La rétro-conception est souvent confinée à cette méthode standard précédemment décrite, c'est à dire à l'analyse topologique. Cependant les techniques par canaux auxiliaires permettent aussi de reconnaître des fonctions exécutées par du code embarqué voire de retrouver l'implémentation matérielle d'un algorithme cryptographique [37].

Attaques combinées

Généralement, on retrouve dans la littérature l'utilisation d'un type d'attaque et l'utilisation de protections afférentes à cette seule attaque, par exemple contre les attaques par fautes ou

contre les attaques par canaux auxiliaires. Ces protections sont appelées contremesures. Il existe cependant quelques références de combinaisons d'attaques dont l'idée générale est d'utiliser plusieurs moyens d'attaques pour se défaire de contremesures classiques. Ainsi, Skorobogatov [72] utilise un faisceau laser pour augmenter la consommation de courant d'une partie sensible de la puce. Une combinaison d'attaque active et passive a donc été réalisée. La plupart des attaques combinées réunissent attaque en fautes et attaque par canaux auxiliaires [65, 32]. De même, des travaux ont fait part d'attaques invasives avant la perturbation du circuit intégré. En 2010, Loubet-Moundi *et al.* [40] a effectué une attaque par fautes couplée à une approche invasive. Une source de lumière UV est utilisée pour modifier les bits d'une mémoire EEPROM $0.35\mu m$ de '1' vers '0' après avoir modifié physiquement le circuit intégré afin d'accéder à la surface de ces mémoires. Tarnovsky [78] injecte des fautes par micro probing après avoir réalisé une rétro-conception poussée.

La réalisation d'attaques combinant rétro-ingénierie et observation par canaux auxiliaires a été approchée par Strobel *et al.* [75]. L'utilisation d'acide nitrique permet de mettre en évidence les principales fonctions implémentées sur un circuit pour en déduire que la brique sécuritaire recherchée était présente sur un deuxième circuit. Une analyse par canaux auxiliaires a ensuite été effectuée sur ce deuxième circuit. Néanmoins, il existe très peu d'articles combinant attaque invasive et analyse par canaux auxiliaires. De même, il en existe encore moins combinant rétro-conception et attaque en fautes. Nous avons choisi de poursuivre cette approche pour évaluer la complexité et le coût de la rétro-conception.

1.2.2 Processus d'évaluation de circuits intégrés

Les circuits intégrés sont utilisés dans différents moyens de communication, d'identification ou de paiement. Ils nécessitent un certificat de la part d'un organisme extérieur agrée évaluant leur niveau de sécurité. L'obtention du dit certificat permet ainsi de pouvoir mettre sur le marché un produit testé pour sa conformité aux spécifications et sa robustesse aux attaques. Sa non-attribution ou son retard d'attribution impacte directement sur les marges de vente d'un produit. Il est généralement considéré que l'introduction d'un nouveau produit génère les marges les plus avantageuses dans les six premiers mois de la mise sur le marché. Dans ce domaine fortement concurrentiel le moindre retard se traduirait donc par un fort impact.

Les critères d'évaluations diffèrent selon l'organisme et le niveau de certification visé. Dans ce domaine de la caractérisation de dispositifs sécurisés, les produits se doivent de résister à diverses attaques. Grâce à l'amélioration du niveau des implémentations logicielles, les attaques logiques ou cryptanalytiques semblent de moins en moins facilement réalisables. A contrario les attaques physiques restent des menaces de plus en plus pertinentes pour les systèmes embarqués.

Pour une entreprise soumise à la certification de ses produits, de multiples investigations sécuritaires doivent être réalisées par des organismes extérieurs. Ce processus est long et coûteux. Ainsi les développeurs disposent souvent d'équipes d'ingénieurs dédiées à la caractérisation sécuritaire des circuits. Ils disposent aussi d'outils qui s'approchent souvent de ceux utilisés par les laboratoires agréés. Par exemple, pour évaluer la résistance des produits contre les attaques laser, la méthodologie généralement utilisée suit le principe de la figure 1.17.

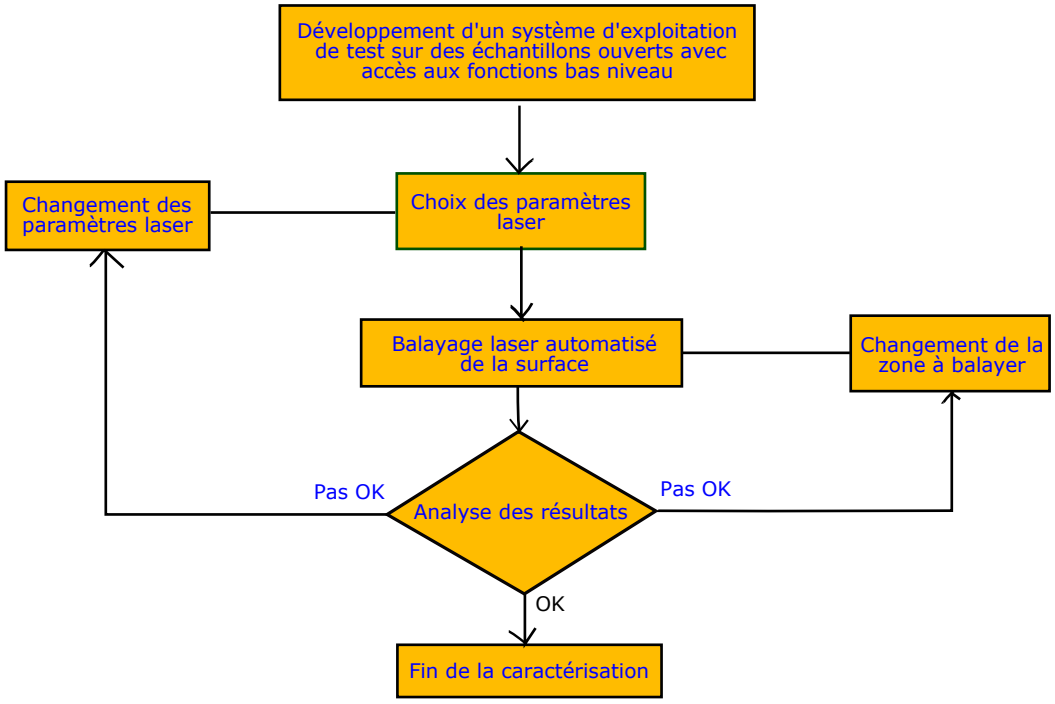


FIGURE 1.17: Méthodologie généralement utilisée pour les caractérisations laser

Cette méthodologie montre des limites car l'évaluation du circuit contre ce type d'attaques peut prendre des jours d'autant que la zone à attaquer est inconnue et que les paramètres laser le sont également. La couverture de test n'est pas optimale et la campagne de tests doit être effectuée à nouveau pour chaque nouveau composant même si celui-ci est de la même famille que le précédent ou provient encore du même fabricant de circuits intégrés.

Pour les raisons évoquées, on conçoit que l'efficacité, la flexibilité et l'optimisation de ces équipements permet une meilleure couverture de test et une meilleure rapidité permettant ainsi d'avantager la mise sur le marché du produit. De plus, une optimisation des outils peut possiblement augmenter la réalisation d'attaques plus complexes nécessitant plus de temps. C'est notamment dans ce cadre que se situe mes travaux de recherche.

1.2.3 Types de contremesures et d'attaquants

Lorsqu'une vulnérabilité est mise en évidence par une attaque, des contremesures doivent être implémentées pour répondre aux exigences requises pour l'obtention des dits certificats. On peut citer les contremesures matérielles (redondance spatiale, capteurs de lumière...), et les contremesures logicielles. L'ensemble de ces contremesures peut affecter les performances du circuit en termes de taille de code, de surface silicium utilisée, de rapidité et de consommation du circuit. Ainsi, un compromis doit être trouvé car la contremesure idéale n'existe pas. Les contremesures sont ainsi tout d'abord listées avant d'avoir un aperçu sur les profils d'attaquants et sur les hypothèses émises sur ses capacités.

Les différentes contremesures Parmi les différentes contremesures possibles, nous pouvons notamment répertorier, celles :

- empêchant l'accès à la puce comme les résines d'encapsulation ou les boucliers actifs ou non (shields) qui empêchent de visualiser et d'accéder aux couches inférieures du circuit.
- modifiant l'organisation au sein du composant comme la logique synthétisée, 'le scrambling mémoire' (organisation mélangée des mémoires), les cellules de camouflages, les cellules de remplissages ou fausses cellules et enfin les modifications au niveau des cellules de base pour masquer d'éventuelles différences entre les niveaux logiques '0' et '1'.
- ajoutant des éléments dans le circuit tels que les détecteurs de lumière ou de courant ou des blocs dupliqués permettant une redondance spatiale afin de se protéger d'injection de fautes par exemple.
- modifiant le comportement temporel/logiciel tels que l'insertion de fausses opérations, un ordonnancement et des délais aléatoires, des compteurs de passage/de boucle, différentes couches logicielles ou encore du traitement temps constant.
- utilisant différentes technologies, comme les SOI (Silicon on Insulator) et les technos 'CMOS deep well'.

Type d'attaquant et modèle de fautes Un profil d'attaquant [4] peut être spécifié de part sa compétence, sa connaissance du système et son matériel disponible. Dans ce même document [4], un niveau de protection est associé à un circuit entre autres de part la combinaison de contremesures dans le produit, le profil de l'attaquant et le coût des outils d'attaque. On parle donc de niveau d'attaquant et de niveau de protection. Pour les attaques en fautes, lorsque de nouvelles attaques sont publiées [55] ou lorsque des contremesures sont recherchées [61], des hypothèses sont émises sur les effets possibles des attaques.

Ainsi des modèles de fautes sont considérés prenant en compte le type d'attaquant, du type de circuit intégré ou encore de la capacité d'attaque de l'attaquant. Les modèles de fautes sont très variés et sont le plus souvent des modèles de fautes théoriques émis avec hypothèses. Maimut *et al.* [55] associe des types d'attaques possibles sur un algorithme et ses contremesures vis-à-vis du modèle de fautes utilisé ; multiples fautes, deux fautes ou encore une faute connue. Pour Zhang *et al.* [83], l'attaquant peut choisir un message à chiffrer et peut injecter une faute dans un chiffrement à un moment donné et sur une partie d'une entrée d'une certaine fonction. L'attaquant est également considéré comme connaissant la position de la faute mais ne sachant ni la localisation exacte ni la valeur des fautes. Par exemple, on peut également considérer des modèles de fautes de mise à '0' ou de mise à '1' pour un bit donné, pour un registre ou d'une faute aléatoire sur une partie d'un chiffrement. Un des objectifs de mes travaux est de connaître ce qui est réalisable par un attaqaunt en pratique.

1.2.4 Techniques de détection de Chevaux de Troie Matériels

Par analogie avec le logiciel, les Chevaux de Troie Matériels (CTMs) sont des fonctions malveillantes directement insérées dans la structure physique du composant. Les CTMs font l'objet de nombreuses études récentes. Il est vrai que le marché du semi-conducteur est propice à l'insertion de modifications malicieuses de circuits du au fait que de plus en plus d'entreprises (désignées par fabless) n'ont plus leurs propres unités de fabrication. La fabrication est déléguée à des industriels localisés principalement en Asie. Ce manque de contrôle sur la chaîne de fabrication peut poser problème dans le suivi de fabrication. Même si aucun cas concret (sur le terrain) n'a été mis en avant, les menaces sont telles que des groupes de recherche se sont crées, notamment diligentés par différentes organisations gouvernementales.

Les CTMs sont également classifiés selon leur effet, leur type d'activation, leur localisation, etc...Il peut en exister autant qu'il est possible d'en imaginer. On peut cependant distinguer les CTMs logiques (combinaison d'état pour l'activation du Cheval de Troie Matériel) des CTMs plutôt paramétriques (qui vont au final donner un déni de service par exemple). De même pour les types de détections, ils sont classés selon les méthodes utilisées : leur niveau invasif, le taux de détection atteignable, le besoin d'un modèle de référence, etc... Des aspects préventifs pour empêcher l'insertion de CTMs ont également été développés [35] Les CTMs sont généralement constitués d'une partie 'payload' (charge/effet du CTM) et d'une partie 'trigger' (déclenchement du CTM) sauf si le CTM est tout le temps actif. Ainsi, plusieurs familles de techniques théoriques de détection ont été proposées et étudiées afin de couvrir une partie de la grande variété de CTMs, cf. figure 1.18. Cette figure permet ainsi de repérer l'étendue à couvrir par une méthode de détection de CTMs.

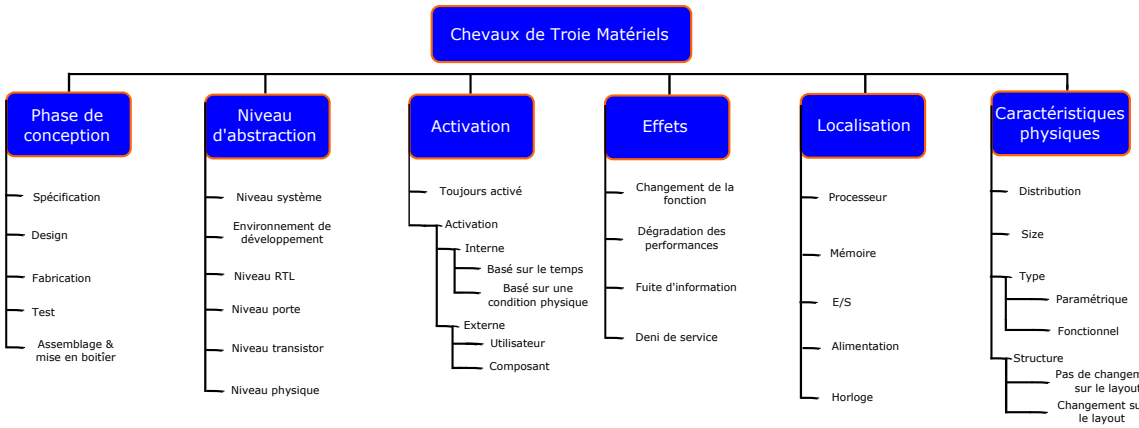


FIGURE 1.18: Taxinomie des Chevaux de Troie Matériels, figure tirée de [1]

1.2.5 Besoins et techniques de rétro-conception

Une entreprise peut avoir recours à la rétro-conception afin d'analyser son propre circuit pour des besoins de validation (debug). Elle peut aussi s'en servir à des fins d'analyse de défaillance ou de conformité (Détection de Chevaux de Troie Matériels (CTMs)). Des produits de la concurrence peuvent être la cible de rétro-conception afin de vérifier si aucune propriété intellectuelle (IP) propriétaire n'a été utilisée de manière cachée, d'extraire des caractéristiques d'intérêt ou encore de connaître les coûts et procédés de conception. La rétro-conception peut aussi bien s'appliquer à l'extraction d'un paramètre spécifique d'un transistor qu'à un produit complet composé de plusieurs blocs IPs. Elle peut se décliner soit sous forme logicielle soit sous forme matérielle. Nous nous intéressons uniquement à la partie matérielle dans ces travaux de recherche. Ce qui nous intéresse est l'application à la sécurité des circuits intégrés [63, 76].

Des méthodes non invasives ont été développées pour effectuer de la rétro-conception. Il existe entre autres les méthodes SCARE (Side Channel Analysis for Reverse Engineering) qui sont basées sur les émissions par canaux auxiliaires du circuit de test et les méthodes FIRE (Fault Injection for Reverse Engineering) qui sont basées sur la perturbation par fautes pour obtenir de l'information sur le circuit. La thermographie [20, 38] peut permettre d'identifier des blocs fonctionnels au niveau spatial tandis que la photoémission a permis dans les travaux de

Schlosser *et al.* [70] de récupérer des informations spatiales et temporelles au niveau de granularité transistor et de l'instruction jouée. On peut également citer les impressionnants travaux de Bajura *et al.* [59] sur un circuit de noeud technologique $90nm$. Bajura *et al.* a extrait une image par couche d'un circuit intégré sur une zone de $10X10\mu m^2$, du niveau contact au niveau 'metal9'. Ce résultat visible sur la figure 1.19 est obtenu de manière non destructive avec un microscope rayons X modifié dans un cadre expérimental.

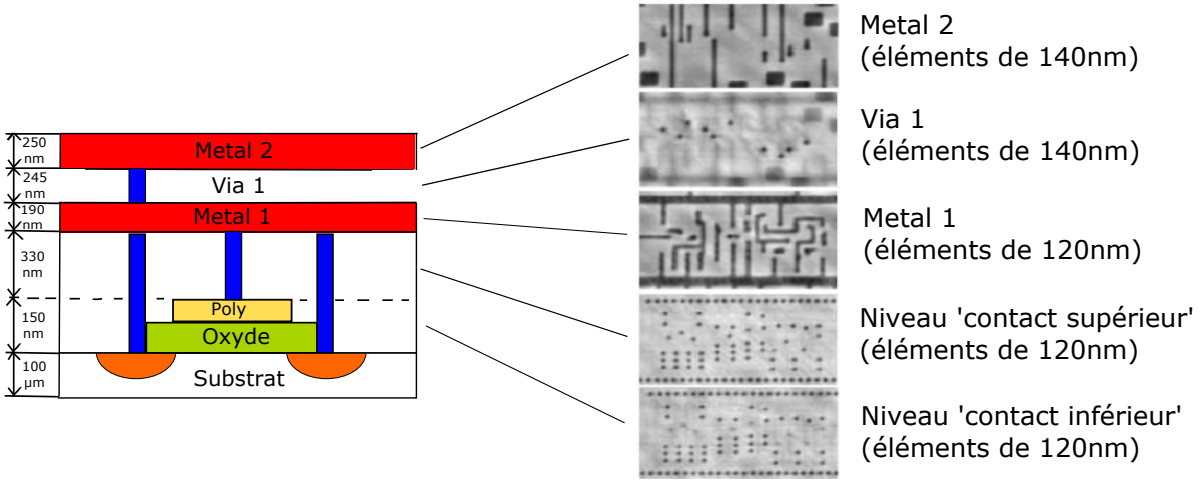


FIGURE 1.19: Différenciation aux Rayons X des éléments par niveaux d'une cellule de base en technologie 90nm, figure adaptée de Bajura *et al.* [59]

D'un autre côté, la technique de rétro-conception invasive standard [79] consiste à préparer le circuit, à photographier chacune de ses couches et à les traiter pour reconstruire une description des fonctions du circuit intégré. Dépendant de la complexité du circuit et de son noeud technologique, plusieurs dizaines de milliers d'images peuvent être nécessaires par niveaux. De même, pour certains composants, le nombre de couches peut être supérieur à une douzaine. Pour réussir ce type d'attaque, il est nécessaire d'avoir plusieurs échantillons du même produit. En effet, le nombre d'échantillons à considérer est proportionnel au nombre de couches de ces derniers.

1.3 Méthode de rétro-conception matérielle standard

La rétro-conception matérielle standard se compose des étapes présentées dans le tableau 1.3. Des entreprises sont spécialisées dans la rétro-conception matérielle et proposent donc leur expertise pour évaluer n'importe quel circuit. Outre l'accès à un laboratoire de chimie, et un accès à un outil d'acquisition d'images comme un Microscope Electronique à Balayage (MEB), ces entreprises utilisent des logiciels dédiés une fois les images de chaque couche du circuit intégré acquises. Par exemple, la société *Chipworks* [2] propose une solution de navigation sur une large image et ce sur différents niveaux en même temps. Sous l'outil il est notamment possible de faire une correspondance directe entre la vue schématique du circuit et l'image MEB récupérée, de même il est possible d'extraire la netlist (description) du circuit. Ces outils d'extractions ne sont pas (ou pas encore) disponibles par la communauté académique. Degate [71] est un développement libre accès pour effectuer une rétro-conception de circuit.

TABLEAU 1.2: Etapes de rétro-conception matérielle standard, domaine d'expérience et coût associé

Etape	Domaine
Retrait du boîtier dans lequel se trouve le composant à analyser	Préparation mécanique ou attaque chimique
Retrait successif des couches déposées ('metal1', polysilicium...)	Polissage ou gravure sélective
Acquisition d'images à chacun des niveaux	Microscopie optique ou électronique
Identification de chaque élément	Annotation manuelle ou développement logiciel
Création du schéma équivalent	Développement logiciel
Simulation et analyse	Electronique numérique / Simulation

Pour chaque étape, différentes méthodes sont applicables et différentes recettes sont possibles vis-à-vis des différentes technologies utilisées pour la composition complète d'un circuit. Ces méthodes changent avec l'évolution de la technologie et des capacités de calcul dans les différents domaines que sont notamment la microscopie et le traitement d'images. Le coût de la méthode standard de rétro-conception matérielle se situe à plusieurs centaines de milliers d'euros en incluant celui des équipements et l'expertise nécessaire.

1.3.1 Les différentes étapes

Retrait du boitier et des couches métalliques Le type de boitier utilisé dépend du besoin d'intégration, du nombre de pins, ou encore de l'environnement de fonctionnement. Il peut s'agir de boîtiers plastiques ou céramiques, et ceux-ci peuvent intégrer un fond métallique et différentes résines. Les possibilités pour arriver jusqu'au circuit intégré lui-même (sur la couche de passivation située au dessus du niveau métallique le plus haut et qui permet d'atténuer les contraintes mécaniques) sont multiples. Par exemple pour une gravure humide, l'utilisation d'aluminium adhésif et d'acide nitrique fumant comme représenté la figure 1.20 permet de venir à bout d'une zone choisie d'un boitier plastique.

De même il existe des machines conçues spécialement pour enlever le capot d'un composant et ce sans agir sur les autres composants d'un circuit imprimé (support également appelé PCB : Printed Circuit Board). Pour un composant de type carte à puce, le module peut être retiré mécaniquement (avec un cutter) ou thermiquement pour accéder au substrat du circuit.

La rétro-conception standard nécessite l'accès à la piste métallique la plus haute, l'approche en face avant est ainsi nécessaire. Il faut ensuite effectuer un retrait des couches successives ('metalX' vers 'metal1', polysilicium, substrat) qui s'opère selon différentes techniques de préparation d'échantillons [10]. Une première technique est basée sur le polissage mécanique qui débute généralement par le niveau métallique le plus haut. L'épaisseur de chaque couche étant très faible

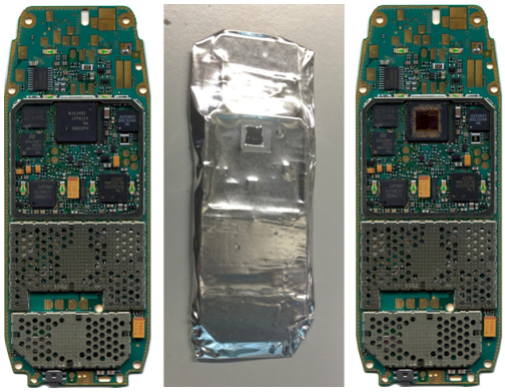


FIGURE 1.20: Ouverture d'un seul circuit d'un PCB à l'acide nitrique fumant

(quelques centaines de nm), il faut faire en sorte d'avoir une excellente planéité pour n'enlever qu'une seule couche du composant. Cette opération très délicate est assez difficilement réalisable compte tenu du ratio surface/épaisseur de la puce. Des machines de polissage sont utilisées. Le coût d'un tel équipement est de quelques dizaines de milliers d'euros et nécessite un opérateur expérimenté. D'autres techniques, comme le retrait par gravure plasma, peuvent être utilisées et les paramètres de ce type de gravure peuvent être automatisés si la composition chimique des circuits intégrés est préalablement mesurée ou connue. L'application du retrait niveau par niveau est généralement effectuée sur plusieurs circuits, à chaque niveau de retrait des photos sont prises.

Imagerie et reconstruction du circuit complet Le système de microscopie nécessaire à la reconstruction du circuit doit répondre à la capacité de balayer une surface de quelques mm^2 tout en étant capable de visualiser des objets micrométriques. De plus, une acquisition rapide de quelques heures et la plus automatisée possible est un critère exigé des industriels. Une succession de photos à fort grossissement (généralement x500) est acquise pour chaque couche afin de couvrir l'intégralité d'un circuit intégré. Ces images sont concaténées pour obtenir une seule image par couche. Chaque ensemble d'images correspondant à une couche est ensuite réajusté avec la couche précédente, cf figure 1.21.

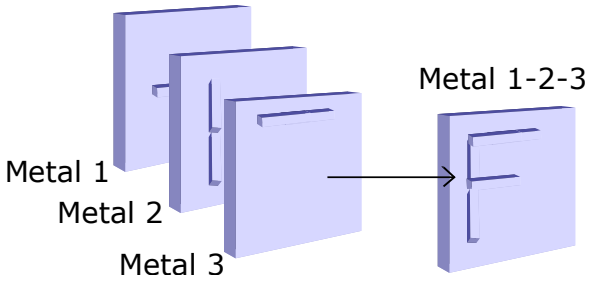


FIGURE 1.21: Reconstruction à partir de chaque couche du CI

Des librairies libres d'accès ou autres logiciels peuvent être utilisés pour ce besoin de resynchronisation d'images [45], ces derniers peuvent par exemple être basés sur des éléments invariants entre deux images successives.

Reconnaissances de formes, identification et création de la netlist Une fois l'image reconstruite obtenue, il faut pouvoir marquer individuellement chaque élément visible. Sur l'image reconstruite, une étape de traitement d'images peut être rajoutée pour la reconnaissance automatique des différents éléments [16, 51, 56].

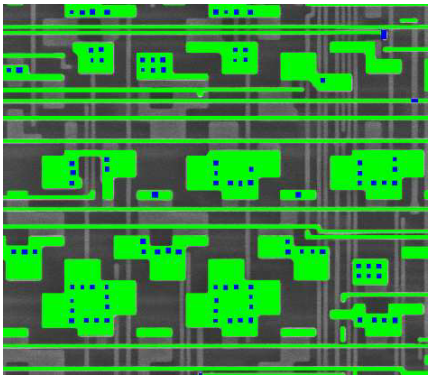


FIGURE 1.22: Reconnaissance d'éléments sur un circuit intégré, figure extraite de [79]

Des outils basés sur la corrélation croisée normalisée [53, 21] peuvent être utilisés pour reconnaitre des éléments similaires. Chaque forme et fil reconnus sont donc annotés pour leur donner une identité. Une fois les éléments reconnus puis identifiés, il faut extraire le schéma électrique à l'aide d'un logiciel spécifique. Ensuite, il est possible d'obtenir une description en langage de programmation (de type VHDL notamment) conduisant à l'analyse du circuit et permettant d'effectuer des simulations fonctionnelles.

La description de ces étapes met en avant la difficulté d'exécution d'une rétro-conception matérielle comme présente dans l'état de l'art. Par la suite, les techniques de microscopies appliquées à la visualisation de circuits intégrés sont plus amplement détaillées tout comme les techniques de traitement d'images.

1.3.2 Techniques de visualisation

Nous nous attachons ici à décrire des outils permettant de visualiser l'ensemble d'un circuit intégré soit en face avant (Optique/Confocal/Electronique à Balayage) soit en visualisant la face arrière (caméra infrarouge + optique de microscope) et permettant d'obtenir une résolution microscopique.

Microscopie face avant :

Le microscope optique utilise une source de lumière monochromatique, la résolution maximale est liée à la diffraction de cette dernière, la planéité du composant doit être bonne pour satisfaire la caractéristique de faible profondeur de champ des microscopes optiques. Le mode confocal d'un microscope optique permet d'obtenir des images avec une profondeur de champ plus importante et peut être utilisé pour visualiser différents niveaux adjacents. Un des principaux inconvénients est l'illumination non uniforme sur chaque image acquise. La figure 1.23 illustre ce fait avec l'image brute acquise en microscopie optique et une image où le bruit d'illumination non uniforme est extrait.

Le Microscope Electronique à Balayage (MEB) [81] utilise une source d'électrons, ces derniers sont accélérés puis bombardés sur la matière. Suivant notamment le niveau d'énergie des électrons envoyés, ceux-ci interagissent sur plus ou moins de volume, différents types de réactions

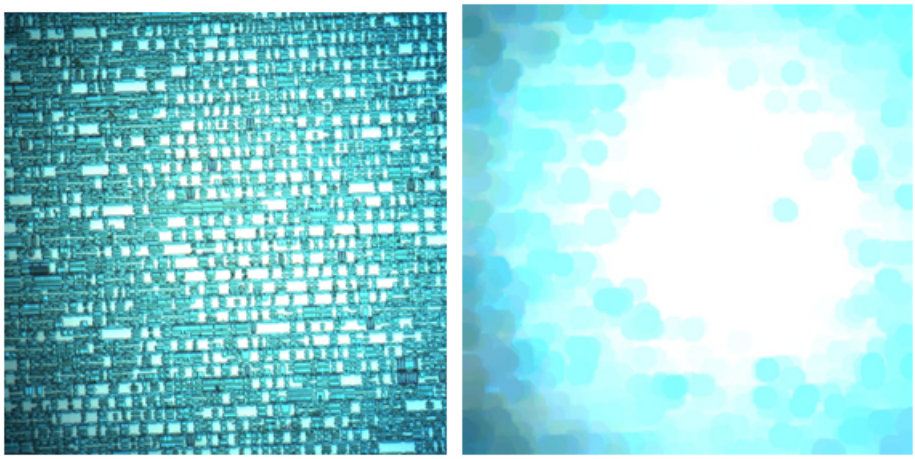


FIGURE 1.23: a) Microscopie optique d'une partie d'un circuit intégré b) Extraction du bruit d'illumination

(cf figure 1.24) ont lieu (modification de direction des électrons primaires, production d'électrons secondaires ou encore la production de rayons X). L'utilisation d'un faisceau d'électrons incidents de faible tension d'accélération permet de récupérer des électrons secondaires provenant de la surface de l'échantillon observé. Une information de topologie est ainsi récupérée. De plus les électrons rétrodiffusés permettent d'obtenir des informations sur la composition chimique de l'échantillon. En fait, la profondeur de pénétration du faisceau d'électron et le volume de l'échantillon avec lequel il interagit est fonction, de l'angle d'incidence, du courant, de la tension d'accélération et du nombre atomique moyen de l'échantillon.

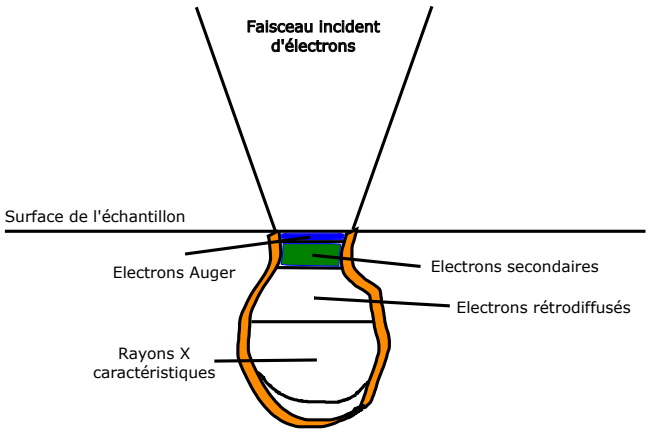


FIGURE 1.24: Poire d'intéraction d'un MEB

La formation de l'image est obtenue par le déplacement du faisceau d'électrons point par point sur la surface de l'échantillon. Outre le type de détecteur utilisé, la qualité de l'image est affectée par les propriétés intrinsèques du MEB (puissance de la lentille de balayage, taille d'ouverture de l'objectif) ou par les changements utilisateurs tels que le réglage de la tension d'accélération ou de la distance de travail [46]. La taille du faisceau, la finesse et la résolution, le courant de la pointe, les signaux SE, BSE et X-ray, la profondeur de champ, l'information de surface, l'information de profondeur et enfin la contamination sont affectés.

Visualisation face arrière :

Vu que le silicium est quasi transparent dans le proche infrarouge (longueur d'onde au voisinage d'1μm). Cette propriété est également mise à profit pour l'imagerie passive de CIs. Une caméra infrarouge avec une illumination côté substrat couplée à une partie optique (permettant un fort grossissement) permet d'apercevoir les différents blocs d'un circuit intégré (avec un objectif de microscope X5) et différentes formes de cellules de bases (avec un objectif de microscope X50). Suivant la caméra utilisée, aucun amincissement du composant n'est nécessaire. Il est alors possible d'observer différentes formes sur le circuit (couches actives) à travers le substrat sans toutefois avoir une image comparable à celle obtenue en microscopie face avant.

1.3.3 Traitement d'images

Formats Une fois l'acquisition des images obtenue, il est important de prêter attention à leur enregistrement et à leur pré-traitement. Le choix du format et le pré-traitement de l'image a toute son importance, il doit tenir compte des informations nécessaires pour l'alignement des images et la reconnaissance des motifs. L'image ainsi obtenue ne doit pas être trop volumineuse (moins d'1Mo), il est donc nécessaire de supprimer des informations non utiles telles qu'une échelle de représentation par pixel de l'image où les pas de variations d'intensités sont trop faibles ou encore de changer le système de codage informatique des données (des couleurs notamment avec RGB (Red, Green, Blue)).

Les principaux paramètres de l'image sont donc le type de compression, la taille de l'image, ou encore le nombre de bits caractérisant l'intensité du signal lumineux observé. De façon générale, dans le domaine du traitement numérique des images, le format TIFF est préféré au format JPEG notamment parce que la compression se fait sans perte d'information. Les outils développés et utilisés s'appliquent uniquement sur des images 2D codés sur 256 niveaux de gris dans le cadre de ces travaux.

Alignement d'images Par la suite, nous verrons dans le chapitre 2 que différentes images sont acquises et regroupées pour former une seule et unique "image de base". Différents outils et librairies sont actuellement disponibles notamment pour de l'imagerie dédiée à des applications biologiques ou encore pour la retouche de photos numériques (Hugin, PTgui ou encore sous OpenCV). Ils sont basés sur différents algorithmes de traitement de signal (SIFT : transformation de caractéristiques visuelles invariante à l'échelle, RANSAC : permettant d'ajuster les points similaires entre images, FFT : permet par exemple de filtrer des fréquences). Ces outils permettent d'obtenir une image globale, ou image de base, issue de la fusion d'images partielles avec une perte d'information quasi nulle. Si l'image finale nécessite trop de ressources matérielles (RAM), des outils de visualisation de données tels que Paraview permettent l'ouverture de données mêmes si celles-ci sont volumineuses.

Les transformées possibles pour le traitement d'images 2D sont représentées sur la figure 1.25. Ces transformées nous seront utiles pour le traitement des images acquises au MEB. En effet, celles-ci nécessitent la mise en place d'une solution prenant en compte des changements entre images inhérentes à la microscopie.

Reconnaissance de motifs

Différents domaines d'applications traitent les images ainsi obtenues pour repérer et classifier les objets d'intérêts (cellules dans le domaine de la biologie, identification de personnes...en fait toute identification dans une base de données) [14]. Une fois ces objets classés, il est alors pos-

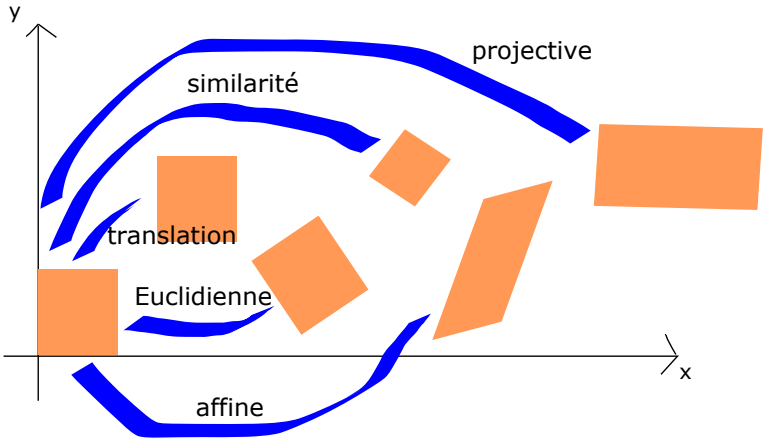


FIGURE 1.25: Différents types de transformations spatiales

sible d'émettre des hypothèses sur leur fonction et sur leur répartition statistique. Nous verrons dans le chapitre 3 que cette méthode de reconnaissance de motifs est intéressante pour identifier des zones de vulnérabilités matérielles impactant alors à la sécurité des circuits intégrés. Comme dans le cas de l'alignement multiple d'images, il existe diverses méthodes [14] et logiciels comme AMIRA et MATLAB intégrant des fonctions pré-construites dédiées à la reconnaissance de motifs.

Nohl *et al.* [63] applique une technique de reconnaissance de motifs basée sur une corrélation croisée normalisée. C'est une mesure de la similitude indépendante de la valeur moyenne des signaux. Leur technique (appliquée après polissage) est semble t-il appliquée à une partie d'un circuit intégré (μm^2) sur des images optiques et implémentée sous MATLAB. Basé sur ce même algorithme, un outil libre d'accès (Degate) a été développé pour la rétro-ingénierie de circuits intégrés. Cet outil, intègre un processus de rétro-ingénierie sous une interface utilisateur. Des essais nous ont notamment permis de statuer sur des reconnaissances de motifs avec erreurs [71] où un seuil doit être défini sans réel connaissance vis-à-vis de l'algorithmie utilisé. Des outils commerciaux proposés par Chipworks (ICworks), Cellixsoft (Hierux System) ou encore UBM TechInsights (Matrix) sont proposés à des fins de service mais aucune information sur leurs caractéristiques et performances ne sont disponibles ; ces informations ne sont pas publiques. Sur ces outils, le processus de rétro-ingénierie est interactif et permet de remonter jusqu'à la netlist du circuit. Le coût de ces solutions (environ $100k$), le non contrôle de ces dernières, la présence d'une interface utilisateur non nécessaire sont des freins à la rétro-conception bas coût.

Le choix des critères de la solution de reconnaissances de motifs est dépendant ou se caractérise par :

- Des différents types d'applications,
- des différents types de méthodes et d'algorithmes de reconnaissances (par apprentissage ou non), des variations entre motifs d'une même acquisition ou d'acquisition différente,
- du seuil de détection pour classifier les motifs,
- de taux de faux positifs ; un motif est reconnu comme identique alors qu'il ne l'est pas,
- et par le taux de négatifs cachés ; un motif n'est pas reconnu alors qu'il est identique,

1.4 Injection de fautes laser

Après avoir décrit le principe de rétro-conception, nous poursuivons donc par les attaques par fautes injectées par faisceau laser.

A l'origine, ces techniques lasers se sont développées dans le domaine spatial afin de reproduire des effets du à l'environnement de fonctionnement. Dans ce domaine, l'utilisation du laser est une solution préférée aux systèmes de caractérisation utilisant neutrons et ions lourds. L'avantage est effectif niveau coût et radioactivité tout en permettant d'émuler des phénomènes naturels. Par la suite, cette approche fut appliquée à l'injection de fautes, cf partie 1.2.1, sur des circuits sécurisés (entre autres carte à puce) dans les années 1998. Les premières attaques ont été réalisées à l'aide d'un simple flash photographique. Elles ont ensuite été régulièrement affinées par l'utilisation du laser. L'injection de fautes laser permet, moyennant une bonne maîtrise de l'équipement et du logiciel, de dérouter du code, de modifier des droits d'accès ou encore de récupérer des données sensibles [73].

But, application L'injection de fautes laser est réalisée pour caractériser la résistance d'un circuit intégré aux perturbations. Le faisceau laser permet une très bonne couverture spatiale et temporelle. L'injection de fautes laser nécessite toujours un accès à la puce, soit sur la face active où le laser choisi émet dans le visible, soit côté substrat où seul un faisceau de longueur d'onde avoisinant les 1064nm, cf 1.28, est efficace. L'approche face active est de moins en moins utilisée avec l'augmentation de la densité des pistes métalliques. Ces dernières obstruent le passage du faisceau de lumière. A cela s'ajoute souvent des protections appelées boucliers (ou 'shields') qui rajoutent un niveau de difficulté supplémentaire. Ces boucliers peuvent empêcher la visualisation ou le passage d'une perturbation soit de manière passive soit de manière active via la détection des tentatives de fautes ou d'intrusions sur le circuit à l'aide d'un système de contrôle.

Le principal avantage de la face arrière est que le substrat est vierge de tout élément, de sorte qu'une énergie qui lui est appliquée le sera de manière homogène sur toute la surface du composant. Les zones sensibles sont ainsi atteintes avec le même niveau d'énergie. Cependant la résolution des images obtenues côté substrat est plus faible que celles obtenues côté face active comme indiqué dans la sous-section 1.3.2. Afin de mieux décrire la difficulté de la réalisation d'attaques laser, nous présentons une plateforme typique d'injection de fautes laser.

1.4.1 Plateforme d'attaque laser

La figure 1.26 représente une partie d'un banc type d'injection de fautes laser YAG (Yttrium Aluminium Garnet, matériau utilisé comme milieu amplificateur de lasers). Ce banc est généralement constitué d'une carte de synchronisation pour le déclenchement d'impulsion(s) laser, d'un système de contrôle, d'un laser, d'une partie optique d'injection, d'une partie optique pour la visualisation et d'une partie mécanique pour notamment contrôler le déplacement de la colonne optique ou de l'échantillon. Une caméra infrarouge est utilisée pour visualiser les différentes zones d'un circuit intégré et une table de positionnement [X,Y,Z] permet d'effectuer la mise au point du circuit puis de se positionner sur la bonne zone à perturber sur les axes [X,Y,Z]. Il est intéressant de noter l'inclinaison que le circuit peut avoir (ayant donc un effet entre deux positions spatiales distinctes) et l'existence de techniques d'ajustement pour automatiquement gérer la mise au point de l'échantillon en tout point malgré son déplacement. L'effet du laser est localisé. Ainsi, une plateforme laser est optimale si elle est caractérisée par un bon contrôle du profil du faisceau laser, par une précision spatiale importante et répétable (à l'échelle du μm),

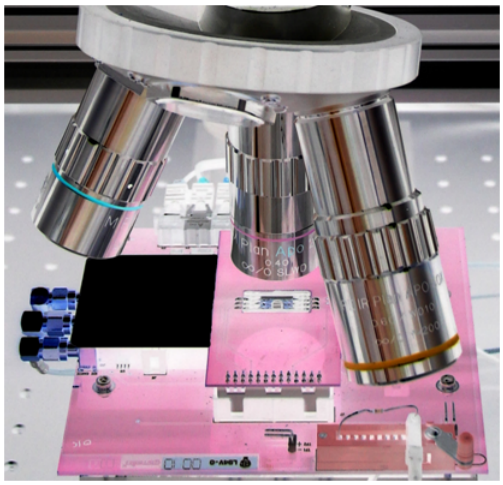


FIGURE 1.26: Partie d'une plateforme d'attaque laser

tout comme une localisation temporelle importante (à l'échelle de la ns). Le tableau 1.4.1 résume les différents paramètres d'une plateforme laser.

TABLEAU 1.3: Les différents paramètres et choix d'injection laser

Paramètre/Choix/Outils	Unité (si applicable)
Attaque par la face avant ou face arrière du composant	NA
Longueur d'onde de l'impulsion laser	Entre 300 et 1100 nm
Distance de travail	En mm
Taille du faisceau laser	Diamètre en μm
Durée de l'impulsion	En ps ou ns
Puissance de la source laser	Quelques Watts
Chemin optique fixe (lentille, lame, collimateur, atténuateur, fibre)	NA
Tourelle d'objectifs	x5, x20, x50, x100
Balayage spatial à effectuer ou point ciblé	NA
Pas de balayage	De dixièmes de μm à plusieurs dizaines de μm
Précision du déplacement	Aux alentours de quelques dixièmes de μm
Disponibilité d'une caméra de visualisation	NA
Amincissement nécessaire ou non	Aux alentours des 100 μm

Au niveau spatial, le déplacement du faisceau laser doit être sub-micrométrique, la stabilité doit être importante (d'un tir laser à un autre, ou encore lors du passage d'une colonne à une autre lors d'un balayage spatial) et la précision de déplacement doit être fine. Le contrôle d'un niveau d'énergie quasiment identique entre deux tirs lasers successifs est aussi obligatoire pour

assurer une bonne couverture de test. Un faisceau laser est caractérisé par sa taille (proche d'$1\mu m$), son profil d'intensité et sa durée d'impulsion.

1.4.2 Intéraction laser/matière

Les zones sensibles à un faisceau laser sont les jonctions PN des transistors. Selon leur état lors de l'injection, il peut résulter une commutation d'un ou plusieurs transistors. Ces commutations de transistors peuvent alors modifier l'état de sortie d'une cellule et perturber un processus en cours de fonctionnement sur le circuit intégré dans certains cas. L'énergie créée par un faisceau laser supposé Gaussien, atteignant les jonctions PN du composant crée un courant transitoire dont la forme d'onde est visible sur la figure 1.27.

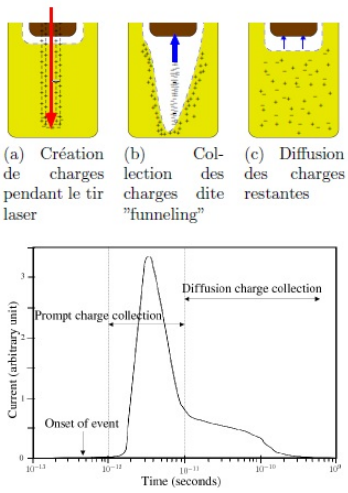


FIGURE 1.27: Forme d'onde du courant transitoire, figure extraite de [80]

La technologie CMOS repose aujourd'hui sur l'utilisation du silicium, comme vu au chapitre 1, le silicium est parfaitement transparent aux longueurs d'ondes supérieures à $1.1\mu m$. Ces longueurs d'onde constituent donc un excellent moyen d'observer les circuits intégrés à travers leur substrat. Illustré par la figure 1.28, le coefficient d'absorption dans le silicium dépend du niveau de dopage du composant et de la longueur d'onde du laser utilisé [47].

En 2013, Roscian *et al.* [67] a ciblé un noeud technologique $0.25\mu m$ dont la cellule mémoire est de $9\mu m$ par $4\mu m$. Dans cette étude, un laser a été utilisé ($532\mu m$) et a permis de réduire la taille de spot à environ $1\mu m$ contre $10\mu m$. Les auteurs mettent en évidence la répartition spatiale des zones de bit set et de bit reset. Darracq *et al.* [31] montre l'impact de la distance du tir laser sur le niveau d'énergie crée tandis que Douin *et al.* [34] apporte des éléments sur l'influence du niveau d'énergie sur le courant généré. Le contrôle du positionnement spatial du faisceau laser impacte le niveau d'énergie atteignant les jonctions. La figure 1.29 illustre la variation du photocourant suivant le positionnement sur l'axe Z du faisceau.

Modélisation Outre l'application directe d'un faisceau laser sur un circuit intégré, la modélisation des effets possibles avec un laser permet de comprendre ce qu'il se passe au niveau physique et ainsi de proposer des contremesures matérielles efficaces. En ce sens, nous pouvons citer les travaux centrés sur les modélisations sur un transistor unique [69, 19]. Les travaux de Sarafianos *et al.* [69] effectués en technologie 90nm et pour un procédé donné, mettent en avant la création

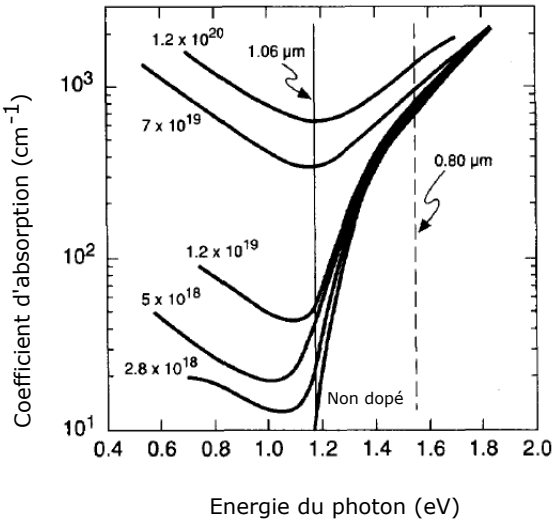


FIGURE 1.28: Absorption optique dans le silicium, figure extraite de [58]

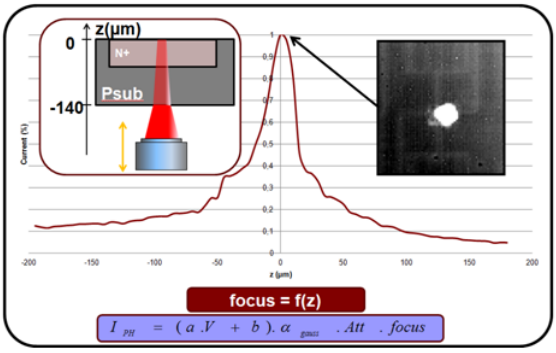


FIGURE 1.29: Photocourant généré dépendant de l'axe z, figure extraite de Sarafianos *et al.* [69]

d'un photocourant six fois plus élevé pour une jonction d'un transistor NMOS (N+/P-sub) que pour une jonction d'un transistor PMOS (P+/N-well). Ceci est illustré sur la figure 1.30.

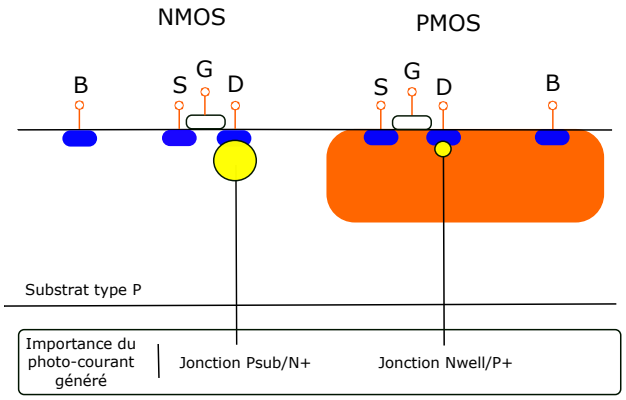


FIGURE 1.30: Différence de photocourant entre jonctions, illustration depuis [68]

De plus, Roscian *et al.* [67] obtient des simulations de sensibilité laser sur une cellule mémoire. L'impact de l'effet du laser en termes de bit set, bit reset et bit flip d'une cellule mémoire y est étudié. La cellule mémoire est une SRAM composée de 6 transistors de noeud technologique $0,25\mu m$. Il met en évidence la possibilité de localiser des zones de 'bit set' et de 'bit reset' qui ne sont pas situées aux mêmes endroits spatiaux. Cette particularité permet la mise à '0' ou à '1' de points mémoires si l'attaquant a connaissance au préalable de ces zones et la capacité de se positionner de manière précise sur ces zones. Dans ces travaux le possible attaquant aurait connaissance de ces zones seulement après attaques. Par convention nous parlons de 'reset' ou 'bit reset' quand la valeur bascule de '1' vers '0' et de 'bit set' ou 'bit set' quand la valeur passe de '0' à '1'.

1.4.3 Injection et exploitation de fautes laser

Roscian *et al.* a mis en pratique la possibilité de contrôler une cellule SRAM à l'aide de la localisation spatiale d'un faisceau laser, cf figure 1.31.

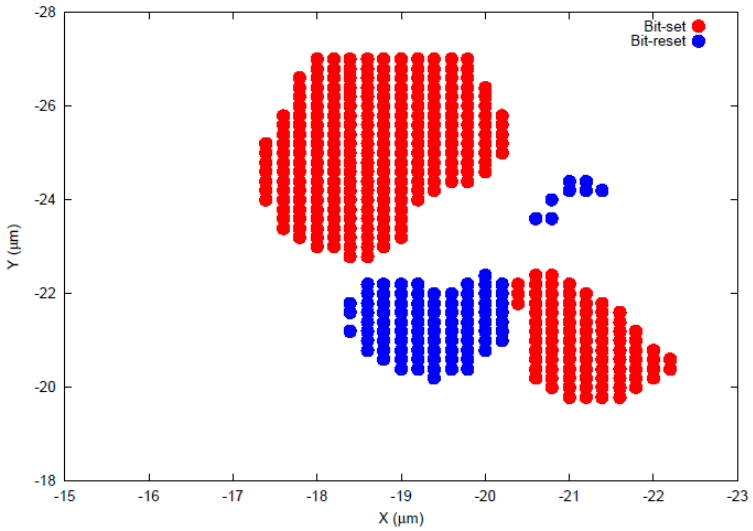


FIGURE 1.31: Différenciation sur une porte SRAM de zones sensible au laser [66]

Outre les cellules mémoires de type SRAM stockant des informations en dehors de la logique synthétisée il existe dans cette dernière des cellules également capables de stocker un bit de donnée, appelées cellules flip-flop. Pour perturber ces points mémoires, la campagne d'injection de fautes laser consiste à balayer l'ensemble de cette logique synthétisée jusqu'à obtenir la perturbation souhaitée. Généralement, avec cette approche un compromis couverture de test/temps de balayage est effectué en choisissant un nombre de registres à relire ou de résultats d'opérations à récupérer, un pas de balayage, une taille de faisceau, une durée d'impulsion et une puissance de faisceau laser.

Outre les travaux de Roscian *et al.* [66] visant une cellule SRAM, Loubet-Moundi *et al.* [54] vise les registres d'un algorithme de chiffrement matériel DES présents dans la logique synthétisée d'un circuit carte à puce (de noeud technologique $0.13\mu m$). Au terme de la mise en pratique de leur attaque sur ces registres statiques, les points suivants ont été remontés :

- La relation entre les positions physiques du registre et la cartographie des erreurs n'est pas systématique,

- la conception d'un registre utilisé par le fondeur pourrait avoir un impact sur les résultats,
- l'expérimentation pourrait être améliorée avec un pas de balayage plus fin (pas de $100\mu m$ utilisé pour trouver la zone où les registre DES sont présents, puis $10\mu m$ pour obtenir une matrice de localisations des bits du DES) et un faisceau plus petit (faisceau utilisé de plusieurs μm^2).

De plus les auteurs mettent en avant les limites suivantes concernant le positionnement entre le circuit de test utilisé pour calibrer la plateforme et la cible réelle :

- Faire un nouveau balayage avec le risque d'être détecté par des contremesures sur le produit réel,
- utiliser une caméra infrarouge dédiée avec une optique de fort grossissement.

Dans Leveugle *et al.* [52], les auteurs ont évalués des protections contre les attaques en fautes. Ils ont notamment émis comme conclusion que 'les conditions réelles d'attaques sont clairement loin du modèle classique de fautes 'bit-flip'. Le 'bit flip' est un modèle de fautes dont l'effet est l'obtention de la valeur inverse de celle de départ pour un bit donné indépendamment de la valeur de départ.

Exploitation des fautes injectées Une fois la faute laser injectée, il faut pouvoir extraire de l'information grâce à cette perturbation externe réalisée. Les méthodes d'analyse de fautes comme l'analyse différentielle de fautes ou l'analyse en 'safe error' répondent à ce besoin.

L'Analyse différentielle de fautes (qui est plus connue sous le nom de Differential Fault Analysis (DFA)) compare un message chiffré avec un message chiffré fauté pour des valeurs de texte clair et de clé identiques et permet ainsi de remonter jusqu'à l'information souhaitée. Introduite par Boneh *et al.* [18], l'acronyme DFA a été ensuite proposé par Biham *et al.* [13]. Par la suite Giraud *et al.* a appliqué la DFA sur un algorithme de chiffrement AES [41]. Cette attaque nécessite l'injection d'une faute mono-bit juste avant la dernière transformation SUBBYTES de l'algorithme, cf figure 1.16. Elle requiert donc une grande précision temporelle et spatiale et impose que la faute soit strictement de type mono-bit. Roscian *et al.* [66] a caractérisé un circuit implémentant un chiffrement AES 128 bits avec un faisceau laser assez large ($125\mu m$). Il démontre qu'il est possible de récupérer des fautes utilisables pour remonter jusqu'à la clé de chiffrement qu'elles soient monobits ou multibits. Cependant, l'approche proposée face avant ne leur a pas permis de récupérer l'ensemble de tous les fautés possibles.

L'analyse de fautes dite 'safe error' a été introduite par Yen *et al.* [82]. Elle impose un modèle de fautes 'bit set' ou 'bit reset' connu au préalable par l'attaquant. Prenons le cas du modèle de fautes 'bit reset'. Si le chiffré est fauté, cela signifie que la valeur initiale était '1', tandis que si le chiffré reste correct alors la valeur initiale était '0'. Cela permet ainsi de connaître la valeur stockée avant la tentative de perturbation. L'attaque 'safe error' a été appliquée notamment sur un circuit de chiffrement AES par Blomer et Seifert [15].

Au travers notamment des pertinentes mises en oeuvre pratique, il apparait intéressant de travailler sur le contrôle de l'effet laser sur un circuit complet et actuel sans balayage spatial et visant une cellule critique en matière de sécurité.

1.5 Conclusion

Cet état de l'art permet de mettre en avant l'aspect pluridisciplinaire des travaux effectués dans le cadre de ces travaux de recherche. On a présenté les circuits intégrés à travers leur composante matérielle. Les propriétés du silicium sont tout d'abord décrites puis celles du semi-conducteur également qui permettent par la suite de comprendre le fonctionnement et les propriétés des transistors. Ces transistors forment les cellules de base de part leur association. Cette association est optimale en termes de consommation, temps d'accès et de surface silicium utilisée. Elles sont présentes dans des librairies dédiées à la conception des circuits et sont rendues disponibles aux concepteurs. Nous avons décrit les outils et le flot de conception. Ces cellules de base se composent de deux à une vingtaine de transistors pour respectivement une cellule inverseur et une cellule dite flip-flop. L'inverseur est à la base de chaque cellule tandis qu'une flip-flop permet de stocker un '0' ou un '1' logique. Nous avons vu qu'un circuit, de type carte à puce, comprend plusieurs centaines de milliers de cellules dans une partie appelée communément 'logique synthétisée'. Cette partie a été mise en avant dans nos travaux de part sa nature à recéler des éléments sensibles voire secrets. En termes de sécurité, cette logique synthétisée est donc très intéressante. Les besoins de sécurité ont été évoqués tout comme les différents types d'attaques pouvant être réalisés. Nous avons mis l'accent sur les techniques d'attaques par fautes qui s'avèrent avoir des effets locaux et les techniques de rétro-conception en incluant des précisions quant à la microscopie électronique et au traitement d'image. Nous avons porté une attention toute particulière aux techniques d'imagerie dont l'intérêt est nécessaire pour étudier les capacités de rétro-conception. Différents circuits de tests, outils de visualisation et algorithmes standards principalement utilisés pour le traitement d'image sont présentés. L'objectif de repérer, par cette technique, la présence de Chevaux de Troie Matériels est de toute importance pour le milieu industriel, notamment à cause de l'externalisation de la fabrication des circuits à l'étranger.

Chapitre 2

Proposition d'une méthodologie de rétro-conception partielle : SEMBA

SEMBA : Scanning Electron Microscope Based Acquisition technique

Dans le chapitre précédent, l'état de l'art sur la sécurité des circuits intégrés a été présenté. La connaissance de l'architecture d'un CI et le positionnement spatial de cellules de base y est notamment présenté comme d'intérêt pour effectuer des attaques localisées ou encore pour vérifier l'intégrité d'un circuit. Ce présent chapitre apporte une méthodologie permettant d'obtenir des informations sur la localisation des cellules de base d'un circuit intégré de manière efficace, bas coût, rapide et reproductible. Une reconnaissance de formes peut par exemple être effectuée pour connaître le positionnement spatial de cellules intéressantes à attaquer. Nous recherchons les formes correspondantes à des bascules flip-flop : ces bascules étant des plus critiques en matière de sécurité peuvent notamment stocker des clés de chiffrement. Cette méthodologie se décompose en trois étapes, une première de préparation d'échantillon où seule une couche du composant est conservée, une deuxième étape où la surface entière de la couche est acquise de manière automatique à l'aide d'un Microscope Electronique à Balayage (MEB) et une troisième où des points d'intérêts sont extraits à l'aide d'un outil de reconnaissance de motifs.

Sommaire

2.1 Proposition de la méthodologie SEMBA

2.1.1 Objectifs de SEMBA

La méthodologie SEMBA (Scanning Electron Microscope Based Acquisition technique) proposée a pour but de récupérer la localisation spatiale des cellules de base. Nous nous attachons à vouloir récupérer cette information car ces cellules sont représentatives du plus bas niveau fonctionnel dans un circuit intégré. Ainsi, obtenir ce niveau permet de récupérer des informations sur les fonctions matériellement implémentées dans un composant. Dans le chapitre 1, l'organisation de ces cellules a été présentée. Nous rappelons brièvement ici que ces cellules de base sont composées d'éléments sur plusieurs niveaux physiques : les niveaux BULK (caissons des transistors), polysilicium (grilles des transistors), 'metal1' ou 'metal2' (connexions entre transistors).

Tout d'abord nous mettons en avant la difficulté d'observer à travers la face avant d'un CI de part le nombre de couches métalliques présentes sur les circuits actuels associé à la présence d'un bouclier ou d'une couche de passivation, cf figure 2.1. Ainsi, pour identifier ces cellules de base, il faudrait utiliser une méthode capable de passer à travers les autres niveaux métalliques pour une visualisation dite en 'face avant' ou encore une méthode capable de visualiser le substrat avec une grande résolution en 'face arrière'.

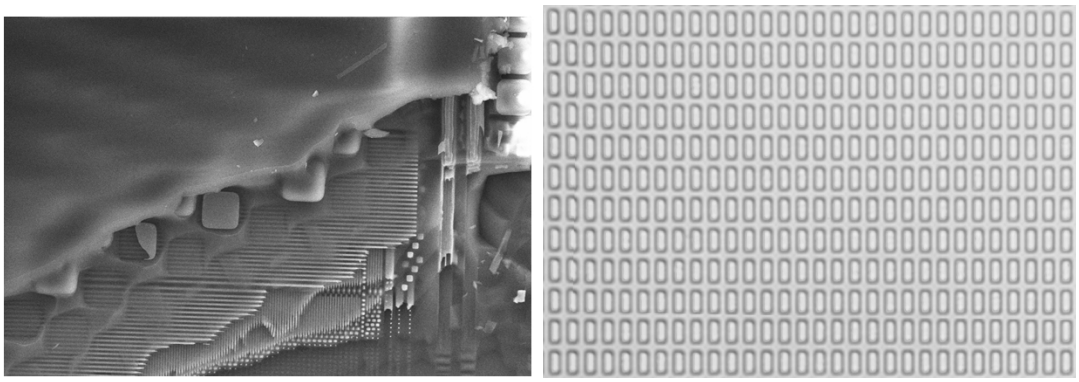


FIGURE 2.1: Obstruction de la vue en face avant

L'impossibilité d'identifier les cellules de base à travers le silicium en 'face arrière' est démontrée en photographiant un circuit avec une caméra sensible dans le domaine du visible et une caméra infrarouge, cf figure 2.2. En visible, l'imagerie via la face arrière silicium polie du circuit intégré ne donne aucune information. En infrarouge, nous pouvons uniquement distinguer des tailles variables de cellules de base. Nous insistons sur le fait que nous ne pouvons pas clairement les distinguer.

Ces éléments démontrent la nécessité d'une préparation afin d'accéder aux couches d'intérêt constituant les cellules de base précédemment décrites. Les techniques de rétro-conception permettent de répondre à ce besoin. Néanmoins, dans le chapitre 1, nous avons vu que la technique de rétro-ingénierie standard est applicable mais qu'elle est coûteuse en temps, en expertise et nécessite des outils dédiés à ce besoin. Nous nous orientons donc vers une méthode permettant de récupérer uniquement la localisation spatiale des caissons des transistors.

Des verrous ont été exposés dans le premier chapitre, notamment en termes de coût et d'expertise requis pour une campagne de rétro-conception classique. Comme alternative, nous proposons une méthode de rétro-conception partielle permettant de retrouver les cellules de base. Cette méthode proposée, SEMBA, a donc pour objectifs de répondre aux contraintes et besoins suivants :

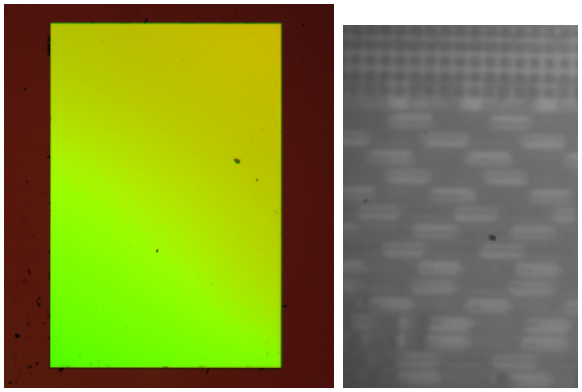


FIGURE 2.2: a) Imagerie visible de l'ensemble d'un CI (à gauche), b) Imagerie infrarouge d'une partie d'un CI (à droite)

- Rapidité de mise en oeuvre et de développement,
- couverture de l'ensemble de l'échantillon,
- solution peu coûteuse à l'utilisation,
- répétable sans besoin d'expertise,
- peu sensible à la préparation des échantillons,
- robuste aux différents types de circuits et noeuds technologiques utilisés par les fondeurs.

Dans ce manuscrit, le but final de la méthodologie est de pouvoir récupérer le positionnement de ces cellules de base afin d'effectuer des perturbations localisées ou de détecter des modifications malicieuses de ces cellules.

2.1.2 Définition de SEMBA

Vis-à-vis des contraintes évoquées, notre méthodologie "SEMBA" est composée des différentes étapes du tableau 2.1.

TABLEAU 2.1: Liste des étapes et sous-étapes de la méthodologie SEMBA

Etape 1 : préparation d'échantillons
Extraction du circuit intégré de son boitier
Retrait de toutes les couches métalliques
Bain de nettoyage
Etape 2 : acquisition et alignement d'images multiples automatisés
Paramétrage du MEB
Acquisition d'une mosaïque d'images couvrant la surface du CI
Alignement d'images multiples
Etape 3 : extraction de points d'intérêts
Localisation des différentes cellules de base
Outil de reconnaissance

Avec cette approche, les niveaux polysilicium et 'metal1'-'metal2' ne seront plus présents sur le composant, seul le substrat subsiste après préparation. Ainsi, il n'est pas possible de reconnaitre la fonction réalisée par chaque cellule de base en associant ces différents niveaux comme une

méthode de rétro-conception classique le permet. Cependant nous verrons que les formes de ces caissons observées vont permettre d'émettre des hypothèses sur leurs fonctionnalités.

Les techniques utilisées pour chacune des étapes sont ainsi décrites une à une avant d'être appliquées à trois échantillons différents. Il est évident que ce type de préparation rend l'échantillon non fonctionnel, cependant les résultats obtenus sont réutilisés sur d'autres CIs, fonctionnels.

2.1.3 Echantillons

Dans le cadre de ces travaux de recherche, la méthodologie SEMBA a été appliquée sur différents circuits afin de ne pas dévoiler des informations sensibles sur certains des dits circuits tout en mettant en évidence différent cas d'utilisation de SEMBA. Ces circuits sont répertoriés dans le tableau 2.1.3. Aucun des circuits n'a été aminci dans le cadre de nos travaux. L'amincissement est une opération mécanique de préparation qui consiste à réduire l'épaisseur du substrat. Cette dernière permet de réduire l'absorption du substrat.

Cet amincissement peut être réalisé pour réduire l'absorption du substrat de différents signaux pouvant le traverser.

Tableau 2.2: Liste des circuits utilisés

Numéro de circuit	Type de circuit	Utilisation dans ce manuscrit
N.1	Un ASIC implémentant un mécanisme de chiffrement	Illustration de la récupération de zones intéressantes à attaquer et illustration de l'application directe de méthodes d'analyse de fautes
N.2	Un circuit de type carte à puce	Illustration de l'injection contrôlée de fautes laser
N.3	Deux ASICs, un authentique (CHIPIT) et le deuxième intégrant un CTM (CHAMELEON)	Illustration de la détection de modifications malicieuses

2.2 Etape 1 : préparation d'échantillons

2.2.1 Accès aux couches métalliques et retrait

Un seul des échantillons (circuit N.2) utilisé dans cette étude n'a pas ses pistes métalliques directement accessibles. Les deux autres échantillons n'avaient expressément pas été mis en boitiers afin de mettre en oeuvre notre méthodologie. Le circuit intégré N.2 est encarté, comme schématisé dans la partie 1.15, et la face avant de ce dernier est recherchée pour l'application de la méthodologie SEMBA. Un masque fabriqué à l'aide de scotch aluminium est aposé sur le module afin de n'affecter que la zone où le circuit intégré est présent. De l'acide nitrique fumant (HNO_3) est appliqué sur cette fenêtre ouverte sans altérer les fils de connexion entre le circuit et le micromodule. La résine présente est ainsi retirée rendant la première couche métallique accessible.

Les couches métalliques sont ensuite intégralement retirées. Nous utilisons une gravure humide permettant d'enlever tous les oxydes présents entres les couches métalliques. Un bain d'acide fluorhydrique (HF) est utilisé. Les circuits intégrés sont trempés dans une solution HF 50% pendant plusieurs minutes. Les échantillons sont ensuite rincés à l'acétone et à l'eau. Au final, le circuit ne contient plus que le niveau BULK avec les zones actives des différents transistors comme seuls éléments visibles.

La gravure humide est suffisamment lente pour retirer/détacher toutes les couches du circuit. Elle se prémunie ainsi de possible différences de niveaux de préparations (couches métalliques toujours en place sur le circuit). A contrario, à des fins d'utilisation différentes, il est possible d'utiliser les avantages d'une gravure humide plus rapide. En effet des informations supplémentaires, provenant de plusieurs niveaux, peuvent être récoltées. Cette possibilité est détaillée dans l'annexe A.1.

2.2.2 Bain de nettoyage

Une photographie acquise à ce stade de la préparation permet de mettre en avant la présence aléatoire de résidus, cf figure 2.3. Nous notons, par exemple, la présence de plots tungstène et autres artefacts provenant des couches supérieures. Afin d'enlever ces résidus liés à la gravure, les circuits sont plongés d'un bain à ultrasons. Il en résulte une surface avec un nombre de défauts réduits, cf figure 2.3.

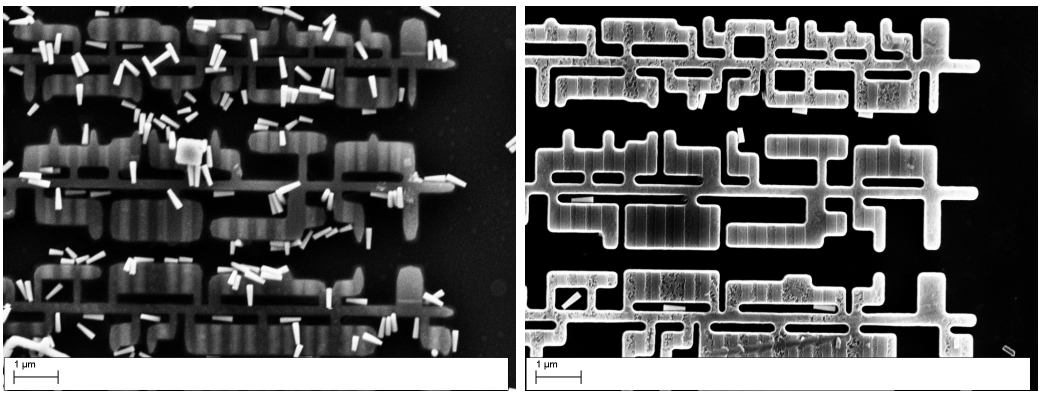


FIGURE 2.3: a) Acquisition après retrait des couches métalliques (à gauche), b) Acquisition après nettoyage au bain à ultrasons (à droite)

La plupart des artefacts de préparation sont retirés à l'aide d'un bain à ultrasons de quelques minutes. On obtient ainsi une surface homogène d'une couche du CI, la prochaine étape est donc l'acquisition d'images de l'intégralité de cette surface. Ainsi, à l'aide du MEB disponible, on visualise sur la figure 2.3 la même zone acquise avant et après nettoyage aux ultrasons.

A partir de photos sur plusieurs zones de la puce, on s'apercevoit que la préparation est homogène sur l'ensemble du composant.

2.3 Etape 2 : acquisition et alignement d'images multiples automatisés

2.3.1 Paramétrage du MEB

L'acquisition d'images se fait à l'aide d'un MEB, les différents circuits sont placés sur le porte-échantillon (8 supports présents), permettant ainsi de ne pas devoir 'casser' le vide nécessaire sous la colonne du dit équipement.

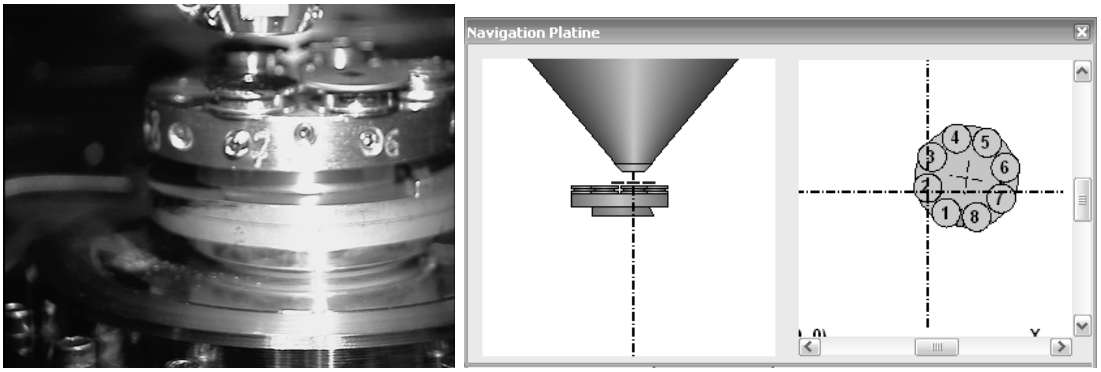


FIGURE 2.4: Sous la colonne du Microscope Electronique à Balayage (MEB)

Les circuits sont visualisés avec un détecteur classique d'électrons rétrodiffusés. Sur cette même figure 2.4, nous apercevons la courte distance de travail (distance entre la colonne et les échantillons). Elle est proche de 8mm afin de permettre d'obtenir la meilleure qualité d'image possible.

Les paramètres d'acquisition du MEB sont ensuite réglés pour obtenir une image permettant la distinction des différentes cellules de base (contraste, luminosité, type de détecteur, courant, tension d'accélération, astigmatisme) tout en prenant en compte la durée d'acquisition (vitesse de balayage, grossissement, surface à acquérir).

Prendre en compte le compromis vitesse d'acquisition et rapport signal/bruit

La vitesse d'acquisition dépend quant à elle principalement du temps que met le faisceau d'électrons pour balayer l'image et récupérer chaque électron rétrodiffusé. Le temps de balayage du faisceau d'électrons peut être modifié et affecte le rapport signal/bruit présent sur l'image, cf figure 2.5. Ainsi, plus la vitesse de balayage sélectionnée est petite et plus le rapport signal sur bruit sera important. A noter, le temps de balayage influe directement sur le temps d'acquisition de chaque image.

Dans le cadre de nos travaux, les images acquises servent de support de base pour la reconnaissance de motifs. En choisissant une vitesse de balayage plutôt moyenne (sélectionné à la valeur intermédiaire8 sous l'interface logiciel) et un grossissement faible (aux alentours de 3kX) par rapport au capacité du microscope (échelle de balayage possible de 1 à 15 et plage de grossissement allant jusqu'à 100 kX), nous avons récupérer des images sur lesquelles nous avons valider la détection de motifs avec un temps d'acquisition supportable (de l'ordre de l'heure). Le rapport signal sur bruit et la taille du motif sont fortement dépendants de ces 2 paramètres d'acquisition. Nous verrons que ce signal sur bruit est moins préoccupant pour un cas d'utilisation de la méthodologie SEMBA (la détection de Chevaux de Troie Matériels avec un circuit intégré comme référence).

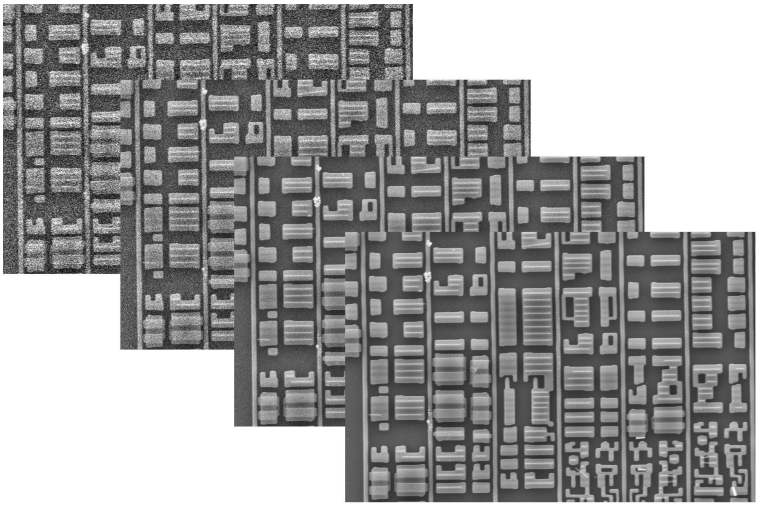


FIGURE 2.5: Modification du temps de balayage du plus au moins rapide (de gauche à droite)

Prendre avantage du type de détecteur

Il peut être intéressant de changer de détecteur et d'utiliser ainsi le détecteur 'BackScattered electron Detector' (BSD), dont un exemple est visible à droite de la figure 2.6. Avec ce détecteur et des paramètres donnés, on peut ainsi mettre en évidence la localisation de résidus. Dans ce cas, ce sont tout particulièrement les éléments conducteurs qui sont visualisés, on distingue les plots Tungstène qui réalisent en fait la jonction entre le niveau M1 et le niveau Grille. A terme, cette image pourrait être soustraite à une autre image composant le signal utile comme l'image acquise de la même zone avec le détecteur 'SE2'. Il en résulterait la suppression d'artefacts de préparation grâce à l'utilisation des avantages de plusieurs types de détecteurs (également réalisable en post-traitement).

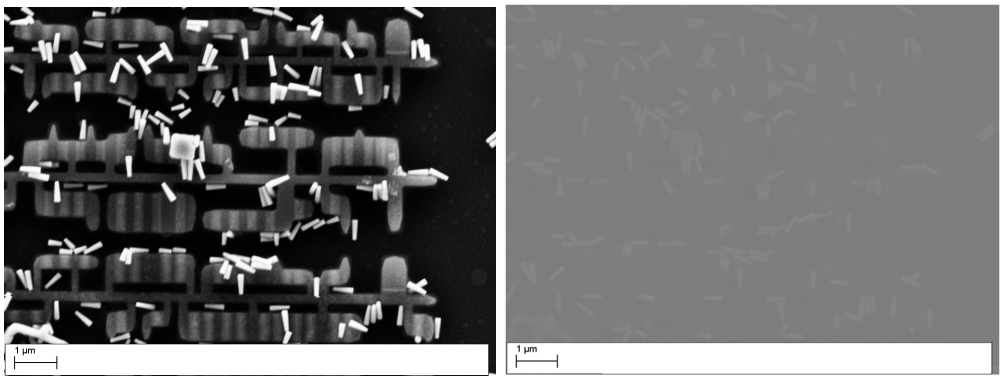


FIGURE 2.6: Utilisation du détecteur BSD pour mise en avant des résidus (vias)

On visualise figure 2.7 une même zone acquise avec deux modes de détecteur différents, le mode 'SE2' et le mode 'InLens'. Le grand avantage du mode Inlens est la rapidité d'obtention de l'image. Il faut environ 17 secondes pour acquérir la première image (détecteur SE2) et 8 secondes environ pour la deuxième image (détecteur InLens). Nous notons pour notre cas d'étude une différence de 9 secondes correspondant à une acquisition 53% fois plus rapide avec le mode 'InLens' qu'avec le mode 'SE2'. Même si l'optimisation du balayage de la matrice est

manuellement définie, on relève une grande différence de temps nécessaire entre les 2 modes utilisés pour une qualité d'image comparable. En effet pour notre besoin de repérer des motifs identiques, l'image InLens est tout autant intéressante.

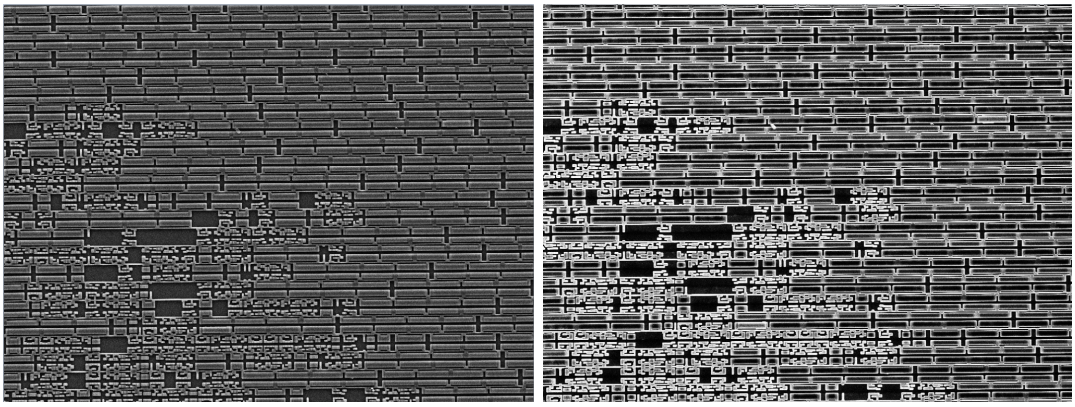


FIGURE 2.7: a) Acquisition avec détecteur SE (à gauche) et b) Acquisition avec détecteur Inlens (à droite)

2.3.2 Acquisition et alignement automatique d'une mosaïque d'images

Le MEB permet ainsi clairement de visualiser les différentes formes présentes sur le substrat silicium, image des zones d'implémentations des caissons des transistors. Ensuite, le but est de pouvoir récupérer cette information sur l'ensemble du circuit. Déplacer manuellement l'échantillon, enregistrer manuellement chaque zone, et enfin aligner une à une l'ensemble de ces images est possible mais prendrait des heures voire des jours. En effet, l'acquisition de plusieurs milliers d'images peut être requise. Bien heureusement, dépendant des caractéristiques du MEB utilisé, il est possible de rendre cette tâche automatisée. Notre équipement permet la création de routines. Nous définissons tout d'abord une matrice d'images à acquérir puis nous créons une routine parcourant chaque champ de la matrice à enregister. La définition de la matrice à acquérir comprend 4 étapes :

- Définition de la surface à balayer,
- vérification et modification des coordonnées de balayage,
- définition du grandissement souhaité,
- rajout de dépassement entre images successives.

Il en résulte la configuration finale de la matrice à acquérir telle que présentée figure 2.8. La taille de la matrice d'images (et donc le temps requis) dépend de la zone à balayer, du niveau de grossissement souhaité et du dépassement entre images souhaité.

Une fois la matrice définie, l'utilisateur doit ensuite contrôler le MEB afin de parcourir chacun de ses champs et les enregistrer. Ceci est effectué au travers d'une interface de programmation proposée par le logiciel du microscope utilisé. Une macro (script de quelques lignes) est ainsi écrite, cf figure 2.8. La macro créée intègre des délais pour laisser au faisceau d'électrons le temps de balayer l'échantillon. Chaque champ est ainsi sauvegardé dans un dossier sous la forme d'une image avec une compression non destructive (.TIFF).

Nous cherchons ensuite à reconstruire l'ensemble du circuit, ceci est réalisé par le biais de librairies libres accès. L'utilisation de ces librairies permet également l'automatisation de cette étape. Un dépassement entre images est rajouté, augmentant le nombre d'images à acquérir mais

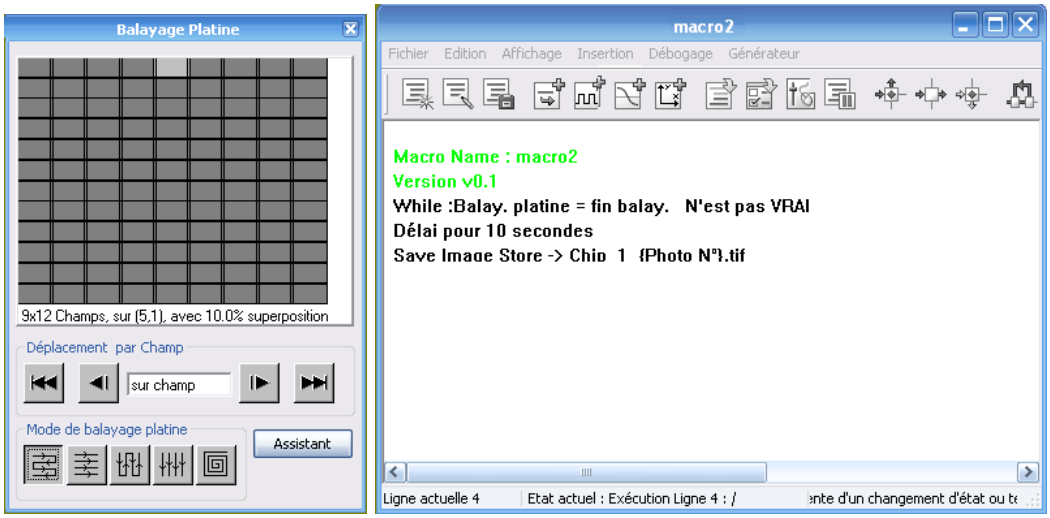


FIGURE 2.8: a) Définition de la matrice d'images à acquérir (à gauche), b) Acquisition de chaque champ de la matrice d'image (à droite)

permettant un recalage non erroné. En effet, dans le cas où des structures sont sensiblement identiques, le recalage peut être décalé de quelques μm. L'alignement d'images est basé sur les structures identiques présentes sur deux images successives.

L'alignement est effectué avec un outil dédié dont les paramètres d'entrés sont les suivants :

- Le nombre d'images par ligne de la matrice à acquérir,
- le nombre d'images par colonne de la matrice à acquérir,
- la manière dont la matrice est acquise (serpentin, de gauche à droite...),
- le dépassement entre chaque image successive utilisé lors de l'acquisition,
- le répertoire de travail et le numéro de la première image,

Notre solution est basée sur la méthode d'alignement par corrélation de phase, cf Kuglin et Hines [23]. Cette dernière comprend une transformée de Fourier de chaque image, la création d'une matrice de différence de phase et une fonction de corrélation utilisant la transformée inverse de Fourier sur la matrice précédemment créée. Cela permet de retrouver le décalage en [X,Y] d'une image par rapport à une autre. La jonction entre deux images est ensuite lissée de manière non-linéaire. La figure 2.9 illustre le résultat issu de l'alignement d'une partie de deux images successives d'un échantillon donné. Aucun défaut d'alignement n'est visible.

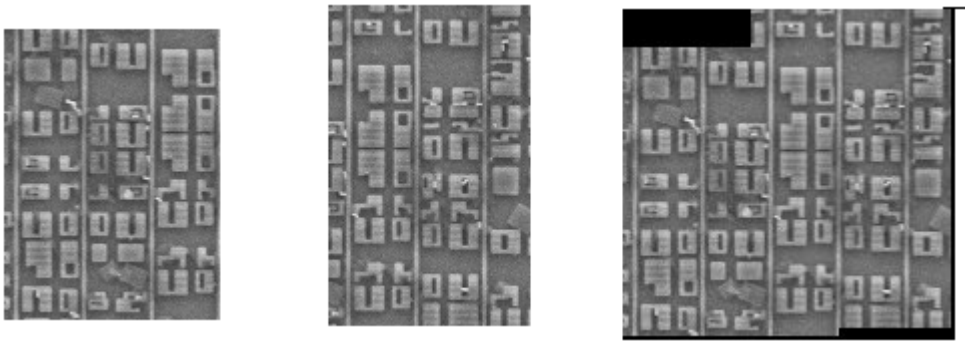


FIGURE 2.9: a) Première acquisition, b) Deuxième acquisition, c) Alignement des deux images successives

2.4 Etape 3 : extraction de points d'intérêts

2.4.1 Localisation des différentes cellules de base

Au vu de l'état de l'art (chapitre 1) des injections de fautes peuvent avoir des effets spatialement peu étendus, il semble intéressant de coupler approche invasive (chapitre 2) et une attaque précise par fautes. Les fautes de type laser, dont nous avons vu leur avantage en zone d'impact et en reproductibilité, sont choisies aux dépens d'attaques supposées avoir des effets moins localisés et supposées plus facilement détectables par un circuit intégré comme les perturbations électromagnétique, d'horloge ou d'alimentation (glitch).

Comme vu dans le chapitre 1, chaque circuit intégré standard (de type carte à puce) se compose de plusieurs milliers de cellules de base. L'image de base extraite avec notre méthodologie permet de différencier chaque instanciation de ces cellules de base. Pour un circuit de type carte à puce standard, nous notons qu'il existe environ 40 fonctions de cellules de base différentes, 600 cellules de base différentes pour obtenir au total une logique synthétisée d'environ 200000 cellules de bases. En comptant en moyenne 10 transistors par cellule, une logique synthétisée comporte au final 'seulement' 2 millions de transistors (contrairement aux PCs et leurs milliards de transistors).

Avec l'approche développée dans le chapitre 2, nous ne pouvons pas remonter jusqu'à la fonction effectuée par chaque forme répertoriée. En effet nous n'avons pas accès aux niveaux polysilicium et 'metal1'. Cependant en utilisant un grossissement plus important que celui utilisé pour acquérir l'ensemble du CI, il nous est rendu possible de repérer le nombre de transistors présents dans chaque cellule de base. Une fois ce nombre de transistors identifié, des hypothèses fortes peuvent être faites sur la fonction de la cellule de base observée [48].

2.4.2 Outil de reconnaissance de motifs

Dans la logique synthétisée, les cellules de base possèdent toutes la même hauteur mais la largeur de ces dernières diffère notamment en raison du nombre de transistors présents. Nous nous intéressons principalement aux bascules flip-flop qui sont d'un intérêt particulier car elles peuvent stocker des bits de clés, des données et des états internes de coprocesseurs. La sensibilité de ces cellules face à de possibles attaques est donc critique en matière de sécurité.

Nous avons développé notre propre outil de reconnaissance de motifs afin de ne pas dépendre de licence quelconque, de pouvoir créer un outil dédié à nos images issues d'un MEB et à notre besoin (un seul niveau du circuit intégré), et d'avoir plus de contrôle sur son efficacité et sur son temps de traitement. En annexe A.2, nous notons la pertinence d'une approche sur une image pré-traitée permettant de filtrer les informations présentes sur une image extraite de notre méthode de rétro-conception. De plus, un des grands atouts est de pouvoir choisir le type de sortie de l'outil de reconnaissance de motifs vis-à-vis des traitements ultérieurs.

L'outil est dédié à notre méthodologie SEMBA et utilise donc comme entrée l'image de base d'un niveau d'un circuit intégré après alignement de centaines d'images. Nous notons que cette image possède les propriétés suivantes :

- Un type d'image TIFF en noir et blanc dont chaque pixel est codé sur 8 bits,
- une taille de plusieurs millions de pixels et donc un espace mémoire de plusieurs centaines de Moctets,
- des motifs formés de quelques centaines de pixels à plusieurs milliers,

– des différences entre motifs portant sur seulement quelques dizaines de pixels,
– des artefacts liés à la préparation très bas coût et rapide effectuée.

Outre les caractéristiques fréquemment rencontrées pour la reconnaissance de motifs comme sa robustesse et son efficacité, cette application industrielle de reconnaissance de motifs sur circuits intégrés doit tenir compte des paramètres suivants :

– Des symétries horizontales, verticales et des rotations à 180 degrés des motifs à reconnaître,
– de la mémoire RAM pour parcourir les différentes images,
– et enregistrer des informations pertinentes relatives aux occurrences d'un motif (position, fiabilité de la détection, visuel du motif détecté comme identique)

Un algorithme de corrélation croisée normalisée peut être utilisé dans les applications où des variations de contraste ou de motifs sont enregistrées. Cet algorithme a notamment fait des preuves par le passé dans le domaine. Notre outil est également basé sur une implémentation de la fonction de corrélation croisée normalisée. Notre outil se compose d'une phase d'instanciation et de définition des motifs à reconnaître. L'outil parcoure ensuite l'ensemble de l'image et génère des fichiers de sortie enregistrant les propriétés de chaque cellule reconnue sur l'image (positionnement, orientation, valeur de seuil de détection définie et valeur de corrélation obtenue).

2.5 Mise en pratique de SEMBA

2.5.1 Outils et circuit de test

La préparation d'échantillon est effectuée en salle blanche, à proximité de la zone où se trouvait le microscope électronique à balayage. Ce microscope utilisé, cf figure 2.10, dispose de caractéristiques et de fonctionnalités bien supérieures à celles requises pour la méthodologie SEMBA. Un MEB Zeiss Ultra55 a été utilisé, il inclut notamment différentes sondes pour l'analyse chimique des matériaux. De plus, la résolution pouvant être atteinte est bien supérieure à notre cas d'utilisation où l'élément à isoler est déjà de plusieurs dizaines de microns.

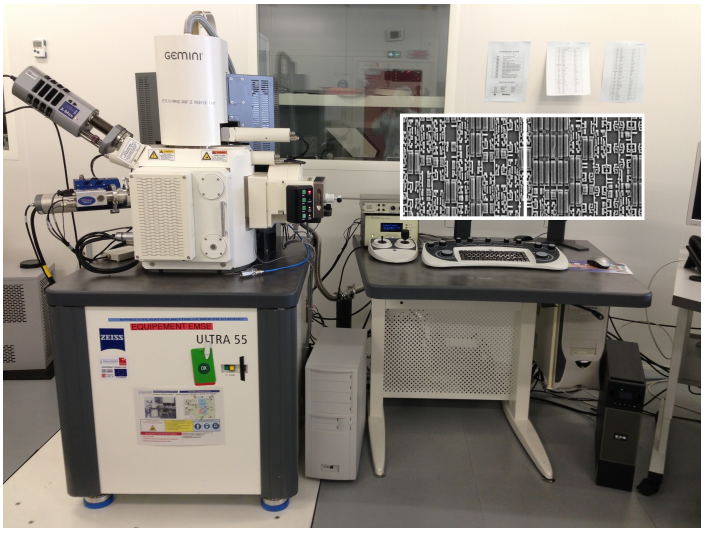


FIGURE 2.10: Microscope Electronique à Balayage utilisé

L'étape d'alignement des images est effectuée sur un ordinateur portable standard embarquant un processeur Intel Core Duo à 2.80 Ghz, 8GB de RAM et fonctionnant sur Windows 64-bit.

La méthodologie SEMBA a été appliquée sur différents circuits, nous indiquons dans ce chapitre l'application à un seul de ces circuits : le circuit N.1, cf 2.1.3. Ce dernier embarque de manière matérielle l'algorithme de chiffrement AES 128-bits fabriqué en technologie $0.13\mu m$ et conçu par le département 'Systèmes et Architectures Sécurisées' de l'Ecole des Mines de Saint-Etienne [39]. Une acquisition en microscopie optique face avant du circuit N.1 avant préparation est visible figure 2.11.

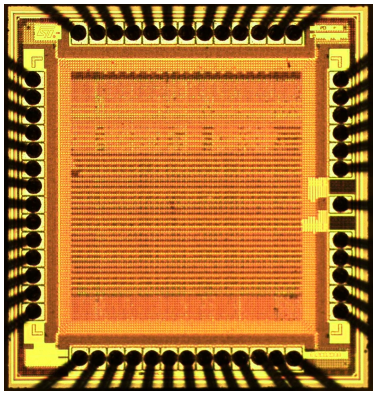


FIGURE 2.11: Vue face avant du circuit N.1 avant préparation, figure de Roscian *et al.* [66]

Nous appliquons ensuite la gravure humide évoquée précédemment. A noter tout de même que cette même microscopie optique aurait aussi pu répondre à notre besoin de visualisation de la topologie pour cet échantillon de quelques milliers de cellules de base, de noeud technologique assez grand et couvrant une petite surface. La figure 2.12 met en évidence la qualité d'acquisition entre une acquisition par microscopie optique et une acquisition par microscopie électronique de ce circuit préparé.

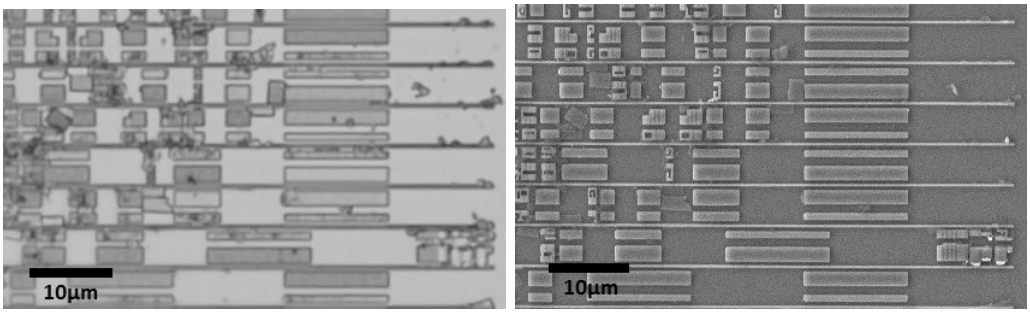


FIGURE 2.12: a) Imagerie optique (à gauche), b) Imagerie électronique (à droite)

Nous arrivons tout de même à distinguer des formes en microscopie optique . En effet, la valeur $0.13\mu m$ correspond seulement à la longueur de grille des transistors tandis que nous cherchons à photographier des cellules de base qui sont elles mêmes composées de plusieurs transistors, cf chapitre 1. Ces cellules sont de l'ordre de plusieurs μm^2, cf chapitre 1. Ainsi la microscopie optique peut répondre au besoin mais est moins intéressante que la microscopie électronique car :

- Un grossissement important (supérieur à 15kX) peut être nécessaire pour l'identification du nombre de transistors,

– la définition de la méthode doit être valable pour les prochains noeuds technologiques (en dessous de 65nm),
– l'illumination non uniforme et surtout la faible profondeur de champ en optique est trop contraignante sur de larges surfaces.

2.5.2 Acquisition de l'image de base du circuit N.1

Après validation de l'utilisation d'un MEB, un exemple d'image acquise est donné figure 2.13. On repère différentes formes après préparation de l'échantillon.

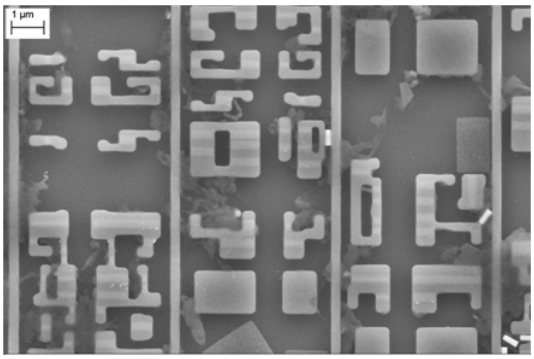


FIGURE 2.13: Différentes formes visibles après préparation

Nous y repérons différentes tailles et formes de motifs. Nous cherchons à récupérer l'ensemble de la logique synthétisée du circuit. Sur cet échantillon un grossissement de $2.2kX$ est choisi, un dépassement de 10% entre deux images successives est ajouté et la quasi-totalité du circuit est sélectionné (circuit presque uniquement constitué d'une logique synthétisée). Il en résulte pour cet échantillon une matrice de 8 images par ligne et de 7 images par colonne, cf figure 2.14.

FIGURE 2.14: Ensemble d'images acquises du circuit N.1

En utilisant notre outil d'alignement d'images multiples, la figure 2.15 permet de justifier la récupération d'une image d'un niveau d'un CI de manière automatique et ne présentant aucun défaut d'alignement visible. Cette image est appelée par la suite, image de base.

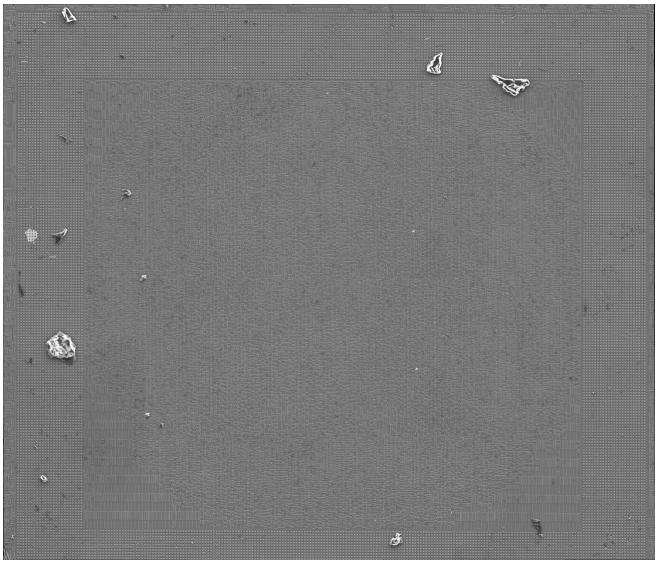


FIGURE 2.15: Image de base du circuit N.1 (intégralité de la surface acquise)

2.5.3 Recherche et identification de cellules d'intérêt

L'utilisation d'un microscope calibré permet de faire une correspondance entre pixels et taille réelle. Ainsi dans ce cas où le grossissement utilisé est de $2.2kX$, une distance de $10\mu m$ équivaut à 75 pixels. La figure 2.16 propose un grossissement numérique sur cette image. Sur ce cas d'acquisition, la largeur et la hauteur de chaque pixel est de $0.13\mu m$, un pixel couvre ainsi $0.018\mu m^2$. Nous identifions la forme correspondante à la plus petite (la moins large) cellule

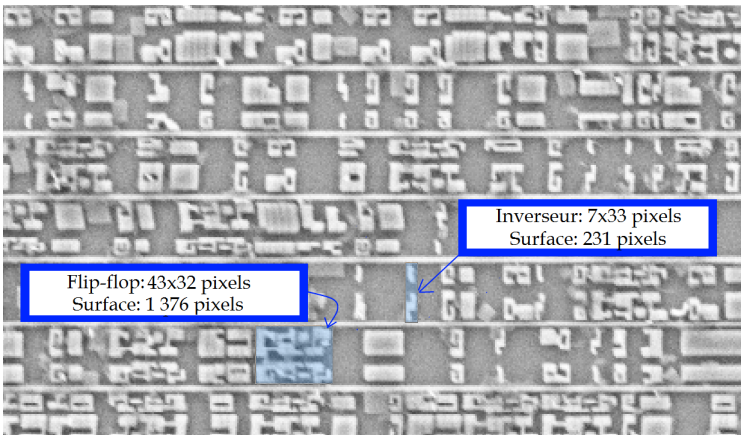


FIGURE 2.16: Couverture en pixels d'un inverseur et d'une flip-flop sur le circuit N.1

de base (l'inverseur) sur la figure 2.16. Cette cellule occupe 231 pixels soit environ 4.1 μm^2. Inversement la forme correspondante à la plus grande cellule de base se compose de 1376 pixels. Cette cellule couvre environ 24.5 μm^2. Comme indiqué précédemment, nous cherchons à retrouver un type de cellules d'intérêt et nous utilisons un grossissement plus important, cf figure 2.17.

Cette image est acquise au MEB avec un grossissement de $18kX$ sur l'échantillon N.1, outre les défauts de préparation qui sont visibles sans traitement de l'image, on peut tout d'abord voir que la zone la plus large correspond aux transistors PMOS et que la zone la plus fine

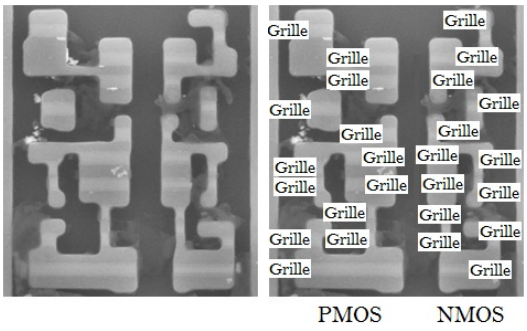


FIGURE 2.17: Identification du nombre de transistors dans une cellule de base acquise avec un grossissement de 18kX

correspond aux transistors NMOS. On peut également distinguer où était présente chaque grille de transistors au sein de cette cellule de base acquise. En affectant une grille entre chaque drain et source du composant, on trouve ainsi dans ce cas 13 transistors NMOS d'un côté et 13 transistors PMOS d'un autre côté. Cette forme de motif et ce nombre de transistors permettent d'émettre l'hypothèse que cette forme correspond à l'implémentation physique d'une bascule flip-flop.

L'hypothèse étant émise, le but est donc de retrouver toutes les instances de flip-flop sur l'ensemble du circuit. Sur l'image de base obtenue du circuit intégré (figure 2.15), nous appliquons la reconnaissance de motifs en sélectionnant directement le motif présumé comme étant une cellule flip-flop.

Quelques minutes suffisent pour obtenir le nombre total d'occurrences de la forme sélectionnée sur le circuit analysé. La figure 2.18 met visuellement en avant les résultats de la reconnaissance de motifs appliquée à ce circuit en associant un rectangle noir pour chaque cellule de base localisée. Ce résultat présenté est obtenu en utilisant un seuil de corrélation faible. Ce choix est pris afin de récupérer les occurrences de toutes les cellules flip-flop présentes dans le circuit. Avec un seuil de reconnaissance bas, des faux positifs sont présents dans le fichier de sortie (en effet d'autres cellules sont considérées par l'outil comme des cellules flip-flop). Nous anticipons ainsi le fait que la récupération de zones sensibles supplémentaires (alors qu'elles ne le sont pas) est moins contraignant que la non reconnaissance d'une cellule sensible. Les résultats sont enregistrés au format texte pour être facilement traités. Nous enregistrons notamment la valeur de corrélation, le seuil de corrélation choisi, le positionnement XY de la cellule en pixels ainsi que l'orientation de la cellule reconnue (symétrie horizontale, verticale ou miroir).

Sur ce dit circuit, notre outil de reconnaissance de motifs récupère 396 occurrences de cette forme sélectionnée car supposée être une cellule flip-flop. Le nombre d'occurrences obtenu n'est pas 256 comme le nombre de flip-flop utilisés dans le chemin de données (128 bits de données qui sont doublés par une contremesure) car notamment ces mêmes cellules flip-flop peuvent être utilisées pour d'autres besoins dans ce circuit.

Cet outil de reconnaissance a été utilisé sur un circuit composé d'environ 15000 cellules de base, ce qui signifie que trouver une forme 'supposée' de flip-flop est plutôt simple vis-à-vis d'une application sur des circuits type carte à puce où le nombre de cellules différentes est plus important.

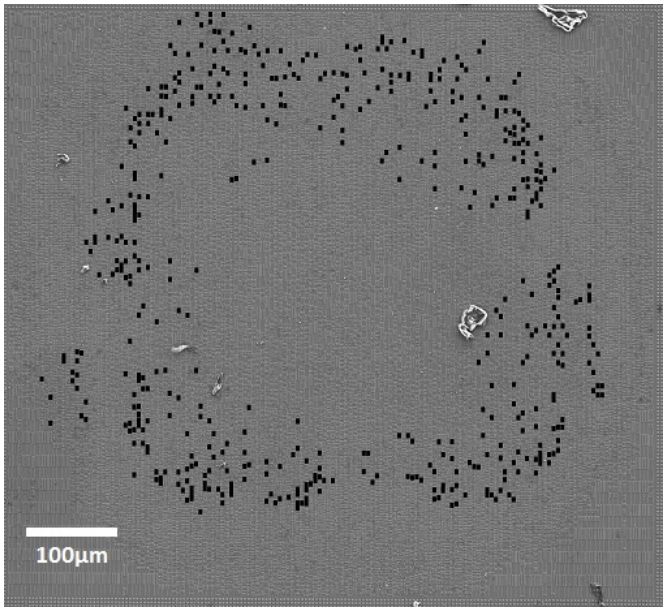


FIGURE 2.18: Reconnaissance du motif sur l'ensemble du circuit N.1, grossissement : 2.2kX

2.5.4 Coût jusqu'à l'extraction de zones à attaquer

Le tableau 2.3 donne l'effort nécessaire depuis la mise à disposition du circuit jusqu'à l'extraction des cellules intéressantes à perturber. Ce tableau 2.3 permet de distinguer les avantages en termes de temps et de coût de la technique proposée.

TABLEAU 2.3: Tableau d'effort pour retrouver la zone d'intérêt

Tâche	Coût (si équipement acheté)	Coût/heure (si équipement loué)	Temps de développement ou de mise en place	Temps opérateur	Automatisé ?
Préparation du circuit	3kEuros	50Euros	5min	5min	Non
Acquisition d'images	200kEuros	300Euros	5min	15min	Oui
Alignement d'images	NA	NA	2 semaines	2min	Oui
Sélection de motifs	NA	NA	0min	10min	Non
Extraction de flip-flop	NA	NA	2 mois	2min	Oui

2.6 Conclusion

Ce chapitre présente une méthodologie de rétro-conception matérielle partielle baptisée SEMBA pour 'Scanning Electron Microscope Based Acquisition technique'. Cette technique permet de récupérer des informations sur les cellules de base implémentées dans un circuit intégré, de connaître le nombre d'occurrences et les localisations spatiales pour chacune des cellules de base constituant la logique synthétisée. SEMBA nécessite trois étapes ; la première où le circuit intégré est préparé, la deuxième où des acquisitions d'images sont effectuées et enfin la troisième où ces images sont traitées afin de reconnaître chaque occurrence de cellules de base et ce sur l'ensemble du composant. Le tableau 2.4 récapitule les différentes étapes de SEMBA et associe leur rôle, le temps de développement et de mise en oeuvre pour chacune d'entres elles.

Tableau 2.4: Récapitulatif de la mise en oeuvre de SEMBA

Tâche	Rôle	Temps opérateur / (temps de développement)
Décapsulation du circuit intégré	Accéder au niveau métal le plus haut	5min / NA
Retrait total des couches métalliques	Accéder au niveau substrat	10min / NA
Bain de nettoyage	Enlever les résidus de gravure	10min / NA
Paramétrage du MEB	Visualiser les régions actives des cellules de base	15min / NA
Acquisition MEB d'un circuit intégré	Acquérir automatiquement une puce complète	Environ 20min pour 1 mm^2* / (15min)
Alignement d'images multiples	Recaler chaque sous-partie de la puce	Environ 3min pour 1 mm^2* / (20min)
Développement d'un outil de reconnaissance de motifs	Avoir un outil robuste de reconnaissance de cellule de base	NA / Plusieurs mois
Sélection d'un motif à reconnaître	Enregistrer la forme d'une cellule de base d'intérêt	Quelques minutes
Application de la reconnaissance de motif	Récupérer le positionnement de chaque cellule de base d'intérêt	Quelques minutes

* = Exemple pris pour un grossissement de 2500X et une vitesse de balayage moyenne

Les informations spatiales récupérées à l'aide de la méthodologie SEMBA peuvent être vues comme des empreintes du circuit intégré à tester, cf figure 2.19.

La nouveauté de notre approche réside dans la combinaison et l'automatisation de ces différentes étapes. Outre la définition de la méthodologie, sa mise en oeuvre a été validée sur de multiples échantillons confirmant ainsi l'accès à des informations au niveau transistor. Nous avons démontré qu'il est possible de passer d'une rétro-conception standard à une rétro-conception partielle pour obtenir des informations de localisation sur le circuit. Les ressources en termes d'outil,

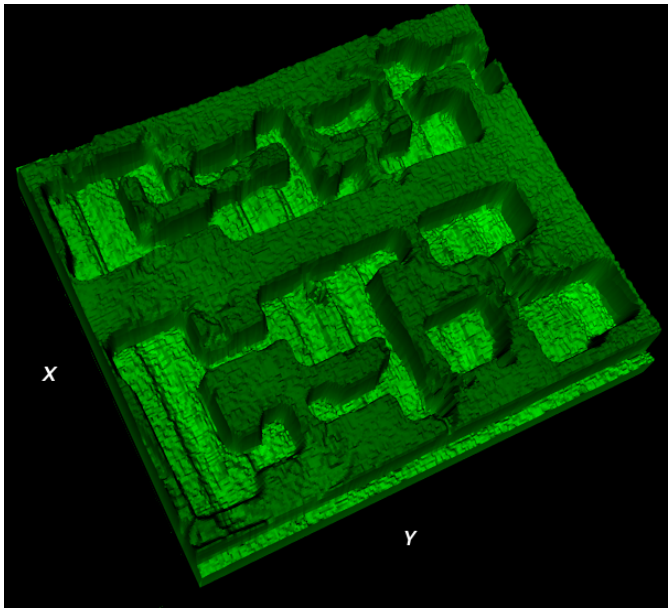


FIGURE 2.19: La méthodologie SEMBA permet de récupérer les empreintes de circuits intégrés (Même données vues figure 2.17)

de coût, de temps, et d'expertise sont ainsi minimisées avec notre approche et permettent d'avoir une autre vision de la rétro-conception matérielle [28]. Les avantages de la méthodologie SEMBA proposée sont récapitulés dans le tableau 2.5.

TABLEAU 2.5: Avantage de la méthodologie SEMBA

Domaine	Avantages
Robustesse	Indépendance vis-à-vis du noeud technologique, du fondeur
Avantage industriel	Rapidité d'application
Avantage industriel	Coût total faible
Avantage industriel	Expertise opérateur requise faible
Avantage industriel	Méthode standard et réutilisable
Avantage industriel	Nombre d'échantillon nécessaire réduit à 1
Multiples utilisations	Une méthodologie permettant de construire des bibliothèques d'images de CIs
Multiples utilisations	Une méthodologie dont la sortie peut être utilisée pour différentes applications
Flexibilité	Une méthodologie flexible où d'autres étapes peuvent être greffées.

Chapitre 3

SEMBA appliquée aux attaques lasers ciblées et contrôlées

La possibilité de récupérer la localisation des cellules de base de l'ensemble d'un circuit intégré a été démontrée dans le chapitre 2. Une fois ces cellules spatialement localisées, les capacités de notre plateforme laser nous permettent de viser directement ces cellules. On démontre qu'il est possible de contrôler le modèle de fautes suivant l'énergie utilisée ou encore la localisation du faisceau laser. Ce contrôle est effectué sur un circuit de technologie récente ($90nm$) et sur une cellule complexe composée de quelques dizaines de transistors (26). Nous validons également l'application de l'analyse de fautes avec de telles capacités d'injections laser.

Sommaire

3.1 Proposition d'attaque combinée : faute laser et rétro-conception partielle

Dans l'état de l'art, nous avons vu que le succès des attaques laser étaient dues à la localisation du faisceau appliqué sur le circuit intégré, en effet des zones sont plus ou moins sensibles à l'injection laser. Avec la méthodologie SEMBA nous avons vu également que nous sommes capables de retrouver des zones sensibles à l'échelle de la cellule de base. La méthode est répétable et efficace. Vis-à-vis de l'état de l'art, peu de publications proposent de combiner attaque par fautes laser et attaque invasive. Notre idée est donc de proposer une combinaison efficace d'attaque par fautes (localisées) et de rétro-conception (partielle). L'utilisation de la méthodologie SEMBA appliquée à la génération de fautes laser ciblées et contrôlées nécessite deux circuits identiques, un circuit dont la face avant est accessible et un deuxième dont la face arrière est accessible, cf figure 3.1. Le premier, sur lequel SEMBA est appliquée, sera irréversiblement non fonctionnel tandis que des injections laser seront effectuées sur le second à l'aide d'informations récoltées par SEMBA sur le premier circuit.

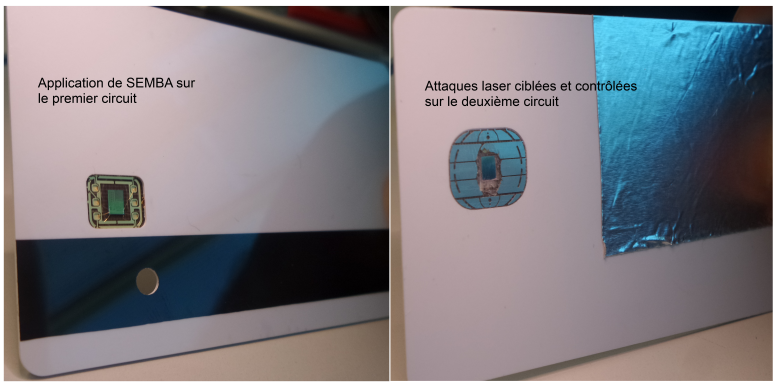


FIGURE 3.1: a) Accès au circuit face avant (à gauche), b) Accès au circuit face arrière (à droite)

3.2 Application de SEMBA pour la perturbation de cellules flip-flop d'un AES matériel

Le circuit N.1 est réutilisé pour cette application, nous donnons plus de détails sur ce dernier avant l'application aux attaques laser. Ce circuit fabriqué en technologie $0.13\mu m$ a une épaisseur d'environ $300\mu m$. Nous communiquons avec ce circuit par une liaison série, un message en clair et une clé de chiffrement sont ainsi envoyés. Le circuit renvoie en retour un message chiffré sur le même canal de communication. Ce circuit comporte 15k cellules et intègre une redondance matérielle comme contremesure. Le chemin de données est dupliqué comme illustré sur la figure 3.2. Ainsi, si une faute est obtenue, plusieurs octets seront fautés lors de la réception du chiffrement effectué.

Sur ce circuit, nous utilisons notre capacité à localiser les cellules de bases. Les cellules flip-flop qui ont été identifiées avec la méthodologie SEMBA du chapitre 2 sont ainsi la cible d'injections laser car elles stockent entre autres les données intermédiaires du calcul de l'AES. Nous rappelons que notre outil de reconnaissance de motifs a permis de retrouver 396 motifs supposés être des formes plausibles de cellules flip-flop.

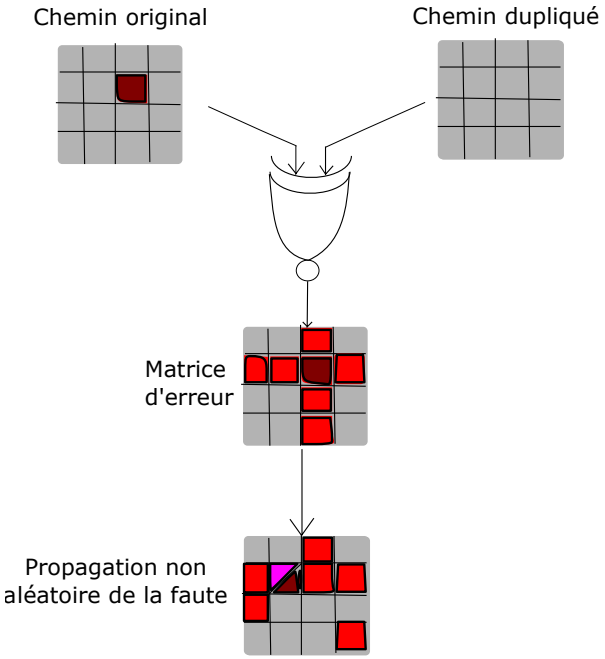


FIGURE 3.2: Contremesure embarquée sur le circuit N.1

3.2.1 Intégration des coordonnées sous la plateforme laser

Le fichier de sortie de la reconnaissance de motifs est conservé, tout comme l'image MEB du circuit intégré. Afin de placer le faisceau laser sur les motifs identifiés, il faut tout d'abord faire une correspondance entre ces motifs reconnus sur le premier circuit détruit et le circuit actuellement sous l'objectif de la plateforme laser. Les propriétés données dans la sous-section 1.3.2 sont utilisées ; l'imagerie face arrière infrarouge est le lien entre la plateforme laser et l'image MEB. Ainsi sur la figure 3.3, il est possible de visualiser les mêmes références sur les images face avant et face arrière. Nous rappelons que contrairement à la technique de visualisation face avant au MEB, l'imagerie face-arrière permet de photographier la puce tout en la gardant fonctionnelle mais que la différenciation des formes est très limitée.

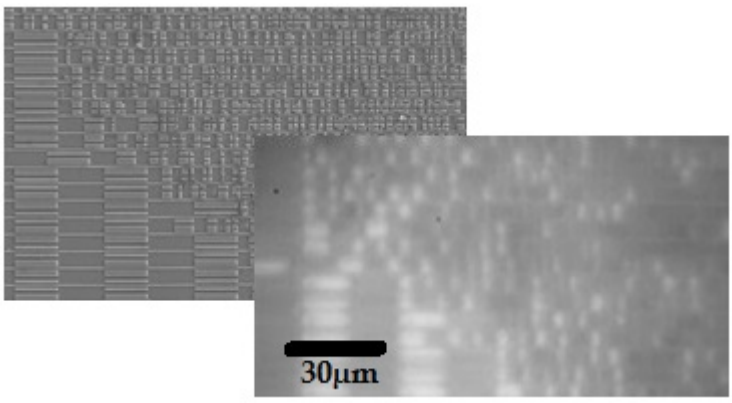


FIGURE 3.3: a) Image face active acquise au MEB (à gauche), b) Image face arrière acquise avec une caméra infrarouge (à droite)

Avec cette correspondance effectuée, il est donc possible de positionner le faisceau laser sur chaque motif détecté de la figure 3.4. Le pas de déplacement le plus faible de notre plateforme est de $0.1\mu m$, et le setup matériel de notre plateforme nous permet d'obtenir un repositionnement sans dérive. Toutes les cellules flip-flop identifiées ont leurs positions marquées dans un fichier .txt que l'outil d'attaque peut récupérer. Cet outil contrôle la communication avec le circuit de test, le positionnement de l'échantillon par rapport à la colonne optique ainsi que les paramètres de déclenchement du faisceau laser. Un des paramètres est l'énergie du faisceau, pour ce cas d'étude il est choisi de manière empirique et est de plusieurs dizaines de nJ.

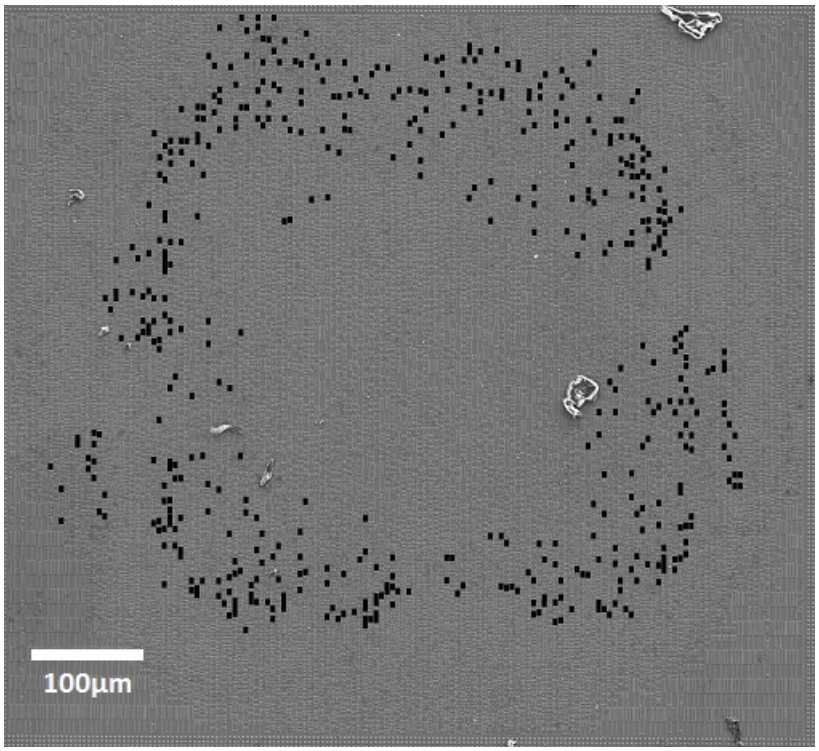


FIGURE 3.4: Résultat de reconnaissance des cellules flip-flop (sous forme graphique)

3.2.2 Mise en pratique de l'analyse de fautes

La possibilité de viser des zones spatiales précises est intéressante pour injecter des fautes dites locales. Le déplacement et le tir pour couvrir l'ensemble de ces 396 positions nécessite seulement 7 minutes avec notre plateforme d'injection. Dans notre cas, un seul tir par position est effectué car la contrainte temporelle est facilement maitrisée sur ce circuit. En effet il nous est possible de récupérer la consommation de courant du circuit et de distinguer les différents tours de chiffrement. Le but est d'attaquer juste avant le dernier tour de chiffrement pour retrouver plus facilement la clé de chiffrement utilisée. Le composant a une fréquence de fonctionnement de $25MHz$ et effectue un tour de chiffrement à chaque coup d'horloge. Une sonde de courant est utilisée pour observer la consommation du circuit. Dans la mesure où ce composant ne propose pas de contremesure, les différents tours de l'AES sont repérables en particulier l'avant dernier qui nous intéresse plus particulièrement. Ainsi, l'injection de fautes est synchronisée avec ce signal grâce à l'électronique de déclenchement présent sur la plateforme laser. Sur notre échantillon, la synchronisation nécessaire (attaque sur l'avant dernière ronde de l'AES) est facile à obtenir avec

la récupération du courant consommé par le circuit et visualisé à l'oscilloscope, cf figure 3.5.

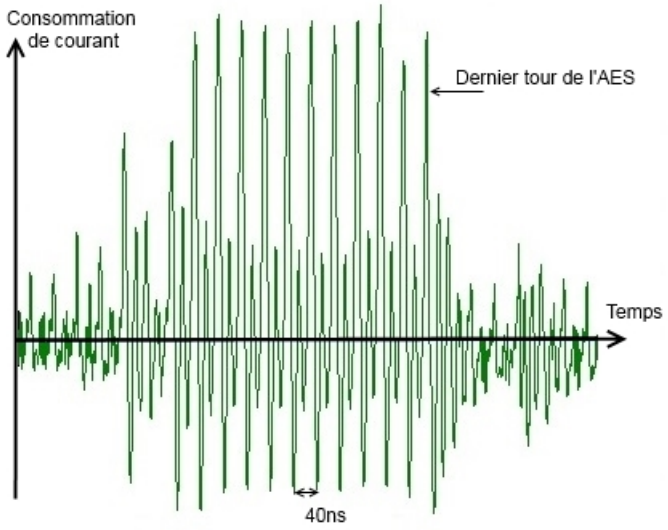


FIGURE 3.5: Courbe de consommation du circuit intégré

Sur cet échantillon sans contremesure temporelle, les pics correspondent au chargement des données et à chaque ronde de l'AES ; ils sont facilement identifiables. On se place juste après le 10ème pic car le premier pic correspond au chargement des données. Un décalage de quelques ns est rajouté pour que l'attaque intervienne juste avant le 10ème et dernier tour du processus d'encryption.

Nous verrons dans les sections suivantes qu'il est possible de contrôler avec un seul tir laser la valeur contenue dans chacune de ces bascules, cf partie 3.3.1. En prenant cette réalité en compte, le temps requis de 7 minutes pour contrôler chacune de ces 396 cellules est conforme à nos possibilités d'injection de fautes laser contrôlées. Sans information de localisation de ces cellules flip-flop au préalable, il aurait fallu balayer l'ensemble du composant pour récupérer des fautes d'intérêt. A titre de comparaison, nous avons balayé l'ensemble de la puce avec un pas d'un μm, sur la même plateforme laser (104400 tirs laser), le temps requis est de 1680 minutes soit un temps d'utilisation de la plateforme laser 240 fois plus important. Les fautes obtenues sont représentées sur la figure 3.6. Outre la possibilité de comparer la vitesse atteignable entre les deux approches, nous validons par le résultat de la cartographie laser que les cellules reconnues étaient bien des cellules flip-flop (le visuel d'effets obtenus est également en forme de cercle). Cette capacité est intéressante car comme brièvement indiqué dans la section 1.4.3, il est possible de retrouver des valeurs de clé avec l'injection de quelques fautes.

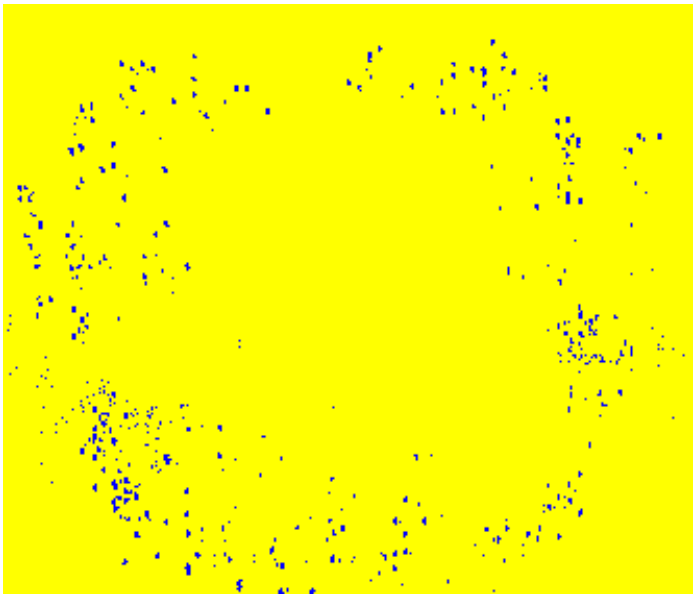


FIGURE 3.6: Cartographie de fautes laser avec un balayage d'un μm sur l'ensemble de la puce

En entrée du circuit utilisé, un message à chiffrer et une clé de chiffrement sont instanciés. Un message chiffré en sortie de l'AES est attendu. Pour illustrer l'analyse différentielle de fautes et l'analyse en "safe error", les valeurs ci-dessous sont utilisées à titre d'exemple.

- Message clair : 21 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- Clé de chiffrement : 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- Message chiffré attendu : 89 1D 0C E5 EA 68 16 12 AA 98 9C A2 79 77 3F 01

Analyse différentielle de fautes Pour un attaquant, le meilleur moyen d'exploiter une faute injectée est d'effectuer cette dernière sur un seul bit et à un moment précis du processus d'encryption [41].

De manière répétable, nous arrivons à obtenir des fautes mono-bits sur les cellules repérées qui font partie du chemin de données de l'AES. Par exemple nous obtenons la valeur suivante à une position spatiale donnée : 89 1D **2**C **C**5 EA **4**8 16 **3**2 **8**A 98 9C **8**2 79 77 3F **63**. Cette dernière est à comparer avec le message chiffré attendu. La contremesure de ce circuit n'étant pas aléatoire, il est possible de remonter jusqu'au bit fauté et donc d'avoir une méthode où l'application de l'analyse différentielle de fautes est directe. En effet, la contremesure est non reliée à un générateur d'aléas, on obtient seulement 6 octets avec le même vecteur d'erreur et un octet avec une valeur différente.

Afin de récupérer des informations sur la perturbation effectuée, nous utilisons un fichier de traitement dédié avec comme seul contenu la réponse prévue et celle obtenue après perturbation. En sortie de ce fichier de traitement, nous obtenons, le temps de l'injection dans l'algorithme (numéro du tour de l'AES fauté), la position de l'octet fauté (quel octet est perturbé) et enfin la faute générée (quel bit a basculé). Ainsi, avec la possibilité de retrouver une cellule flip-flop, cf partie 2.4, et la possibilité de contrôler chaque cellule flip-flop, cf partie 3.3.1, la mise en oeuvre de l'analyse différentielle de fautes est facilitée.

Safe error L'application de notre technique semble adaptée à l'analyse 'safe error'. Comme vu dans l'état de l'art au chapitre 1, la 'safe error' est aussi basée sur la capacité à comparer un chiffrement fauté et un chiffrement correct. Le principe de la 'safe error' est simple, l'attaquant émet l'hypothèse sur un modèle de fautes, si la valeur change alors une faute a été injectée et permet d'être retrouvée. Blömer et Seifert [15] vise le tour initial de l'AES pour retrouver bit à bit la valeur de la clé. On reconnaît que cette technique pourrait être appliquée aux flip-flop stockant les clés. Avec notre technique nous ne pouvons pas connaître à priori quelle flip-flop correspond à quelle fonction (stocker des valeurs de contrôle, des valeurs de clés ou des valeurs de données).

Un seul tir laser peut être utilisé par flip-flop repérée (au nombre de 396). Si le choix porte à considérer le modèle de fautes 'mise à 1' obtenu par positionnement du faisceau laser, cf partie 3.3.1, l'attaquant peut viser les transistors PMOS pour chaque flip-flop. Si un changement est détecté, cela signifie que la valeur originale (avant perturbation) du bit visé était '0', si rien ne se passe alors cela signifie que la valeur originale du bit visé était de '1'. Sur ce cas d'étude, près de deux tirs sur trois (256 sur 396) peuvent avoir un impact sur le chemin de données. En effet, le chemin de données dupliqué de cet AES 128 bits utilise un nombre de 256 flip-flop physiquement implémentés, le reste étant utilisé pour d'autres besoins. Pour attaquer ces 396 positions à l'aide de notre plateforme laser, seulement quelques minutes sont nécessaires. La capacité de retrouver où sont placées les cellules flip-flop combinée à la capacité de les perturber individuellement permet de récupérer bit à bit les données stockées.

3.3 Attaques laser ciblées et contrôlées sur un circuit intégré 90nm

Des attaques laser ciblées et contrôlées ont été effectués sur le circuit N.2, conçu en technologie $90nm$ provenant du marché actuel de la carte à puce. Son épaisseur est d'environ $150\mu m$. Sur ce circuit, on distingue les différentes parties d'un circuit intégré dont la logique synthétisée composée de quelques 200000 cellules soit environ 14 fois plus que le circuit de chiffrement précédent étudié dans ce chapitre 2. Il intègre des capteurs de lumière comme contremesure notamment. L'ensemble du circuit couvre environ 6*8mm et est constitué de 5 niveaux métalliques.

Deux circuits identiques sont utilisés, un restera fonctionnel tandis que l'autre est le terrain d'application de SEMBA. La zone à acquérir tout comme le grossissement utilisé sont plus grand sur ce composant. Il en résulte l'acquisition de plusieurs centaines d'images. Pour des raisons de confidentialité, nous ne donnerons ni la surface de la logique synthétisée ni les dimensions de l'image finale obtenue par la concaténation de plusieurs centaines d'images. L'image finale résultante fait 250Mb et plus de 217 millions de pixels. Un grossissement de 3kX est utilisé sur ce composant, il faut environ 1h30 pour acquérir l'ensemble de la logique synthétisée correspondant donc à la matrice d'images définie. Une partie de cette image est visible sur la figure 3.7 qui met en évidence des différences caractéristiques entre les caissons de circuit et ceux du précédent étudié. On peut notamment apercevoir l'aspect complètement différent de l'implémentation des caissons sur ce circuit intégré par rapport au circuit précédent. Néanmoins, on note tout de même sur cette image des correspondances avec le précédent échantillon, les prises au substrat de la masse et de l'alimentation, les côtés P et les côtés N, et des formes assez proches et rectangulaires qui se répètent.

L'identification de cellules sensibles ayant déjà été démontrée, nous nous attachons dans les sections suivantes à caractériser l'effet laser sur une zone où plusieurs cellules d'intérêt sont présentes. Cette zone peut être récupérée par la méthodologie précédemment décrite (cf partie 2.4). Ainsi, une zone restreinte de 30 par 38 μm où seuls 8 bits d'un registre sont implémentés est donc conservée. Nous rappelons que seules deux valeurs peuvent être stockées dans une bascule flip-flop, un '0' ou un '1' logique. C'est un échantillon ouvert sur lequel il nous est notamment possible d'avoir accès à différents registres en lecture et en écriture. On utilise un protocole de communication de type ISO classique carte à puce (cf partie 1.1.3) afin de récupérer la valeur stockée dans ce registre. Notre plateforme laser nous permet d'enregistrer pour chaque faute obtenue sa position spatiale dans un fichier texte. Nous avons ensuite un outil qui nous permet d'attribuer pour chaque type de faute une couleur donnée et de l'afficher sur une cartographie spatiale [X,Y]. D'après l'état de l'art, le maximum de photocourant est généré lorsque la mise au point est réglée au niveau des caissons, cf partie 1.29. Ainsi, l'axe Z est réglé de manière à obtenir une visualisation niveau caissons des transistors (visualisation du circuit).

3.3.1 Contrôle de la valeur d'un bit par localisation du spot laser

Dans cette sous-section, nous démontrons la possibilité de contrôler la valeur de ce registre en faisant varier le positionnement spatial du spot laser. Nous jouons sur les valeurs d'initialisation du registre avant de balayer la zone restreinte de 1140 points (30*38μm) par pas d'un μm. L'énergie laser est gardée constante sur les trois prochaines acquisitions et elle est de plusieurs dizaines de nJ. La taille du faisceau laser utilisé est d'environ 1μm. Un pixel noir obtenu dans les prochaines cartographies repère les positions où le faisceau laser n'impacte pas la valeur stockée.

Ainsi, pour le premier balayage (à gauche sur la figure 3.8), les valeurs de départ de chacun des bits de ce registre sont à '0' (le registre de 8 bits est initialisé à $0000\ 0000_2$) avant de balayer la zone de 30 par 38 μm. Le taux d'injection est de 100%, un seul tir par position est utilisé. En parcourant plusieurs fois la matrice, nous avons seulement quelques pixels qui varient entre balayages identiques. Comme tous les bits du registre sont initialisés avec une valeur '0' avant ce premier balayage laser, nous pouvons détecter lorsque l'injection laser a pour effet de basculer la sortie à '1'. Grâce à ce premier balayage laser, on obtient la localisation spécifique où le laser doit être appliqué pour changer la valeur d'un bit de '0' vers '1' est obtenue, cf en orange sur la figure 3.8. Huit ensembles de pixels sont facilement identifiables et un ensemble correspond donc à la sensibilité à la transition de '0' vers '1' d'un bit de ce registre.

La même méthodologie est appliquée pour récupérer les positions sensibles à une transition de '1' vers '0' en initialisant cette fois le registre à $1111\ 1111_2$. La cartographie récupérée est au milieu de la figure 3.8. Nous repérons en bleu les zones sensibles au bit set.

Ensuite, grâce à notre précision spatiale nous pouvons superposer ces deux précédentes cartographies pour obtenir une dernière cartographie (à droite sur la figure 3.8) indiquant les positions sensibles au bit set en orange et les positions sensibles au bit reset en bleu. On peut apercevoir que ces zones sensibles sont distinctes les unes des autres. Ainsi, on en déduit que pour chacun des bits composant ce registre l'utilisation d'un seul tir laser visant la position sensible permet de contrôler avec certitude la valeur stockée. Un tir laser effectué à une localisation où un carré bleu est présent permet de mettre à '0' la valeur d'un bit. Inversement, un tir laser effectué à une localisation où un carré orange est présent permet de mettre à '1' la valeur d'un bit.

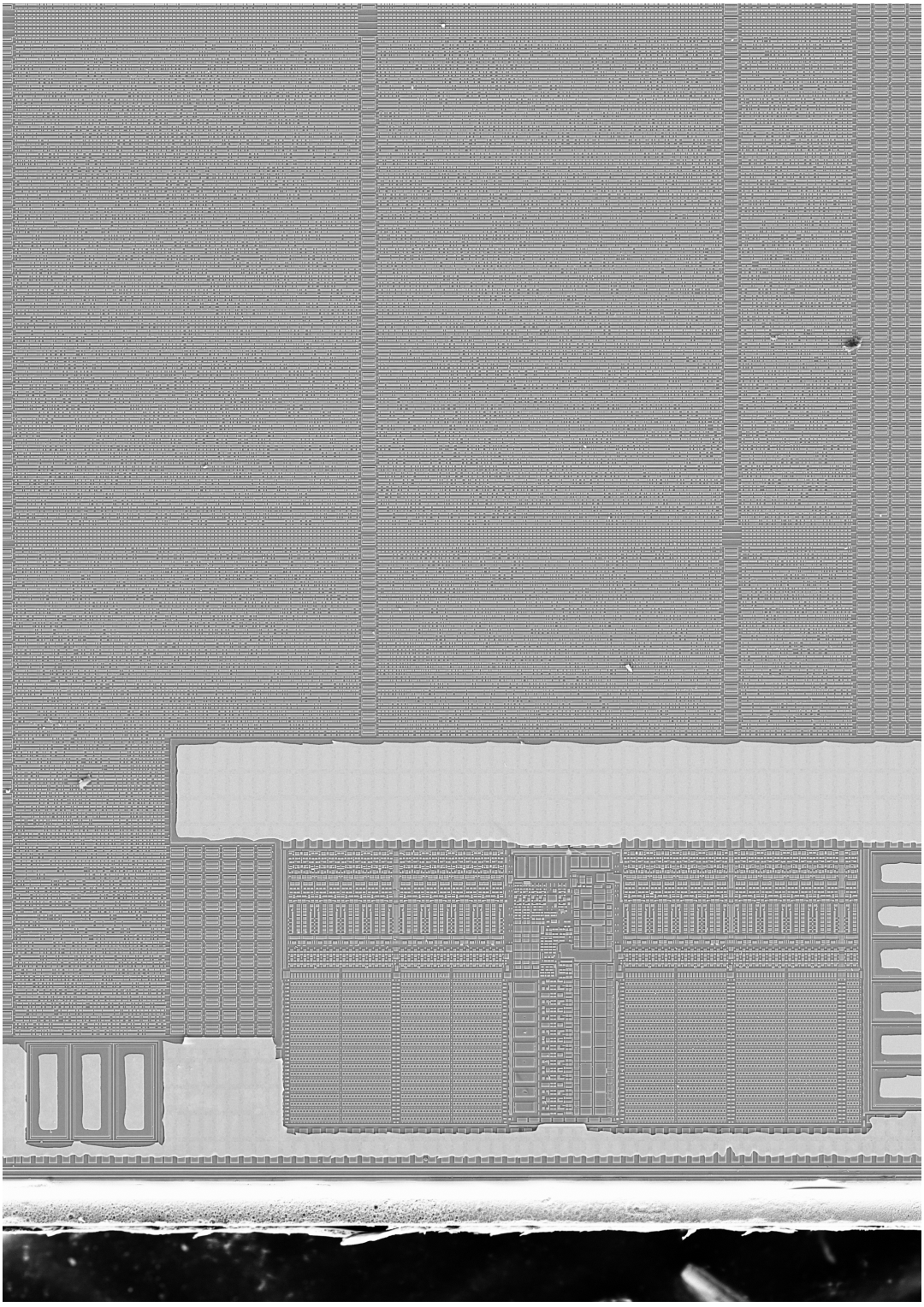


FIGURE 3.7: Vue d'une partie de la logique synthétisée du circuit N.2

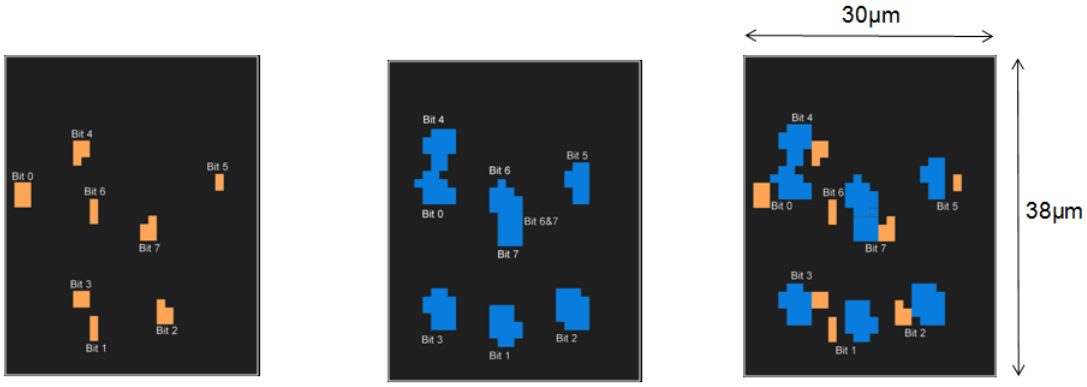


FIGURE 3.8: a) Positions sensible au bit set, b) Positions sensible au bit reset, c) Superposition des cartographies bit set et bit reset

3.3.2 Collage d'un registre à '0' par énergie laser

Le placement du faisceau laser influe sur l'énergie affectant les positions sensibles d'un registre et peut être contrôlé pour affecter la sortie des bascules flip-flop. La campagne suivante a été conduite pour trouver si d'autres paramètres du laser pouvaient être intéressants afin d'améliorer notre capacité à changer les contenus des registres. Après avoir initialisé la valeur du registre, nous modifions successivement le temps d'exposition et la puissance du faisceau laser afin de réduire progressivement l'énergie atteignant la face arrière du circuit intégré. Notre plateforme laser nous permet de mesurer la puissance atteignant la face arrière d'un circuit intégré pour chaque valeur de la commande d'entrée. Notre puissance de sortie peut varier de quelques mW à 800mW en crête, tandis que la durée de l'impulsion laser peut être réglée à quelques dizaines de ns. D'après les mesures de puissances et les observations effectuées à l'oscilloscope, on peut mesurer l'énergie atteignant la face arrière de la surface du circuit intégré.

$$E = P_{peak} * \Delta T$$
$$E(Joules) = P_{peak}(W) * \Delta T(s)$$

Outre la puissance de la source laser, les pertes optiques et la durée d'impulsion, l'énergie atteignant les zones actives des transistors dépend de la longueur d'onde utilisée et de la concentration de dopage du substrat. Pour démontrer le contrôle de la valeur d'un registre en fonction de l'énergie du faisceau laser utilisé, nous utilisons la même zone de 30 par 38 μm et cette fois la moitié des bits du registre est initialisée à '1' et l'autre moitié à '0'. Nous effectuons trois balayages laser avec trois énergies différentes atteignant la face arrière du composant, respectivement 32, 13 et $10nJ$. La taille du faisceau laser est toujours d'environ $1\mu m$. Nous récupérons ainsi les trois différentes cartographies de la figure 3.9 utilisant le même code couleur que précédemment (en bleu pour les positions sensibles à la transition de '1' vers '0' et en orange pour les positions sensibles à la transition de '0' vers '1').

La première cartographie de la figure 3.9 est obtenue avec une énergie laser de $32nJ$ et permet de visualiser des carrés bleus mais aussi des carrés orange. Avec ce niveau d'énergie, des bit set et des bit reset sont ainsi possibles. La deuxième cartographie de la figure 3.9 est obtenue avec une énergie laser de $13nJ$ et permet de visualiser toujours le même nombre d'ensemble de carrés bleus mais une diminution du nombre d'ensemble de carrés orange. Avec ce niveau d'énergie, tous les bits initialisés à '1' peuvent passer à '0' tandis que certains bits ne peuvent plus

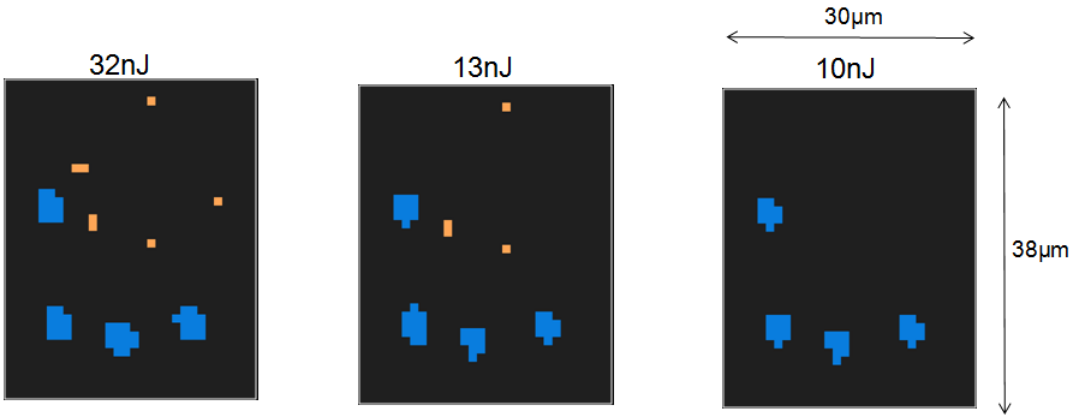


FIGURE 3.9: Collage d'un registre à '0' par contrôle de l'énergie laser atteignant la face arrière du composant : a) 32 nJ, b) 13nJ, c) 10nJ

passer de '0' vers '1'. Et enfin la dernière cartographie de la figure 3.9 obtenue avec une énergie de $10nJ$ permet de visualiser des bits reset mais plus aucune transition de '0' vers '1' possible.

Nous démontrons ainsi qu'il est possible de façon expérimentale de n'obtenir que des bits à '0' en utilisant une énergie laser assez faible, 10nJ pour un type de cellules flip-flop de ce circuit. Théoriquement, nous émettons l'hypothèse que la dernière énergie appliquée sur ce circuit est suffisante pour perturber un type de transistors (les transistors NMOS) sans toutefois perturber l'autre type de transistors (les transistors de type PMOS). Le faisceau laser génèrerait plus de photocourant pour un transistor NMOS que pour un transistor PMOS. Ce qui serait cohérent avec les investigations de Sarafianos *et al.* [68] pré-citées dans la partie 1.4.2 et illustrées par la figure 1.30.

Le modèle de fautes peut être contrôlé précisément avec l'énergie utilisée, dans notre cas le registre entier est mis à zéro avec une énergie de $10nJ$. Un attaquant peut être sur que chaque cellule flip-flop présente sous le faisceau laser aura une valeur '0'.

Niveau de sensibilité Le tableau 3.1 regroupe les résultats obtenus au laser, et présente les différentes réactions obtenues avec les différentes énergies laser utilisées. Pour ce circuit intégré, qui dispose donc d'une implémentation donnée pour ce registre, il est donc possible d'indiquer différents niveaux de sensibilité pour différentes énergies laser utilisées.

3.4 Informations de rétro-conception par attaque laser

3.4.1 Connaître l'orientation des portes logiques visées

Dans cette sous-section, nous illustrons que la précision et la répétabilité de notre plateforme d'injection nous permet même d'obtenir des informations sur l'orientation des différentes cellules de base. Ainsi comme autre résultat, si on émet l'hypothèse que la même cellule (au niveau de sa structure physique) est utilisée pour tous les bits, on obtient également l'orientation de chacune des cellules flip-flop de ce registre. On utilise toujours la même zone de balayage et le même code couleur.

Par exemple, si le bit numéro '1' a une orientation de référence alors le bit numéro '3' est

TABLEAU 3.1: Effet observé dépendant du niveau d'énergie arrivant sur la face arrière du circuit

Cas	Niveau d'énergie	Bit reset	Bit set
1	Quelques nJ	Quelques bits passent à '0'	Aucun bit set
2	10nJ	Tous les bits passent à '0'	Aucun bit set
3	13nJ	Tous les bits passent à '0'	Quelques bit set
4	32nJ	Tous les bits passent à '0'	Tous les bits passent à '1'
5	Supérieur à quelques dizaines de nJ	Tous les bits passent à '0' mais résolution spatiale supérieure à la taille de la cellule	Tous les bits passent à '1' mais résolution spatiale supérieure à la taille de la cellule

présent avec une orientation 'miroir'. Dans la figure 3.10, on met en évidence que la moitié des bits présents sur cette zone ont leurs parties sensibles au bit set sur le côté gauche de leurs parties sensibles au bit reset.

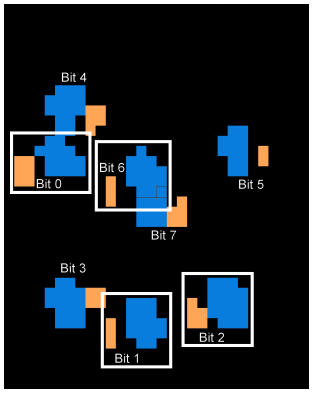


FIGURE 3.10: Détermination de l'orientation des portes logiques visées : 4 bits ont une sensibilité au bit set (en orange) localisée à gauche de leur sensibilité au bit reset (en bleu)

Ce type de résultat peut notamment être intéressant à des fins de rétro-conception.

3.4.2 Différencier la valeur des bits par cartographie laser

La figure 3.11 illustre la cartographie des fautes obtenues pour quatre valeurs d'initialisation différentes pour ce registre de 8 bits avant le balayage laser de la zone de 30 par 38 μm.

Pour la partie supérieure gauche de la figure 3.11, le registre est initialisé uniquement avec des '0'. Pour la partie supérieure droite, que des '1' sont écrits dans le registre. Enfin, les valeurs 1111 0000_2 et 0000 1111_2' sont respectivement les valeurs de départ sur les parties inférieures gauche et droite.

Nous observons que les points sensibles au 'bit set' et au 'bit reset' ont différentes allures vis-à-vis du même faisceau laser. L'observation directe de la cartographie des fautes obtenues donne une

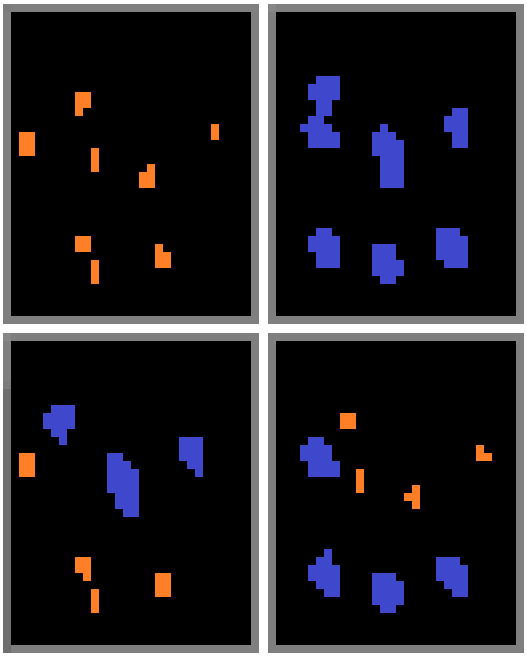


FIGURE 3.11: Cartographies laser obtenues avec initialisation du registre à 0000 0000_2, 1111 1111_2, 1111 0000_2 et 0000 1111_2 (de gauche à droite puis de haut en bas)

information de la valeur du bit à l'état initial. Les bits initialisés à '1' permettent d'obtenir des ensembles de points sensibles au bit reset pour chaque bit (en bleu) tandis que les bits initialisés à '0' permettent d'obtenir des ensembles de points sensibles au bit reset pour chaque bit (en orange). Ces cartographies mettent en évidence que les ensembles de points sensibles à la transition de '1' vers '0' occupent une surface plus large que pour les points sensibles à la transition de '0' vers '1'. Ainsi, sans avoir accès à la valeur de départ d'un registre, il est possible de récupérer cette dernière vis-à-vis de la surface du nombre de points sensibles pour un bit donné.

3.4.3 Corrélation cartographies laser et implémentation physique

Les sensibilités aux faisceaux laser décrites dans les sections précédentes sont liées à l'implémentation matérielle sous-jacente. Nous souhaitons corréler les différents effets laser obtenus et l'implémentation matérielle de ce circuit N.2. La figure 3.12 est l'acquisition au niveau substrat de la zone balayée pendant les tests laser. Huit colonnes de cellules sont visibles sur cette zone. Les zones actives 'p-well' et 'n-well', représentatives du process CMOS, peuvent être facilement distinguées en colonne. Sur cette même figure, une cellule flip-flop est repérée, tandis que le cercle blanc donne une idée de la taille du spot du faisceau laser utilisé.

Dans les circuits CMOS, on peut donner une approximation du courant de sortie des transistors NMOS et PMOS en s'appuyant sur l'équation $I_p = \mu_p$ * W/L et $I_n = \mu_n$ * W/L où μ est la mobilité des porteurs, W et L respectivement la largeur et la longueur de la grille du transistor. L est fixé par le nœud technologique utilisé. Ce courant de sortie doit être équilibré et cela est partiellement réalisé en ajustant le paramètre W. La mobilité μ_P des trous (porteurs) est plus petite que la mobilité des électrons μ_N donc la largeur des transistors PMOS doit être plus grande. Sur l'image obtenue au MEB, ce paramètre est utilisé pour clairement identifier les côtés d'implémentations des transistors PMOS et des NMOS.

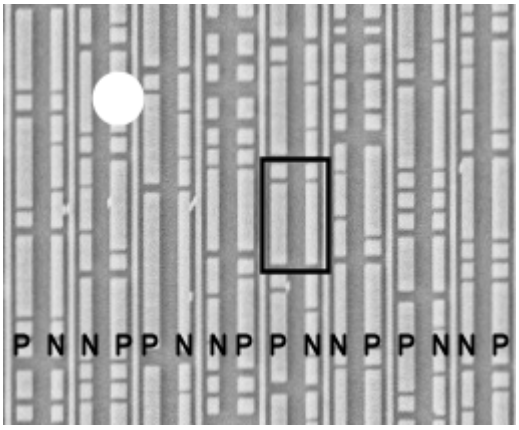


FIGURE 3.12: Image issue de SEMBA de la zone du registre incluant taille de la cellule flip-flop, taille du faisceau laser et types de transistors PMOS ou NMOS

Nous superposons une cartographie laser obtenue à l'aide de l'implémentation physique des transistors (figure 3.13). On peut tout d'abord distinguer que les fautes apparaissent de manière répétées colonne par colonne. Ainsi, on peut directement voir les positions relatives des zones de bit reset (en bleu) et de bit set (en orange). Sur notre cas d'application, il est très intéressant de voir que les zones sensibles au bit set sont présentes sur les transistors PMOS tandis que les zones sensibles au bit reset sont présentes sur les transistors NMOS. Ce résultat corrèle avec les observations faites lors de la variation de l'énergie laser utilisée, cf partie 3.3.2.

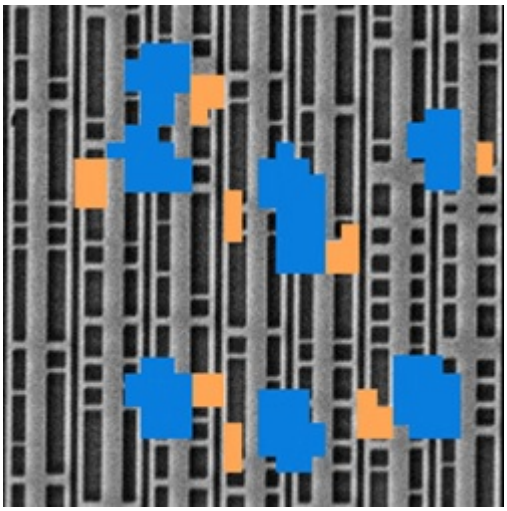


FIGURE 3.13: Superposition des fautes laser avec l'implémentation physique, bit reset (bleu) présent sur les transistors NMOS et inversement

3.4.4 Corrélation attaques en fautes et schéma électrique

Principe de fonctionnement Au front montant de l'horloge, une bascule flip-flop sensible sur ce même front transfère la valeur présente sur son entrée vers sa sortie. La valeur de cette bascule est maintenue le reste du temps. A l'intérieur de la cellule de base, la configuration d'une partie 'maître' permet de mettre à jour la valeur d'une flip-flop à chaque coup d'horloge.

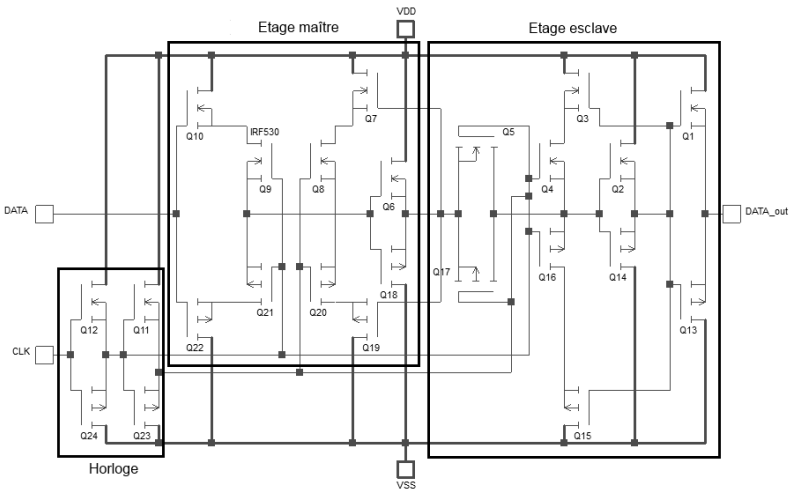


FIGURE 3.14: Schéma électrique d'une cellule flip-flop standard

En utilisant le schéma donné sur la figure 3.14, la valeur à l'entrée de la cellule flip-flop va être présente à la sortie de la cellule inverseur formée par les transistors $Q6$ et $Q18$. Tandis que la partie 'esclave' affecte la valeur stockée aux sorties des transistors $Q6$ et $Q18$ à la sortie de la cellule flip-flop.

Effet laser modélisé sur une cellule flip-flop Sur le schéma électrique proposé, nous pouvons apercevoir plusieurs couples de transistors formant des inverseurs. En visant un couple de transistors tels que $Q6$ ou $Q18$, l'hypothèse est faite qu'il est possible de passer la valeur de sortie de l'inverseur soit à '0' ou soit à '1'. Ce qui serait conforme aux investigations de Roscian *et al.* [66] sur une seule cellule inverseur. On suppose que le passage de l'état bloqué à passant du transistor connecté au rail d'alimentation supérieur (le PMOS) est responsable de la transition de '0' vers '1'. Inversement, nous supposons que le passage de l'état bloqué à passant d'un transistor NMOS est responsable d'un changement de '1' vers '0'.

La figure 3.15 représente le layout d'une cellule flip-flop sur lequel est hypothétiquement indiqué le côté sensible au faisceau laser obtenu grâce aux précédentes cartographies.

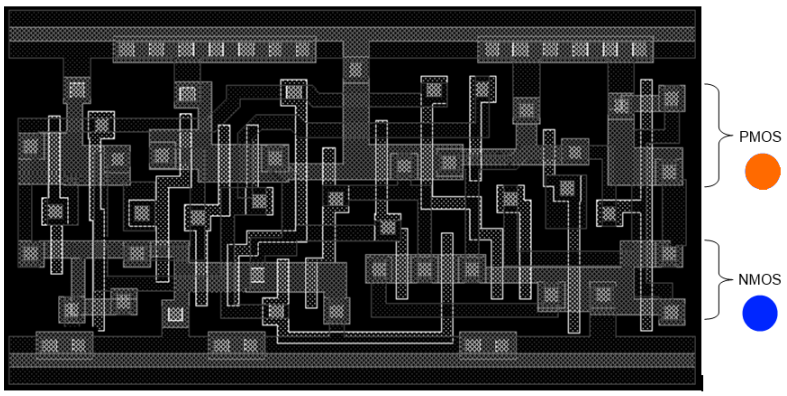


FIGURE 3.15: Layout d'une cellule flip-flop et côté de sensibilité au bit reset (en bleu) et bit set (en orange)

3.5 Conclusion

Nous avons tout d'abord utilisé SEMBA, méthodologie proposée au chapitre 2, afin de perturber uniquement les cellules d'intérêt d'un algorithme de chiffrement implémenté matériellement. En effet, sur ce circuit la sortie de l'outil SEMBA permet de récupérer la position spatiale de chaque cellule flip-flop présente dans le circuit. Ces coordonnées ont été intégrées sous la plateforme laser avec la synergie de la visualisation face avant au MEB sur un premier circuit préparé de manière destructive et la visualisation face arrière avec une caméra infrarouge sur un circuit fonctionnel. La capacité de notre plateforme laser nous permet de nous positionner cellule par cellule reconnue. Nous avons démontré la validité de deux modèles de fautes avec l'application directe de SEMBA, l'analyse différentielle de fautes et l'analyse en 'safe error'. Sur cet échantillon, viser uniquement les cellules flip-flop à l'aide de la méthodologie SEMBA permet de réduire grandement le temps d'utilisation de la plateforme laser, d'assurer une couverture de test ciblant l'ensemble des cellules sensibles dans le processus visé et permet d'éviter d'activer des contre-mesures présentes sur le circuit (capteurs laser par exemple). L'ensemble de la méthodologie, les outils nécessaires et leur rôle sont répertoriés dans le tableau 3.2.

Tableau 3.2: Tableau récapitulatif de l'attaque en fautes améliorée à l'aide de la méthodologie SEMBA

Tâche	Outil/Moyens	Rôle
Adpatation de la sortie de SEMBA	Adapte les coordonnées [X,Y] des motifs en pixels à l'image de la puce fonctionnelle en face arrière	Faire une correspondance entre le motif reconnu sur l'image MEB et le circuit sous la plateforme laser
Injection de fautes	Plateforme laser à l'état de l'art capable de faire des balayages sub-micrométrique, avec une précision temporelle de l'ordre de la ns, de durée aussi courte que quelques dizaines de ns avec une puissance maximale de quelques Watts	Permet de satisfaire les besoins temporels (avec une sonde de courant pour retrouver les tours de l'AES), permet de retrouver les localisations spatiales à attaquer grâce à une caméra IR et avec une table motorisée [X,Y,Z]
Contrôle de l'effet généré	Tir localisé sur le côté PMOS ou sur le côté NMOS, ou encore tir contrôlé en énergie	100% de contrôle de la valeur stockée dans une cellule flip-flop
Application de la DFA ou de la 'safe error'	Utilisation de méthodes comparant des chiffrés fautés ou non fautés	Permet de trouver quel numéro de bit ou fonction est stockée dans une flip-flop donnée ou bien de trouver des données sensibles

Ensuite, un circuit de type carte à puce (noeud technologique $90nm$) a été la cible de nos expérimentations. C'est un échantillon ouvert sur lequel nous pouvons notamment lire et écrire dans des registres particuliers. Sur une zone restreinte du circuit où un registre 8bits est matériellement présent, nous mettons en avant la possibilité de contrôler chacun des bits de ce registre avec un faisceau laser.

D'une part, nous obtenons en pratique des zones de bit set et de bit reset différentes suivant le côté de la cellule de base cible du faisceau laser. Ainsi avec un seul tir laser, l'évaluateur peut choisir de faire basculer le bit visé soit à '0' soit à '1' de manière contrôlée et reproductible.

Avec l'avancement des technologies et des bancs d'attaques, nous pouvons définir aujourd'hui l'état de l'art des attaques laser avec le tableau 3.3. Avec nos travaux, nous rajoutons ainsi la possibilité de contrôler une cellule complexe (composées de plusieurs dizaines de transistors) critique en matière de sécurité (les cellules flip-flop peuvent stocker des clés de chiffrement par exemple) et de technologie récente (90nm) [27].

Tableau 3.3: Etat de l'art de l'injection de fautes optiques

	Skorobogatov (2002)	Roscian et al.(2013)	Courbon et al.(2014)
Noeud technologique	1200nm	250nm	90 nm
Taille d'une cellule SRAM	$20\mu m$*$20\mu m$ (6T)	$9\mu m$*$4\mu m$ (5T)	$3\mu m$*$1.5\mu m$ (6T)
Cellule visée	SRAM	SRAM	Flip-flop
Taille du faisceau lumineux	$10\mu m$	$1\mu m$	$1\mu m$

D'autre part, nous démontrons la possibilité de contrôler la valeur des bits de ce même registre en faisant varier l'énergie laser atteignant la face arrière du circuit. En diminuant l'énergie, nous récupérons une cartographie où seules les transitons de '1' vers '0' sont réalisables. Ainsi avec un seul tir laser, l'évaluateur peut faire basculer un bit donné à la valeur '0'.

Sur ce deuxième circuit, nous démontrons l'intérêt de l'identification de zones d'intérêt pour l'amélioration des attaques en fautes mais aussi l'intérêt de l'utilisation des cartographies laser obtenues à des fins de rétro-conception. Avec la précision du positionnement spatial et du contrôle de l'énergie sur notre plateforme laser, nous obtenons des cartographies avec des zones de bit set à gauche ou à droite des zones de bit reset. On peut ainsi conclure sur l'orientation de chacune des cellules flip-flop avec l'observation de ce type de cartographie. Toujours sur la même zone d'intérêt, la capacité de pouvoir initialiser chaque bit de ce registre à une valeur donnée nous permet de mettre en avant la possibilité de différencier la valeur des bits par cartographie laser. Des zones sensibles plus larges pour un bit donné permettent de savoir que le bit était initialisé à '1' et des zones sensibles moins larges pour un bit donné permettent de savoir que le bit était initialisé à '0'.

Ensuite, nous réutilisons SEMBA pour corréler les résultats laser obtenus avec l'implémentation physique des transistors. Avec SEMBA, nous récupérons l'implémentation physique des régions actives des transistors. Nous identifions des colonnes où seuls des transistors de type P sont

présents et d'autres colonnes où seuls des transistors de types N sont présents. Nous superposons ensuite la cartographie laser obtenue avec l'image de base du circuit acquise au MEB. Nous validons que les zones de sensibilité se situent bien au niveau des colonnes d'implémentations des transistors. De plus, nous obtenons des zones sensibles à la transition de '1' vers '0' plus larges et positionnées sur le côté où les transistors NMOS sont présents. Inversement, les zones sensibles à la transition de '0' vers '1' couvrent moins de surface et sont positionnées sur le côté où les transistors PMOS sont présents.

Sans connaissance de la conception réelle du circuit (non accès au layout du circuit et donc au layout de la cellule visée), nous avons émis des hypothèses sur l'explication théorique des phénomènes observés. Nous corrélons un schéma possible de cellule flip-flop avec nos résultats expérimentaux d'injection laser. L'obtention de fautes de type bit reset sur les transistors PMOS et de fautes de type bit set sur les NMOS est en ligne avec les hypothèses précédemment émises sur une cellule inverseur [26].

L'avancée notable des travaux est le contrôle démontré de la valeur d'une cellule de stockage individuelle présente dans une quelconque zone de la logique synthétisée. Cette capacité est en opposition aux travaux faits sur des mémoires, sur des matrices d'éléments de test ou encore sur des transistors uniques.

Chapitre 4

SEMBA appliquée à la détection de Chevaux de Troie Matériels

Des informations représentatives de chaque implémentation de cellules sont récupérables à l'aide de la méthodologie SEMBA proposée au chapitre 2. Cette possibilité semble ainsi tout à fait intéressante dans le cadre de la détection de modifications malicieuses apportées au niveau matériel. Bien que la méthodologie présentée ne permette de visualiser qu'un seul niveau du circuit, la pertinence de notre approche est tout d'abord détaillée. En fonction de la référence disponible, différents traitements d'images sont appliqués sur cette image de base pour détecter la présence de Chevaux de Troie Matériels. Un cas simulé illustre et démontre ces différentes possibilités. De plus, notre méthodologie a été appliquée sur deux ASICs dont le second intègre volontairement un Cheval de Troie Matériel. Nous verrons ainsi que notre technique quasi automatisée permet de détecter chaque cellule frauduleusement insérée sur l'échantillon à tester.

Sommaire

4.1 Les Chevaux de Troie Matériels

4.1.1 Description des Chevaux de Troie Matériels

Tout d'abord, nous nous attachons à décrire les étapes de fabrication d'un circuit intégré afin de visualiser le moment où des CTMs pourraient être le plus probablement insérés dans un circuit intégré. Les étapes du cycle de vie d'un circuit intégré avec leurs niveaux de confiance respectifs ont été précisés par Chakraborty *et al.* [25] comme illustré par la figure 4.1. On y distingue notamment que l'étape de fabrication est l'étape avec le niveau de confiance associé le plus faible. Elle comprend la génération des masques et l'application des étapes de lithographie.

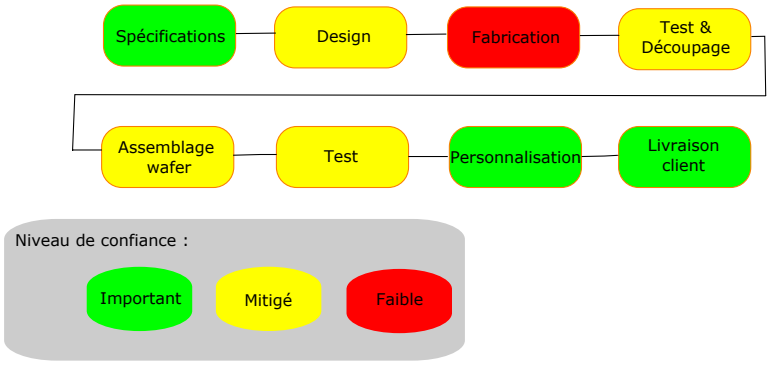


FIGURE 4.1: Cycle de vie d'un circuit intégré standard, figure tirée de [25]

Aucune méthode à ce jour ne propose un taux d'efficacité de '100'% et une couverture de détection englobant tous les types de CTMs. Même une méthode de rétro-conception totale, qui de plus est couteuse et chère en temps d'application, ne pourrait contrer des CTMs paramétriques par exemple.

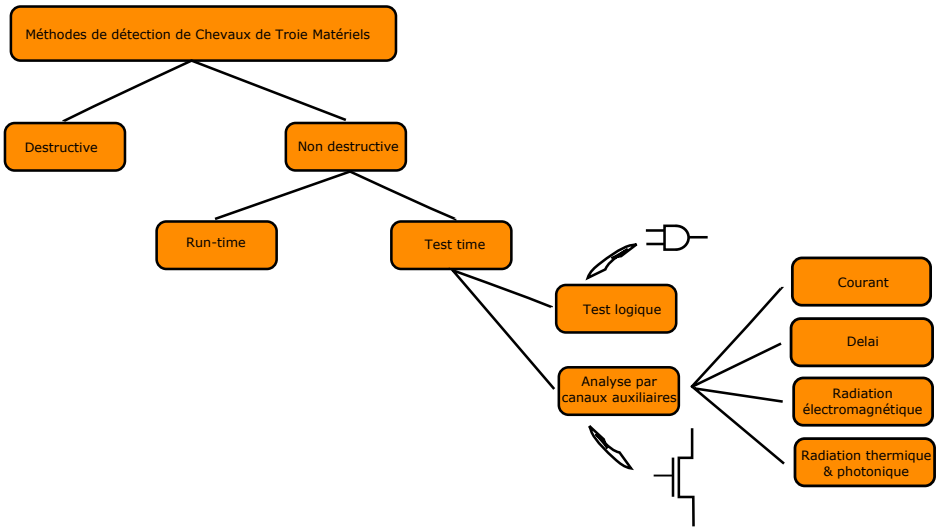


FIGURE 4.2: Différentes méthodes de détection, figure extraite de [25]

Concernant les méthodes par canaux auxiliaires (SCA), elles se retrouvent affectées par les variations de mesures et de fabrication donnant un taux de détection faible et peuvent ne pas

couvrir toutes tailles de CTMs ou toutes activités de CTMs. Par exemple, Aarestad *et al.* [3] ne détecte pas les CTMs amenant de légères modifications sur le circuit (moins de quelques % de modifications vis-à-vis de l'intégralité du circuit), ne prend pas en compte les variations de procédés entre circuits et donne seulement des résultats de simulations. Les techniques basées sur les mesures de délais ne donnent pour l'instant que des résultats exploitables en simulation ou sur FPGA. Les deux méthodes, par canaux auxiliaires et basées sur le délai, peuvent nécessiter d'importantes séries d'acquisitions de données et sont sensibles aux variations de mesures et de process. On peut noter la description d'une méthode de rétro-conception partielle basée sur des simulations pour la détection de CTMs [7] et une détection via des images du niveau métal le plus haut sous un outil de design FPGA [12].

De plus, la modification malicieuse d'un circuit peut exister au niveau dopant [11]. Le fait que la modification soit à l'intérieur même des caissons des transistors ne rendrait pas possible l'observation visuelle d'un éventuel changement de type de dopant d'après Becker *et al.* [11]. En réponse à cet article Suguwara *et al.* [77] a démontré que le type de jonction peut être différencié par observation au Microscope Electronique à Balayage. Un faisceau d'électrons faible en énergie est appliqué au niveau des contacts, la teinte de gris observé avec le MEB permet de connaître le type de jonction réalisé et d'en déduire la présence ou non de CTMs. Il faut bien entendu préalablement avoir réussi une préparation de l'échantillon au niveau contact.

Il en résulte qu'aucune technique permette une détection de CTMs efficace, bas coût, indépendante des variations de fabrication et de mesure tout en étant possiblement intégrable dans le cycle de vie d'un circuit intégré.

4.1.2 Une détection directement basée au niveau matériel

Dans notre étude, le cas réel du développement de circuits intégrés sécurisés et de la chaine d'approvisionnement de type cartes à puce sont utilisés comme exemple. Le rôle d'un développeur logiciel qui reçoit un circuit par un fabricant de puces est pris comme hypothèse. Le flot de conception d'un circuit intégré a été présenté dans la partie 4.1.1. La description de leur cycle de vie a été adaptée, figure 4.1, afin de proposer une nouvelle méthodologie de détection de Chevaux de Troie Matériels. La figure 4.3 représente le flot de conception ainsi modifié. Nous y repérons notre proposition de méthode de détection de CTMs qui se situe à l'étape de réception du wafer. Certaines de ces étapes sont effectuées 'in-house' et apparaissent par conséquent comme étapes de confiance de notre point de vue d'intégrateur de solutions sécurisées. Deux étapes signalées par une croix sont maintenant considérées de confiance grâce à l'application de notre technique de détection de Chevaux de Troie Matériels, l'étape de "Test et découpage" et l'étape de "Fabrication".

L'étape de conception inclut l'utilisation de différentes briques propriétaires (IP), différents outils de conception, différentes cellules de base et encore différents modèles électriques provenant d'une tierce partie (cf sous section 1.1.3). Comme notre méthode nécessite de se référencer à un design authentique, une quelconque modification de circuit effectuée durant cette étape ne pourrait être détectée. Cependant, comme illustré sur la figure 4.3, une autre méthode de détection pourrait potentiellement être ajoutée lors de la phase de test afin de détecter des CTMs insérés pendant la phase de conception. Celle-ci ne fait pas partie de notre étude.

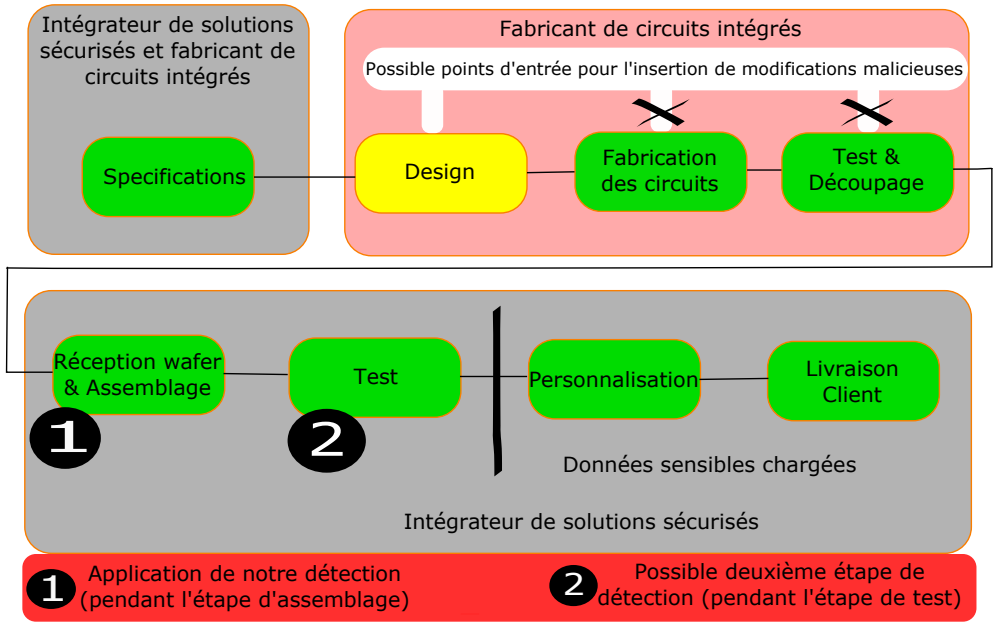


FIGURE 4.3: Flot de conception de CIs modifié avec notre méthode de détection

4.1.3 Une méthode adaptée au cycle de vie des circuits intégrés

Pour satisfaire les besoins du flot industriel, notre technique de détection de Chevaux de Troie Matériels (CTMs) doit répondre à des critères accessibles par la couverture ou la prise en compte des différents points suivants :

- Temps disponible pour la détection,
- types de CTM détectés par la méthodologie présentée,
- taux de succès de la méthode proposée,
- robustesse vis-à-vis de la taille du CTM détecté par la méthodologie présentée,
- robustesse vis-à-vis de la variation de process inhérente aux circuits intégrés,
- prise en compte de la disponibilité de la référence,
- coût de l'application de la méthode de détection.

4.1.4 Principe général et méthodologie

Nous proposons ainsi la méthodologie de détection basée sur les techniques vues dans SEMBA et illustrée par la figure 4.4. L'ensemble de la méthodologie de détection de CTMs est composée des 3 étapes suivantes :

- 1ère étape : Préparation d'échantillons,
- 2ème étape : Imagerie au Microscope Electronique à Balayage,
- 3ème étape : Détection de Chevaux de Troie Matériels.

Les deux premières étapes sont ainsi issues de notre technique SEMBA. Nous rappelons que nous sommes capables au travers de ces deux étapes de préparer efficacement et rapidement les échantillons pour atteindre les zones actives des transistors puis de faire l'acquisition de toute cette surface de manière automatisée afin d'obtenir une image dite de base. Cette approche est effectuée à la réception du wafer, les circuits non fonctionnels ont été marqués et sont ainsi identifiables par la machine d'assemblage, ces derniers restent sur le wafer et sont mis au rebut.

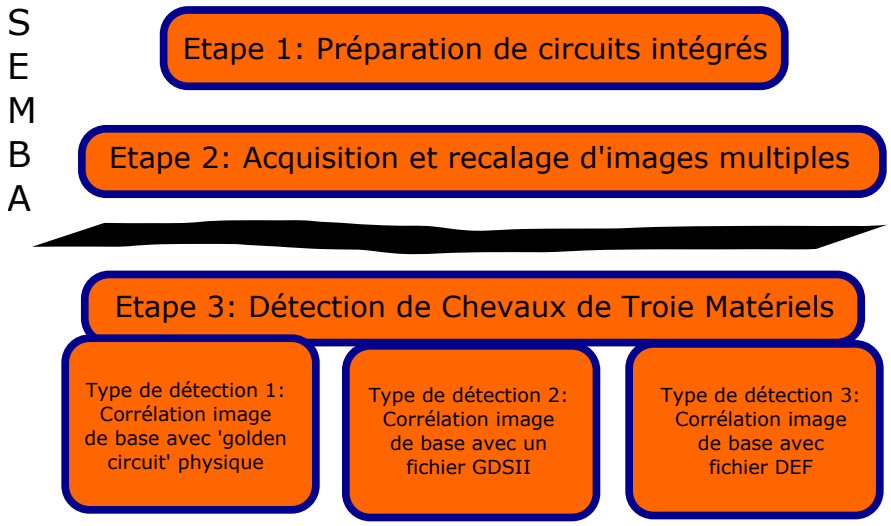


FIGURE 4.4: Méthodologie appliquée pour la détection de Chevaux de Troie Matériels

Ce sont ces circuits non fonctionnels que nous récupérons pour l'application de notre méthode de détection. En effet, dans le cas de la rétro-conception nous n'avons pas besoin d'utiliser de produits fonctionnels, seule la topologie du circuit nous intéresse. Ainsi, l'addition de notre étape de détection de CTMs dans le flot de conception n'impacte pas le rendement de fabrication. Au final, la couverture de tests de notre méthode de détection est fortement dépendante du rendement de fabrication, du nombre de circuits pouvant être conçus en parallèle avec le même masque (dépend du stepper de lithographie vu dans le chapitre 1), et du positionnement des circuits non fonctionnels sur le wafer.

La figure 4.5 montre un exemple de puces restantes sur la plaquette après l'assemblage des puces fonctionnelles. Dans notre cas, ce sont ces puces que nous utiliserons pour nos tests et qui seront donc enlevées de la plaquette avant que les puces fonctionnelles ne soient retirées pour assemblage (étape du 'pick and place'). Cela permettrait de détecter si un CTM est présent avant même que le reste du lot ne soit assemblé. Nous n'avons pas besoin d'un circuit dans son support final pour le tester.

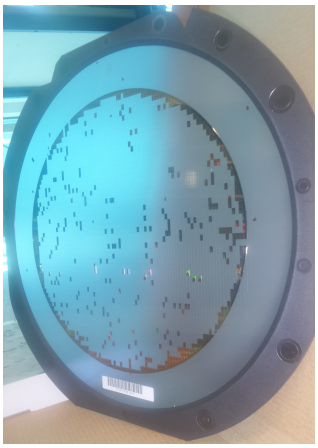


FIGURE 4.5: Vue de la plaquette après assemblage

Une fois les deux premières étapes réalisées, il en ressort une image correspondant aux zones actives des transistors présents sur l'ensemble du composant. Dépendant de la référence disponible, le type de détection diffère lors de la troisième étape, cf figure 4.4. Si un modèle physique de référence (golden model, circuit conçu et supposé de confiance) est disponible alors nous verrons qu'il est possible d'extraire de la même manière sur l'échantillon à tester une image correspondant aux zones actives des transistors. L'image de l'échantillon à tester sera corrélée avec l'image du golden model afin de mettre en évidence la présence de cellules malicieusement modifiées ou rajoutées sur le circuit intégré.

Cependant, un circuit de référence fabriqué dans un environnement de confiance peut ne pas être disponible, dans ce cas là, la référence intègre sera extraite du fichier de conception graphique GDSII. C'est le deuxième type de détection dans cette étape 3. Un autre fichier de sortie d'un outil de conception assistée par ordinateur peut également être utilisé comme référence. Il peut s'agir par exemple d'un fichier de type DEF. Le positionnement spatial ainsi que le nom de chaque cellule de base sont écrits dans ce type de fichier. Il apparait donc intéressant de l'utiliser pour la modification/addition de cellules de base. De plus, ce type de fichier est directement lisible sans outil contrairement à un fichier GDSII, notons qu'il faut pour ces deux types de détection posséder la dernière version de ces fichiers. Par exemple, le fabricant de circuits intégrés rajoute des cellules dites de remplissage. Ces dernières doivent être présentes dans le fichier de référence afin de ne pas être détectées comme Cheval de Troie Matériels.

4.2 Différents scénarii de détection d'un Cheval de Troie fictif

La première partie de nos travaux est réalisée sur l'AES130, partie 2.1.3, circuit ne contenant pas à l'origine un CTM. Cependant, afin de valider notre méthode, un CTM a été introduit volontairement et directement sur l'image de base par l'ajout de cellules supplémentaires. Nous utilisons le terme fictif pour qualifier ce CTM. Cette opération a pour but de valider notre méthode SEMBA avant l'application sur un cas réel.

L'introduction du CTM fictif suit donc le flot suivant et ce CTM fictif est utilisé pour les trois prochains scénarii de détection présentés :

- Préparation, acquisition et alignement d'images multiples : c'est l'utilisation directe de SEMBA,
- puis rajout du Cheval de Troie Matériel par l'insertion de 4 cellules (simple copie directement sur l'image extraite de la méthodologie SEMBA), on obtient ainsi l'image de base du circuit à tester dans le cadre de cette détection de Cheval de Troie fictif.

4.2.1 Scénarii 1 : Détection de CTM avec Golden Model physique

Dans ce premier scénarii, on s'intéresse à la façon dont on peut mettre en place une méthodologie de détection basée sur un 'golden model' physique. En effet, partant de l'hypothèse que modifier intelligemment les masques de lithographie ne serait pas possible si la production doit être lancée rapidement, on peut donc considérer que les tous premiers lots produits n'auront pas eu le temps de subir de modifications malicieuses. Les premières puces issues de ce lot seraient alors vierges de toute modification et seraient considérées comme golden référence. De même, on peut émettre l'hypothèse qu'une petite unité de fabrication serait disponible à l'intérieur d'une même entreprise pour obtenir un circuit référence mais que la production, elle, est externalisée et sujet à une modification malicieuse de circuits intégrés.

A ce stade, nous avons donc en notre possession l'image de base du circuit à tester et le circuit intégré de référence. Les deux circuits subissent le même traitement. Par l'application des deux premières étapes de SEMBA, nous récupérons ainsi une image de base du circuit de référence. Notre acquisition utilise les mêmes paramètres d'acquisition que pour le circuit à tester. Cependant, malgré l'utilisation de paramètres MEB identiques sur ces deux images de base acquises, les caractéristiques de ces deux images varient et une soustraction directe d'image ne peut être réalisée. La vérification d'intégrité nécessite donc le traitement de ces images.

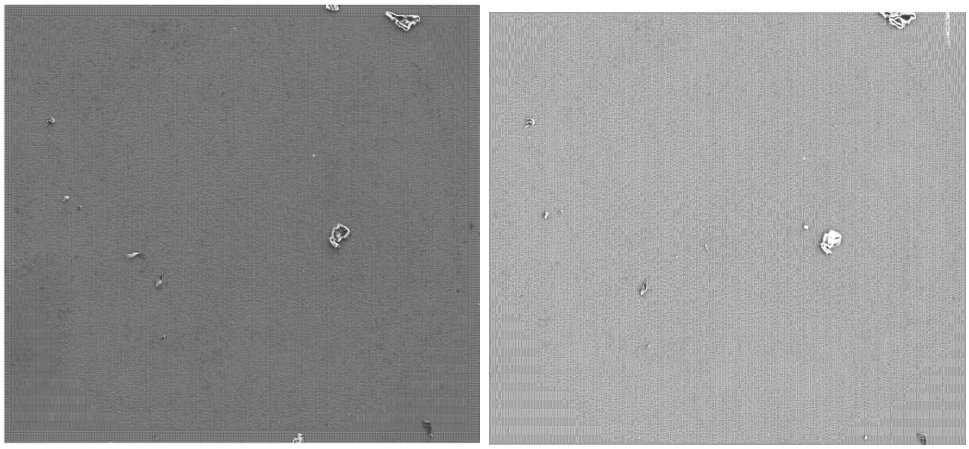


FIGURE 4.6: Même puce, acquisitions différentes

Inhérentes à la microscopie effectuée et ce malgré la conservation de paramètres d'acquisition identiques, ces images extraites des puces n'ont ni la même orientation, ni la même zone scannée ni le même histogramme. Nous recalons manuellement les deux images en termes de rotation et de translation sur la zone où le CTM est présent. Les distorsions sont telles que ce recalage ne peut être effectué de manière globale sur le circuit en réglant seulement les aspects de rotation et de translation. En effet, nous notons des décalages entre les deux images sur d'autres localisations du circuit. Une égalisation d'histogramme est ensuite appliquée avant de finalement pouvoir soustraire les deux images. Les 4 cellules additionnelles sont ainsi mises en évidences sur la figure 4.7.

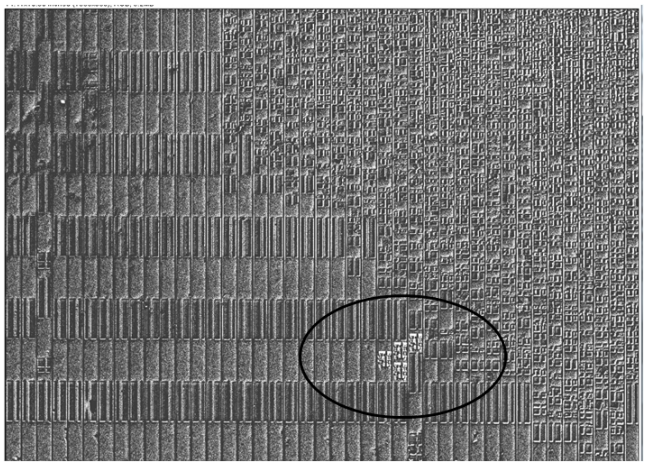


FIGURE 4.7: Détection du CTM simulé avec un circuit physique de référence

Nous notons sur ces deux images, la présence d'artefacts qui sont situés à des localisations différentes. Ils sont principalement dus à la préparation qui peut dans certains cas laisser des résidus. Ceux-ci seront repérables lors d'acquisition au MEB. La technique de préparation s'effectuant de manière empirique, les paramètres tel que le temps d'attaque, la concentration de l'acide ne sont pas totalement maitrisés. Ces disparités peuvent conduire à des différences en termes de préparation d'échantillons qui de fait conduiront à des différences en termes de comparaisons d'images (contraste, contaminant, planéité).

Nous concluons que ce scénarii est plausible et permettrait une détection couvrant l'ensemble de la surface d'un circuit (sur un seul niveau).

4.2.2 Scénarii 2 : Détection de CTM avec fichier graphique de CAO (.GDSII)

Dans ce scénarii, un fichier de conception est disponible il s'agit du GDSII (cf partie 1.1.3). Une fois le GDSII chargé sous un outil de conception assistée par ordinateur (CAO) ou sous un logiciel permettant d'ouvrir ce type de fichier, il est possible de voir niveau par niveau les différents éléments nécessaires à la réalisation du circuit. Nous avons donc dans ce cas d'étude un fichier de type GDSII et l'image de base du circuit à tester. Afin de pouvoir comparer les données contenues dans ces deux types différents de fichiers, seuls les niveaux d'implémentation n-well et p-well sont conservés sous l'outil de CAO.

Ensuite, nous prenons le cas d'une cellule de base, la cellule flip-flop. La figure 4.8 est obtenue en ne sélectionnant sous l'outil de conception uniquement les zones d'implémentation n-well et p-well de cette cellule flip-flop. Afin de se rapprocher de son implémentation physique, cette image est modifiée. Des opérations basiques de morphologie sont utilisées, de type fermeture et dilatation. Il en résulte le deuxième motif présent sur cette même figure 4.8.

FIGURE 4.8: a) Visualisation du GDSII original d'une cellule (à gauche), b) Visualisation du GDSII modifié

Via notre méthodologie, l'opérateur peut obtenir les formes physiquement extraites vues sur la figure 4.1 pour deux zones spatiales différentes du circuit où la même cellule de base doit être implémentée. Un test de corrélation est effectué entre le GDSII modifié et la vue de la même cellule de base physiquement extraite. Nous utilisons toujours comme base la corrélation croisée normalisée. A cette localisation donnée, le niveau de corrélation chute significativement, cela confirme qu'une modification malicieuse a alors été détectée. Ce processus peut être effectué sur l'ensemble du circuit.

Bien entendu, vu que notre technique se base sur une référence de design, il faut prendre en compte la dernière référence possible. Il est à noter que pour des raisons de faisabilité du procédé de fabrication, le fondeur peut remplir les espaces non occupés avec des motifs additionnels.

Tableau 4.1: Détection de CTMs avec un GDSII modifié

	Localisation 1	Localisation 2
GDSII modifié		
Image SEMBA		
Coefficient NCC	Grand	Petit
Présence d'un CTM	Non	Oui

4.2.3 Scénarii 3 : Détection de CTM avec fichier texte de CAO (.DEF)

Dans ce scénarii, nous utilisons un fichier texte de CAO, de type DEF. Dans ce type de fichier, chaque nom de cellule de base est inscrit tout comme sa localisation en μm vis-à-vis d'une origine. L'idée est de premièrement classer les différentes occurrences par nom de cellules de base. Ensuite, chaque occurrence de cellules identiques (type et taille) est additionnée pour obtenir un nombre total de formes similaires à retrouver sur le circuit de test.

C'est à ce moment que la correspondance entre l'image de base du circuit à tester et les informations extraites du fichier DEF peut être effectuée. Nous utilisons la troisième étape de la méthodologie SEMBA, la reconnaissance de motifs afin de savoir si une cellule de base est présente au bon endroit. Si ce n'est pas le cas alors un CTM est présent dans le circuit testé. Avec la préparation effectuée, nous rappelons que nous ne pouvons pas connaître la fonction réalisée par tel motif. Cependant nous pouvons dire si la bonne forme est présente au bon endroit du circuit et ainsi conclure sur l'insertion ou non d'un CTM. La bonne forme est obtenue en émettant l'hypothèse qu'il y a plus de cellules non modifiées que de cellules infectées ou placées à des endroits différents. Avec la localisation écrite dans le fichier de type DEF par cellule, il est ainsi possible d'associer une fonction donnée à une forme visible sur notre image de base. Ceci est réalisé en se déplaçant sur plusieurs de ces cellules de base (pour en extraire la forme de la cellule en limitant les chances de tomber sur une cellule modifiée). En effet il y a peu de chances que plus de cellules soient modifiées que non modifiées.

Dans notre cas d'étude, nous prenons directement comme motif à reconnaître, une des 4 cellules rajoutées pour ce CTM fictif. Cette cellule est reconnue sur l'ensemble du circuit. Vu dans le chapitre 2, les motifs identiques sont reconnus grâce à l'utilisation de librairies basées sur l'algorithme de corrélation croisée normalisée. Connaissant le CTM fictivement présent dans le CI, l'outil de reconnaissance est arrêté une fois que les 4 motifs correspondants au CTM s'affichent. Dans un cas réel, il faudra optimiser le seuil choisi pour la reconnaissance de motifs. Une option serait d'utiliser un seuil plutôt faible pour ensuite retirer manuellement les faux positifs (contrairement au besoin de l'injection laser). Pour en revenir à notre cas, la figure 4.9 illustre visuellement les occurrences obtenues avec la reconnaissance de cette forme sur l'ensemble du circuit. Comme précédemment, un fichier texte enregistre également le positionnement de chaque motif reconnu.

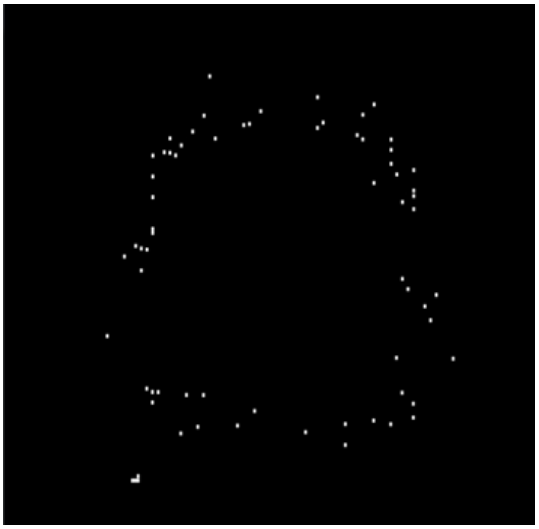


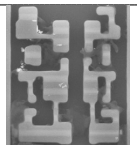
FIGURE 4.9: Localisations des flip-flop reconnus

Ce fichier texte obtenu en sortie de l'outil de reconnaissance de motifs est finalement comparé avec le fichier de type DEF modifié. Dans notre cas d'étude 4 occurrences sont présentes à des localisations où le fichier DEF n'indique pas la présence de ces mêmes cellules. Cette solution permet ainsi de mettre en évidence la présence de CTMs. En général, comme présenté dans le tableau 4.2 si le nombre d'occurrences présent sur le fichier DEF N_{occ} diffère du nombre d'occurrences reconnu N_{rec} alors un CTM est présent. De même si le bon nombre de cellules est présent mais que leur localisation diffère alors une modification malicieuse a été effectuée. Dans un cas industriel, ce type de détection de CTM proposé doit reposer sur ces différents points listés :

- Etre sûr de la robustesse de l'outil de reconnaissance de motifs,
- etre sûr de sa préparation d'échantillons,
- pouvoir faire une vérification manuelle au cas où.

En effet, si des faux positifs ou négatifs cachés sont obtenus en sortie de l'outil de reconnaissance alors la corrélation serait mauvaise et donc les lots des circuits présumés infectés seraient mis au rebut ou renvoyés à tort.

TABLEAU 4.2: Exemple de détection avec un fichier CAO

Nom de la cellule	Localisation en microns dans le fichier DEF	Nombre total du nombre d'occurrences	Image de la cellule de base	Nombre d'occurrences reconnues	Localisation des occurrences reconnues (en pixels)
FF1	DX_1, DY_1 DX_2, DY_2 DX_n, DY_n	N_{occ}		N_{rec}	RX_1, RY_1 RX_2, RY_2 RX_n, RY_n

4.3 Détection d'un Cheval de Troie réel avec Golden Model physique

Nous avons décrit différents scénarii de détections possibles pour un cas de CTM fictif. Ayant l'opportunité d'obtenir un circuit réellement infecté et son homologue non infecté (couple de circuit N.3), nous avons mis en pratique notre méthodologie de détection de CTMs nécessitant une référence physique (type de détection 1). Ces circuits, CHAMELEON et CHIPIT sont en technologie $0.18\mu m$ et ont été conçus par l'Université de Zurich [62]. Ces circuits mesurent 1.525 mm x 1.525mm dont la partie logique couvre environ 1 mm x 1 mm et est constitué d'environ 40kGE (GE : Gate Equivalent, unité utilisée pour décrire le nombre de cellules dans le circuit en portes NAND) et embarquant le même algorithme de chiffrement décrit précédemment (AES) mais aussi d'autres fonctions pour des besoins sécuritaires. Sur un des deux circuits, une modification malicieuse (Cheval de Troie Matériel) au niveau layout (GDSII) du circuit a été insérée, cette dernière comporte environ 190GE (0.5% du circuit). Comme vu précédemment, le layout est un fichier contenant le schéma d'implémentation des masques. Trente cellules flip-flop ont remplacées des cellules de remplissage et quelques autres portes ont été rajoutées pour créer un CTM combinatoire. Quand une séquence spéciale est présente (sur 30bits), un autre bit du circuit bascule et créé une perturbation de l'horloge résultant à un deni de service du composant. Ces circuits ne seront pas utilisés en fonctionnement, leur protocole de communication n'est donc pas abordé.

4.3.1 Application de SEMBA

Les circuits se présentent dans des boîtiers sans résine et avec capot ouvert. Les échantillons possèdent une logique synthétisée d'une surface d'environ '$1mm^2$'. Ces circuits intégrés ont été préparés avec la méthodologie SEMBA. Premièrement, les composants ont été plongés dans un bain HF. Cette action a eu pour effet de détacher les circuits de leurs boîtiers, cf figure 4.10.

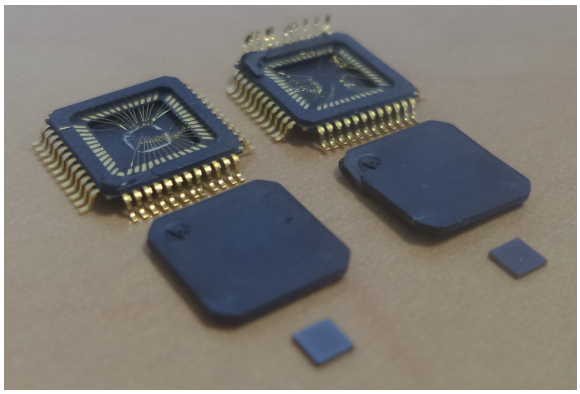


FIGURE 4.10: Vue face avant du circuit utilisé

Ensuite l'imagerie MEB a été réalisée sur ces deux circuits. Malgré les réglages identiques utilisés, dû au tilt et à la sélection manuelle de la zone à acquérir, une rangée d'images supplémentaire est acquise pour un des deux circuits. Pour cette application, des matrices de balayage de la platine de '$9X11$ et '$9X12$' images ont été définies puis les images acquises. Ces images sont enregistrées dans un dossier commun, cf figure 4.11. Chacune de ces images est de dimension 1024 par 768 pixels, et 8 octets codent le niveau de gris de chaque pixel (échelle de 256 niveaux), on obtient donc une image d'à peu près $800k$ octets (1024*768*8 = 786 432 octets caractérisant le

niveau de chaque pixel pour l'ensemble de l'image). Au niveau spatial, avec cette image acquise à un grossissement de $2.2kX$ nous rappelons que chaque pixel couvre 130nm en largeur et hauteur.

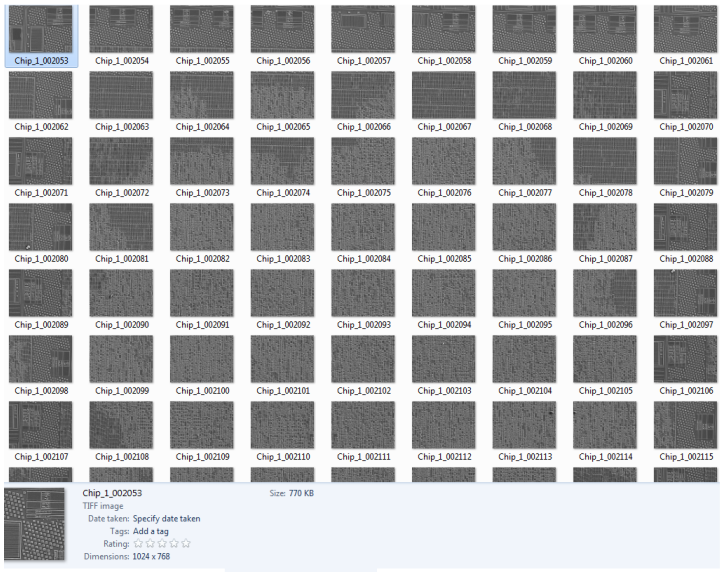


FIGURE 4.11: Ensemble des acquisitions du circuit infecté

Respectivement 27 et 29 minutes ont été nécessaires pour acquérir le circuit non infecté et son homologue infecté. Avec la vitesse de balayage du faisceau choisie, chaque champ de la matrice est parcouru et enregistré en 16 secondes. En quelques minutes supplémentaires les deux matrices d'images formeront deux seules images correspondantes au circuit authentique et au circuit à tester, cf figure 4.12.

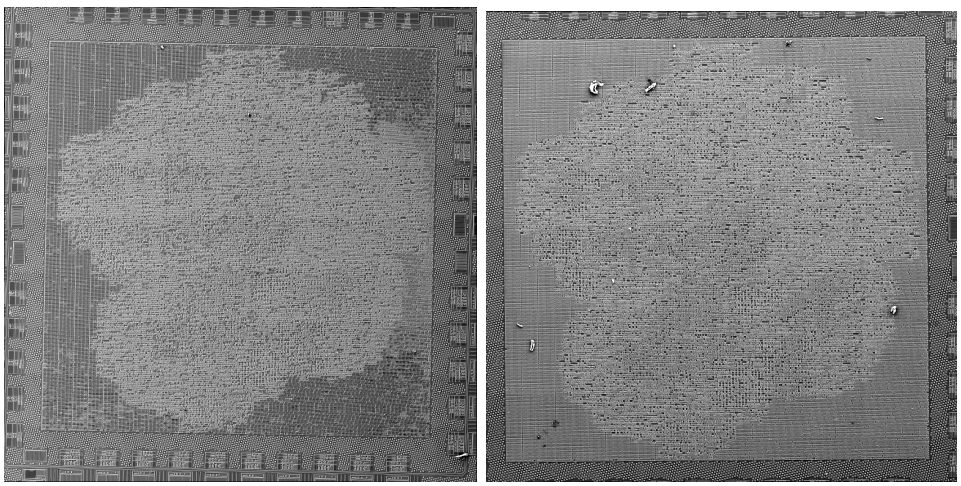


FIGURE 4.12: a) Vue globale du circuit authentique, b) Vue globale du circuit infecté

Tout comme le cas fictif évoqué précédemment, cf partie 4.2.1, la superposition directe des deux images ne permet pas de directement retrouver leurs différences. En effet, lors de l'acquisition d'image, chaque échantillon est placé sur un adhésif Carbone, une surface retenant l'échantillon mais non plate, cette inclinaison est plus forte que celle due au porte échantillon (cette dernière peut être aisément réglée). Le positionnement [X,Y,Z] diffère également, tout

comme la taille de la matrice de balayage (étant manuellement définie). Compte-tenu de ces propriétés, les images doivent être recalées car il existe notamment des distorsions en termes de rotation, translation et d'étirement entre ces deux images.

4.3.2 Détection manuelle ayant connaissance de la zone infectée

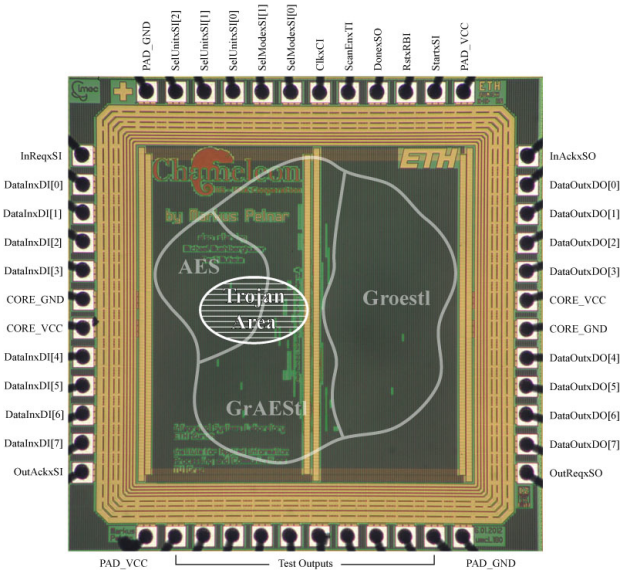


FIGURE 4.13: Vue d'ensemble du circuit intégré avec la zone infectée, figure extraite de [62]

Nous prenons avantage de la connaissance de la localisation approximative du Cheval de Troie. Cette localisation est illustrée dans la figure 4.13. Nous rappelons que le CTM représente 0.5% de cellules de base par rapport au circuit authentique. Les deux images sont dans cette partie recalées manuellement pour mettre en évidence les différences entres elles.

Pour le recalage manuel, un simple éditeur d'images peut être utilisé. Afin de superposer les deux images sur la zone infectée nous jouons sur la rotation et la translation de la deuxième par rapport à la première. Par exemple nous notons, dans le tableau 4.3.2, les dérives suivantes pour les éléments de la logique synthétisée placés aux quatre extrémités des deux images.

TABLEAU 4.3: Dérive observée lors du recalage manuel

Localisation	Dérive en X (en pixels)	Dérive en Y (en pixels)
Nord-Ouest	-6	-2
Sud-Ouest	-9	-10
Nord-Est	15	19
Sud-Est	12	16

Nous notons que les autres points de l'image ne sont pas recalés dus aux différentes distorsions de l'imagerie inhérentes à la microscopie. Nous récupérons ainsi la figure 4.14 où ces traits caractéristiques évoqués sont visibles. Cette image provient de la partie inférieure gauche lors de la superposition des deux images faite manuellement sur une autre zone d'intérêt (celle avec le Cheval de Troie). Cette image montre une dérive de quelques pixels entre les deux images du circuit acquises.

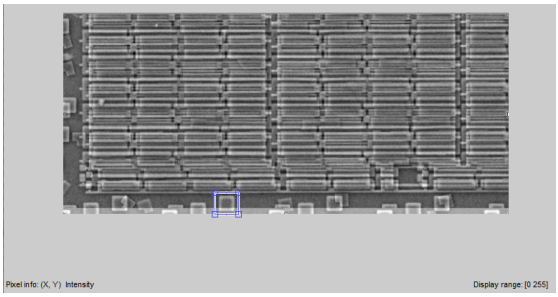


FIGURE 4.14: Alignement manuel de la zone : grossissement sur la partie bas gauche

Un grossissement sur cette zone, figure 4.15, permet également d'apercevoir la différence de contraste en fonction des variations d'intensités pour un même élément visualisé avec deux acquisitions différentes.

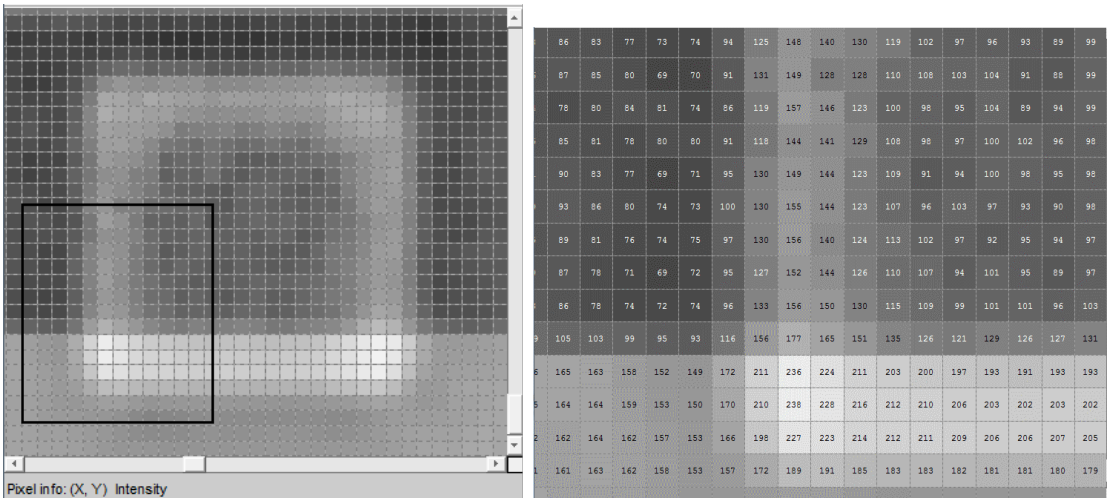


FIGURE 4.15: Grossissement des images superposées sur la partie inférieure gauche

Afin de faire correspondre les 2 images, nous modifions seulement les valeurs de rotation, de translation et de mise à l'échelle de la deuxième image. Nous arrivons à identifier très facilement les motifs différents entre les deux zones, quelques uns de ces motifs sont visibles sur la figure 4.16. Nous repérons que les cellules dites de remplissage ont été remplacées principalement par des motifs dont leur forme peut hypothétiquement faire penser à des cellules flip-flop. Outre le fait que l'on détecte un CTM, nous pouvons aussi connaître avec notre méthode le nombre de cellules rajoutées ou modifiées et émettre des hypothèses sur la nature du CTM sans que le circuit ne soit fonctionnel.

En résumé, notre méthode permet de retrouver toutes les cellules modifiées sur ce composant malgré l'utilisation de deux circuits différents, et malgré l'acquisition de deux images résultantes différentes en termes de translation, de rotation, de contraste, de mise à l'échelle ou encore d'histogramme. Ainsi notre méthode est compatible avec les variations de process et les variations de mesure (imagerie MEB sur de grandes zones). Avec cette mise en pratique réalisée, nous pouvons donc valider, en connaissance de la zone infectée, qu'il est alors possible d'utiliser cette approche pour détecter un Cheval de Troie Matériel.

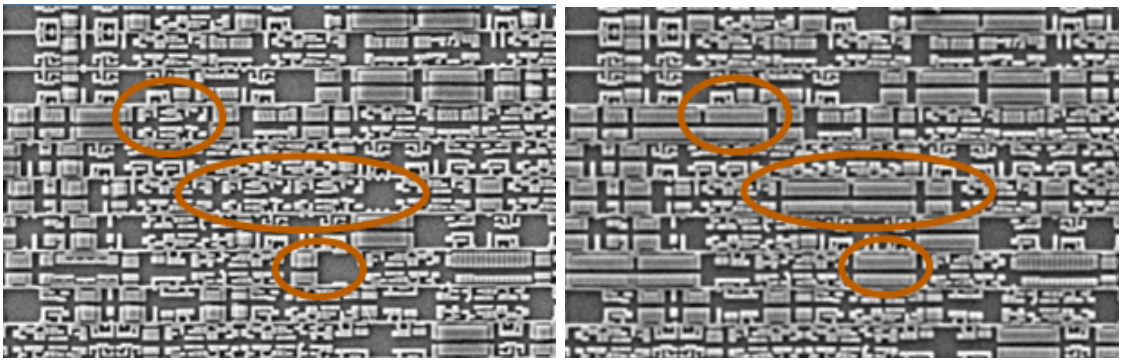


FIGURE 4.16: a) Circuit infecté (à gauche), b) Circuit non infecté (à droite)

Cependant, dans un cas réel, nous admettons que la connaissance de cette zone d'insertion ne sera jamais révélée. Nous cherchons alors à rendre possible la détection de CTMs sans aucune connaissance a priori du Cheval de Troie Matériel.

4.3.3 Détection automatique sans connaissance de la zone infectée

Nous avons vu que des défauts inhérents à la microscopie ne permettent pas de directement superposer les images de base de chaque circuit afin de détecter des modifications malicieuses. Les deux images de base ont des propriétés différentes, cf figure 4.17.

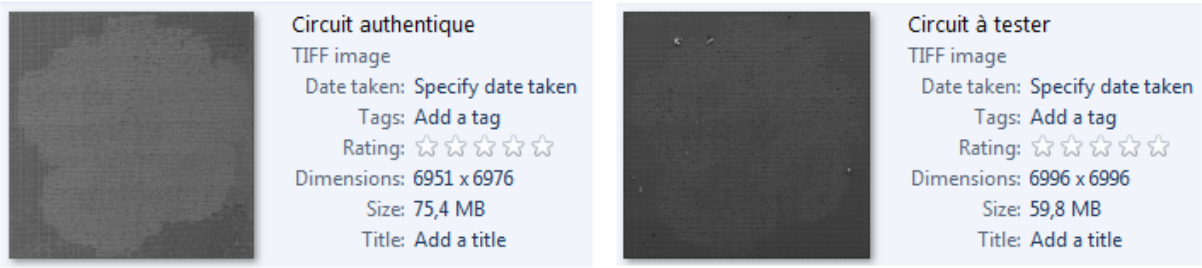


FIGURE 4.17: Différentes propriétés entre les images de base du circuit authentique et du circuit infecté

Une transformée affine est donc nécessaire pour appliquer rotation, translation et mise à l'échelle sur la deuxième image acquise. La distribution des intensités de l'image n'est pas ajustée par rapport à l'image du premier circuit. Cette approche permet une meilleure visualisation des différences entre les deux images (une image est à la base moins contrastée que l'autre). Les lignes droites présentes sur les deux images permettent tout d'abord de régler de manière globale la rotation de chacune d'elles.

L'image résultante est ensuite corrélée avec l'image du premier circuit restée inchangée. Notre processus est basé sur un outil permettant de rapidement trouver les coefficients de transformation à appliquer sur la deuxième image. Seuls quelques points similaires entre les 2 images des circuits sont à renseigner manuellement. De manière non optimale, nous en utilisons 10, cf figure 4.18.

Les différences entre le circuit authentique et le circuit infecté sont mises en évidence figure 4.19. Notre méthodologie permet ainsi de repérer toutes modifications au niveau caissons

base_points2 <10x2 double>

	1	2
1	29.0000	63.0000
2	6923	19
3	6927	6911
4	39	6935
5	1358	5984
6	2089	5257
7	2655	4354
8	3.4050e+03	3350
9	4335	2345
10	5050	1.2660e+03

input_points2 <10x2 double>

	1	2
1	41.0000	68.0000
2	6956	46.0000
3	6958	6936
4	48	6934
5	1371	5988
6	2103	5264
7	2673	4364
8	3425	3.3640e+03
9	4357	2362
10	5076	1.2870e+03

FIGURE 4.18: Points définis sur les deux images

des transistors effectuées sur tout ou une partie du circuit. Pour ce travail, des fonctions prédéfinies sous Matlab ont été utilisées. L'approche globale est quasi automatisée, seule la préparation d'échantillons, la définition des matrices à acquérir et à aligner et enfin la sélection de points similaires entre une image d'un circuit authentique et une image d'un circuit à tester sont à définir manuellement.

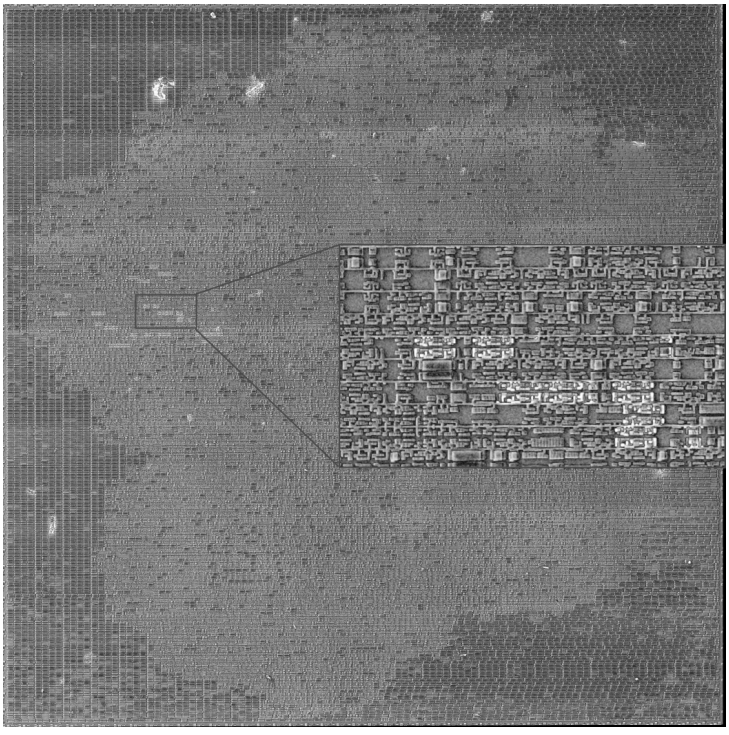


FIGURE 4.19: Superposition finale et grossissement sur la zone de présence des cellules modifiées

4.4 Avantages et inconvénients de la méthode proposée

Une rétro-conception totale allant du retrait niveau par niveau jusqu'à l'extraction de la netlist du composant ne permettrait pas de détecter tout type de Chevaux de Troie Matériels. En effet, une modification paramétrique des lignes d'alimentation par exemple ne serait pas ainsi détectée. Cette illustration permet de bien distinguer qu'il y a pour chaque technique de détection des avantages et des inconvénients et aucune méthode n'est efficace à 100%. De notre côté, notre méthode permet de détecter des CTMs avec l'avantage d'être non sensible à la taille du CTM, à l'activité du CTM, au noeud technologique du circuit intégré. Notre technique est robuste et flexible et permet à un utilisateur quelconque de l'utiliser afin d'émettre une conclusion sur l'intégrité d'un circuit intégré complet.

TABLEAU 4.4: Avantages et inconvénients de notre méthodologie de détection de CTMs

Type	Caractéristique de notre méthode de détection
Avantage	Intégrable dans le flot de fabrication de circuit intégré
Avantage	Peu coûteux, Rapide d'utilisation, efficace et n'affectant pas le rendement
Avantage	Robuste vis-à-vis de la taille du CTM présent dans le circuit
Avantage	Robuste vis-à-vis de l'activité du CTM présent dans le circuit
Avantage	Indépendant du niveau d'insertion du CTM
Avantage	Indépendant de l'effet du CTM
Avantage	Indépendant de la localisation spatiale du CTM
Avantage	Indépendant des variations des procédés de fabrication
Avantage	Prise en compte de la disponibilité de la référence
Avantage	Détection avant mise sur le marché et avant chargement de données sensibles (personnalisation)
Avantage	Méthodologie validée sur un exemple concret
Inconvénient	Ne détecte pas les CTMs insérés durant l'étape de design
Inconvénient	Ne couvre pas les insertions de CTMs au niveau métal ou au niveau dopant

4.5 Conclusion

Dans ce chapitre, nous avons défini une nouvelle méthode de détection de Chevaux de Troie Matériels rendue possible grâce aux performances de notre outil SEMBA. La méthode proposée est adaptée au cycle de vie des circuits intégrés d'un point de vue d'intégrateur de solutions sécurisées.

Notre méthode de détection prend en compte le type de référence disponible. Cependant elle ne couvre pas l'étape de conception car la référence est récupérée après l'étape de design. Grâce à notre méthode de détection appliquée aux différentes études de cas proposées dans ce travail, nous pouvons affirmer qu'hormis l'étape de design toutes les autres étapes de fabrication deviennent de confiance. Notre méthode se décompose en trois étapes ; les deux premières provenant de SEMBA où les circuits intégrés sont préparés jusqu'au niveau substrat puis photographiés sur l'ensemble de la surface de ce seul niveau. L'empreinte de chaque cellule de base est ainsi visualisée et permet de savoir quelle forme de cellule de base est présente à chaque localisation spatiale. L'image obtenue est ensuite corrélée à une référence émanant de l'outil de conception de circuits intégrés. Cette référence peut soit être un circuit identique dont la fabrication est de confiance, soit un fichier graphique de type GDSII ou encore un fichier textuel de type DEF. Ces trois scénariis ont été décrits [29].

La validation de notre approche a notamment été mise en oeuvre sur une paire de circuits dont l'un intégrait réellement un Cheval de Troie Matériel. Les deux images des caissons des transistors ont été obtenues puis manuellement superposées pour mettre en évidence le Cheval de Troie présent dont la position nous était connue. Cependant, nous avons cherché à trouver une méthode permettant de récupérer l'ensemble des cellules de base du CTM sans connaissance de celui-ci. Ainsi, nous avons mis en avant la détection automatique de modifications malicieuses avec la mise en place d'un traitement d'image automatisé. Toutes les cellules composant le CTM sont détectées et une représentation visuelle de ces dernières a été donnée. Nous avons ainsi démontré sur ce circuit l'efficacité de notre méthode avec une reconnaissance de toutes les cellules rajoutées [30].

Tableau 4.5: Flot de détection complet de CTM

Tâche	Rôle	Temps opérateur / (Temps développement)
Application de SEMBA sur le circuit authentique	Acquérir l'image de base du circuit authentique	50min / (15min)
Application de SEMBA sur le circuit à tester	Acquérir l'image de base du circuit à tester	40min / (NA)
Recalage de l'image du circuit de référence et de l'échantillon à tester	Permettre la comparaison entre deux images semblables	2min / (20min)
Détection finale par soustraction d'images	Mettre en évidence la présence de CTMs	1min / (2min)

La méthode de détection peut être insérée dans le cycle de vie des circuits intégrés. Elle n'a pas d'impact ni sur le délai de fabrication, ni sur le coût de fabrication. De plus, l'efficacité de la méthode, sa reproductibilité ainsi que sa prise en main rapide par l'utilisateur sont des caractéristiques intéressantes pour une éventuelle standardisation de la méthode au niveau industriel. Notre méthode est indépendante de l'activité du CTM, ainsi même un CTM avec une faible activité (consommation ou autre) serait couvert par notre méthode tout comme les CTMs avec une faible empreinte physique sur le circuit.

Conclusion générale

L'objectif de ces travaux de recherche était d'utiliser une approche invasive de rétro-conception afin d'améliorer la localisation spatiale ainsi que la maîtrise de la faute injectée et de proposer une méthode de vérification d'intégrité aux avantages industriels multiples (taux de détection, rapidité, coût, reproductibilité...)

L'état de l'art est pluri-disciplinaire, il porte sur la composition matérielle des circuits intégrés, de leur conception jusqu'à l'exploitation de leurs failles de sécurité. Nous avons notamment décrit les cellules dites de base qui constituent un ensemble appelé la logique synthétisée. On y trouve notamment les cellules flip-flop au milieu d'autres types de cellules. Nous avons vu dans ce premier chapitre que ces cellules sont particulièrement intéressantes pour la sécurité des circuits intégrés mais que l'accès physique ou visuel à cette logique synthétisée est limité. Nous avons ensuite présenté les buts des attaques, les types d'attaques possibles et les contremesures associées. Peu de références bibliographiques traitent d'attaques combinant à la fois des approches invasives et des attaques par injections de fautes. Nous avons choisi de combiner rétro-ingénierie et attaques laser ciblées. La complexité des circuits actuels (5-6 niveaux de métal) rendant difficile les attaques côté face active nous exploitons le substrat. L'intérêt de ces attaques dites face arrière réside dans le fait qu'un niveau d'énergie identique en tout point d'un circuit intégré peut être obtenu.

Dans le chapitre 2, nous proposons la méthodologie SEMBA (Scanning Electron Microscope Based Acquisition). C'est une méthodologie de rétro-conception invasive et partielle organisée en trois étapes : préparation d'échantillon, acquisitions et alignements automatique d'images, et reconnaissance de motifs. Une gravure humide permet d'obtenir une surface homogène du niveau où les caissons des transistors sont implantés (niveau substrat). En utilisant un Microscope Electronique à Balayage (MEB/SEM), nous montrons qu'il est ensuite possible de visualiser ces zones d'implantations. Le MEB utilisé permet d'acquérir des images à fort grossissement de l'ensemble du circuit. Un premier outil permet d'aligner l'ensemble de ces images entre elles pour obtenir une image globale dite de base. Puis un deuxième outil permet de reconnaître des motifs particuliers sur cette image de base. Nous démontrons que la mise en oeuvre de la méthodologie permet de localiser chaque cellule flip-flop présente dans un circuit de chiffrement matériel. Notre méthode est ainsi validée expérimentalement et a pour avantage d'être bas coût, rapide, reproductible à 100% et utilisable pour divers besoins.

Dans le chapitre 3, nous exploitons SEMBA pour localiser les cellules d'intérêt afin d'améliorer les attaques en fautes par injections laser. Les localisations spatiales sont obtenues sur un premier échantillon qui lui est rendu non fonctionnel, ces données de localisations sont ensuite utilisées par la plateforme d'injections laser sur un deuxième échantillon restant quant à lui fonctionnel. Un lien est établi entre l'image obtenue avec le MEB en face avant et celle obtenue en

face arrière à l'aide de la caméra IR présente sur le banc d'injections laser. Ce lien nous permet de positionner avec précision le faisceau laser au "dessus" des cellules d'intérêt. Nous démontrons le gain de temps obtenu pour la caractérisation de la sensibilité du circuit au laser ainsi que l'application directe des méthodes d'analyse de fautes telles que 'l'analyse en fautes différentielle' et l'analyse en 'safe error'. Ensuite, sur un circuit de type carte à puce en technologie 90nm, nous avons démontré qu'il est possible de contrôler l'état d'une cellule flip-flop (cellule complexe composée de plus d'une vingtaine de transistors). Ce contrôle est fait premièrement par la maîtrise de la localisation du faisceau laser. Nous montrons que les zones sensibles à la transition de '0' vers '1' sont différentes de celles sensibles à la transition de '1' vers '0'. Deuxièmement, nous démontrons qu'il est possible de contrôler la valeur des bits moyennant un ajustement précis de l'énergie laser atteignant la face arrière du circuit intégré. Nous sommes en mesure de réaliser une cartographie de sensibilité laser où seules les transitions de '1' vers '0' demeurent réalisables. Sur cet échantillon, nous avons extrait des cartographies en fonction des variations du niveau d'énergie qui atteint la face arrière du circuit intégré. Ensuite par l'application de notre méthodologie SEMBA, nous sommes en mesure de corréler les cartographies laser obtenues avec l'implémentation physique des transistors. En effet SEMBA nous permet de récupérer l'implémentation physique des régions actives des transistors. Il apparaît sur l'image de base SEMBA des colonnes où seul un type de transistors est présent (les PMOS) et d'autres colonnes où seul le type NMOS est présent (largeur de grille plus faible). En superposant cette image et la cartographie laser, nous validons dans un premier temps que les zones de sensibilité sont en adéquation avec la distribution des colonnes de transistors. De plus, sur la cartographie laser, les zones sensibles aux transitions de '1' vers '0' sont plus larges et se situent sur la colonne où les transistors NMOS sont présents. Inversement, les zones sensibles aux transitions de '0' vers '1' se situent sur la colonne où les transistors PMOS sont présents. Par la suite, sans connaissance de l'organisation de la cellule visée, nous faisons des hypothèses sur son schéma électrique et sur sa disposition spatiale. Nous validons ainsi que la sensibilité de la cellule dépend de la façon dont celle-ci est implantée physiquement. Ensuite, nous synthétisons les propriétés de l'attaque en fautes améliorée avec la méthodologie invasive SEMBA.

Dans le chapitre 4, la capacité d'obtenir avantageusement des informations spatiales sur les cellules de base est également utilisée à des fins de vérification d'intégrité. Nous définissons une nouvelle méthode de détection de Chevaux de Troie Matériels, cette dernière est de plus adaptée au cycle de vie des circuits intégrés. Bien que l'approche proposée soit destructrive, celle-ci n'a aucun effet sur le rendement de fabrication. En effet, notre méthode est appliquée sur les circuits non fonctionnels en sortie de production. Le principal intérêt de notre méthodologie est son indépendance vis-à-vis des caractéristiques physiques du circuit intégré testé et du Cheval de Troie Matériel. Son principal inconvénient est la nécessité de posséder une image ou un circuit de référence, ainsi un Cheval de Troie Matériel introduit au cours de l'étape de design n'est pas détectable. Depuis l'image obtenue via SEMBA, les empreintes de chaque cellule de base sont corrélées avec une référence disponible. Nous proposons trois différents scénarii de détection, soit avec une référence de type physique avec un 'Golden Model', soit avec un fichier de design de type graphique ('GDSII') ou soit avec un fichier de design de type texte ('DEF file'). Nous avons ainsi défini les besoins en termes d'imagerie pour chacun des scénariis de détections de détection proposés. Nous avons validé notre méthodologie sur un cas de Cheval de Troie Matériel simulé puis sur un cas réel. La mise en oeuvre de notre méthodologie sur un circuit réellement infecté et son équivalent non infecté a permis la détection d'un Cheval de Troie Matériel combinatoire de manière quasi-automatique. L'utilisation de traitements d'images permet de comparer les deux

images de base de ces deux circuits et de s'affranchir des caractéristiques inhérentes à l'imagerie et au microscope électronique. Seules les étapes de préparation d'échantillons, de définition de la zone à balayer et de sélection de points similaires demeurent manuelles. Notre traitement d'images nous permet de mettre en avant chaque cellule de base modifiée et d'émettre également des hypothèses sur le type de CTM présent dans le circuit. Dans notre cas d'application, le CTM combinatoire composé de trente flip-flop est localisé et de ce fait détecté. Nous synthétisons dans un tableau les tâches et le temps nécessaire pour ce type de détection. L'insertion de notre méthode de détection de CTMs semble tout à fait appropriée aux contraintes industrielles. De plus, il semble intéressant de coupler cette méthode de détection à une autre pour atteindre une couverture de test maximale en rendant de confiance l'étape de design.

A travers ce travail, il résulte la possibilité d'obtenir des informations sur l'implémentation matérielle d'un circuit intégré. Cette rétro-conception proposée est certes partielle mais fournit déjà beaucoup d'informations. On obtient ainsi une alternative à une méthode de rétro-conception complète et coûteuse. Notre méthodologie a été utilisée afin d'améliorer les attaques en fautes et afin de détecter des modifications malicieuses de circuits intégrés. Ces deux applications nous ont permis d'obtenir des résultats intéressants pour l'amélioration de la caractérisation de dispositifs sécurisés et pour la vérification d'intégrité de ces mêmes dispositifs.

Sur un plan plus général, cette capacité à obtenir ces informations spatiales peut être utilisée pour améliorer (ou corréler) d'autres types d'attaques. De nombreuses perspectives s'ouvrent en termes d'attaques en injection de fautes laser atteignant de tels niveaux de contrôle et de précision dans un circuit intégré. Nous pensons notamment à toutes les applications en cryptographie avec les modèles de fautes validés en pratique dans ce manuscrit. Il apparait également intéressant de modéliser les effets obtenus et de pouvoir comparer les résultats avec le layout de la cellule visée. Il subsiste encore un grand nombre de travaux à réaliser en imagerie, en optique et en microscopie autour de ces travaux réalisés et, *in fine*, autour de la sécurité matérielle des systèmes embarqués.

Annexe A

Autour de la rétro-conception partielle

Sommaire

A.1 Prendre avantage d'une préparation non parfaite

Le principal intérêt de l'acide fluorhydrique (HF) est la facilité avec laquelle on obtient des résultats relativement bons sans avoir besoin de contrôler attentivement les conditions de gravure. Cependant, des variations dans la préparation finale peuvent apparaître sur l'ensemble de la surface du composant en terme de présence de polysilicium ou non. On indique brièvement comment ces désavantages pourraient être utilisés pour obtenir des informations additionnelles sur la nature d'une cellule de base.

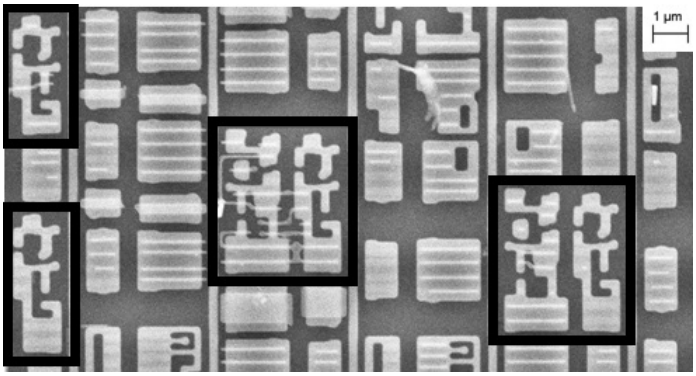


FIGURE A.1: Mise en évidence de cellules similaires avec différents niveaux

Sur la figure A.1, 4 cellules identiques sont encadrés. Nous pouvons apercevoir que le niveau polysilicium n'est pas identique sur ces cellules, nous repérons notamment pour 3 d'entres elles qu'il reste du polysilicium, la matière utilisée pour l'implémentation des grilles des transistors. Tandis que la cellule en bas à gauche n'affiche aucun niveau polysilicium. Suivant la préparation du circuit, des informations sur plusieurs niveaux de la puce peuvent être visibles. Ainsi nous

illustrons l'intérêt de combiner les différentes informations présentes sur ces cellules avec la figure A.2.

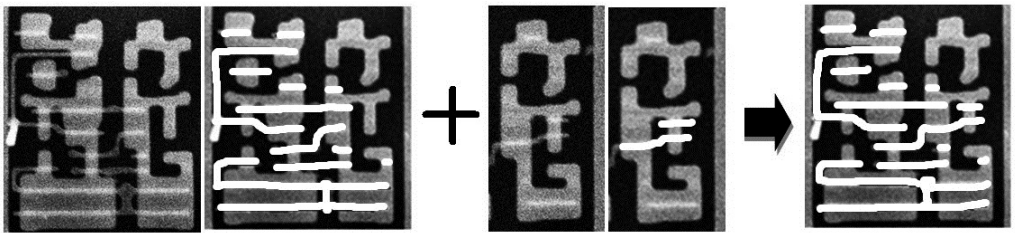


FIGURE A.2: Reconstructions à l'aide de plusieurs cellules

Il est ainsi possible de remonter plus facilement dans ce cas à la fonctionnalité réalisée par une cellule de base étudiée. Les différentes localisations du même type de cellules sur l'ensemble de la puce sont utilisées jusqu'à pouvoir redessiner chaque connection entre grille des transistors présents à l'intérieur d'une cellule de base. Appliquer différents temps de gravure sur le même type d'échantillons permettrait également de faire des acquisitions de la même cellule mais sur différents niveaux. Cela permet ainsi de photographier les cellules et d'avoir plus d'informations sur leurs fonctions.

A.2 Pré-traitement de l'image globale d'un circuit intégré

L'avantage de la méthodologie présentée dans le chapitre 2 est notamment d'avoir une seule image regroupant la totalité des informations d'un niveau d'un circuit intégré. Par contre, l'image peut contenir plusieurs dizaines de millions de pixels résultant en une image gourmande en terme de mémoire pour son futur traitement malgré un enregistrement dans un format d'image compressé sans pertes, en noir et blanc et avec seulement 255 niveaux de gris définissant chaque pixel de l'image.

Cette image peut-être pré-traitée pour ne conserver que de l'information utile pour le reste de nos expérimentations. On peut penser par exemple que de multiples niveaux de gris ne sont pas utiles ou encore que l'information contenue à l'intérieur des cellules de bases ne sont pas nécessaires lors de l'étape de reconnaissances de formes. Cette approche est visible sur la figure A.3.

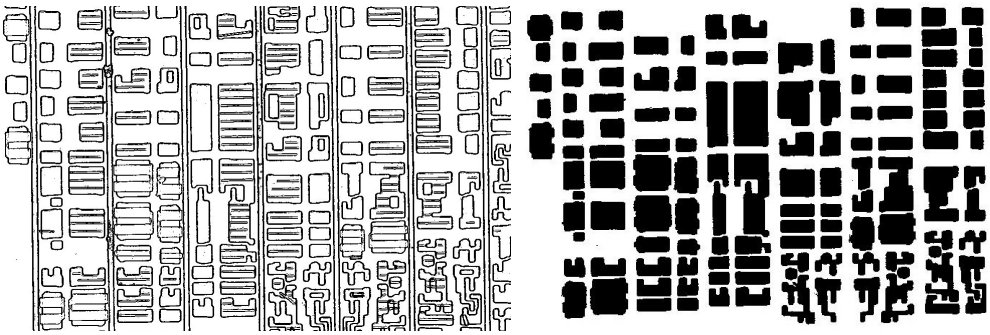


FIGURE A.3: Exemples de pré-traitement des images : a) Image binaire représentant les motifs, b) Forme 'extérieure' représentant les motifs

A.3 Difficultés/Spécificités et Améliorations de la détection de CTMs

Vers la détection au niveau métal et dopant

Rajout d'étapes Notre méthodologie ne nécessite l'accès qu'au niveau substrat d'un circuit intégré dont l'accès est très simple à obtenir en termes de préparation d'échantillons et dont les propriétés topologiques offrent des informations suffisantes sur la modification ou l'ajout de cellule de base. Cependant, en prenant en compte la grande variété de CTMs possibles, cet avantage peut se transformer en un inconvénient. En effet, avec la méthodologie présentée tout CTMs insérés sur un niveau supérieur (niveaux métalliques) ou sur un niveau inférieur (niveaux dopants) ne seraient pas détectés. Cependant, l'avantage de notre méthodologie est d'être assez flexible et de permettre l'ajout d'étapes supplémentaires.

Détection niveau dopant Dans l'état de l'art, cf partie 4.2, des possibilités d'insertion CTMs au niveau dopant ont été présentées. Cette insertion a été jugée comme non repérable par l'utilisation de technique de microscopie passive. Cependant, par la suite il a été mis en pratique la détection de ces CTMs. Les propriétés de la microscopie électronique sur une puce préparée au niveau contact ont permis de détecter les différents types de jonctions. Nous cherchons donc à compléter notre méthodologie par l'ajout d'une étape supplémentaire permettant d'effectuer ce même type de détection mais de manière rapide et efficace sur l'ensemble d'un circuit.

Nous nous sommes ainsi dirigés vers une seconde gravure humide, sélective, permettant de graver plus rapidement les zones P que les zones dopées N [10]. Pour ce besoin, nous utilisons de l'Hydroxyde de Potassium (KOH) et obtenons la figure A.4 après un bain de gravure de quelques secondes.

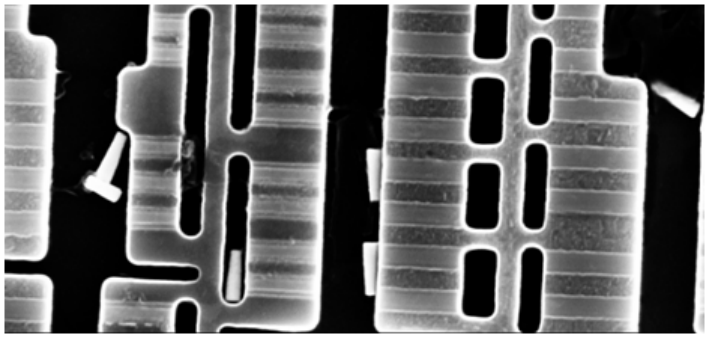


FIGURE A.4: Quelques μm^2 d'un circuit intégré après bains de gravure HF et KOH

Sur cette figure A.4, il existe seulement des disparités entre colonnes de transistors. La mise en pratique ne permet pas d'amener des conclusions. Mais la mise à disposition d'échantillons infectés par des CTMs insérés au niveau dopant devrait nous permettre de conclure sur l'efficacité de notre méthode à l'intérieur même des cellules de bases où des modifications malicieuses seront présentes.

Détection niveau Metal Tout changement, toute suppression ou encore toute modification de cellules de bases est détectée grâce à notre technique, cependant des questions se posent pour vérifier la connectivité de cellules qui sont présentes au niveau 'metal1' et qui peuvent être interconnectés pour satisfaire des besoins de modifications de circuits sans pour autant devoir

concevoir à nouveau l'intégralité du circuit. Ainsi, des cellules dites 'ECO' sont présentes dans les circuits intégrés et peuvent être connectées entres elles pour également créer un Cheval de Troie Matériel. Dans cette optique, nous avons pensé à modifier notre flot de préparation pour détecter ces changements. En effet, le niveau substrat n'est pas intéressant car aucune modification ne pourrait être visible, de même pour le niveau Métal1. Par contre la connaissance de la présence ou non de contacts sous M1 répondrait au besoin. A ce stade, seule une proposition de réflexion existe et elle porte sur une solution permettant de savoir où sont connectés des plots au niveau M1. L'idée est d'avoir une approche similaire que celle entrevue dans SEMBA.

Vers une amélioration de l'imagerie et de son traitement

Traitement de l'image Dans notre cas d'étude les techniques de traitement d'image reposent sur l'utilisation d'un algorithme standard pour la reconnaissance de motifs. Nous pensons qu'il est notamment possible d'optimiser la reconnaissance de motifs en jouant sur la manière de parcourir l'image, de sélectionner le seuil, de sélectionner l'ordre des motifs à reconnaître et d'avoir un apprentissage qui se réalise suivant l'image acquise au MEB ou encore suivant une famille de circuits intégrés.

Vers une méthode d'imagerie efficace face arrière Bien que notre méthode de détection de CTMs ne soit appliquée qu'à des circuits non fonctionnels, il serait intéressant de développer une méthode de détection qui n'intègre pas d'étapes destructrices et qui de surcroit pourrait être réalisable directement sur wafer. Nous avons envisagé d'utiliser des techniques d'imagerie infrarouge à travers le substrat. A ce jour en imagerie passive, nous arrivons seulement à visualiser la taille de l'empreinte de chacune des cellules de base sans pour autant retrouver le nombre de transistors présents dans la cellule de base. Il n'est pas possible de remonter à la fonction de la cellule ou encore de permettre la différenciation de plusieurs cellules entre elles.

Références

[1] https ://www.trust-hub.org/taxonomy (Citée sur les pages xv et 21.)

[2] http ://www.chipworks.com/ (Citée sur la page 22.)

[3] Aarestad, J., Acharyya, D., Rad, R., Plusquellic, J. : Detecting trojans through leakage current analysis using multiple supply pad s. Information Forensics and Security, IEEE Transactions on 5(4), 893–904 (Dec 2010) (Citée sur la page 75.)

[4] Abraham, D.G., Dolan, G.M., Double, G.P., Stevens, J.V. : Transaction security system. IBM Syst. J. 30(2), 206–229 (Mar 1991), http://dx.doi.org/10.1147/sj.302.0206 (Citée sur la page 20.)

[5] Agoyan, M., Dutertre, J.M., Naccache, D., Robisson, B., Tria, A. : When clocks fail : On critical paths and clock faults. In : Gollmann, D., Lanet, J.L., Iguchi-Cartigny, J. (eds.) Smart Card Research and Advanced Application, Lecture Notes in Computer Science, vol. 6035, pp. 182–193. Springer Berlin Heidelberg (2010), http://dx.doi.org/10.1007/978-3-642-12510-2_13 (Citée sur la page 16.)

[6] Anderson, R., Kuhn, M. : Low cost attacks on tamper resistant devices (1997) (Citée sur la page 14.)

[7] Bao, C., Forte, D., Srivastava, A. : On application of one-class svm to reverse engineering-based hardware trojan detection. In : Quality Electronic Design (ISQED), 2014 15th International Symposium on. pp. 47–54 (March 2014) (Citée sur la page 75.)

[8] Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., Whelan, C. : The sorcerer's apprentice guide to fault attacks. IACR Cryptology ePrint Archive p. 100 (2004) (Citée sur la page 14.)

[9] Barenghi, A., Bertoni, G., Breveglieri, L., Pellicioli, M., Pelosi, G. : Low voltage fault attacks to aes. In : Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on. pp. 7–12 (June 2010) (Citée sur la page 16.)

[10] Beck, F. : Integrated Circuit Failure Analysis : A Guide to Preparation Techniques. Quality and Reliability Engineering Series, Wiley (1998), http://books.google.fr/books?id=7VNfvKjlzYAC (Citée sur les pages 23 et 99.)

[11] Becker, G.T., Regazzoni, F., Paar, C., Burleson, W.P. : Stealthy dopant-level hardware trojans : extended version. J. Cryptographic Engineering 4(1), 19–31 (2014), http://dx.doi.org/10.1007/s13389-013-0068-0 (Citée sur la page 75.)

[12] Bhasin, S., Danger, J.L., Guilley, S., Ngo, X., Sauvage, L. : Hardware trojan horses in cryptographic ip cores. In : Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on. pp. 15–29 (Aug 2013) (Citée sur la page 75.)

[13] Biham, E., Shamir, A. : Differential fault analysis of secret key cryptosystems. In : CRYPTO. pp. 513–525 (1997) (Citée sur la page 34.)

[14] Bishop, C.M. : Pattern Recognition and Machine Learning (Information Science and Statistics). Springer-Verlag New York, Inc., Secaucus, NJ, USA (2006) (Citée sur les pages 27 et 28.)

[15] Blomer, J., Seifert, J.P. : Fault based cryptanalysis of the advanced encryption standard (aes). In : Financial Cryptography. Lecture Notes in Computer Science, vol. 2742, pp. 162–181. Springer (2003) (Citée sur les pages 34 et 61.)

[16] Blythe, S., Fraboni, B., Lall, S., Ahmed, H., de Riu, U. : Layout reconstruction of complex silicon chips. Solid-State Circuits, IEEE Journal of 28(2), 138–145 (Feb 1993) (Citée sur la page 25.)

[17] Bond, M., Choudary, O., Murdoch, S.J., Skorobogatov, S.P., Anderson, R.J. : Chip and skim : cloning emv cards with the pre-play attack. CoRR (2012) (Citée sur la page 14.)

[18] Boneh, D., DeMillo, R., Lipton, R. : On the importance of checking cryptographic protocols for faults. In : Fumy, W. (ed.) Advances in Cryptology — EUROCRYPT '97, Lecture Notes in Computer Science, vol. 1233, pp. 37–51. Springer Berlin Heidelberg (1997), http://dx.doi.org/10.1007/3-540-69053-0_4 (Citée sur la page 34.)

[19] Borrel, N., Champeix, C., Lisart, M., Sarafianos, A., Kussener, E., Rahajandraibe, W., DUTERTRE, J.M. : Characterization and simulation of a body biased structure in triple-well technology under pulsed photoelectric laser stimulation. In : International Symposium for Testing and Failure Analysis (ISTFA). Houston, United States (Nov 2014), http://hal-emse.ccsd.cnrs.fr/emse-01099035 (Citée sur la page 31.)

[20] Breitenstein, O., Altmann, F., Riediger, T., Karg, D., Gottschalk, V. : Lock-in thermal IR imaging using a solid immersion lens. Microelectronics Reliability 46(9-11), 1508–1513 (2006), http://dx.doi.org/10.1016/j.microrel.2006.07.027 (Citée sur la page 21.)

[21] Briechle, K., Hanebeck, U.D. : Template matching using fast normalized cross correlation. vol. 4387, pp. 95–102 (2001), http://dx.doi.org/10.1117/12.421129 (Citée sur la page 25.)

[22] Brier, E., Clavier, C., Olivier, F. : Correlation power analysis with a leakage model. In : CHES. pp. 16–29 (2004) (Citée sur la page 14.)

[23] C D Kuglin, D.C.H. : The phase correlation image alignment method. In : in Proceedings of the Int. Conf. Cybernetics and Society'75 (1975) (Citée sur la page 45.)

[24] Carl F. Nielsen, S.R.G. : Wpi 0.5 mm cmos standard cell library databook (2000) (Citée sur la page 8.)

[25] Chakraborty, R., Narasimhan, S., Bhunia, S. : Hardware trojan : Threats and emerging solutions. In : High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International. pp. 166–171 (Nov 2009) (Citée sur les pages xvii et 74.)

[26] Courbon, F., Fournier, J.J.A., Loubet-Moundi, P., Tria, A. : Combining image processing and laser fault injections for characterizing a hardware AES. IEEE Trans. on CAD of Integrated Circuits and Systems 34(6), 928–936 (2015), http://dx.doi.org/10.1109/TCAD.2015.2391773 (Citée sur la page 72.)

[27] Courbon, F., Loubet-Moundi, P., Fournier, J.J.A., Tria, A. : Adjusting laser injections for fully controlled faults. In : Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers. pp. 229–242 (2014), http://dx.doi.org/10.1007/978-3-319-10175-0_16 (Citée sur la page 71.)

[28] Courbon, F., Loubet-Moundi, P., Fournier, J.J.A., Tria, A. : Increasing the efficiency of laser fault injections using fast gate level reverse engineering. In : 2014 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2014, Arlington, VA, USA, May 6-7, 2014. pp. 60–63 (2014), http://dx.doi.org/10.1109/HST.2014.6855569 (Citée sur la page 54.)

[29] Courbon, F., Loubet-Moundi, P., Fournier, J.J.A., Tria, A. : A high efficiency hardware trojan detection technique based on fast SEM imaging. In : Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, DATE 2015, Grenoble, France, March 9-13, 2015. pp. 788–793 (2015), http://dl.acm.org/citation.cfm?id=2755932 (Citée sur la page 90.)

[30] Courbon, F., Loubet-Moundi, P., Fournier, J.J.A., Tria, A. : Semba : A sem based acquisition technique for fast invasive hardware trojan detection. In : Proceedings of the 2015 European Conference on Circuit Theory and & Design, ECCTD 2015, Trondheim, Norway, August 24-26, 2015. pp. 788–793 (2015) (Citée sur la page 90.)

[31] Darracq, F., Lapuyade, H., Buard, N., Mounsi, F., Foucher, B., Fouillat, P., Calvet, M.C., Dufayel, R. : Backside seu laser testing for commercial off-the-shelf srams. Nuclear Science, IEEE Transactions on 49(6), 2977–2983 (Dec 2002) (Citée sur la page 31.)

[32] Dassance, F., Venelli, A. : Combined fault and side-channel attacks on the aes key schedule. In : Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on. pp. 63–71 (Sept 2012) (Citée sur la page 18.)

[33] Deboy, G., Kolzer, J. : Fundamentals of light emission from silicon devices. Semiconductor Science and Technology 9(5), 1017 (1994), http://stacks.iop.org/0268-1242/9/i=5/a=004 (Citée sur la page 15.)

[34] Douin, A., Pouget, V., Darracq, F., Lewis, D., Fouillat, P., Perdu, P. : Influence of laser pulse duration in single event upset testing. Nuclear Science, IEEE Transactions on 53(4), 1799–1805 (Aug 2006) (Citée sur la page 31.)

[35] Dupuis, S., Ba, P.S., Flottes, M.L., Di Natale, G., Rouzeyre, B. : New testing procedure for finding insertion sites of stealthy hardware trojans. In : Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition. pp. 776–781. EDA Consortium (2015) (Citée sur la page 21.)

[36] Feigelson, R. : 50 Years Progress in Crystal Growth : A Reprint Collection. Elsevier Science (2004), https://books.google.fr/books?id=0lEcYdpLlBOC (Citée sur la page 4.)

[37] Ferrigno, J., Hlavac, M. : When aes blinks : introducing optical side channel. Information Security, IET 2(3), 94–98 (September 2008) (Citée sur la page 17.)

[38] Forli, L., Picart, B., Reverdy, A., Schlangen, R. : Scan chain debug using dynamic lock-in thermography. In : 37th, International Symposium for Testing and Failure Analysis ; ISTFA 2011, pp. 153–157. ASM international (2011) (Citée sur la page 21.)

[39] Fournier, J., Rigaud, J.B., Bouquet, S., Robisson, B., Tria, A., Dutertre, J.M., Agoyan, M. : Design and characterisation of an aes chip embedding countermeasures. IJIEI 1(3/4), 328–347 (2011) (Citée sur la page 48.)

[40] Fournier, J.J.A., Loubet-Moundi, P. : Memory address scrambling revealed using fault attacks. In : 2010 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2010, Santa Barbara, California, USA, 21 August 2010. pp. 30–36 (2010), http://dx.doi.org/10.1109/FDTC.2010.13 (Citée sur la page 18.)

[41] Giraud, C. : Dfa on aes. In : AES Conference. pp. 27–41 (2004) (Citée sur les pages 34 et 60.)

[42] Guilley, S., Hoogvorst, P., Pacalet, R. : Differential power analysis model and some results. In : Quisquater, J.J., Paradinas, P., Deswarte, Y., El Kalam, A. (eds.) Smart Card Research and Advanced Applications VI, IFIP International Federation for Information Processing, vol. 153, pp. 127–142. Springer US (2004), http://dx.doi.org/10.1007/1-4020-8147-2_9 (Citée sur la page 14.)

[43] Habing, D. : The use of lasers to simulate radiation-induced transients in semiconductor devices and circuits. Nuclear Science, IEEE Transactions on 12(5), 91–100 (1965) (Citée sur la page 16.)

[44] Helfmeier, C., Nedospasov, D., Tarnovsky, C., Krissler, J.S., Boit, C., Seifert, J.P. : Breaking and entering through the silicon. In : Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. pp. 733–744. CCS '13, ACM, New York, NY, USA (2013), http://dx.doi.org/10.1145/2508859.2516717 (Citée sur la page 17.)

[45] Hugin : Panorama stitching tools (Citée sur la page 24.)

[46] JEOL : A guide to scanning microscope observation (Citée sur la page 26.)

[47] Johnston, A. : Charge generation and collection in p-n junctions excited with pulsed infrared lasers. Nuclear Science, IEEE Transactions on 40(6), 1694–1702 (1993) (Citée sur la page 31.)

[48] Kaeslin, H. : Digital Integrated Circuit Design : From VLSI Architectures to CMOS Fabrication. New York, USA, 1st edn. (2008) (Citée sur les pages 8 et 46.)

[49] Kocher, P.C., Jaffe, J., Jun, B. : Differential power analysis. In : CRYPTO. pp. 388–397 (1999) (Citée sur la page 14.)

[50] Koeune, F., Standaert, F.X. : A tutorial on physical security and side-channel attacks. In : Aldini, A., Gorrieri, R., Martinelli, F. (eds.) Foundations of Security Analysis and Design III, Lecture Notes in Computer Science, vol. 3655, pp. 78–108. Springer Berlin Heidelberg (2005), http://dx.doi.org/10.1007/11554578_3 (Citée sur la page 14.)

[51] Lagunovsky, D., Ablameyko, S., Kutas, M. : Recognition of integrated circuit images in reverse engineering. In : International Conference on Pattern Recognition. vol. 2, pp. 1640–1642 (1998) (Citée sur la page 25.)

[52] Leveugle, R., Ammari, A., Maingot, V., Teyssou, E., Moitrel, P., Mourtel, C., Feyt, N., Rigaud, J.B., Tria, A. : Experimental evaluation of protections against laser-induced faults and consequences on fault modeling. In : DATE. pp. 1587–1592 (2007) (Citée sur la page 34.)

[53] Lewis, J. : Fast normalized cross-correlation. Vision interface 10(1), 120–123 (1995) (Citée sur la page 25.)

[54] Loubet-Moundi, P., Vigilant, D., Olivier, F. : Static Fault Attacks on Hardware DES Registers. Cryptology ePrint Archive, Report 2011/531 (Sep 2011), http://eprint.iacr.org/2011/531 (Citée sur la page 33.)

[55] Maimuţ, D., Murdica, C., Naccache, D., Tibouchi, M. : Fault attacks on projective-to-affine coordinates conversion. In : Prouff, E. (ed.) Constructive Side-Channel Analysis and Secure Design, Lecture Notes in Computer Science, vol. 7864, pp. 46–61. Springer Berlin Heidelberg (2013), http://dx.doi.org/10.1007/978-3-642-40026-1_4 (Citée sur la page 20.)

[56] Masalskis, G., Navickas, R. : Reverse engineering of CMOS integrated circuits. Electronics and Electrical Engineering, Kaunas Technologija (8), 88 (2008) (Citée sur la page 25.)

[57] Mayer-Sommer, R. : Smartly analyzing the simplicity and the power of simple power analysis on smartcards. In : CHES. pp. 78–92. Springer-Verlag, London, UK (2000) (Citée sur la page 14.)

[58] Melinger, J., Buchner, S., McMorrow, D., Stapor, W., Weatherford, T., Campbell, A., Eisen, H. : Critical evaluation of the pulsed laser method for single event effects testing and fundamental studies. Nuclear Science, IEEE Transactions on 41(6), 2574–2584 (Dec 1994) (Citée sur les pages xv et 32.)

[59] Michael Bajura, Greg Boverman, J.T.G.W.C.M.R.M.F.J.R.A.T.S.A.P.R. : Imaging integrated circuits with x-ray microscopy (2011) (Citée sur les pages xv et 22.)

[60] Miller, V.S. : Use of elliptic curves in cryptography. In : Lecture Notes in Computer Sciences ; 218 on Advances in cryptology—CRYPTO 85. pp. 417–426. Springer-Verlag New York, Inc., New York, NY, USA (1986), http://dl.acm.org/citation.cfm?id=18262.25413 (Citée sur la page 13.)

[61] Moro, N., Heydemann, K., Encrenaz, E., Robisson, B. : Formal verification of a software countermeasure against instruction skip attacks. Journal of Cryptographic Engineering 4(3), 145–156 (2014), http://dx.doi.org/10.1007/s13389-014-0077-7 (Citée sur la page 20.)

[62] Muehlberghuber, M., Gürkaynak, F.K., Korak, T., Dunst, P., Hutter, M. : Red team vs. blue team hardware trojan analysis : detection of a hardware trojan on an actual ASIC. In : HASP 2013, The Second Workshop on Hardware and Architectural Support for Security and Privacy, Tel-Aviv, Israel, June 23-24, 2013. p. 1 (2013), http://doi.acm.org/10.1145/2487726.2487727 (Citée sur les pages xvii, 83, et 85.)

[63] Nohl, K., Evans, D., Starbug, S., Plötz, H. : Reverse-engineering a cryptographic rfid tag. In : Proceedings of the 17th conference on Security symposium. p. 185–193 (2008) (Citée sur les pages xv, 10, 21, et 28.)

[64] Rivest, R., Shamir, A., Adleman, L. : A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21, 120–126 (1978) (Citée sur la page 13.)

[65] Roche, T., Lomné, V., Khalfallah, K. : Combined fault and side-channel attack on protected implementations of aes. In : CARDIS. pp. 65–83 (2011) (Citée sur la page 18.)

[66] Roscian, C., Dutertre, J.M., Tria, A. : Frontside laser fault injection on cryptosystems - application to the aes' last round -. In : HOST. pp. 119–124 (2013) (Citée sur les pages xv, xvi, 33, 34, 48, et 69.)

[67] Roscian, C., Sarafianos, A., Dutertre, J., Tria, A. : Fault model analysis of laser-induced faults in SRAM memory cells. In : 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography, Los Alamitos, CA, USA, August 20, 2013. pp. 89–98 (2013), http://dx.doi.org/10.1109/FDTC.2013.17 (Citée sur les pages 31 et 33.)

[68] Sarafianos, A., Llido, R., Dutertre, J.M., Gagliano, O., Serradeil, V., Lisart, M., Goubier, V., Tria, A., Pouget, V., Lewis, D. : Building the electrical model of the PhotoelectricLaserStimulation of a PMOS transistor in 90 nm technology. Journal of Microelectronics Reliability pp. 2035–2038 (Sep 2012), 23rd European Symposium on Reliability of Electron Devices, Failure Physics and Analysis Cagliari, ESREF2012 (Citée sur les pages xv, 32, et 65.)

[69] Sarafianos, A., Roscian, C., Dutertre, J.M., Lisart, M., Tria, A. : Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an sram cell. ESREF 53, 1300 – 1305 (2013) (Citée sur les pages xv, 31, et 32.)

[70] Schlösser, A., Nedospasov, D., Krämer, J., Orlic, S., Seifert, J.P. : Simple Photonic Emission Analysis of AES. In : Prouff, E., Schaumont, P. (eds.) Cryptographic Hardware and Embedded Systems (CHES). Lecture Notes in Computer Science (LNCS), vol. 7428, pp. 41–57. Springer Berlin/Heidelberg (Sep 2012), http://dx.doi.org/10.1007/978-3-642-33027-8_3 (Citée sur la page 22.)

[71] Schobert, M. : http ://www.degate.org/documentation (Citée sur les pages 22 et 28.)

[72] Skorobogatov, S. : Optically enhanced position-locked power analysis. In : Goubin, L., Matsui, M. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2006, Lecture Notes in Computer Science, vol. 4249, pp. 61–75. Springer Berlin Heidelberg (2006), http://dx.doi.org/10.1007/11894063_6 (Citée sur la page 18.)

[73] Skorobogatov, S.P., Anderson, R.J. : Optical fault induction attacks. In : CHES proceedings. pp. 2–12. Springer-Verlag (2002) (Citée sur les pages 16 et 29.)

[74] of Standards, N.I., Technology : Advanced encryption standard. NIST FIPS PUB 197 (2001) (Citée sur la page 13.)

[75] Strobel, D., Driessen, B., Kasper, T., Leander, G., Oswald, D., Schellenberg, F., Paar, C. : Fuming acid and cryptanalysis : Handy tools for overcoming a digital locking and access control system. In : Canetti, R., Garay, J. (eds.) Advances in Cryptology – CRYPTO 2013, Lecture Notes in Computer Science, vol. 8042, pp. 147–164. Springer Berlin Heidelberg (2013), http://dx.doi.org/10.1007/978-3-642-40041-4_9 (Citée sur la page 18.)

[76] Strobel, D., Driessen, B., Kasper, T., Leander, G., Oswald, D., Schellenberg, F., Paar, C. : Fuming acid and cryptanalysis : Handy tools for overcoming a digital locking and access control system. In : CRYPTO. pp. 147–164. Springer (2013) (Citée sur la page 21.)

[77] Sugawara, T., Suzuki, D., Fujii, R., Tawa, S., Hori, R., Shiozaki, M., Fujino, T. : Reversing stealthy dopant-level circuits. In : Batina, L., Robshaw, M. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2014, Lecture Notes in Computer Science, vol. 8731, pp. 112–126. Springer Berlin Heidelberg (2014) (Citée sur la page 75.)

[78] Tarnovsky, C. : Inducing momentary faults within secure smartcards (2010) (Citée sur la page 18.)

[79] Torrance, R., James, D. : The state-of-the-art in ic reverse engineering. In : CHES. pp. 363–381 (2009) (Citée sur les pages xv, 22, et 25.)

[80] Wang, F., Agrawal, V.D. : Single event upset : An embedded tutorial. In : in VLSI Design, 2008. Held jointly with 7th International Conference on Embedded Systems., 21th International Conference on, 2008. pp. 429–434 (Citée sur les pages xv et 31.)

[81] Weilie Zhou, Robert P. Apkarian, Z.L.W., Joy, D. : Fundamentals of scanning electron microscopy (Citée sur la page 25.)

[82] Yen, S.M., Joye, M. : Checking before output may not be enough against fault-based cryptanalysis. IEEE Trans. Computers 49(9), 967–970 (2000) (Citée sur la page 34.)

[83] Zhang, F., Zhao, X., Guo, S., Wang, T., Shi, Z. : Improved algebraic fault analysis : A case study on piccolo and applications to other lightweight block ciphers. In : Prouff, E. (ed.) Constructive Side-Channel Analysis and Secure Design, Lecture Notes in Computer Science, vol. 7864, pp. 62–79. Springer Berlin Heidelberg (2013), http://dx.doi.org/10.1007/978-3-642-40026-1_5 (Citée sur la page 20.)

École Nationale Supérieure des Mines
de Saint-Étienne

NNT : *2015 EMSE 0788.*

Franck COURBON

PARTIAL HARDWARE REVERSE ENGINEERING APPLIED TO FINE GRAINED LASER FAULT INJECTION AND EFFICIENT HARDWARE TROJANS DETECTION

Speciality : Microelectronic

Keywords : Hardware Security, partial reverse engineering, cells localization, laser injection, fault model, Hardware Trojans

Abstract :

The work described in this thesis covers an integrated circuit characterization methodology based on a partial hardware reverse engineering. On one hand in order to improve integrated circuit security characterization, on the other hand in order to detect the presence of Hardware Trojans. Our approach is said partial as it is only based on a single hardware layer of the component and also because it does not aim to recreate a schematic or functional description of the whole circuit.

A low cost, fast and efficient reverse engineering methodology is proposed. The latter enables to get a global image of the circuit where only transistor's active regions are visible. It thus allows localizing every standard cell. The implementation of this methodology is applied over different secure devices.

The obtained image according to the methodology declined earlier is processed in order to spatially localize sensible standard cells, nay critical in terms of security. Once these cells identified, we characterize the laser effect over different location of these standard cells and we show the possibility with the help of laser fault injection the value they contain. The technique is novel as it validates the fault model over a complex gate in 90nm technology node.

Finally, a Hardware Trojan detection method is proposed using the partial reverse engineering output. We highlight the addition of few non listed cells with the application on a couple of circuits. The method implementation therefore permits to detect, without full reverse-engineering (and so cheaply), quickly and efficiently the presence of Hardware Trojans.

École Nationale Supérieure des Mines
de Saint-Étienne

NNT : *2015 EMSE 0788.*

Franck COURBON

RETRO-CONCEPTION MATERIELLE PARTIELLE APPLIQUEE A L'INJECTION CIBLEE DE FAUTES LASER ET A LA DETECTION EFFICACE DE CHEVAUX DE TROIE MATERIELS

Spécialité: Microélectronique

Mots clefs : sécurité matérielle, rétro-conception partielle, localisation de portes, injection laser, modèles de fautes, Chevaux de Troie Matériels

Résumé :

Le travail décrit dans cette thèse porte sur une nouvelle méthodologie de caractérisation des circuits sécurisés basée sur une rétro-conception matérielle partielle : d'une part afin d'améliorer l'injection de fautes laser, d'autre part afin de détecter la présence de Chevaux de Troie Matériels (CTMs). Notre approche est dite partielle car elle est basée sur une seule couche matérielle du composant et car elle ne vise pas à recréer une description schématique ou fonctionnelle de l'ensemble du circuit.

Une méthodologie invasive de rétro-conception partielle bas coût, rapide et efficace est proposée. Elle permet d'obtenir une image globale du circuit où seule l'implémentation des caissons des transistors est visible. La mise en œuvre de cette méthodologie est appliquée sur différents circuits sécurisés.

L'image obtenue selon la méthodologie déclinée précédemment est traitée afin de localiser spatialement les portes sensibles, voire critiques en matière de sécurité. Une fois ces portes sensibles identifiées, nous caractérisons l'effet du laser sur différentes parties de ces cellules de bases et nous montrons qu'il est possible de contrôler à l'aide d'injections de fautes laser la valeur contenue dans ces portes. Cette technique est inédite car elle valide le modèle de fautes sur une porte complexe en technologie 90 nm.

Pour finir une méthode de détection de CTMs est proposée avec le traitement de l'image issue de la rétro-conception partielle. Nous mettons en évidence l'ajout de portes non répertoriées avec l'application sur un couple de circuits. La méthode permet donc de détecter, à moindre coût, de manière rapide et efficace la présence de CTMs.