Évaluation de méthodes faible consommation contre les attaques matérielles

Sébastien Ordas

Collège Doctoral du Languedoc-Roussillon

THÈSE

Pour obtenir le grade de

Docteur

Délivré par l'**Université de Montpellier**

Préparée au sein de l'école doctorale **Information Structures Systèmes (I2S)**
Et de l'unité de recherche **LIRMM, UMR 5506**

Spécialité: **Microélectronique**

Présentée par **Sébastien Ordas**

Évaluation de méthodes faible consommation contre les attaques matérielles

Soutenue le 30 Novembre 2015 devant le jury composé de :

M. Jean Luc Danger	Professeur	Télécom ParisTech	Rapporteur
M. Régis Leveugle	Professeur	Université de Grenoble	Rapporteur
M. Mathieu Lisart	Expert sécurité	STMicroelectronics	Examinateur
M. Philippe Loubet-Moundi	Expert sécurité	GEMALTO	Examinateur
Mme. Edith Kussener	Maitre de conférence	ISEN, IM2NP	Invité
M. Pierre-Yvan Liardet	Expert sécurité	STMicroelectronics	Invité
M. Philippe Maurine	Maitre de conférence	Univ. Montpellier	Directeur
M. Bruno Rouzeyre	Professeur	Univ. Montpellier	Examinateur
M. Yannick Teglia	Expert sécurité	STMicroelectronics	Examinateur
M. Lionel Torres	Professeur	Univ. Montpellier	Examinateur

Université Montpellier

Résumé

Évaluation de méthodes faible consommation contre les attaques matérielles

by Sébastien Ordas

La consommation des circuits intégrés n'a cessé d'augmenter cette dernière décennie. Avec l'augmentation du prix de l'énergie et la démocratisation des systèmes embarqués, des méthodes permettant de gérer le compromis consommation performance, comme la gestion dynamique de la fréquence et de la tension d'alimentation ou encore du potentiel de substrat, ont été élaborées. Ces méthodes, qui sont de plus en plus couramment mises en œuvre dans les systèmes intégrés, permettent de diminuer la consommation de ceux-ci, et de mieux gérer le compromis consommation performance.
Certains de ces circuits, embarquant ces méthodes peuvent avoir à effectuer des opérations traitant des informations confidentielles. Il est donc nécessaire de s'interroger sur l'éventuel impact de ces méthodes sur la sécurité des systèmes intégrés. Dans ce contexte, les travaux de thèse reportés dans le présent document, ont eu pour objectif d'analyser la compatibilité de ces méthodes de gestion des performances avec la conception de circuits robustes aux attaques matérielles.
Plus particulièrement, l'objectif a été de déterminer si ces techniques de conception faible consommation, constituent des obstacles réels ou bien facilitent les attaques matérielles par observation et perturbation exploitant le canal de fuite électromagnétique. Dans un premier temps, une étude sur l'efficacité des attaques par observation en présence de gestion aléatoire de la tension, de la fréquence et de la polarisation de substrat a été conduite. Dans un deuxième temps, l'impact de la gestion dynamique des tensions d'alimentation et de substrat sur la capacité à injecter des fautes par médium électromagnétique a été étudié. Ce document présente l'ensemble des résultats de ces analyses.

Mots-clés : Attaques Matérielles, Attaques par Canaux Auxiliaires, Attaques par fautes, Canal électromagnétique, DVFS, Body-Biasing.

Abstract

Attaque matériel sur SoC

by Sébastien Ordas

The consumption of integrated circuits has been increasing over the last decade. With the increase of energy prices and the democratization of embedded systems, methods to manage the power/performance trade off, such as the dynamic management of the frequency, of the supply voltage and of the substrate bias, were developed. These methods, which are becoming more commonly implemented in integrated systems, allow reducing the consumption of those latter, and to better manage the tradeoff between consumption and performance.

Some of these circuits, embedding these methods, may have to perform some operations with confidential information. It is therefore necessary to consider the possible impact of these methods on the safety of the integrated systems. Within this context, the work reported in this thesis aimed at analyzing the compatibility of these methods with the design of circuits robust against physical attacks.

Specifically, the objective was to determine whether these low-power techniques constitute real obstacles or facilitate the attacks by observation or perturbation exploiting the electromagnetic channel. Initially, a study on the effectiveness of attacks by observation in the presence of random management of voltage, frequency and substrate bias was done. Secondly, the impact of the dynamic management of supply voltages and substrate polarization on the ability to inject faults by electromagnetic medium was studied. This document presents the overall results of these analyzes.

Keyword : Hardware Attacks, Side Channel Attacks, Faults Attacks, Electromagnetic canal, DVFS, Body-biasing.

Remerciements

Dans un premier temps, je tiens à remercier l'ensemble du laboratoire LIRMM où j'ai pu réaliser ma thèse dans d'excellentes conditions de travail. Je souhaite remercier plus particulièrement M. Philippe Maurine, mon directeur de thèse, pour sa disponibilité, ses conseils et les nombreuses corrections effectuées dans ce manuscrit.

Je suis également très reconnaissant envers Régis Leveugle et Jean-Luc Danger pour l'intérêt qu'ils ont bien voulu accorder à cette thèse en acceptant d'évaluer ce travail. J'adresse aussi mes remerciements à Mathieu Lisart, Philippe Loubet-Moundi, Bruno Rouzeyre, Lionel Torres, Yannick Teglia, Edith Kussener et Pierre-Yvan Liardet, pour avoir accepté de participer à ce jury.

Dans un second temps, je souhaiterai remercier Yannick Teglia, Michel Agoyan et Nicolas Borrel pour leur aide et leur support sur les circuits de STMicroelectronics. Au sein du LIRMM je souhaiterai remercier particulièrement Alberto Bosio et Arnaud Virazel pour m'avoir permis d'effectuer des modules d'enseignement, Laurent Deknyff et Ludovique Guillaume-Sage pour avoir résolu de nombreux soucis technique.

En second lieu, j'aurai une pensée amicale envers toutes les personnes que j'ai pu côtoyer pendant ces années dont les échanges autant sur le plan humain que scientifique ont rendu cette période de ma vie passionnante et enrichissante. Je pense notamment à Sébastien Tiran, Mathieu Carbone, Florent Bruguier, Feng Lu, Patcharee Kongpark, Guilherme Perin, Marina Aparicio, Anastasiia Butko, Raphael Brum, Joao Azevedo.

Un grand merci aussi à tous les proches et amis qui n'étaient pas présents au quotidien mais qui ont partagé ces années à mes côtés. Je pense en particulier à Emeric, Lulu, Marie, Esther, ...

Je voudrais remercier spécialement mes parents qui ont toujours cru en moi et qui ont su m'encourager et me soutenir dans les moments les plus difficiles qui jalonnent une thèse.

Table des matières

Résumé i

Abstract ii

Remerciements iii

Table des matieres iii

Liste des Figures vii

Liste des Tableaux xi

1 Introduction 1

2 Etat de l'art 4
2.1 Généralités . . . 4
2.2 La cryptographie symétrique . . . 6
2.2.1 Le chiffrement par bloc . . . 6
2.2.1.1 Data Encryption Standard . . . 6
2.2.1.2 Advanced Encryption Standard . . . 7
2.2.2 Le chiffrement par flot . . . 9
2.3 La cryptographie asymétrique . . . 10
2.4 Les systèmes sécurisés . . . 12
2.4.1 La carte à puce . . . 12
2.4.1.1 Historique . . . 12
2.4.1.2 Description . . . 13
2.4.2 Les systèmes sécurisés de demain . . . 14
2.5 Classification des attaques matérielles . . . 15
2.5.1 Les attaques par canaux auxiliaires . . . 16
2.5.2 Fuites physiques . . . 16
2.5.3 Attaque SPA . . . 18
2.5.4 Les attaques verticales . . . 20
2.5.4.1 Attaque par différence des moyennes . . . 22
2.5.4.2 Attaque par analyse de la corrélation . . . 23
2.5.4.3 Contre-mesures aux attaques par observation . . . 25
2.5.5 Injection de fautes . . . 26

2.5.5.1 Description . . . 26
2.5.5.2 Attaques par perturbation globale . . . 27
2.5.5.3 Attaque par perturbation localisée . . . 28
2.5.5.4 Attaque optique . . . 28
2.5.5.5 Electro-Magnétisme . . . 29
2.5.6 Modèles de fautes . . . 30
2.5.6.1 Modèles de fautes logiques . . . 30
2.5.6.2 Modèles de fautes algorithmique . . . 30
2.5.7 Exploitation des fautes . . . 31
2.5.7.1 Analyse différentielle . . . 31
2.5.7.2 Safe error . . . 31
2.5.7.3 Modification dans l'exécution de l'algorithme . . . 31
2.5.7.4 Rétro-ingéniérie . . . 32
2.5.8 Contremesures aux attaques par injection . . . 32
2.6 Synthèse des méthodes d'attaque . . . 33
2.6.1 Synthèse des sources physiques des SCA . . . 33
2.6.2 Synthèse des sources physiques l'injection de faute . . . 34
2.6.3 Récapitulatif sur les moyens d'attaques . . . 35
2.7 Positionnement des travaux de thèse . . . 35

3 Gestion dynamique aléatoire de V_{dd}, F, V_{bb} et analyse SCA 38
3.1 Introduction . . . 38
3.2 Body-biasing . . . 39
3.3 Dynamic Voltage and Frequency Scaling . . . 41
3.4 Impact sur la sécurité . . . 41
3.4.1 Impact de la tension d'alimentation sur la CPA . . . 44
3.4.2 Impact de la fréquence sur la CPA . . . 48
3.4.3 Impact de la tension de polarisation de substrat sur la CPA . . . 49
3.4.4 RDVFS . . . 50
3.4.5 Explication théorique . . . 54
3.5 Attaque CPA sur la contre-mesure RDVFS . . . 57
3.6 Optimisation de la CPA . . . 60
3.6.1 Resynchronisation des traces EM . . . 61
3.6.2 Regroupement . . . 63
3.6.3 Contre-mesure RDVFS contre les attaques CPA améliorées . . . 63
3.7 Conclusion . . . 65

4 Les impulsions EM comme moyen d'injection de fautes 67
4.1 Généralités . . . 67
4.2 Etat de l'art sur l'injection EM . . . 68
4.3 Mise en place d'un banc d'injection EMP . . . 69
4.3.1 Plateforme d'injection EMP . . . 70
4.3.2 Sondes d'injection EMP . . . 71
4.4 Sources de défaillance des circuits synchrones . . . 72
4.4.1 Structure d'un circuit synchrone . . . 72
4.4.2 Contraintes de fonctionnement des portes logiques . . . 73
4.4.3 Contraintes de fonctionnement au niveau circuit . . . 75

4.4.4 Tests de discrimination . . . 76
4.5 Production de bitset et bitreset sur DFF au repos . . . 77
4.5.1 Description de la procédure et du circuit de test . . . 78
4.5.2 Occurence de fautes de type bitset et bitreset . . . 79
4.5.3 Effet de la polarité de l'injection EMP . . . 81
4.6 Injection EMP sur un circuit en fonctionnement . . . 82
4.6.1 Circuit de test en fonctionnement . . . 83
4.6.2 Objectifs du test . . . 83
4.6.3 Résultats expérimentaux . . . 84
4.6.3.1 Cartographie et localité des fautes lors d'une injection EMP . . . 84
4.6.3.2 Modèle de faute de l'injection EMP ? . . . 86
4.7 Modèle 'faute d'échantillonnage' . . . 90
4.8 Conclusion . . . 93

5 Etude des effets de la gestion dynamique aléatoire de V_{dd}, F, V_{bb} sur l'injection EMP et BBI 94
5.1 Généralités . . . 94
5.2 Comparaison entre l'injection EMP et BBI . . . 96
5.2.1 Mise en place des expérimentations . . . 96
5.2.2 Analyse des résultats obtenus . . . 97
5.3 Effet de la RDVFS sur les méthodes d'injection . . . 100
5.3.1 Effet d'une variation de tension sur l'efficacité de l'injection EMP . 101
5.3.2 Effet d'une variation de tension sur l'efficacité de l'injection BBI . 102
5.3.3 Effet d'une variation de fréquence sur l'injection EMP . . . 106
5.3.4 Effet d'une variation de fréquence sur la BBI . . . 107
5.3.5 Effet d'une variation de la polarisation de substrat sur les capacités d'injection EMP . . . 110
5.3.6 Effet d'une variation de polarisation de substrat sur la BBI . . . 113
5.4 Conclusion . . . 114

6 Conclusion 117

A Modèle de fuite dans le domaine fréquentiel 119
A.1 Introduction . . . 119
A.2 Contribution . . . 120
A.2.1 Validation du critère LNR . . . 120
A.2.2 Optimisation du matériel d'attaque . . . 124
A.2.3 Comparatif entre les différents matériels . . . 124
A.3 Conclusion . . . 126

Bibliographie 127

Liste des publications 127

Table des figures

2.1 Structure du DES . . . 8
2.2 Structure de l'AES . . . 9
2.3 Première carte à microprocessseur . . . 13
2.4 Connecteur d'une carte à puce défini dans la norme ISO.7816 . . . 13
2.5 Banc d'acquisition de traces EM . . . 18
2.6 Traces EM collectées au dessus d'un circuit effectuant (a) un chiffrement DES et (b) un chiffrement AES . . . 19
2.7 SPA sur la consommation d'un RSA non protégé . . . 20
2.8 Principe d'une attaque verticale . . . 22
2.9 (a) Trace EM d'un chiffrement AES, (b) Evaluation de Δ_{K_s} pour une valeur de sous-clé dans le temps . . . 23
2.10 (a)Trace EM d'un AES, (b)Attaque CPA réalisé sur un AES . . . 24

3.1 Transistor MOSfet à canal N . . . 40
3.2 (a) et (c) rayonnement EM relatif à un chiffrement AES pour $F = 30MHz$ et $F = 42MHz$, (b) et (d) rayonnement EM relatif à un chiffrement AES pour $V_{dd} = 1V$ et $V_{dd} = 1.5V$ . . . 42
3.3 (a) Chiffrement AES avec (V,F) = (1.2V, 62MHz) fixe, (b) Chiffrement AES avec 11 couples (V,F) différents . . . 44
3.4 (a) Traces EM d'un AES pendant la fuite d'information pour trois valeurs de V_{dd} différentes, (b) valeurs de corrélation considérées par la CPA pour trois valeurs de V_{dd} différentes . . . 45
3.5 Coefficient $\alpha_{Y/X}$ en fonction de la valeur de V_{dd} . . . 46
3.6 (a) Traces EM d'un AES pendant la fuite d'information pour trois valeurs différentes de V_{dd} , (b) valeurs de corrélation considérées par la CPA pour trois valeurs de V_{dd} . . . 47
3.7 (a) Traces EM d'un AES pendant la fuite d'information avec deux valeurs différentes de F, (b) valeur de corrélation pour des attaques CPA avec deux valeurs différentes de F . . . 49
3.8 (a)Traces EM d'un AES pendant la fuite d'information pour trois valeurs différentes de V_{bb}, (b) corrélations considérées par la CPA pour trois valeurs différentes de V_{bb} . . . 51
3.9 (a)Évolution de la corrélation associée à chaque hypothèse de sous clé pour les six couples (V, F) pris séparément, (b) évolution de la corrélation associée à chaque hypothèse de sous clé lorsque la RDVFS est activée avec les six couples (V, F) . . . 53
3.10 Oscillateur en anneau fournissant le signal d'horloge à l'AES. . . . 57
3.11 évolution du rapport de robustesse $\frac{S_n}{S_1}$ en fonction du nombre n de couples (V,F) utilisés sur FPGA . . . 59

3.12 évolution du rapport de robustesse $\frac{S_n}{S_1}$ en fonction du nombre de triplets n utilisés sur un micro-contrôleur 32 bits 60
3.13 a) traces EM d'un chiffrement AES a deux fréquences différentes, b) traces EM d'un chiffrement AES resynchronisées 62
3.14 Evolutions du rapport de robustesse $\frac{S_n}{S_1}$ en fonction du nombre n de couples utilisés avec une CPA 'standard', une CPA avec resynchronisation et une CPA avec regroupement 65

4.1 Plateforme d'injection EMP du LIRMM 70
4.2 (a) Sondes d'injection plate, (b) Sonde d'injection appointée, (c) Sonde d'injection oméga 71
4.3 Schéma d'un circuit synchrone 73
4.4 Symbole d'une DFF et définition du temps de setup (t_{setup}) et du temps de hold (t_{hold}) 74
4.5 FIFO de 640x8 DFF implémentées sur FPGA pour démontrer l'occurrence des fautes de type bitset et bitreset 78
4.6 Probabilité de produire (a) une faute de n'importe quel type, (b) une faute de type bitset, (c) une faute de type 'muet'. (d) orientation de la sonde d'injection oméga 80
4.7 Probabilité de produire (a) une faute de type bitset avec un V_{pulse}=+140V et (b) une faute de type bitreset avec un V_{pulse}=-140V 81
4.8 Placement des différents blocs du circuit de test 83
4.9 Probabilité de générer (a) un texte chiffré fauté avec la sonde d'injection oméga, (b) un texte chiffré fauté avec la sonde d'injection plate et (c) que le circuit soit muet avec la sonde d'injection plate 85
4.10 Probabilité de générer une faute pour chaque octet de l'AES en fonction de la position de la sonde d'injection (oméga) 87
4.11 Nombre d'octets fautés à une position (X,Y) fixe en fonction du moment d'injection (t_{pulse}) pour 100 injections avec $F_{AES} = 100MHz$ et une sonde d'injection oméga 88
4.12 Probabilité de générer une faute sur un AES hardware implémenté sur un FPGA spartan3-1000 en fonction du moment de d'injection (t_{pulse}) pour 3 valeurs de fréquences différentes et avec une sonde d'injection oméga . . 89
4.13 Probabilité de générer une faute sur un AES matériel implémenté sur un micro-contrôleur 32bit en fonction du moment de d'injection (t_{pulse}) pour 3 valeurs de V_{pulse} et avec une sonde d'injection oméga 90
4.14 Image d'un champ EM émis par une sonde d'injection lors d'une injection EMP 91
4.15 Image d'un champ EM émis par une sonde d'injection lors d'une injection EMP 92
4.16 Modèle 'faute d'échantillonnage' 92

5.1 Placement des différents blocs du micro-contrôleur 95
5.2 Sondes d'injection utilisées (a) sonde BBI et (b) sonde EMP 97
5.3 Probabilité d'induire : (a) et (c) des fautes de nature quelconque avec l'injection EMP (a) et BBI (c), (b) et (d) des fautes de chiffrement avec l'injection EMP (b) et BBI (d) 98
5.4 Probabilité de générer une faute en fonction de l'instant d'injection t_{pulse} de l'EMP et du pic de tension (BBI) 99

5.5 Image de l'impulsion perturbant le circuit pour l'injection EMP et BBI . 100
5.6 Cartographie de la probabilité d'induire (a,b,c) n'importe quel type de fautes avec une injection EMP lorsque le circuit est alimenté sous 1.1V(a), 1.2V(b) et 1.3V(c), (d,e,f) des fautes de chiffrement dans l'AES matériel alimenté sous 1.1V(d), 1.2V(e) et 1.3V(f) 102
5.7 Probabilité de générer une faute sur un AES hardware implémenté sur un micro-contrôleur 32bit en fonction du moment de d'injection (t_{pulse}) pour 3 valeurs de tension d'alimentation et avec une sonde d'injection plate 103
5.8 Cartographies (a,b,c) de la probabilité d'induire un comportement erroné quelconque lorsque le circuit est alimenté à 1.1V(a), 1.2V(b) et 1.3V(c). Cartographies (d,e,f) de la probabilité de générer un chiffré fauté lorsque le circuit est alimenté à 1.1V(d), 1.2V(e) et 1.3V(f) 104
5.9 Evolution avec t_{pulse} de la probabilité d'induire une faute de chiffrement dans l'AES matériel du microcontrôleur et ce pour trois valeurs de tension d'alimentation 105
5.10 Cartographies de la probabilité, (a,b,c) d'induire un comportement erroné quelconque avec une impulsion EM et (d,e,f) une faute de chiffrement . . 106
5.11 Probabilité de générer une faute sur un AES matériel implémenté sur un micro-contrôleur 32bit en fonction du moment d'injection (t_{pulse}) pour 3 valeurs de fréquence de fonctionnement 108
5.12 Cartographies de la probabilité (a,b,c) d'induire n'importe quel comportement erronée avec l'injection BBI lorsque le circuit fonctionne à 50MHz(a), 80MHz(b) et 100MHz(c) ; (d,e,f) d'induire des fautes de chiffrement avec l'injection BBI lorsque le circuit fonctionne à 50MHz(d), 80MHz(e) et 100MHz(f) 109
5.13 Probabilité de générer une faute sur un AES hardware implémenté sur un micro-contrôleur 32bit en fonction du moment d'injection (t_{pulse}) pour 3 valeurs de fréquence de fonctionnement et avec une sonde d'injection plate 110
5.14 Cartographies (a,b,c) de la probabilité d'induire un comportement erroné quelconque lorsque le circuit a une polarisation de substrat de 0V(a), 200mV(b) et 400mV(c). Cartographies (d,e,f) de la probabilité de générer un chiffré fauté lorsque le circuit a une polarisation de substrat de 0V(d), 200mV(e) et 400mV(f) 111
5.15 Probabilité de générer une faute sur un AES hardware implémenté sur un micro-contrôleur 32bit en fonction du moment d'injection (t_{pulse}) pour 3 valeurs de tension de polarisation du substrat et avec une sonde d'injection plate 112
5.16 Zones de susceptibilité du micro-contrôleur pour n'importe quel type d'erreur avec des tension de polarisation du substrat de (a) 0mV, (b) 200mV et (c) 400mV. Zones de susceptibilité du micro-contrôleur pour une erreur sur le texte chiffré avec des tension d'alimentation de (d) 0mV, (e) 200mV et (f) 400mV 114
5.17 Probabilité de générer une faute sur un AES hardware implémenté sur un micro-contrôleur 32bit en fonction du moment d'injection (t_{pulse}) pour 2 valeurs de tension de polarisation du substrat 115

A.1 Evolution du $LNR_{EM}(f)$ et du $SNR(f)$ 122

A.2 Ancien et nouveau matériels du LIRMM. a) Amplificateur [100MHz,1GHz], b) sonde d'acquisition [30MHz,1GHz], c) amplificateur [10KHz,200MHz] et d) sonde d'analyse avec un cœur de ferrite 125

Liste des tableaux

2.1 Récapitulatifs sur les moyens d'attaques 35

A.1 Nombre de traces EM traitées pour atteindre un taux de réussite de 20% ou 80% pour des attaques CPA et DPA 121
A.2 Nombre de traces EM traitées pour atteindre un taux de réussite de 20% ou 80% pour des attaques CPA et DPA 122
A.3 Résultat d'attaque CPA sur les traces EM du micro-contrôleur pour différente bande de fréquences 123
A.4 Nombre de traces d'un AES nécessaire à la CPA pour obtenir un taux de réussite de 80% 126

Chapitre 1

Introduction

Avec le développement de la société de l'information et de la monnaie virtuelle, de nouveaux problèmes liés à la sécurité des circuits intégrés sont apparus. Pour cela des circuits intégrés à usage sécuritaire sont devenus indispensables pour assurer les exigences requises par les utilisateurs telles que l'authentification, la confidentialité ou l'intégrité des données sensibles. L'intégration des dispositifs cryptographiques dans les différents composants électroniques est de nos jours largement répandue (communication, services bancaires, service gouvernementaux, *PayTV*, ...).

Les applications embarquées, nécessitant un besoin important de sécurité, utilisent des protocoles et algorithmes cryptographique intégrés, qui sont réputés robustes face aux attaques informatiques. Ces algorithmes et protocoles sont implémentés sous forme logicielle ou matérielle au sein d'un circuit intégré. Malheureusement pour les concepteurs des circuits intégrés, tout calcul exécuté par un système matériel (micro-contrôleur, crypto-processeur,...) laisse transparaitre des traces de consommation de son activité (consommation électrique, émission électromagnétique,...). Ces traces de consommation peuvent alors être mises à profit par un attaquant pour extraire des informations secrètes supposées inaccessibles. Ces failles matérielles sont exploitées par des attaques communément appelées attaques par canaux auxiliaires. Ces attaques peuvent être considérées comme les plus dangereuses, dans la mesure où ce type d'attaque peut être réalisé sans être détecté.

L'attaquant peut également effectuer des attaques par injection de fautes. Elles consistent à perturber une opération cryptographique pendant que celle-ci manipule des données.

Une analyse différentielle entre la valeur fautée et correcte permet alors de remonter à l'intégralité de la clé de chiffrement. Afin d'injecter une faute, plusieurs méthodes existent comme celle consistant à sous-alimenter le circuit ou à augmenter la fréquence de son signal d'horloge afin de créer des violations sur les contraintes de temps d'un circuit. Ces méthodes restent toutefois globales car elles affectent la totalité du circuit. Ainsi des méthodes plus complexes, notamment l'injection laser, ont été mises au point afin de ne cibler qu'une partie spécifique du circuit. Malgré cela, ces attaques nécessitent une altération du boitier. Il est nécessaire d'avoir un accès au circuit et donc de l'extraire de son boitier. De plus une étape de préparation du circuit est aussi nécessaire afin de l'amincir et de le revêtir d'une couche anti-réfléchissante (très peu effectuée en pratique), afin que le faisceau laser puisse pénétrer dans les parties actives du silicium. Les ondes électromagnétiques disposent d'une faculté de pénétration dans les matériaux qui permet, en théorie, de s'affranchir de toute l'étape de préparation du circuit.

De nos jours, lors de la conception d'un circuit, le seul coût en surface n'est plus le seul critère. Avec le développement des appareils mobiles et l'augmentation du prix de l'énergie, il est nécessaire de diminuer la consommation des circuits intégrés. Pour cela, plusieurs méthodes existent comme la répartition des tâches entre les processeurs, le *body biasing* ou la gestion dynamique des performances. Cependant, l'utilisation de ces méthodes de diminution de la consommation peuvent avoir un effet sur la sécurité des circuits. Cette thèse, réalisée dans le cadre du projet FSN MAGE, porte sur l'étude des effets sur la sécurité de ces techniques de réduction de consommation. Dans ce contexte, des études sur l'utilisation de ces techniques ont été réalisées lors d'attaques par canaux auxiliaires et par injection de fautes.

Durant cette thèse, les premières investigations ont été réalisées sur des circuits FPGA. Cependant, il est rapidement apparu que ce type de circuit ne permettait pas d'effectuer toutes les investigations souhaitées (changement de tension de polarisation du substrat, utilisation de PLL, ...). Il a alors été décidé d'utiliser un micro-contrôleur qui répondait à ces différentes contraintes et ainsi de pouvoir effectuer toutes les investigations souhaitées. Toutefois, de nouvelles contraintes, liées à la confidentialité des données du concepteur du micro-contrôleur, sont apparues. Il nous a alors été impossible d'expliquer certains phénomènes qui ont pu être observés durant nos expérimentations.

Ce mémoire de thèse résume donc les différents travaux réalisés pour évaluer sur l'impact sécuritaire des méthodes de gestion dynamique des performances et *body biasing*. Cette thèse a été réalisée au sein du Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM).

Le chapitre 2 présente le contexte actuel dans lequel évolue les système électronique àa but sécuritaire, dont le plus connu est sans doute la carte à puce. Les différentes menaces et les moyens mis a disposition par les attaquants y sont détaillés.

Le chapitre 3 reporte l'étude des effets des méthodes de faibles consommations, connues sous le terme de *Dynamic Voltage and Frequency Scalling* (DVFS), sur les attaques par canaux auxiliaires. Ces études ont principalement été réalisées avec l'attaque par canal auxiliaire la plus répandue, l'attaque *Correlation Power Analysis* (CPA)

Le chapitre 4 présente le développement d'une plateforme d'injection électromagnétique pulsée (EMP). Une étude des fautes générées par l'injection EMP a ainsi permis de définir un modèle sur lequel repose les fautes induites par l'injection EMP.

Enfin, le chapitre 5 montre les effets de la DVFS sur l'injection EMP et sur l'injection de pic de tension dans le substrat (*Body Biasing Injection* : BBI). Une comparaison entre ces deux méthodes d'injection a ainsi pu être réalisée.

Chapitre 2

Etat de l'art

Ce premier chapitre présente les bases des algorithmes cryptographiques utilisés dans le monde de la sécurité. Une présentation des différents types d'attaques couramment utilisées par les laboratoires d'évaluations est donnée.

2.1 Généralités

Afin de sécuriser les données, des systèmes cryptographiques ou crypto-systèmes ont été développés. Ceux-ci permettent de chiffrer/déchiffrer des données afin que ces dernières ne puissent être mises à profit par des utilisateurs non habilités.
La sécurité informatique emploie aujourd'hui des algorithmes et des protocoles cryptographiques afin d'assurer la confidentialité, l'authenticité et l'intégrité des données. Elle se base sur les principes de Kerckhoff [1] qui supposent que toutes les méthodes de chiffrement sont connues de l'ennemi, et affirment que la sécurité d'un système cryptographique doit reposer uniquement sur la confidentialité des clés de chiffrement. Ce choix permet ainsi d'apporter à l'utilisateur la confiance nécessaire pour effectuer un échange de données crucial sans aucun risque. De nos jours, le chiffrement des données est devenu indispensable dans de nombreux domaines comme :

- l'identification (carte d'identité, carte d'accès, carte SIM (Subscriber Identity Module)),
- les services bancaires (carte bancaire, carte moneo),
- les services d'abonnement (carte de transport, carte téléphonique, PAY TV).

Les cartes à puce sont l'exemple le plus connu de systèmes cryptographiques. Elles sont présentes dans bien d'autres systèmes tels que les périphériques de stockage ou même les smartphones. La demande en cartes à puce est en perpétuelle augmentation, le nombre de cartes à puce vendues en 2012 est de 7.095 milliards. Celui de 2013 est de 7.665 milliards, ce qui représente une augmentation de 8%.
La télécommunication est le plus grand marché dans le domaine des cartes à puce. Il représente 70% de la production mondiale (carte SIM des téléphones portables). Le second marché des cartes à puce est le réseau bancaire qui représente près de 20% (cartes bancaires). Une forte croissance des cartes à puce est à prévoir avec l'apparition des technologies de communication sans contact. L'une de ces technologies, le NFC (Near Field Communication), permet l'échange d'information à très courte distance (quelques centimètres). Cette proximité nécessaire à son emploi suppose alors que son utilisation reste une démarche volontaire de l'utilisateur, cependant cela reste une démarche hasardeuse pour les applications dédiées à la sécurité.

Innover dans le domaine des systèmes cryptographiques est une obligation. Cette obligation est due aux progrès technologiques qui profitent également aux personnes mal intentionnées qui peuvent utiliser des méthodes de plus en plus perfectionnées pour récupérer les secrets d'un utilisateur. Ces méthodes que l'on nomme attaque, ont des degrés de complexité et des coûts très variables. L'attaque par force brute est une attaque théorique simple à mettre en place. Elle a pour but de rechercher de manière exhaustive la clé de chiffrement dans un temps dit "raisonnable". Elle est liée à la puissance de calcul des ordinateurs et à l'algorithme de chiffrement utilisé. Durant une courte période (1976 à 1999), le DES a été considéré comme un algorithme résistant aux attaques par force brute. Cependant, en 1999 une attaque par force brute a été réalisée sur un DES, et il n'a pas fallu plus de vingt-quatre heures pour retrouver la clé de chiffrement en effectuant une recherche exhaustive de la clé.
De nos jours, la plupart des systèmes de cryptographie peuvent être classés en deux catégories : les crypto-systèmes basés sur des clés symétriques et des systèmes basés sur des clés asymétriques.

2.2 La cryptographie symétrique

Les algorithmes dit "symétriques", sont des algorithmes qui nécessitent une seule clé de chiffrement/déchiffrement qui doit absolument restée secrète. En effet, cette clé est utilisée pour crypter le message original afin de le rendre illisible par un utilisateur non habilité. Mais également, pour déchiffrer ce message crypté. Ceci explique pourquoi la clé de chiffrement doit restée secrète lors de sa distribution aux divers protagonistes. Compte tenu de ce schéma de chiffrement/déchiffrement, on peut définir un algorithme de chiffrement symétrique de la façon suivante :

$$C = enc_k(P) \tag{2.1}$$

$$P = dec_k(C) \tag{2.2}$$

Avec *enc* la fonction de chiffrement, *dec* la fonction de déchiffrement, P le message, k la clé de chiffrement et C le message chiffré. L'algorithme étant symétrique, la propriété suivante est également vérifiée :

$$dec_k(enc_k(M)) = M \tag{2.3}$$

2.2.1 Le chiffrement par bloc

Le chiffrement par bloc est une des deux grandes catégories d'algorithmes de chiffrement symétrique. Comme son nom l'indique, son principe de fonctionnement revient à découper les données en blocs de taille fixe. La taille des blocs de données à chiffrer est usuellement comprise entre 32 et 512 bits. Les blocs sont alors chiffrés les uns après les autres de manière indépendante.

2.2.1.1 Data Encryption Standard

L'algorithme Data Encryption Standard, plus communément appelé DES, a été développé par les ingénieurs d'IBM. Il se fonde sur le principe du schéma de Feistel [2]. Un schéma

de Feistel repose sur des opérations simples : des permutations, des substitutions, des échanges de blocs de données et une fonction prenant en entrée une clé intermédiaire. Cette structure offre plusieurs avantages. Le premier d'entre eux est que le chiffrement et le déchiffrement ont une architecture similaire voire identique dans certains cas. Un autre avantage est que leur implémentation matérielle est facile et peu coûteuse. Un DES coûte typiquement entre 3000 et 5000 portes équivalentes.

Le DES a été sélectionné par le NIST comme standard en 1976. Celui-ci utilise une clé de chiffrement de 56-bits (représentée sous une forme de 64-bits avec un bit de parité pour chaque octet) et fonctionne avec des blocs de données. La Fig.2.1 représente la structure du DES. Elle consiste en 16 cycles identiques nommés rondes (Rounds en anglais), d'une permutation initiale IP (Initial Permutation) et d'une permutation finale FP (Final Permutation). Ces deux permutations ont pour propriété de s'annuler l'une l'autre $FP = IP^{-1}$ et n'apportent rien à la robustesse du DES.

Lors de chaque ronde, le message clair est divisé en deux blocs de 32-bits : L_i et R_i. Le bloc R_i est combiné avec la clé de ronde $Subkey_i$ dans la fonction F. Le résultat obtenu est combiné avec le bloc L_I puis les deux blocs sont intervertis. Cette structure permet de simplifier l'implémentation matérielle dans la mesure où l'algorithme est itératif et qu'il n'est pas nécessaire de séparer la partie chiffrement de la partie déchiffrement. En effet, pour déchiffrer un message il suffira d'appliquer les clés de rondes dans l'ordre inverse de celui utilisé lors du chiffrement.

2.2.1.2 Advanced Encryption Standard

A cause de l'augmentation de la puissance de calcul des ordinateurs, et de la petite taille de la clé du DES, le NIST a lancé un appel à candidature en 1997 pour trouver un successeur au DES. Celui-ci devait pouvoir chiffrer des blocs de 128 bits avec trois tailles de clé différentes (128, 192 et 256 bits). L'algorithme Rijndael proposé par Joan Daemen et Vincent Rijmen a été retenu en 2000 comme le successeur du DES, et il est nommé l'AES pour Advanced Encryption Standard.

Contrairement au DES, le nombre de rondes de l'AES n'est pas fixe (10, 12 ou 14 rondes) car il dépend de la taille de clé qui est choisie (128, 192 et 256 bits). L'architecture de l'AES est représentée sur la Fig. 2.2. L'AES repose sur cinq opérations différentes :

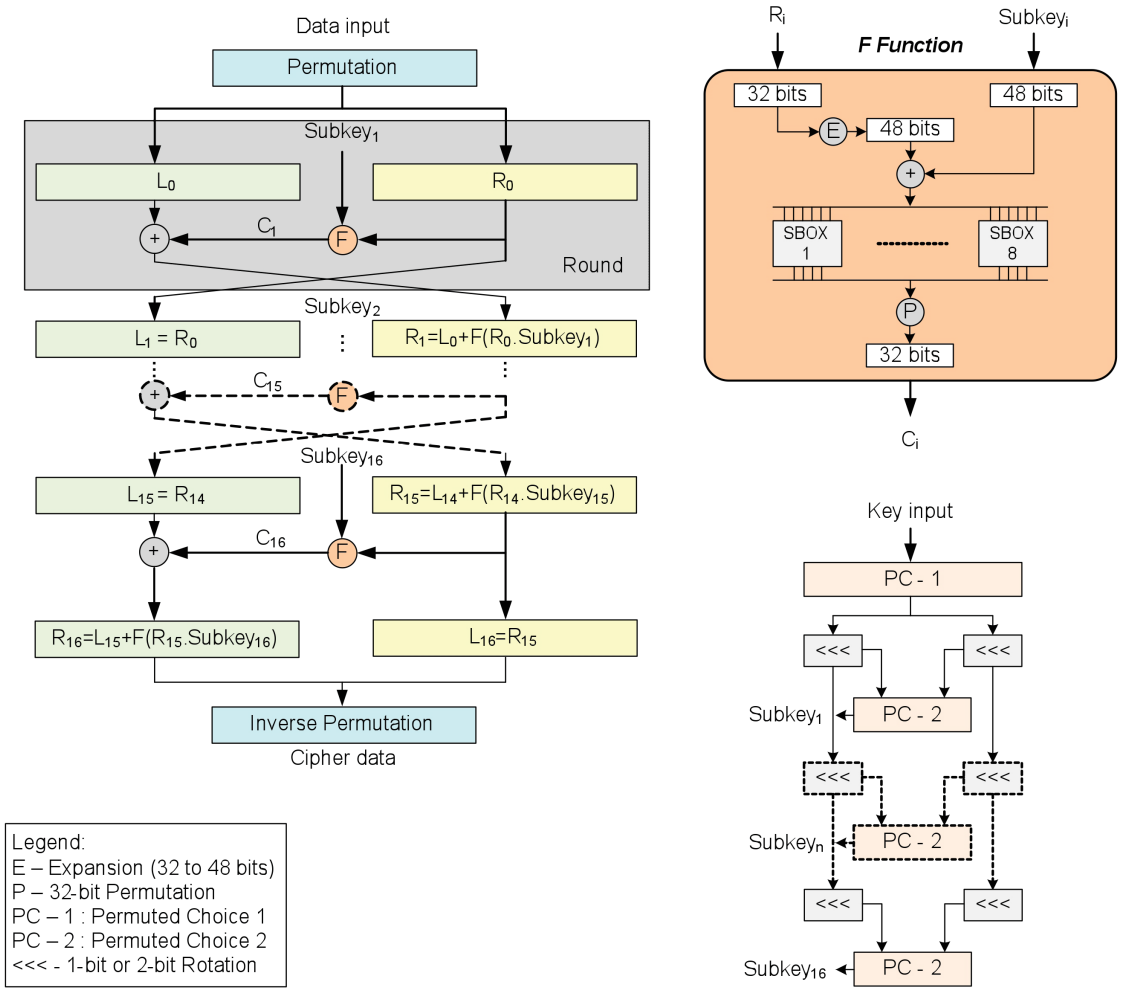

FIGURE 2.1: Structure du DES

– l'opération SubByte : opération non linéaire qui substitue chaque octet en utilisant une table de substitution nommée S-Box.
– l'opération AddRoundKey : chaque octet de l'état est combiné avec la clé de ronde correspondante.
– l'opération ShiftRows : opération cyclique de décalage sur les lignes de l'état. L'offset de décalage n'est pas le même pour toutes les lignes, il a été choisi de façon à ce que chaque colonne de l'état de sortie soit composée d'octets de chaque colonne de l'état d'entrée.
– l'opération Mixcolumns : dans cette opération, les 4 octets de chaque colonne de l'état sont combinés de façon à garantir la diffusion.
– l'opération Key Schedule : opération qui calcul les différentes clés de ronde.

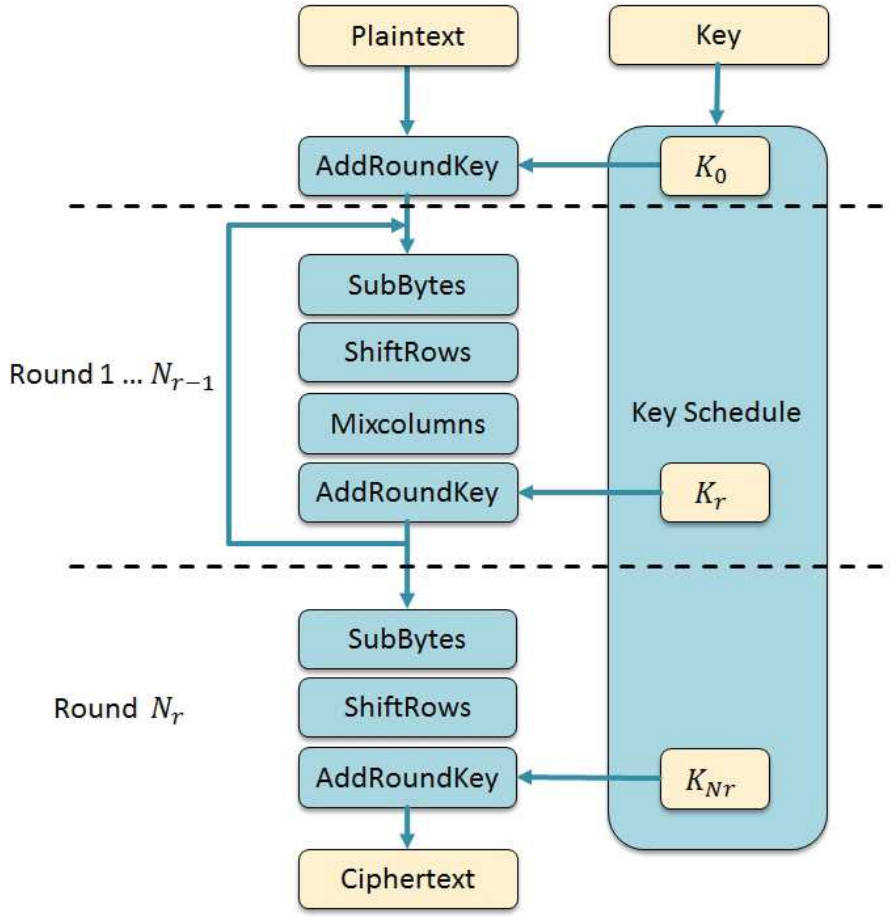

FIGURE 2.2: Structure de l'AES

2.2.2 Le chiffrement par flot

Le chiffrement par flot constitue la seconde catégorie de chiffrement symétrique. Cette méthode de chiffrement arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper en bloc. Notant P, C et σ_t le message clair, le message chiffré et l'état interne à l'instant t respectivement. Le chiffrement par flot est régi par les équations suivantes :

$$\begin{aligned} \sigma_{t+1} &= f(\sigma_t, C, k) \\ C &= P \oplus g(\sigma_t, k) \end{aligned} \tag{2.4}$$

avec f la fonction de mise à jour et g faisant référence au générateur de séquences de clé qui fournit un flux de clés pseudo-aléatoires de longueur arbitraire.

Selon la définition de f, les chiffrements par flot peuvent être classifiés en deux catégories :

– le chiffrement par flot synchrone, dans lequel le flux de clés est généré à partir de la clé secrète k ce qui signifie que l'éq. 2.4 peut être réécrite comme suit :

$$\sigma_{t+1} = f(\sigma_t, k) \tag{2.5}$$

– l'auto-synchronisation du chiffrement par flot, dans lequel la séquence de clé est générée à partir de la clé secrète k et d'un nombre N fixe de caractères de texte préalablement chiffrés. L'éq. 2.4 peut alors être définie de la manière suivante

$$\sigma_{t+1} = f(\sigma_t, C - N, ..., c_t - 1, k) \tag{2.6}$$

En supposant que le flux de clés est parfaitement aléatoire, il a alors été montré dans [3] que le message est parfaitement encrypté et indéchiffrable. Les chiffrements par flot ont des avantages sur les chiffrements par blocs comme par exemple leur débit élevé et leur simplicité d'analyse. Cependant, il est bien connu que le chiffrement par flot est bien moins sûr que le chiffrement par blocs [4]. Les normes d'aujourd'hui, recommandent d'utiliser les techniques de chiffrements par blocs, plutôt que les chiffrements par flot [4].

Le chiffrement par flot est intrinsèquement adapté aux applications en temps réel ou il ne nécessite que peu de ressources informatiques où des dispositifs de traitement limités qui répondent à des exigences de performances extrêmes (la vitesse, la consommation, la surface). La série des A5/X (A5/1, A5/2, A5/3) [5], le E0 [6] ou encore le RC4 [7] sont respectivement les méthodes de chiffrement par flux les plus répandues dans les systèmes de communication mobiles (Global System for Mobile Communication (GSM)), le Bluetooth et la protection du trafic internet sans fil (Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA) ou encore le Secure Sockets Layer (SSL)).

2.3 La cryptographie asymétrique

L'une des plus grandes faiblesses de la cryptographie à clé privée réside dans l'utilisation d'une clé de chiffrement partagée qui doit donc être distribuée à toutes les parties souhaitant communiquer. Pour dépasser les limitations dues à la gestion des clés privées, la cryptographie à clé publique a été proposée par Whitfield Diffie et Hellman Martin

dans leur article sur la nouvelle orientation dans la cryptographie [8] comme une solution à l'échange de clé. Son principe réside dans l'utilisation de deux clés différentes. La première est une clé publique notée pk, tandis que la seconde, sk, est une clé privée ou secrète. Elles sont utilisées pour garantir les différents aspects de sécurité :

– la confidentialité : pk est accessible au public de telle sorte que n'importe quel individu peut l'utiliser pour crypter un message et l'expédier au destinataire possédant la clé sk. En revanche, la clé sk est gardée secrète de sorte que seul son propriétaire peut déchiffrer les messages chiffrés avec la clé pk correspondante.

  Formellement le cryptage par l'expéditeur d'un texte clair p en un texte chiffré c en utilisant la clé pk du receveur est défini de la manière suivante :

$$C = enc_{pk}(P) \tag{2.7}$$

  Le déchiffrement du texte chiffré C en message clair P en utilisant la clé sk est alors défini comme :

$$P = dec_{sk}(C) \tag{2.8}$$

  Afin que le chiffrement à clé publique soit sécurisé, le calcul de dec_{sk} doit être impossible sans connaitre sk même si pk est connue.

– l'authenticité : l'intégrité et la non-répudiation utilisant des schémas de signatures numériques [9, 10]. La clé privée est utilisée pour signer et la clé publique est utilisée pour vérifier la validité de la signature. Un expéditeur produit une signature s d'un message m en utilisant pk qui est vérifiable par un récepteur utilisant sk. Un schéma de signature est donc composé de deux fonctions, à savoir la vérification nommée $verif$ et la signature nommée $sign$ respectivement paramétrée par une clé publique pk et une clé privée sk tel que :

$$verif_{pk}(m, s) = \begin{cases} \text{true if } \text{sign}_{sk}(m) = s \\ \text{false if } \text{sign}_{sk}(m) \neq s \end{cases} \tag{2.9}$$

Pour qu'un schéma de signature soit sécurisé, il doit être impossible de calculer sign_{sk} sans connaitre sk, même si pk est connu.

Il existe trois grandes familles d'algorithmes à clé publique. En effet, ces algorithmes sont classés en fonction de la difficulté du problème mathématique dit "difficile" sur lequel ils reposent :

– La factorisation d'entiers, dont la dureté est essentielle pour la sécurisation de l'encryptage et du schéma de signature de l'algorithme à clé publique RSA [11].
– Le logarithme discret, dont la dureté est essentielle pour la sécurisation de l'encryptage et du schéma de signature de l'algorithme à clé publique de El-Gamal [12] et de ses variantes tel que le DSA (Digital Signature Algorithm) [13].
– Les courbes elliptiques, dont la dureté est essentielle pour la sécurité de tous les schémas cryptographiques à base de courbes elliptiques [14]. Généralement, les courbes elliptiques sont utilisées afin de résoudre le problème de décision de Diffie-Hellmann et leur sécurité repose sur le problème du logarithme discret.

2.4 Les systèmes sécurisés

Même si de nombreuses attaques matérielles ont été réalisées sur divers systèmes électroniques, la majorité des publications scientifiques traitant d'attaques matérielles privilégient la carte à puce comme cible d'attaque. Cela s'explique principalement par le faible coût et la facilité d'obtention de ces supports, par la facilité d'accès au circuit (aussi bien en face avant qu'en face arrière) mais également par le fait qu'elle constitue actuellement le principal élément de confiance du marché de l'électronique et le socle des marchés de la communication mobile et bancaire.

2.4.1 La carte à puce

2.4.1.1 Historique

A partir de 1974, Roland Moreno dépose plusieurs brevets sur des mémoires portatives sécurisées. Ces brevets constituent le prélude des cartes à puce. Cependant, ce n'est qu'en 1977 que la première carte embarquant un microprocesseur fut réalisée et notamment le brevet de Bull sur la CP8 (Fig.2.3). L'industrialisation de la carte à puce n'a cependant pas été effective avant le début des années 1990.

Dorénavant, la carte à puce est très largement répandue dans les domaines de la télécommunication et des services bancaires. Elle s'est imposée comme un standard grâce aux normes ISO.7810 et ISO.7816 qui permettent de définir entre autre la forme et la position des connecteurs électriques.

FIGURE 2.3: Première carte à microprocessseur

2.4.1.2 Description

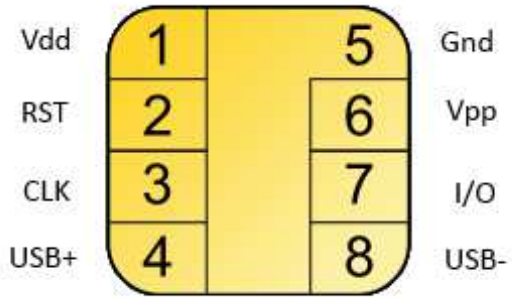

FIGURE 2.4: Connecteur d'une carte à puce défini dans la norme ISO.7816

Une carte à puce est constituée d'un microprocesseur de 8, 16 ou 32bits, d'un générateur de nombres aléatoires (*True Random Number Generation* (TRNG)), d'un ou plusieurs coprocesseurs cryptographiques et aussi de plusieurs mémoires volatiles ou non tel que la ROM, l'EEPROM, la Flash ou encore la RAM. Cette dernière a pour fonction de stocker tous les résultats intermédiaires de calcul durant le fonctionnement de la carte à puce. La ROM contient quant à elle tout le code de programmation du système d'exploitation et des applications que la carte à puce peut être amenée à effectuer. Les mémoires non volatiles (EEPROM ou Flash) sont utilisées pour stocker toutes les données personnelles de l'utilisateur de manière sécurisée.

Comme on peut le voir sur la Fig.2.4, la carte à puce possède huit contacts. Elle possède un contact de masse (Gnd) et un d'alimentation (Vdd). Le contact RST permet de réinitialiser à zéro les compteurs mémoires. Le contact I/O permet de communiquer avec le circuit cadencé par le signal d'horloge fournie par le contact CLK (fréquence

généralement inférieur à 8MHz). Le contact Vpp permet quant à lui de fournir l'alimentation nécessaire pour l'écriture de la mémoire EEPROM. Les deux derniers contacts ne sont pas utilisés actuellement.

De nos jour, les cartes à puce peuvent contenir des algorithmes de chiffrement qui vont permettre de chiffrer les données. Les algorithmes de chiffrement les plus utilisés sont l'AES, le RSA ou encore le 3-DES.

2.4.2 Les systèmes sécurisés de demain

Depuis quelques années, la domotique permet de contrôler tous les appareils ménagés à distance (réfrigérateurs, télévisions, Hi-Fi, éclairage). Ces appareils que l'on nomme objets connectés ("internet of things") sont contrôlables à distance à l'aide d'un ordinateur ou même d'un smartphone. Au-delà du confort qu'offrent au quotidien ces nouvelles technologies, elles permettent de réaliser de substantielles économies d'énergie ("Smart grid"), de renforcer la sécurité du foyer, ou encore de se prémunir d'accidents domestiques (incendie, inondation, ...).

Ces dispositifs communiquent entre eux par le biais de différentes technologies sans fil comme le courant porteur de ligne (plus communément appelé CPL), le Wi-Fi, les radiofréquences, ou des protocoles propriétaires. Pour les contrôler à l'aide d'une tablette ou d'un smartphone depuis le réseau local du foyer ou à distance par Internet, l'utilisateur n'a plus qu'à jouer du bout des doigts avec les icônes représentant les équipements connectés pour planifier des actions immédiates ou différées. Cependant, la sécurité des objets connectés, dédiés à la domotique ou au bien être, est un enjeu majeur car ces objets peuvent induire des actions concrètes sur le monde réel.
Depuis quelques mois, quelques cas concrets d'attaques menées sur des objets connectés prouvent que la menace est bien réelle et que cette dernière peut nuire à la diffusion et à l'adoption de ces objets par les consommateurs.

L'un des premiers exemples fut le lapin connecté "Nabaztag" [15]. Celui-ci dispose d'une caméra, d'un microphone, d'un accès internet et au mail de l'utilisateur. Il a été montré que ce lapin dispose de nombreuses failles sécuritaires et qu'il est possible d'espionner les personnes disposant de cet appareil. Un autre exemple que nous pouvons citer est

celui d'un frigidaire connecté. Celui-ci a été piraté à distance pour être transformé en serveur de spam [16].

Tout comme ces objets, un grand nombre d'objets connectés n'intègre pas de dispositif de sécurité. Avec la prolifération de ces objets, la sécurisation aussi bien matérielle que logicielle va devenir un enjeu primordial pour les industries.

2.5 Classification des attaques matérielles

Comme vu précédemment, le principal but de la cryptographie est de sécuriser les informations à l'aide d'algorithme de chiffrement afin d'éviter à des personnes indiscrètes d'accéder à ces données. La cryptanalyse est une discipline complémentaire à la cryptographie. La cryptanalyse peut être définie comme l'art de l'analyse des informations chiffrées. Le but de la cryptanalyse est de tenter de récupérer les informations qui sont sécurisées par un système cryptographique ou encore de casser ce système. Le processus par lequel on tente de comprendre un message en particulier est appelé une attaque.

Selon les méthodes et moyens mis à sa disposition, l'attaquant peut avoir un rôle actif en modifiant le comportement du système ciblé ou alors se contenter d'un rôle passif en observant les différentes variables physiques liées au dispositif. Parmi les attaques actives ou passives, une classification de ces attaques a été effectuée en fonction des moyens nécessaires pour effectuer l'attaque :

- Les attaques invasives : ce sont des attaques menées en général par des experts. Elles requièrent un matériel spécifique. Typiquement, l'attaque se déroule en deux étapes, la préparation de l'échantillon utilisé, puis l'attaque. Généralement, une attaque invasive aura pour effet de détruire l'échantillon attaqué. L'une des attaques les plus connue est décrite dans [17]. Elle permet de reconstituer le layout d'un circuit en utilisant des techniques chimiques et des microscopes à haute résolution.
- Les attaques semi-invasives : elles ont été introduites par Sergei Skorobogatov et Ross Anderson [18, 19]. Le principe est de décapsuler le boitier contenant la puce afin d'être au plus proche de la surface du circuit sans détériorer ce dernier. Parmi ces attaques, on distingue les attaques actives ou passives utilisant les ondes EM [20, 21] ou la lumière [22].

– Les attaques non-invasives : elles ne nécessitent aucune préparation préalable du circuit intégré. On peut distinguer deux types d'approche. La première consiste à espionner les fuites physiques pendant l'exécution de l'algorithme (attaques par canaux cachés), alors que la seconde consiste à perturber le calcul (attaques par fautes), et ceci soit en perturbant la tension d'alimentation, le signal d'horloge ou encore la température de fonctionnement.

2.5.1 Les attaques par canaux auxiliaires

Les attaques par canaux auxiliaires, communément appelées *Side Channel Attacks* (SCA), sont des attaques passives et non-intrusives. Ce sont probablement les attaques les plus redoutables. Elles ont pour objectif d'extraire de clés cryptographiques utilisées lors d'opérations de chiffrement. Dans tous les systèmes sécurisés, les calculs de cryptage sont effectués par une implémentation matérielle ou mixte (microprocesseurs ou crypto-processeurs) qui laisse fuir des informations (consommation électrique, rayonnement électromagnétique, temps de calcul, etc) pouvant être mises à profit par un attaquant. Cette fuite d'information est principalement due à la technologie CMOS. En effet, les portes logiques CMOS sont conçues de manière à minimiser l'énergie lorsqu'elles ne changent pas d'état. Par contre, de l'énergie est consommée lors d'un changement d'état. Cette énergie est composée de :

– la consommation statique : les réseaux pull-down et pull-up étant conçus de façon à ne jamais avoir une connexion directe entre les lignes Vdd et Gnd, la consommation statique se résume aux courant de fuite des transistors bloqués.
– la consommation dynamique : qui intervient lors du changement de valeur de la sortie de la porte.

Cette thèse se concentre sur la consommation d'énergie et le rayonnement électromagnétique qui sont les deux méthodes les plus utilisées pour réaliser dans la pratique des attaques par canaux cachés.

2.5.2 Fuites physiques

Les émissions EM d'un circuit sont principalement dues aux changements d'état à la sortie des portes logiques CMOS. Ce surplus de consommation énergétique a pour effet de

créer un champ électromagnétique comme cela est montré dans [20]. Cette consommation est en général modélisée par l'attaquant au niveau algorithmique. Deux modèles sont couramment utilisés :

– le poids de Hamming : ce modèle consiste à essayer de deviner la valeur du bit que l'on attaque. Il considère qu'un bit à l'état '0' ne provoque aucune surconsommation tandis qu'un '1' en génère une. Cela implique que les transitions '0' vers '0' et '1' vers '0' ne consomment pas tandis que les transitions '0' vers '1' et '1' vers '1' consomment. Ce modèle ne correspond pas vraiment à la réalité sauf pour des structures particulières comme les bus ou les accès mémoires.
– la distance de Hamming : ce modèle ne va pas se fonder sur l'état de la sortie mais sur les transitions. Il suppose que les changements d'état de '0' vers '0' et '1' vers '1' ne provoquent pas de surconsommation tandis que les transitions de '0' vers '1' et '1' vers '0' en provoquent. Ce modèle est particulièrement bien adapté pour attaquer des crypto-processeurs matériels car il est plus représentatif du comportement réel de la glue logic.

La Fig.2.5 représente une plateforme d'acquisition du rayonnement électromagnétique. Une trace de rayonnement électromagnétique, plus communément appelée trace EM, est une représentation de l'activité électrique et calculatoire du circuit. La plateforme d'acquisition est composée de cinq éléments :

– un PC servant à communiquer avec le circuit à caractériser (CaC) et à récupérer les traces acquises par l'oscilloscope,
– un oscilloscope à échantillonnage digital (*Digital Sampling Oscilloscope* (DSO)) ayant un taux d'acquisition élevé ($>$ 5 Giga échantillons par seconde),
– une sonde d'analyse EM qui permet de récolter le rayonnement électromagnétique du CaC,
– un amplificateur faible bruit qui permet d'amplifier le rayonnement électromagnétique et donc d'élever le rapport signal à bruit des mesures réalisées.

Le rayonnement électromagnétique est collecté par l'oscilloscope puis numérisé en une trace EM qui n'est autre qu'un vecteur de valeurs entières ou réelles. Cette trace est composée d'un nombre de points dépendants du taux d'échantillonnage de l'oscilloscope et de la durée sur laquelle est effectuée la mesure. Sur la Fig. 2.6(a) est représentée la trace EM d'un chiffrement DES, tandis que sur la Fig. 2.6(b) les traces d'un chiffrement AES sont visibles. Sur ces deux traces EM qui sont échantillonnées à 20GS/s, on peut y distinguer le nombre de rondes de chaque algorithme. A partir de ces observations,

et des connaissances sur l'algorithme de chiffrement utilisé, il est possible de connaître approximativement l'instant de calcul de certaines opérations. Cette fuite physique d'informations peut donc fournir des données permettant de retrouver les secrets à l'aide d'une attaque par canal auxiliaire.

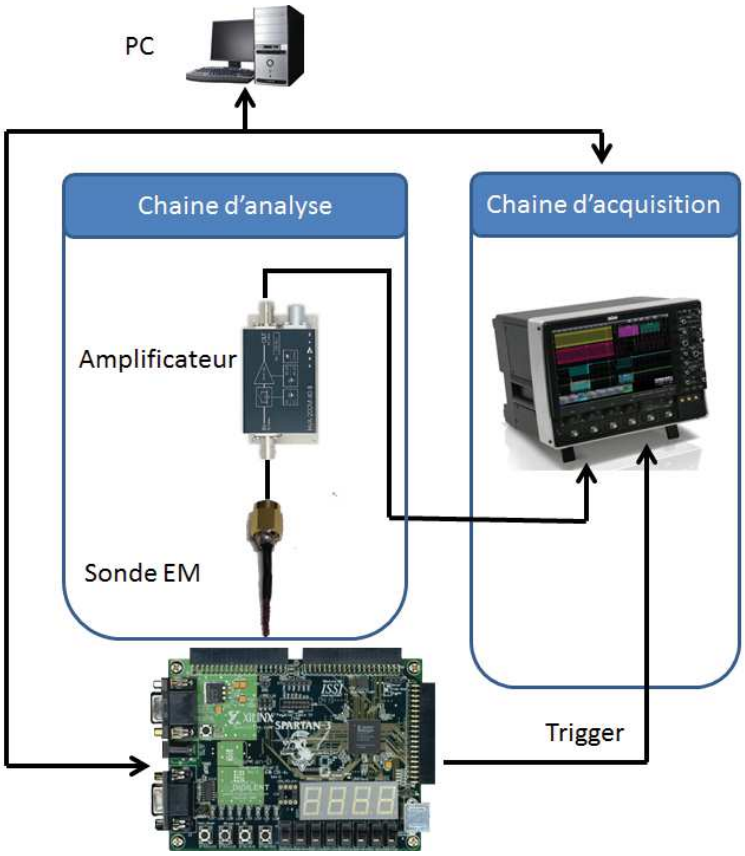

FIGURE 2.5: Banc d'acquisition de traces EM

2.5.3 Attaque SPA

L'une des plus simples attaques par canal auxiliaire, décrite dans [23] est appelée : la Simple Power Analysis (SPA). Elle utilise des traces de courant pour effectuer l'attaque. Cette attaque a été modifiée dans [24] en utilisant des traces EM. Cette modification a pour nom la Simple Electro-Magnetic Analysis (SEMA). Elle s'appuie sur la connaissance de l'algorithme cryptographique exécuté par le CaC, et sur l'observation des traces afin de deviner la clé de chiffrement. Généralement, plusieurs mesures sont moyennées ensemble quand cela est possible, afin d'améliorer le rapport signal à bruit. Si ce n'est pas le cas , des techniques de traitement du signal (filtrage, compression de traces, alignement, etc.) peuvent alors être mises en œuvre. Les différentes opérations réalisées lors de

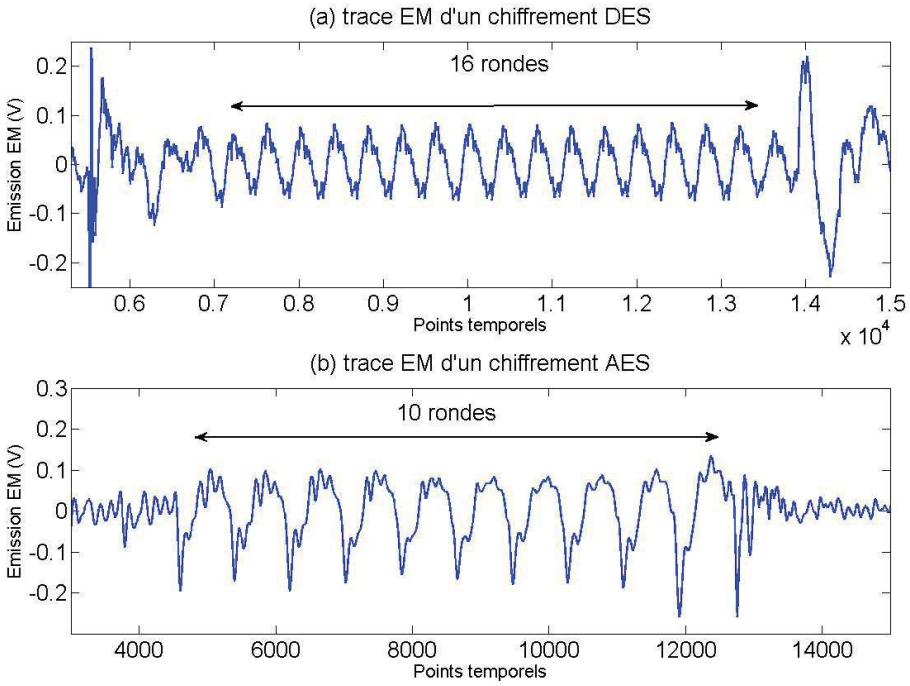

FIGURE 2.6: Traces EM collectées au dessus d'un circuit effectuant (a) un chiffrement DES et (b) un chiffrement AES

l'exécution d'un algorithme cryptographique sont caractérisées par des consommations et des temps d'exécutions différents. Cela explique que plusieurs motifs apparaissent sur les traces. En observant, ces différents motifs dont la clé de manière partielle ou totale dépend, les adversaires peuvent récupérer des informations.

Une attaque SPA classique prend appui par exemple sur une analyse de la consommation d'un algorithme RSA dont le calcul algorithmique est fondé sur l'exponentiation rapide. Le calcul du RSA peut être facilement interprétable en effectuant une lecture binaire de gauche à droite (d_i est le i^{eme} bit de d), comme décrit dans l'algorithme 1. Pour identifier la valeur de chaque bit d_i de la clé de chiffrement, une observation de la trace de consommation est réalisée. Le bit de d_i sera égal à 1 lorsqu'un calcul de carré modulaire suivi d'un calcul de multiplication modulaire est effectué, tandis que d_i sera égal à 0 lorsque que seul un calcul de carré modulaire est réalisé. On peut ainsi visualiser la différence sur la Fig.2.7.

De nos jour, la SPA n'est plus une attaque efficace car il existe plusieurs contre-mesures qui ont pour but de contrecarrer cette attaque tel que l'ajout de calculs fantômes [25] ou plus simplement l'utilisation d'algorithmes dits réguliers en terme d'opérations effectuées.

Algorithm 1 Lecture binaire de gauche à droite

Input : c(ciphertext) ,d(clé :$d_{l-1}, ..., d_0$) ,n (module)
Output : m (message clair)
$n = 1$
for $i = 0 \rightarrow l - 1$ **do**
  $c = c^2 \bmod n$
  if $d_i = 1$ **then**
    $m = m * c \bmod n$
  end if
end for

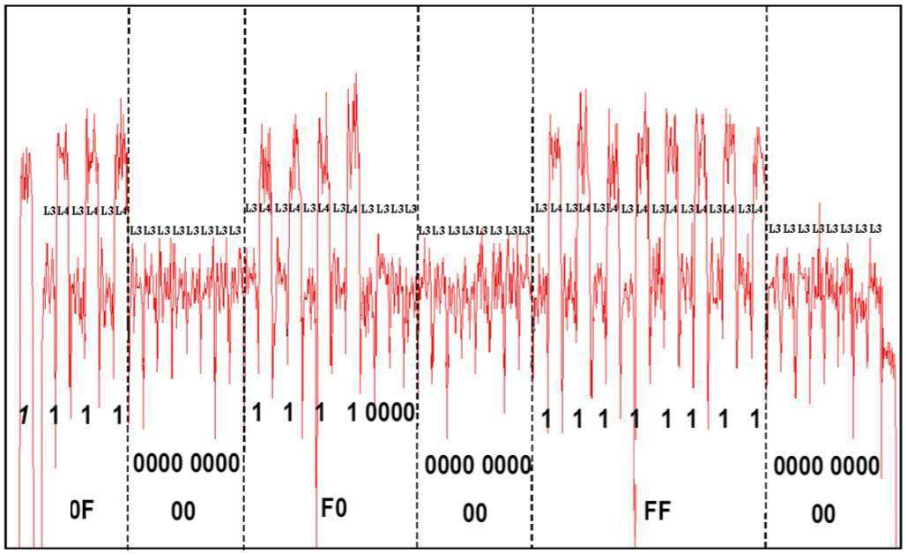

FIGURE 2.7: SPA sur la consommation d'un RSA non protégé

2.5.4 Les attaques verticales

Beaucoup de SCA ciblant les algorithmes de chiffrement par blocs (exemple l'AES) utilisent la stratégie "diviser pour mieux régner". En effet, plutôt que d'essayer d'identifier la totalité de la clé de chiffrement (128 bits pour l'AES), celle-ci va être décomposée en 16 sous-clés de 8 bits. L'attaquant essaie alors de calculer la valeur de chaque sous-clés (256 valeurs possibles par sous-clés pour l'AES). Cela permet ainsi de diminuer le nombre de possibilités à explorer à $16 * 2^8 = 4096$ au lieu de 2^{128} possibilités. Une fois l'attaque terminée, toutes les sous-clés sont alors rassemblées afin d'obtenir la totalité de la clé. L'attaque se concentre en général sur la première ou la dernière ronde de l'AES car le schéma d'attaque y est simplifié. La clé de chiffrement calculée par l'attaquant est une clé de ronde qui permet alors de remonter à la clé de chiffrement car l'algorithme AES est connu.

Le principe des SCA est de supposer que les fuites physiques émanant du circuit contiennent des informations sur la clé de chiffrement. Dans la pratique, les valeurs physiques mesurées sont associées à des valeurs intermédiaires calculées par l'algorithme de chiffrement dont dépend la clé de chiffrement. L'attaquant construit un modèle de fuite pour chaque sous-clé et le compare aux valeurs physiques mesurées.

On notera $f : \chi * \kappa \rightarrow \nu$ la fonction intermédiaire utilisée lors d'une attaque avec $\kappa = \{0, .., k-1\}$ l'ensemble des valeurs possibles de la clé, $\chi = \{0, ..., x-1\}$ l'ensemble des entrées possibles pour la fonction f et, $\nu = \{0, ..., z-1\}$ celui de la sortie de la fonction f. Soit X une variable aléatoire qui représente l'entrée de la fonction intermédiaire, et Z la variable aléatoire représentant le résultat de cette fonction.

La fonction intermédiaire f est connue par l'attaquant, elle est déterministe, et dépend d'une sous clé k. Cette fonction peut être très diverse : une permutation, une fonction non linéaire, etc. On notera $L(Z) = L(f(X,k)) = \Phi(X,k)$, la variable aléatoire représentant la fuite générée par le calcul de Z. La fonction Φ est quant à elle inconnue et non-déterministe, elle ne dépend que du circuit à caractériser pour l'attaque.

Le but d'une attaque par observation est d'estimer la clé secrète notée k^*. On dispose pour cela de n réalisations notées $l_i = \phi(x_i, k^*), i = 1, ..., n$ de $L(Z) = \Phi(X, k^*)$. On considère que ces réalisations proviennent de variables aléatoires indépendantes. Ces réalisations sont obtenues à partir de mesures physiques bruitées qui sont générées par l'environnement où se trouve le circuit. On nommera ces réalisations 'observations'.

Lors d'une attaque par observation, on doit choisir une fonction qui représente la manière dont fuit le composant par rapport aux variables manipulées. Cette fonction sera un des modèles de fuites présenté dans la section 2.5.2. Ce modèle, qui peut être le poids de Hamming ou la distance Hamming est noté H_κ comme évoqué auparavant.

Enfin, un outil statistique, appelé distingueur, D, est utilisé pour chercher toute dépendance entre H_κ et $T_i = \phi(x_i, k^*)$. Le distingueur D permet ainsi de déterminer quelle hypothèse de clé est la plus probable $\hat{k} = \text{argmax}\{D(T_i, H_\kappa)\}$ entre les observations T_i et

les prédictions H_κ. La Fig.2.8 permet de visualiser le principe d'une attaque verticale SCA.

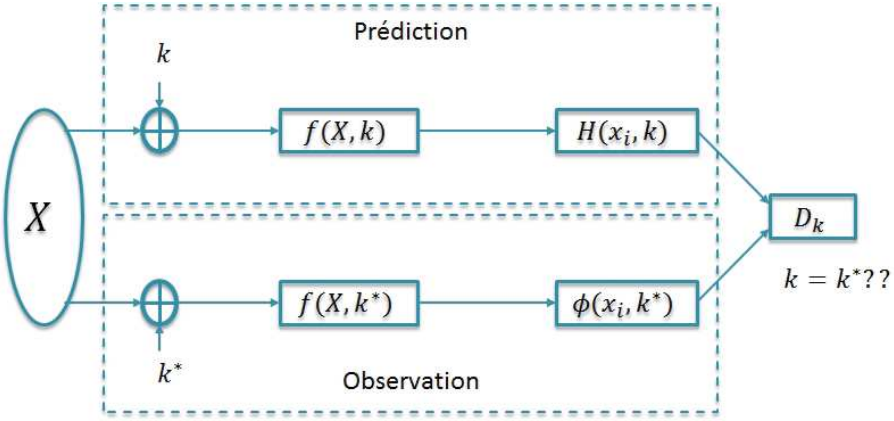

FIGURE 2.8: Principe d'une attaque verticale

Les principales différences entre les différentes attaques verticales, sont essentiellement liées au distingueur utilisé. Les deux distingueurs les plus souvent utilisés dans la littérature sont la différence des moyennes et la corrélation de Pearson.

2.5.4.1 Attaque par différence des moyennes

L'attaque par différence des moyennes a été présentée par P.Kocher [26]. Elle se base sur une analyse différentielle de la consommation (Differential Power Analysis (DPA)). Lors d'une DPA, l'attaquant se focalise sur un seul bit en sortie d'une fonction de l'algorithme de chiffrement. S'il vaut 0, la trace associée $\phi(x_i, k^*)$ est mise dans un paquet A. Par contre si ce bit vaut 1, alors $\phi(x_i, k^*)$ est mise dans un paquet B. Le but étant de classer toutes les traces $\phi(x_1, k^*)$,$\phi(x_2, k^*)$, . . ., $\phi(x_n, k^*)$ dans les deux paquets A ou B et de calculer la différence des moyennes de ces deux paquets. La courbe résultante est appelée courbe différentielle, et correspond à une hypothèse de sous-clés. Dans le cas d'une attaque DPA sur une sous clé d'un AES, l'attaquant est donc censé calculer les 256 courbes différentielles associées aux 256 hypothèses de sous-clés. La courbe différentielle notée Δ, pour une hypothèse de sous-clés notée K_s, est calculée à partir de :

$$\Delta_{K_s} = \frac{\sum_{i=1}^{n} D(x_i, K_s)T_i}{\sum_{i=1}^{n} D(x_i, K_s)} - \frac{\sum_{i=1}^{n}(1 - D(x_i, K_s))T_i}{\sum_{i=1}^{n}(1 - D(x_i, K_s))} \tag{2.10}$$

D étant la fonction de sélection choisie pour ranger les traces dans les paquets A et B. Si l'hypothèse de sous-clés est fausse, toutes les valeurs intermédiaires sont fausses.

Par conséquent, les traces sont aléatoirement mises dans les paquets A ou B, et la différence de leur moyenne a une allure plate et est majoritairement composée de bruit. Au contraire, si l'hypothèse de sous-clés est correcte, les deux paquets A et B, contiennent des traces qui ont une caractéristique différente liée à la valeur prise par le bit cible. Le résultat de calcul de la différence des moyennes des deux paquets dévoile alors un pic se produisant à l'instant où est calculée la valeur intermédiaire.

La Fig. 2.9(a) représente la trace EM d'un chiffrement d'un AES. On peut remarquer que le nombre de pic EM visible sur la Fig. 2.9(a) est supérieur à 10. Ce surplus est dû à lecture et l'écriture des registres internes à l'AES en début et fin de chiffrement. La Fig. 2.9(b) représente quant à elle le résultat d'une attaque DPA sur les traces EM de l'AES. Sur cette figure, 256 traces sont représentées. Elles correspondent aux 256 hypothèses pour la sous-clé 1 de l'AES. On peut ainsi s'apercevoir qu'une courbe en rouge ressort fortement. Celle-ci correspond à la bonne sous-clé. A noter que dans ce cas, l'attaque a été réalisée durant la dernière ronde de l'AES avec un modèle HD.

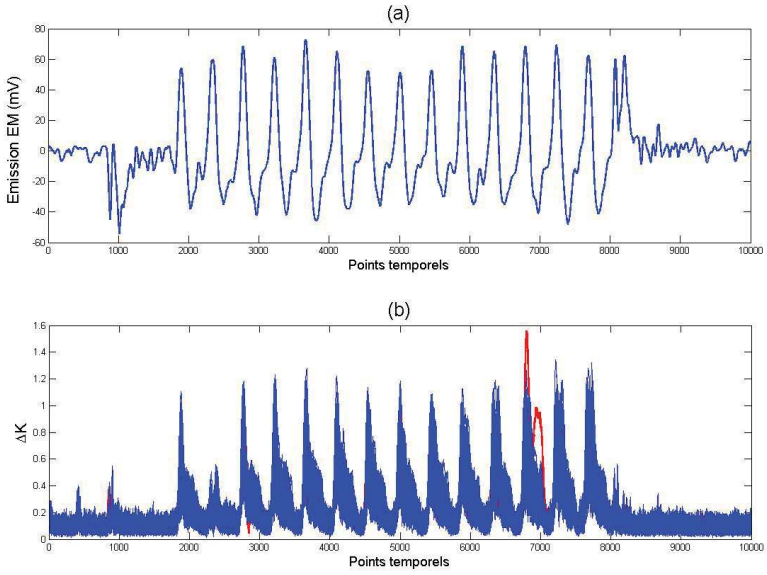

FIGURE 2.9: (a) Trace EM d'un chiffrement AES, (b) Evaluation de Δ_{K_s} pour une valeur de sous-clé dans le temps

2.5.4.2 Attaque par analyse de la corrélation

Lorsque l'on parle de dépendance entre deux variables aléatoires, la première mesure qui vient à l'esprit est celle donnée par le coefficient de corrélation linéaire entre les

observations et les prédictions. Ce coefficient est défini par :

$$\rho(X,Y) = \frac{cov(X,Y)}{\sigma_X.\sigma_Y} = \frac{\mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]}{\sqrt{\mathbb{E}[X^2] - \mathbb{E}[X]^2}\sqrt{\mathbb{E}[Y^2] - \mathbb{E}[Y]^2}} \tag{2.11}$$

avec X et Y deux variables aléatoires, $cov(X,Y)$ la covariance entre X et Y, σ_X et σ_Y la covariance entre ces dernières et $\mathbb{E}[X]$ l'espérance de X. Si $\rho(X,Y) = 1$ ou $\rho(X,Y) = -1$, cela signifie qu'il existe une relation linéaire parfaite entre les deux variables aléatoires. Lors d'une attaque, la sous-clé que l'on considèrera comme 'bonne' sera donc celle qui aura, en valeur absolue, le coefficient de Pearson le plus élevé. La Fig. 2.10b représente le résultat d'une attaque CPA avec en rouge la courbe de corrélation qui correspond à la bonne sous-clé.

En comparant la Fig. 2.9b relative à la DPA et la Fig. 2.10b, on s'aperçoit que la fuite d'informations se produit sur les mêmes points temporels. Sur la Fig. 2.9b, des pics apparaissent sur les rondes suivant l'AES et la lecture et l'écriture des registres interne à l'AES, tandis que sur la Fig. 2.10b ils n'apparaissent pas. Cela peut s'expliquer par le fait qu'une normalisation est effectuée dans la corrélation de Pearson, tandis que pour le calcul de la différence des moyennes, aucune normalisation est effectuée pour la DPA.

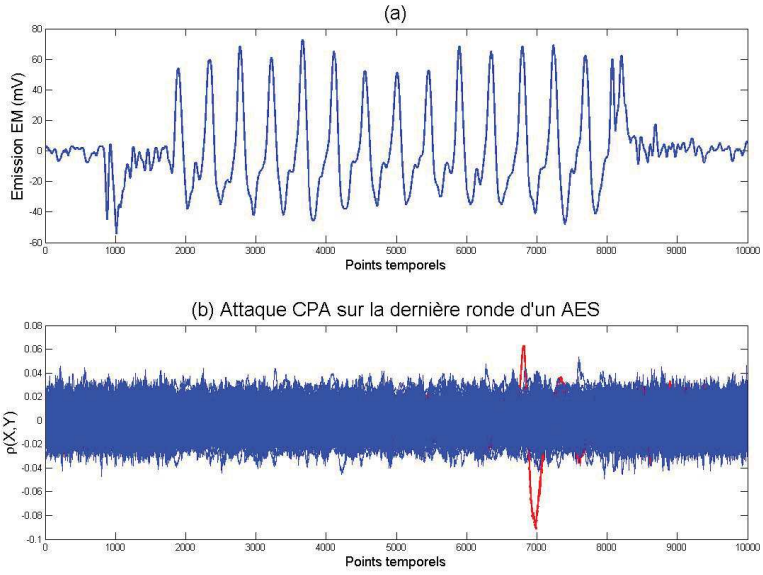

FIGURE 2.10: (a)Trace EM d'un AES, (b)Attaque CPA réalisé sur un AES

L'analyse du courant avec le coefficent de Pearson (CPA) [27] est actuellement l'attaque par observation la plus populaire. Cette popularité est principalement due au fait que

les modèles utilisés le plus couramment sont souvent effectivement proches de la fuite à une fonction linéaire près. Comme montré dans l'article [28], l'utilisation de la CPA avec un modèle mono-bit revient à la DPA normalisée de Kocher. Elle est également très résistante au bruit présent dans les observations que l'on utilise. Si l'on augmente le nombre d'observations dont on dispose, on diminue de plus en plus la contribution du bruit. Néanmoins, afin de se prévenir de cette attaque, les fabricants de cartes à puce essaient de mettre en œuvre des contre-mesures visant à cacher la fuite d'informations et de rendre l'extraction de la clé de chiffrement par ces attaques de plus en plus dure.

2.5.4.3 Contre-mesures aux attaques par observation

Dans cette section, nous présentons brièvement les contre-mesures les plus courantes pour les algorithmes de chiffrement par blocs. Une analyse plus approfondie peut être trouvée dans [29]. Les contre-mesures visent à dissimuler ou au moins à atténuer les informations pertinentes que peut collecter un attaquant en observant un canal auxiliaire. Cependant, elles offrent généralement un compromis entre sécurité et performance. Il existe trois contre-mesures principales qui sont très souvent déployées par les concepteurs pour contrecarrer les SCA : le masquage, la dissimulation, le mixage.

Dissimulation : La dissimulation est une contre-mesure très répandue pour contrecarrer les attaque SCA. Plusieurs techniques peuvent être utilisées pour cela. La première méthode consiste à équilibrer la consommation dynamique du circuit afin d'atténuer la fuite d'informations. La logique double-rail s'inscrit dans cette démarche. Elle est présentée dans [30, 31]. Une autre méthode revient à faire varier la tension et la fréquence du circuit pour cacher la fuite d'informations [32].

Masquage : Le principe du masquage consiste à appliquer un masque aléatoire aux données en entrée de l'algorithme de chiffrement. Les calculs effectués par l'algorithme ne correspondent pas aux valeurs à chiffrer (sauf si la valeur du masque est de 0). Enfin, le masque est de nouveau appliqué au résultat final fourni par l'algorithme afin d'obtenir le résultat correct. Ce type de contre-mesure permet ainsi de rendre les prédictions des valeurs intermédiaires faites par l'attaquant lors d'une attaque SCA complètement caduque et donc la modélisation de la fuite qui en découle erronée.

Mixage : Cette méthode est très répandue et peu coûteuse. Elle consiste à rendre aléatoire l'ordre d'exécution des différentes opérations de l'algorithme [33]. Cette méthode a par exemple été utilisée sur les traces EM du DPA Contest V4.2.

2.5.5 Injection de fautes

2.5.5.1 Description

Alors que la majorité des attaques SCA a pour objectif de retrouver la clé de chiffrement utilisée, les attaques par injection de fautes se caractérisent par un domaine d'utilisation plus vaste et sont potentiellement plus dangereuses bien que souvent elles soit plus difficile à mettre en œuvre. Une attaque par injection de fautes consiste à modifier le fonctionnement du dispositif de manière contrôlée dans le but d'extraire les données confidentielles contenues dans le circuit ou tout simplement de nuire aux applications embarquées afin de tester le niveau sécuritaire d'un circuit.

Les attaques par injection de fautes ont été introduites en 1996 par Boneh [34, 35]. La méthode d'attaque proposée dans ce papier est basée sur l'insertion de valeurs cryptographiques erronées lors d'opérations de signature RSA ou lors de l'authentification. Dans le même temps, Biham a démontré que les algorithmes cryptographiques symétriques étaient également vulnérables à l'injection de fautes. Il propose une attaque par analyse différentielle de fautes (DFA) [36] qui est basée sur la comparaison de chiffrés corrects et fautés. Un grand nombre d'améliorations de l'attaque a depuis été proposé, cependant deux de ces attaques sont désormais considérées comme des références, l'attaque de Giraud [37] et l'attaque de Piret et Quisquater [38].

Cependant, les attaques par fautes ne peuvent pas être cantonnées aux algorithmes cryptographiques. En effet, tous les programmes embarqués sur un circuit peuvent être ciblés. Dans le protocole de carte à puce, il est nécessaire d'effectuer un contrôle par code pin afin d'effectuer l'authentification. Cette classe d'attaque peut permettre de contourner ce contrôle.

Afin de réaliser ce type d'attaque, les conditions d'environnement dans lesquelles évolue le circuit à caractériser doivent être modifiées afin de pouvoir générer des erreurs. Pour effectuer cela, différentes techniques sont utilisées.

2.5.5.2 Attaques par perturbation globale

Lors de la conception d'un circuit, celui-ci est testé dans différentes conditions de fonctionnement afin de vérifier qu'il est conforme au cahier des charges et opère correctement sur la plage de fonctionnement attendue. Cette plage de fonctionnement, qui est déterminée par le fabricant de semi-conducteurs, est définie à *minima*, par la fréquence maximale de fonctionnement, les tensions maximale et minimale, ainsi que par la plage de températures sur laquelle le circuit opère correctement. Les attaques par perturbations globales, plus communément appelées attaques en limite de fonctionnement, consistent à faire fonctionner le circuit en dehors de sa plage de fonctionnement définie par le fabricant afin de produire des fautes.

Température : Le but de cette attaque est de faire varier la température du circuit. Pour cela, plusieurs méthodes peuvent être utilisées (résistance chauffante, refroidissement liquide) afin d'amener le circuit sur une plage de fonctionnement non prévue. D'après [39], qui reporte des résultats obtenus sur des cartes à puce, il est possible d'affecter de façon aléatoire le contenu d'un point mémoire RAM à l'aide de chaleur. Il est également reporté que les seuils de température ne sont pas équivalents lors des opérations d'écriture et de lecture des mémoires non volatiles. Ainsi, il est possible de mettre en place une attaque en jouant sur la température pour autoriser l'écriture dans la mémoire mais refuser la lecture (ou vice-versa). Il a aussi été montré dans [40] qu'il est possible de perturber des générateurs de nombres aléatoires.

Tension : L'alimentation d'un circuit conditionne le temps de transition des portes logiques constituant un circuit [41]. Les temps de propagation des différents signaux d'un circuit peuvent ainsi être augmentés ou diminués. Ainsi, en sous-alimentant un circuit, il est possible de générer des violations de temps de setup. Pour effectuer ce type d'attaque très peu de ressource sont nécessaires. Dans [42], il est démontré qu'il est possible de créer des fautes lors d'instructions mémoires en jouant sur la tension d'alimentation. Cela est principalement dû au fait que la consommation du circuit est plus importante pour les instructions mémoire que pour le reste du jeu d'instructions. Ainsi il a été possible de faire fauter des algorithmes de chiffrement tel que le RSA [43] ou l'AES [44].

Fréquence : L'overclocking ou sur-cadencement en français, est une manipulation ayant pour but d'augmenter la fréquence du signal d'horloge au-delà de la fréquence maximale

définie par le fabricant afin d'augmenter ses performances. Ainsi, en augmentant la fréquence d'horloge jusqu'à des valeurs trop importantes il est possible de générer des erreurs de calcul. La condition pour réaliser ce type d'attaque est que le signal d'horloge soit généré en externe et non pas par une boucle à phase asservie communément appelée Phase Locked Loop (PLL).

2.5.5.3 Attaque par perturbation localisée

Les attaques par perturbation localisée utilisent le circuit dans la plage de fonctionnement définie par le fabricant. L'attaquant génère une perturbation locale d'une durée très courte, qui induit des erreurs dans le circuit. Pour générer ces erreur, plusieurs moyens d'injections de fautes existent.

Pic de tension : Ce moyen d'injection de fautes est plus communément appelé "spike attack" ou "voltage glitch". Il se fonde sur une variation soudaine de la tension d'alimentation du circuit. Cette variation qui est réglable temporellement et en amplitude, permet de corrompre avec précision une ou plusieurs opérations en injectant un pic de tension sur le réseau d'alimentation du circuit [45] ou alors par le substrat [46].

Pic sur front d'horloge Plus communément appelé "clock glitch", cette méthode d'injection de fautes consiste à générer sur le signal d'horloge un pic parasite afin de faire croire au circuit qu'un front d'horloge a eu lieu. En provoquant, l'exécution prématurée de certains calculs, les données manipulées par l'instruction sont alors incorrectes [47]. Fukunaga [48] présente une méthode pour l'insertion d'un pic d'horloge avec une très bonne précision ($<$ 50ps). Cela a ainsi permis de générer des fautes sur plusieurs algorithmes symétriques, puis de lancer une attaque DFA [38] et de retrouver la clé de chiffrement.

2.5.5.4 Attaque optique

L'utilisation de ces moyens d'injection de fautes requière l'accès physique au circuit, en enlevant les différentes protections (boitier plastique, céramique, amincissement de la face arrière du silicium...) grâce à diverses méthodes (polissage, réactions chimiques, abrasion laser...)

Lumière blanche Tous les circuits intégrés sont sensibles à la lumière en raison des effets photoélectriques. Les courants induits par les photons, lors d'une exposition brève et intense, peuvent être utilisés pour induire des fautes. Par exemple, comme cela est présenté dans [49], en utilisant ingénieusement un appareil photo et un oculaire d'une station de test sous pointe, l'émission de la lumière du flash au travers de l'oculaire, focalisée par une simple ouverture dans une feuille d'aluminium à son extrémité, permet de changer l'état d'une cellule SRAM, d'un micro-contrôleur PIC16F84. Cette lumière peut aussi être utilisée pour connaitre l'emplacement des transistors actifs durant une opération spécifique [50].

Laser Avec les progrès des technologies de fabrication des circuits intégrés, la taille des composants des circuits intégrés n'a cessé de diminuer. Des méthodes adaptées à cette diminution ont donc été développées. L'utilisation du laser comme moyen d'injection de fautes est devenue incontournable lors de l'évaluation sécuritaire des circuits sécurisés. L'historique de l'étude des effets laser sur les semi-conducteurs remontent aux années 1960, où le phénomène d'ionisation dans un transistor lors d'irradiation par faisceau laser infrarouge est clairement défini [51]. A l'aide d'un pointeur laser légèrement modifié, et d'un microscope pour concentrer le faisceau, les auteurs de [49] ont prouvé la possibilité de changer un seul bit d'une mémoire SRAM. L'utilisation de diode laser, associée à un guide d'onde composée d'une fibre optique, est également un moyen de monter une attaque laser [52].

Les effets produits par un faisceau laser sont similaires à ceux produits par la lumière blanche. Toutefois l'avantage d'un laser est d'émettre une lumière monochromatique (rouge : 635nm, vert : 532nm et bleu : 445nm) qui permet de cibler précisément une zone ciblée, avec un faisceau de diamètre de l'ordre de 1μm. Cette taille minimale nécessite l'utilisation d'optiques spéciales accessibles seulement à un nombre réduit d'attaquants, compte tenu des coûts de ces optiques.

2.5.5.5 Electro-Magnétisme

L'utilisation de champs électro-magnétiques comme moyen de perturbation est assez récent. Le chapitre 4 de cette thèse est consacré à ce moyen de perturbation. Nous renvoyons donc le lecteur à ce chapitre pour plus d'informations.

2.5.6 Modèles de fautes

Différents modèles peuvent être utilisés pour représenter les différents types de fautes obtenus à l'aide des moyens d'injection présentés précédemment. Plusieurs attaques visant des implémentations cryptographiques supposent qu'un attaquant est capable de réaliser des fautes selon un des différents modèles définis dans [53]. L'article [54] résume les différents types d'attaques physiques possibles et présente les modèles de fautes couramment associés.

2.5.6.1 Modèles de fautes logiques

Il existe différents types de fautes qui peuvent affecter la valeur d'un bit.

- Bitflip : la valeur du bit ciblé est inversée
- Bitset : la valeur du bit ciblé est forcée à '1' (aucun effet si le bit est précédemment à '1')
- Bitreset : la valeur du bit ciblé est forcée à '0' (aucun effet si le bit est précédemment à '0')

Bien qu'il existe plusieurs méthodes d'injection de fautes, il est rare que celles-ci ne génèrent qu'un seul type de faute. Le type de fautes créé peut dépendre de différents paramètres comme le moment de l'injection ou encore la quantité d'énergie injectée par la perturbation dans le circuit.

2.5.6.2 Modèles de fautes algorithmique

Les fautes algorithmiques, sont principalement dues à la modification d'instructions ou à la corruption d'un test conditionnel.

Modification d'instructions : Certaines attaques utilisées sur micro-contrôleurs, peuvent perturber ce dernier et ainsi générer une modification du code d'une instruction [55], [56], [57]. Bien que ce type de fautes soit non négligeable, celles-ci ont rarement été étudié dans la littérature scientifique. Cela peut s'expliquer par le fait qu'il est difficile de connaitre les conséquences de ce type de fautes et donc de les exploiter.

Corruption d'un test conditionnel : Dans un algorithme, les tests conditionnels sont indispensables. Si un de ces tests est corrompu, cela peut créer une modification dans

l'exécution de l'algorithme. Ce type de fautes apparait en injectant une faute sur la donnée conditionnelle. Ce type de fautes a été mis en évidence dans [58], où les auteurs utilisent une attaque laser pour corrompre un branchement conditionnel d'une machine virtuelle Javacard.

2.5.7 Exploitation des fautes

Une attaque par injection de fautes se compose de deux étapes. La première est l'injection de fautes, la seconde est l'exploitation des fautes générées. Il existe plusieurs méthodes pour exploiter ces fautes.

2.5.7.1 Analyse différentielle

Ce type d'attaques par fautes nommées analyse différentielle des fautes (Differential Fault Analysis (DFA)) a été précédemment cité dans la section 2.5.5.1.

2.5.7.2 Safe error

Lors d'une attaque par safe-error, l'attaquant va exploiter le fait qu'une injection de fautes à un moment de l'algorithme produise ou non un résultat fauté en sortie [59]. Une variante de la technique de safe error, nommée Ineffective Fault Analysis (IFA) a également été proposée dans [60]. Le principe est quasiment similaire, mais l'analyse IFA se place au niveau d'une instruction assembleur, alors que la technique de safe error étudie davantage les sorties fautées au niveau de l'algorithme. Une autre variante d'attaques en safe-error est proposée dans [61]. L'attaque proposée exploite à la fois un principe de safe error et des moyens statistiques similaires à ceux de l'analyse DPA.

2.5.7.3 Modification dans l'exécution de l'algorithme

Les modifications dans l'exécution de l'algorithme peuvent notamment permettre de contourner un contrôle d'accès ou d'empêcher l'exécution de certaines fonctions [62]. De telles modifications peuvent notamment être la conséquence de la corruption d'un branchement ou d'un test conditionnel, ou encore être la conséquence du remplacement, ou du saut, d'une instruction. Plusieurs attaques ont ainsi exploité le cas d'un saut

d'instruction ou le saut d'une sous-fonction [45],[63]. De telles modifications peuvent par exemple être utilisées pour permettre l'exécution de code arbitraire par dépassement de tampon [64] ou modifier le nombre de rondes d'un algorithme de chiffrement [65],[66].

2.5.7.4 Rétro-ingéniérie

Les attaques par injection de fautes ont également été utilisées dans un but de rétro-ingénierie, notamment pour identifier certains éléments d'algorithmes partiellement secrets. Dans [67] et [68] les auteurs ont ainsi conçu un procédé de rétro-conception pour retrouver les boites de substitution (S-Box) d'un algorithme DES modifié. Dans [69], les auteurs présentent une méthodologie de rétro-conception pour caractériser l'ensemble des opérations d'un algorithme AES modifié. Pour cela, les auteurs utilisent une technique d'IFA et un modèle de fautes pour lequel un attaquant peut mettre à zéro la valeur d'un octet.

2.5.8 Contremesures aux attaques par injection

Afin de renforcer les circuits intégrés face aux injections de fautes, plusieurs approches ont été proposées dans la littérature scientifique.

Amélioration de la technologie CMOS : Des modifications au niveau de la technologie de fabrication des circuits peuvent permettre de diminuer leur sensibilité à certains moyens d'injection de fautes. Par exemple, dans [70], un changement dans la structure des cellules mémoire SRAM, pour renforcer leur résistance aux tirs laser, est proposé.

Capteurs physiques : Plusieurs capteurs physiques peuvent permettre de détecter des tentatives d'injection. Parmi ceux-ci, on peut notamment mentionner les capteurs de lumière, de variations anormales de la tension d'alimentation ou du signal d'horloge. Un autre mécanisme de détection au niveau de la logique a également été proposé pour détecter des fautes injectées par violation des contraintes temporelles des circuits synchrones [71, 72]. Ce mécanisme consiste à ajouter un signal de délai entre deux éléments de mémorisation synchrones pour assurer que le bloc de logique combinatoire situé entre ces éléments de mémorisation a eu le temps de terminer son calcul.

Détecteurs de Redondance : Dans le cas des attaques par injection de fautes, les contre-mesures existantes visent principalement à ajouter de la redondance dans les calculs effectués par le circuit de manière à pouvoir détecter une éventuelle faute. Cette redondance peut être spatiale (lorsque plusieurs éléments distincts du circuit réalisent la même opération en parallèle) ou bien temporelle (une même opération est répétée plusieurs fois) [39].

Bits de parité : Plusieurs autres méthodes permettant de détecter des fautes intentionnellement injectées ou des erreurs dans un calcul ont également été proposées. Parmi celles-ci, on peut notamment citer l'utilisation de bits de parité [73] ou d'autres codes détecteurs d'erreurs.

Algorithmiques : Le cas des attaques par injection de fautes a été particulièrement traité au niveau des algorithmes cryptographiques. De nombreuses contre-mesures au niveau algorithmique ont alors été proposées. En particulier, pour l'algorithme RSA (et pour son implémentation CRT-RSA qui utilise le théorème des restes Chinois), on peut notamment citer [74–77]. Ces contre-mesures évaluent la validité des relations mathématiques entre variables.

2.6 Synthèse des méthodes d'attaque

Il existe un grand nombre d'attaques différentes. En pratique, il apparait que seulement quelques sources physiques sont utilisées à travers différents moyens d'attaques.

2.6.1 Synthèse des sources physiques des SCA

Il existe un grand nombre de méthodes permettant de collecter des fuites d'informations afin de réaliser une attaque SCA. Cependant, seulement deux sont couramment utilisées. Ces méthodes qui sont l'analyse en courant et l'analyse EM ont l'avantage d'être très faciles à mettre en place et ne nécessite qu'un matériel peu coûteux. Elles ont aussi l'avantage d'être indétectables par le circuit ciblé.
L'analyse en courant utilise le courant consommé par le circuit comme moyen d'accès à la fuite d'informations. Le courant observé est celui consommé par la totalité du circuit. Certaines parties du circuit peuvent fonctionner simultanément avec ce que l'on souhaite

attaquer et donc générer du bruit sur les observations en courant.
L'analyse EM utilise les émissions électromagnétiques du circuit comme fuite d'informations. En fonction de la sonde utilisée, il est possible de ne collecter les émissions EM que de certaines parties du circuit. Du fait que la sonde qui collecte les émissions EM du circuit soit à une distance de quelques millimètres du circuit (à cause du boitier du circuit), le bruit est important. Cependant, il est possible d'améliorer le rapport signal sur bruit du champ EM mesuré par la sonde en décapsulant le circuit et en plaçant la sonde au plus près du circuit ou encore en utilisant des technique de traitement [78].
Pour ces deux méthodes, il est nécessaire d'avoir une fréquence de fonctionnement du circuit stable. Si cette condition n'est pas respectée, cela aura pour effet de créer une désynchronisation entre les différentes traces lors d'une campagne d'acquisition. Il est cependant possible de resynchroniser ces traces de consommation à l'aide de différents algorithmes [79].

2.6.2 Synthèse des sources physiques l'injection de faute

Pour injecter une faute dans un circuit, il est nécessaire d'avoir un moyen de perturbation. Un grand nombre de méthodes de perturbation existent, cependant, très peu de ces méthodes sont utilisées. Les méthodes les plus utilisées sont l'injection laser, ainsi que l'injection de pics de tension dans le substrat et l'injection EM apparues plus récemment.
L'injection laser [71] est le moyen le plus répandu dans les laboratoires d'évaluation pour injecter une faute. Cela peut s'expliquer par le fait que celui-ci dispose d'une grande contrôlabilité (diamètre du faisceau, temps d'illumination). Pour utiliser cette méthode d'injection, il est nécessaire d'avoir un accès au substrat du circuit.
L'injection par pic de tension sur substrat [46] est une méthode moins répandue que le laser. Tout comme celle-ci, elle nécessite d'avoir un accès au substrat du circuit ciblé par l'attaque. La zone d'injection dépend principalement du diamètre de la sonde d'injection utilisée.
L'injection EM [80] dispose d'un avantage non négligeable sur les autres méthodes car elle ne nécessite pas d'accès au substrat du circuit rendant l'injection possible à travers le boitier du circuit aussi bien par la face avant que la face arrière. Cet avantage a une contre-partie liée à la zone affectée par l'émission EM qui est plus étendue que pour les méthodes précédentes.

	Altération du circuit	Orientation
Analyse en courant [23]	Aucune	Aucune
Analyse EM [81]	Aucune	Face avant et face arrière
Injection laser [70]	Décapsulation du circuit	Face arrière
Pic de tension [46]	Décapsulation du circuit	Face arrière
Injection EM [82]	Aucune	Face arrière et face avant

TABLE 2.1: Récapitulatifs sur les moyens d'attaques

Pour tous ces moyens d'injection, le moment de l'injection de la faute est primordial. Afin de pouvoir exploiter la faute injectée, il est nécessaire de connaitre l'opération qu'effectuait le circuit au moment de l'injection de la faute. Pour cela, la fréquence de fonctionnement du circuit se doit d'être stable.

2.6.3 Récapitulatif sur les moyens d'attaques

Il existe un grand nombre d'attaques différentes. Cependant, les moyens pour réaliser ces attaques sont bien moins nombreux et seuls quelques uns sont utilisés couramment. Ces moyens qui sont récapitulés sur le Tab. 2.1 ont chacun des avantages et des inconvénients les uns par rapport aux autres. Mais ils ont toutefois des contraintes en communs comme la stabilité de la fréquence du circuit, la tension d'alimentation ou alors la tension de polarisation du substrat. Il sera beaucoup plus facile de réaliser une attaque si ces trois paramètres sont stables. Si une variation de ces paramètres survient durant l'attaque, cela peut modifier le moment d'injection pour les attaques en fautes ou une désynchronisation des traces de consommation pour une SCA.

2.7 Positionnement des travaux de thèse

La réflexion sur les axes de recherche et les objectifs à atteindre, est importante dans le déroulement d'une thèse et permettent son positionnement au sein de la communauté scientifique. Cette thèse s'inscrit dans le contexte de l'étude de l'impact de l'utilisation de techniques de conception faible consommation sur la robustesse des circuits sécurisés ; ces techniques étant largement utilisées pour la conception de plateformes mobiles qui intègrent de plus en plus d'applications sécurisées. Plus particulièrement, nous nous

intéressons dans cette thèse à l'impact de l'utilisation des techniques d'adaptation dynamique ou statique de la tension d'alimentation (V_{dd}), de la fréquence (F) et de la polarisation de substrat (V_{bb}) sur la robustesse aux attaques exploitant le canal EM. La gestion dynamique de ces grandeurs est un levier efficace permettant de contrôler les performances des circuits. Ces techniques sont généralement désignées par le terme DVFS pour 'Dynamic Voltage and Frequency Scalling' ou AVFS pour 'Adaptive Voltage and Frequency Scalling'.

Il est connu que les attaques par canaux auxiliaires sont sensibles aux variations de tension ou de fréquence. Plusieurs travaux ont d'ailleurs reportés des résultats relatifs à l'exploitation de techniques DVFS comme contre-mesure efficace aux attaques DPA. Cette thèse se concentre sur l'étude des effets de la DVFS sur l'attaque de référence en matière de SCA, la CPA. Cette focalisation sur l'utilisation de la CPA est principalement due à des contraintes matérielles. En effet, le principal effet visible de la DVFS est de créer de la désynchronisation entre les traces de consommations, cela implique alors de lancer les attaques sur une grande quantité de points temporels ($>$ 20000 points temporels) et une grande quantité de traces de consommation ($>$ 1 million de traces). Le temps de calcul étant la plus grosse contrainte, il était nécessaire d'utiliser une attaque ayant un temps de calcul le plus court possible.

L'utilisation des ondes électromagnétiques comme moyen de perturbation est assez récente (2007) [80]et possède un avantage intéressant comparé aux autres méthodes d'injection. En effet, l'injection EM a la faculté de traverser les boitiers des composants. Cette faculté est indispensable pour pouvoir effectuer une attaque par injection de faute sur un circuit complexe sur lequel la face arrière du circuit n'est pas accessible. Cependant le type de fautes réalisées par ce moyen de perturbation était très limité [83]. Dans cette thèse, une étude de ce moyen d'injection a été effectuée et une amélioration des plateformes existantes réalisée. L'impact de l'utilisation de technique DVFS sur l'efficacité de ce nouveau moyen d'injection est également étudié.

Cette thèse a été organisée selon la progression de nos expérimentations de manière à se focaliser sur un certain nombre de questions regroupées en deux chapitres :

Analyse EM et RDVFS

– Quels sont les effets des variations de tension, de fréquence et de polarisation du substrat sur les fuites d'informations exploitées par la CPA ?

– Quel est l'impact réel d'une gestion dynamique aléatoire de la tension d'alimentation, de la fréquence et de la tension de polarisation du substrat sur l'efficacité de la CPA ?
– Cette gestion dynamique aléatoire désignée par le terme RDVFS (Random DVFS) est-elle efficace comme cela est reporté dans [84] ?
– Est-il possible d'estimer de manière théorique l'effet de la RDVFS sur la CPA ?

Injection EM et RDVFS

– Qu'est-il possible de réaliser à l'aide de l'injection EM comme perturbation dans les circuits ?
– Quels sont les effets de variations de tension, de fréquence et de polarisation du substrat sur l'efficacité de l'injection EM ?

Chapitre 3

Gestion dynamique aléatoire de V_{dd}, F, V_{bb} et analyse SCA

Ce chapitre présente différentes méthodes permettant de diminuer la consommation des circuits. Une étude expérimentale des effets de ces méthodes sur l'attaque par analyse de corrélation a été réalisée. Cette étude expérimentale a par la suite été confirmée de manière théorique. Une légère modification de l'attaque par analyse de corrélation est proposé afin de diminuer l'impact des méthodes de diminution de la consommation sur la sécurité. Les travaux reportés dans ce chapitre ont fait l'objet d'une publication à FTFC2014.

3.1 Introduction

Les systèmes embarqués sont présents dans de nombreux domaines tels que l'aéronautique, les transports, les applications militaires. Cependant, le domaine dans lequel ils sont particulièrement répandus reste la téléphonie. Les téléphones mobiles ont énormément bénéficié de la miniaturisation des technologies intégrées avec les smartphones. En 2008, les smartphones ne représentaient que 8% du marché français. En 2014 ceux-ci représentaient une part de marché de 76%. Les smartphones sont maintenant de véritables petits ordinateurs disposant de processeurs, de mémoires et de plusieurs périphériques, dont les performances sont de plus en plus élevées afin de pouvoir exécuter un grand nombre

d'applications et c'est pourquoi, on peut se demander si les smartphones restent de simples téléphones.

Depuis quelques années une problématique devient de plus en plus importante : la consommation énergétique des systèmes embarqués. En effet, les performances des circuits intégrés ont fortement augmenté, ce qui a pour effet d'accroître la consommation en énergie de ceux-ci. Un grand nombre de systèmes fonctionnent à l'aide de batterie, bien que la technologie des batteries ait évolué, celle-ci n'a pas pu suivre l'évolution des circuits et par conséquent leur consommation. Afin de compenser cela, les fabricants de circuits ont du trouver des méthodes afin de diminuer et maitriser la consommation des circuits. Plusieurs méthodes ont ainsi été développées parmi lesquelles :

– la conception du systèmes multi-cœurs afin de répartir la tâche à effectuer sur plusieurs cœurs. Cela permet ainsi de ne pas trop augmenter la fréquence de fonctionnement et par conséquent de ne pas accroître la consommation dynamique de celui-ci,
– la polarisation de substrat ou body-biasing est une méthode qui permet d'améliorer le rapport énergie/performance, en contrôlant au mieux les courants de fuites dont l'importance est très sujette aux variations de *process* : polarisation qui peut être statique ou dynamique,
– la gestion dynamique des performances en fonction des besoins en calculs grâce à des techniques d'adaptation dynamique de la fréquence d'horloge, de la tension d'alimentation, regroupées sous le nom de DVFS pour 'Dynamic Voltage and Frequency Scaling'.

3.2 Body-biasing

Le *body-biasing* est une méthode qui permet de modifier la tension à laquelle un transistor passe d'un état bloqué à un état passant, c'est-à-dire la tension de seuil V_T. Afin que le transistor MOSfet soit passant, le potentiel V_{GS} doit être supérieur au potentiel V_T, avec V_{GS} la différence de potentiel entre la grille et la source du transistor MOSfet.

$$V_T = V_{T0} + \gamma(\sqrt{|2\Phi_F - V_{BS}|} - \sqrt{|2\Phi_F|}) \tag{3.1}$$

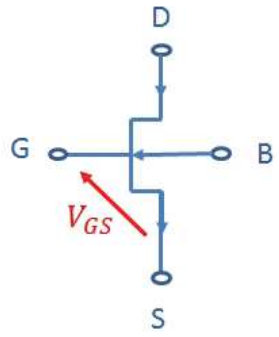

FIGURE 3.1: Transistor MOSfet à canal N

La tension V_T est définie par l'eq.3.1 dans laquelle V_{T0} représente la tension de seuil quand aucune tension n'est appliquée sur le substrat du transistor MOSfet. $2\Phi_F$ représente le potentiel de travail du transistor qui dépend de la densité d'électrons et de trous et enfin γ est un facteur dont la valeur dépend du dopage, de la permittivité du vide et de la valeur de la capacité d'oxyde de grille [85].

En examinant cette équation, dans le cas d'un transistor NMOSfet avec la source reliée à la masse, si une tension négative est appliquée sur le bulk, cela aura alors pour effet d'augmenter la tension de seuil V_T. Cet effet nommé le *Reverse Body Bias* (RBB) induit une diminution des courants de fuites et du courant à l'état passant. En appliquant une tension positive, la tension de seuil V_T diminue. Cet effet que l'on nomme *Forward Body Bias* (FBB), conduit à augmenter les capacités en courant des transistors, tant le courant en régime passant que les courants de fuites.

Le *body-biasing* permet ainsi de jouer sur la tension de seuil V_T d'un transistor et de faire varier la consommation statique des circuit. Celle-ci est définie de la façon suivante :

$$P_{stat} \propto \rho.V_{dd}^{\epsilon}.e^{-\kappa.\frac{V_T}{T}} \tag{3.2}$$

avec V_{dd} la tension d'alimentation du circuit, T la température du circuit et ϵ, κ et ρ des constantes dépendant des caractéristiques du circuit considéré et de la technologie considérée. Ainsi, une modification linéaire de la tension de seuil revient à modifier de manière exponentielle la consommation statique du circuit. D'où l'interêt de l'approche *body-biasing* pour compenser les variations des procédés de fabrication et finalement gérer le compromis performance/consommation.

3.3 Dynamic Voltage and Frequency Scaling

La technique *Dynamic Voltage and Frequency Scaling* (DVFS) est devenue une technique couramment employée lors de la conception des circuits. Elle consiste à faire varier la fréquence de fonctionnement et la tension d'alimentation du circuit en fonction des tâches à exécuter. Ainsi par rapport à la quantité de tâches à exécuter, il est possible de faire varier la consommation dynamique en fonction de la fréquence et de la tension d'alimentation :

$$P_{dyn} \propto C_{sw}.V_{dd}^2.f.a \tag{3.3}$$

avec C_{sw} étant la capacité moyenne à commuter à chaque cycle d'horloge, V_{dd} la tension d'alimentation, f la fréquence de fonctionnement du circuit et a un coefficient représentant l'activité moyenne du circuit. La DVFS permet ainsi de réduire la puissance dynamique de manière quadratique avec la tension d'alimentation et de manière linéaire avec la fréquence de fonctionnement. A noter aussi qu'une variation de V_{dd} permet de faire varier la consommation statique comme cela a été évoqué en 3.2.

Bien que la DVFS permette de diminuer la puissance dynamique et statique d'un circuit, le choix de la fréquence et de la tension d'alimentation doit être effectué judicieusement sous peine de générer des fautes temporelles. Ces fautes sont engendrées lorsque la fréquence de fonctionnement appliquée au circuit est trop grande pour la tension d'alimentation courante.

3.4 Impact sur la sécurité

La DVFS est une technique qui permet de trouver un bon compromis entre consommation et performance. En effet, elle permet d'ajuster la fréquence de fonctionnement du circuit en fonction de la tâche à exécuter et de l'énergie disponible. Pour cela, elle ajuste les paramètres V_{dd}, F, V_{bb}, de sorte à adapter la consommation du circuit mais pas uniquement. En effet :

– la variation de V_{dd} a un effet sur le temps de transition et des délais de propagation des portes logiques d'un circuit comme cela est montré dans [41],

– la variation de F, a quant à elle un impact sur le temps de calcul des tâches devant être exécutées,
– la variation de la tension de polarisation du substrat (V_{bb}) a pour effet de faire varier le temps de transition et les délais de propagation des portes logiques. A noter que cette variation est bien moins importante que celle relative à une même variation de V_{dd}.

Comme évoqué précédemment, les attaques par canaux cachés exploitent les informations contenues dans les courbes de consommation ou les traces EM pour retrouver la clé de chiffrement utilisée. Les variations de V_{dd} et F génèrent deux types de modifications sur les traces de consommation exploitées par les attaques. La principale est de créer une désynchronisation entre les traces. Ainsi pour deux traces de consommation relatives à un même chiffrement, les fuites d'informations ne se situeront pas aux mêmes instants. Une variation de fréquence crée un décalage temporel bien plus important sur les traces de consommation qu'une variation de tension (à fréquence constante).

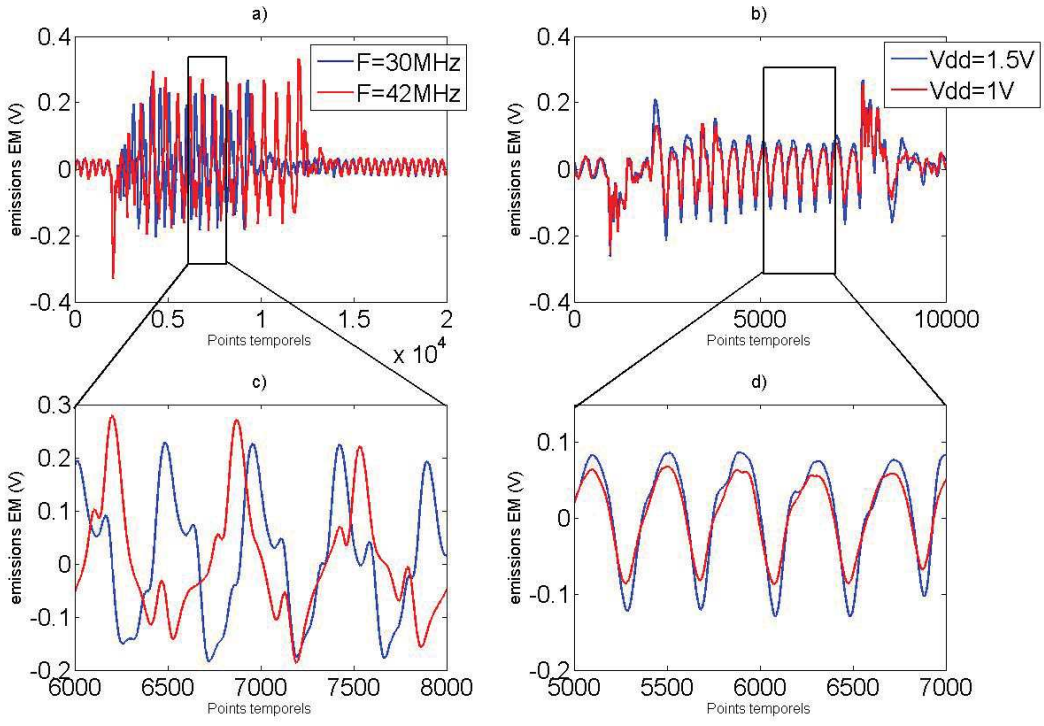

FIGURE 3.2: (a) et (c) rayonnement EM relatif à un chiffrement AES pour $F = 30MHz$ et $F = 42MHz$, (b) et (d) rayonnement EM relatif à un chiffrement AES pour $V_{dd} = 1V$ et $V_{dd} = 1.5V$

En effet, pour des traces de consommation échantillonnées à $20GS/s$ une variation de plusieurs MHz induit un décalage temporel d'au moins 100 points (5ns) tandis qu'une

variation de $100mV$ de V_{dd} crée un décalage inférieur à 10 points comme on peut l'observer sur les Fig. 3.2.a et Fig. 3.2.c
Le second effet induit est une déformation en amplitude des traces de consommation ou des traces EM. Cette déformation est due aux variations de la tension d'alimentation, qui réduit la tension grille source et drain source des transistors et donc altère significativement la consommation instantanée du circuit. Cet effet est observable sur les Fig. 3.2.b et Fig. 3.2.d

Ces décalages ont un impact sur l'efficacité des attaques par canaux cachés comme indiqué dans [32, 86]. Il a ainsi été proposé dans [84] d'utiliser la DVFS comme contremesure aux attaques par canaux cachés et plus particulièrement à la DPA. Celle-ci renommée RDVFS pour l'occasion revient à faire varier la fréquence et la tension d'alimentation de manière aléatoire. Pour chaque chiffrement AES, une valeur de fréquence et une valeur de tension sont alors attribuées. On nommera ces choix un couple (V, F). Le but de la RDVFS est alors d'avoir un nombre maximal de couples différents afin de créer le plus grand nombre de conditions de fonctionnement différents et donc de décalages temporels. Le nombre de couples est toutefois limité et défini lors de la conception du circuit afin que le circuit reste toujours fonctionnel y compris pour le couple $(Vmin, Fmax)$.

La Fig. 3.3 montre l'effet de la RDVFS sur des traces électromagnétiques. Sur la Fig. 3.3a, on peut observer très clairement le chiffrement AES car un seul couple (V,F) y est appliqué. La Fig. 3.3b montre, quant à elle, des chiffrements AES lorsque la RDVFS est appliquée avec 11 couples (V,F) différents. Il n'est plus alors possible de distinguer clairement, et donc de séparer à l'oeil nu, les rondes de l'AES. Pour la Fig. 3.3a la tension d'alimentation a été fixée à $V_{dd} = 1.2V$ et la fréquence à $F = 62MHz$. Pour la Fig. 3.3b, $V_{dd} \in \{1, 1V, 1.2V, 1.3V\}$ et $F \in \{62, 57, 51, 45, 42, 38, 30, 23, 21\}$ MHz.

Afin de connaître exactement l'effet de la RDVFS sur la CPA, l'effet des seules variations de tension d'alimentation a tout d'abord été étudié (RDVS). Puis l'étude de l'effet de variations de fréquence seules a été analysé (RDFS). Enfin, c'est l'impact de la RDVFS sur l'efficacité de la CPA qui a été traité.

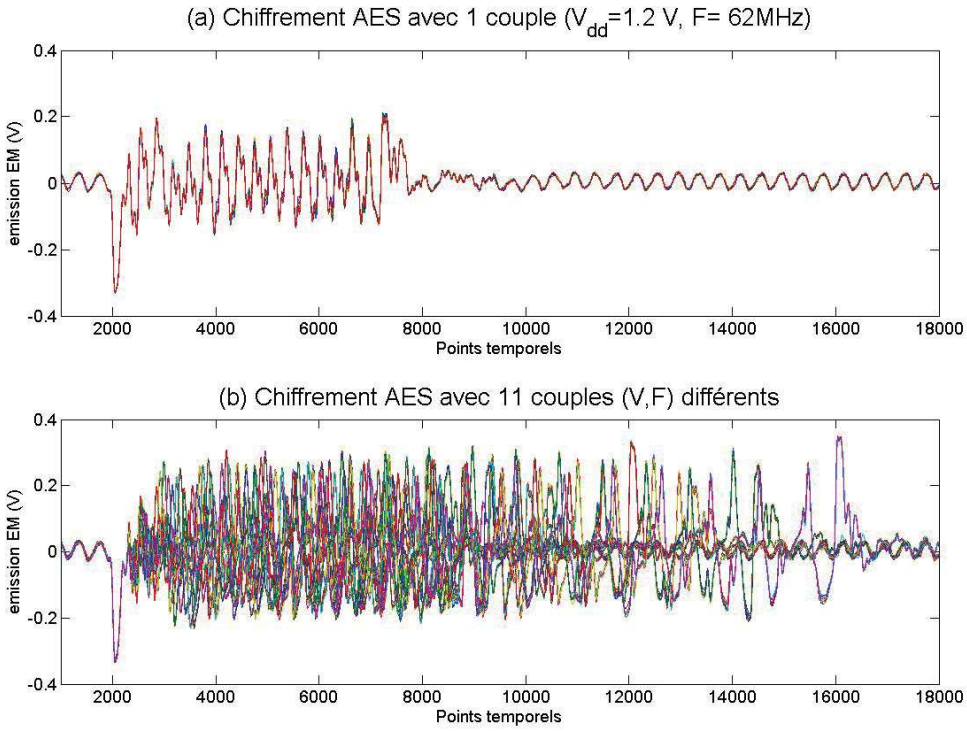

FIGURE 3.3: (a) Chiffrement AES avec (V,F) = (1.2V, 62MHz) fixe, (b) Chiffrement AES avec 11 couples (V,F) différents

3.4.1 Impact de la tension d'alimentation sur la CPA

Afin d'étudier l'effet d'une variation de tension, trois jeux de traces EM ont été collectés au-dessus d'un AES intégré dans un FPGA successivement alimenté par une tension d'alimentation de 1.1V, 1.2V et 1.3V. Afin que la fréquence du circuit ne soit pas perturbée par le changement de la tension d'alimentation, celle-ci est fournie par un quartz situé sur la carte du FPGA. Ce quartz est cadencé à une fréquence de 50MHz. Suite à cette collecte de traces EM, connaissant la clé de chiffrement utilisée par l'AES, la Fig. 3.4 a été tracée. On peut y observer, pour les trois valeurs de Vdd, les allures des traces EM associées aux différentes valeurs de distance de Hamming (HD) calculées en prenant pour cible la Sbox1 de la 9ème ronde de l'AES.

Comme on peut le constater, les traces EM obtenues sont similaires. Seules les amplitudes changent légèrement avec les variations de Vdd de $\pm 100mV$. On peut aussi s'apercevoir qu'avec l'oscilloscope (20GS/s, 3.5GHz) utilisé pour les acquisitions EM, aucune désynchronisation importante n'est visible. Seule une très légère désynchronisation de moins de 20 échantillons est présente et visible en fin de cycle d'horloge.

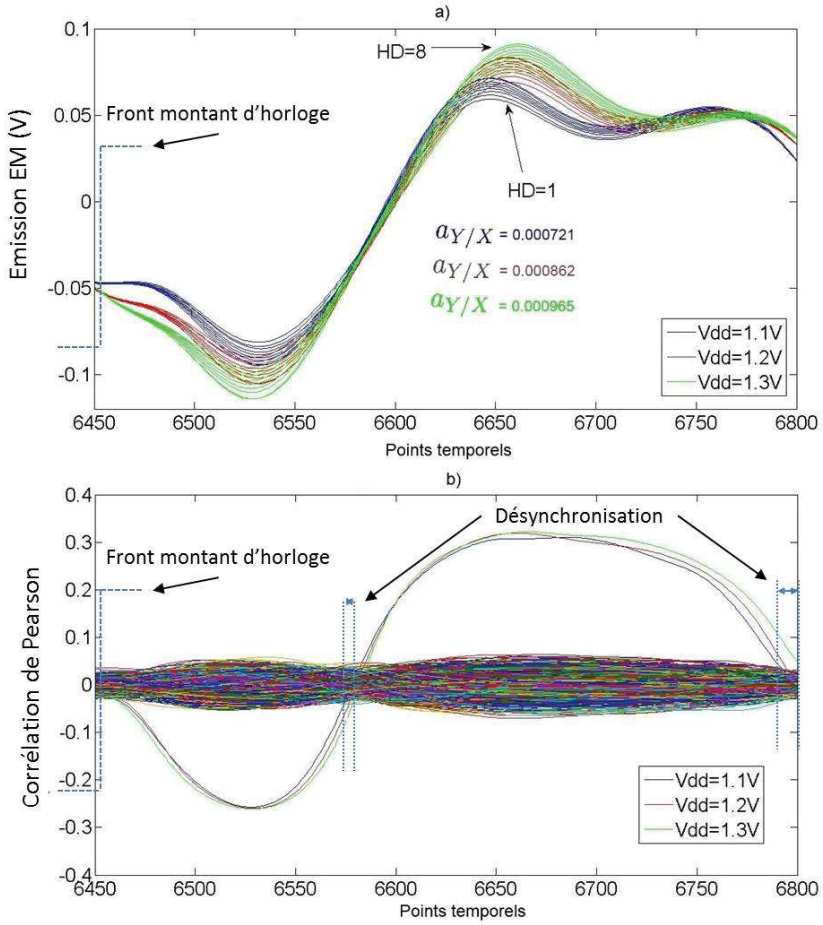

FIGURE 3.4: (a) Traces EM d'un AES pendant la fuite d'information pour trois valeurs de V_{dd} différentes, (b) valeurs de corrélation considérées par la CPA pour trois valeurs de V_{dd} différentes

Afin d'estimer les éventuelles altérations de la fuite, les trois pentes des droites de régression $\alpha_{Y/X}$ entre les mesures et la distance de Hamming ont été calculées pour chaque jeu de courbes. Comme on peut le constater sur la Fig. 3.4a, cette pente augmente en fonction de Vdd. Des caractérisations avec cinq valeurs de Vdd ont ainsi montré que le coefficient directeur de la droite de régression varie linéairement en fonction de Vdd comme cela est reporté sur la Fig. 3.5. On peut donc en déduire que la randomisation de la tension d'alimentation n'annihile en rien la fuite et se traduit pour la CPA par une randomisation de faible variance de la corrélation sans en modifier le signe qui lui est fixé par la covariance.

La Fig. 3.4b, représente les résultats de plusieurs attaques CPA effectuées pour chacune des valeurs de V_{dd} considérées. On y retrouve l'évolution des corrélations dans le temps pour toutes les hypothèses sur la clé. Cette figure confirme ainsi les conclusions qui ont été tirées de la Fig. 3.4a. En effet, on peut aisément distinguer les trois

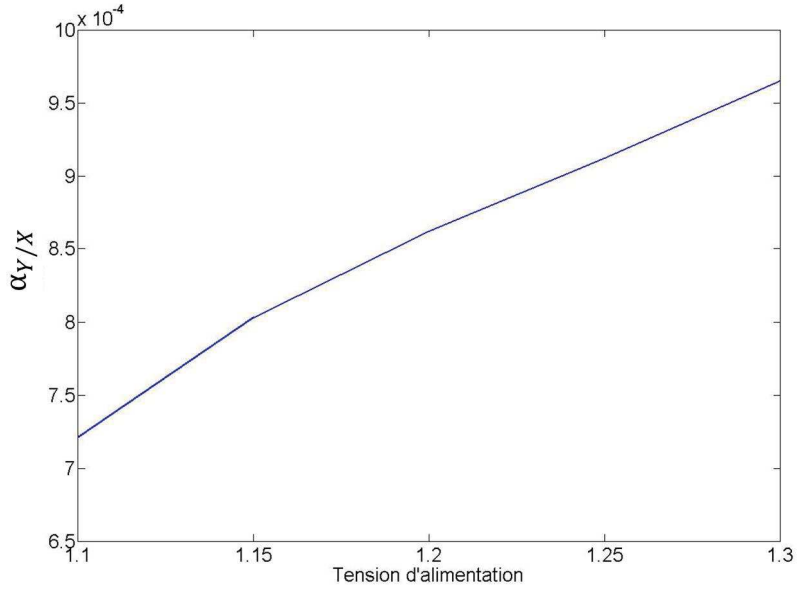

FIGURE 3.5: Coefficient $\alpha_{Y/X}$ en fonction de la valeur de V_{dd}

courbes de corrélations associées à la bonne hypothèse de clé pour les trois valeurs de V_{dd} considérées. On peut aussi observer que l'altération de la corrélation reste de faible valeur pour des écarts de tension de 200mV et que la désynchronisation visible en fin de trace n'excède pas 20 échantillons (1ns). On note également que cette désynchronisation reste nulle lors des fronts montants d'horloge (point temporel 6450).

On peut donc conclure que les variations aléatoires de Vdd seules n'apportent que peu de protection contre les attaques CPA lorsque la fréquence de fonctionnement du circuit est fournie par un générateur d'horloge qui n'est pas influencé par la variation d'alimentation.

De nos jours, les SoC ou les cartes à puce disposent de générateur d'horloge interne à base de *Phase Locked Loop* (PLL). C'est ce qui permet d'ailleurs de rendre obsolètes les attaques par glitch d'horloge. S'il y a une variation de tension, la PLL est alors elle-même affectée par ce changement de tension. Afin d'étudier ce cas là, le même FPGA contenant l'AES a été utilisé sauf que cette fois-ci, la fréquence d'horloge a été générée sur le circuit à partir d'un oscillateur en anneau. La communication RS232 du circuit qui permet de communiquer avec le monde extérieur doit avoir une fréquence parfaitement fixe. Pour effectuer cela, la machine d'état du circuit et la communication du circuit sont

alors reliées à l'horloge fournie par le quartz externe. L'AES est donc rendu asynchrone est lui seul est relié à l'oscillateur en anneau.

Comme on peut le voir sur la Fig. 3.6a, l'oscillateur en anneau fournissant le signal d'horloge du bloc AES est altéré par ce changement. En effet, une désynchronisation des traces de consommation est apparue. On peut ainsi observer que pour une tension d'alimentation de 1.3V la fréquence de fonctionnement est de 47MHz, tandis qu'avec une tension d'alimentation de 1.1V la fréquence prend une valeur de 41MHz. La Fig. 3.6b rapporte les résultats de plusieurs attaques CPA effectuées pour chacune des valeurs de V_{dd}. On observe l'évolution des corrélations dans le temps pour toutes les hypothèses sur la clé de chiffrement. On peut ainsi constater que la fuite d'information a été déplacée dans le temps mais garde la même forme. Tout comme les coefficients $\alpha_{Y/X}$ présents sur la Fig. 3.4a, les coefficients $\alpha_{Y/X}$ de la Fig. 3.6a varient linéairement en fonction de la tension V_{dd}. A noter que les coefficients présents sur la Fig. 3.6a sont plus élevés que ceux de la Fig. 3.4a car dans les traces EM de la Fig. 3.6a ont été converties au format char contrairement a celles de la Fig. 3.4a.

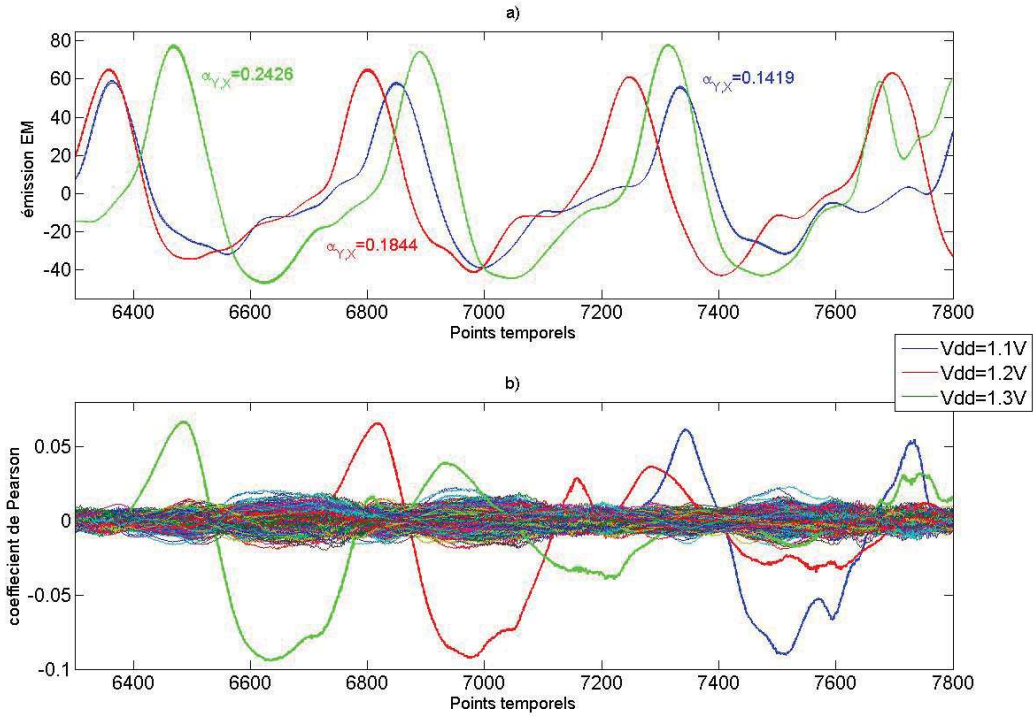

FIGURE 3.6: (a) Traces EM d'un AES pendant la fuite d'information pour trois valeurs différentes de V_{dd} , (b) valeurs de corrélation considérées par la CPA pour trois valeurs de V_{dd}

On peut donc en conclure que les variations aléatoires de V_{dd} peuvent générer plusieurs effets.
Le premier est une faible modification de l'amplitude des émissions EM du circuit. Cependant, la forme globale des émissions EM reste inchangée. Cet effet n'a aucun impact notable sur l'efficacité de la CPA. Cela peut s'expliquer par le fait que la zone temporelle où la fuite d'information se produit reste inchangée et que la fuite d'information n'est pas altérée, ou très faiblement, par le changement de tension.
Le second effet est une modification de la fréquence d'horloge. Cet effet apparait seulement si le bloc générant l'horloge est interne et donc lui même affecté par la variation de V_{dd}. Cet effet peut être expliqué par le fait que les temps de transition et les délais des portes logiques sont liés à la tension d'alimentation du circuit. En ayant une modification de la fréquence d'horloge du circuit, la fenêtre temporelle où la fuite d'information se produit est ainsi affectée.

3.4.2 Impact de la fréquence sur la CPA

Dans cette partie, l'impact d'une variation de fréquence sur la CPA est étudié. Pour cela, des traces EM ont été collectées sur un AES implémenté dans un FPGA. La tension d'alimentation du FPGA est fixée par le régulateur à 1.2V. Le signal d'horloge de l'AES est choisi aléatoirement parmi les sorties de plusieurs oscillateurs en anneau intégrés dans le FPGA. Ces derniers oscillent respectivement à 45, 40, 33, 30, 27 et 25MHz.

La Fig. 3.7a représente les traces EM de l'AES fonctionnant à des fréquences de 30MHz et 27MHz. Comme on pouvait s'y attendre, une désynchronisation de $\Delta t = 50ns$ (1000 points temporels des traces échantillonnées à 20GS/s) des traces de consommation est apparue. En effet, les points de fuites ont été déplacés dans le temps d'une valeur Δt. Les coefficients de la régression linéaire $\alpha_{Y/X}$ n'ont pas, quant à eux, été affectés par ce décalage. On peut donc en déduire que la fuite d'information n'a pas été supprimée mais juste étalée dans le temps. Elle garde d'ailleurs sensiblement la même forme.

La Fig. 3.7b confirme les conclusions obtenues à l'aide de la Fig. 3.7a. En effet, l'évolution des courbes de corrélation pour les deux fréquences considérées sont très similaires. Cependant celles-ci sont décalées dans le temps d'une valeur $\Delta t = 50ns$.

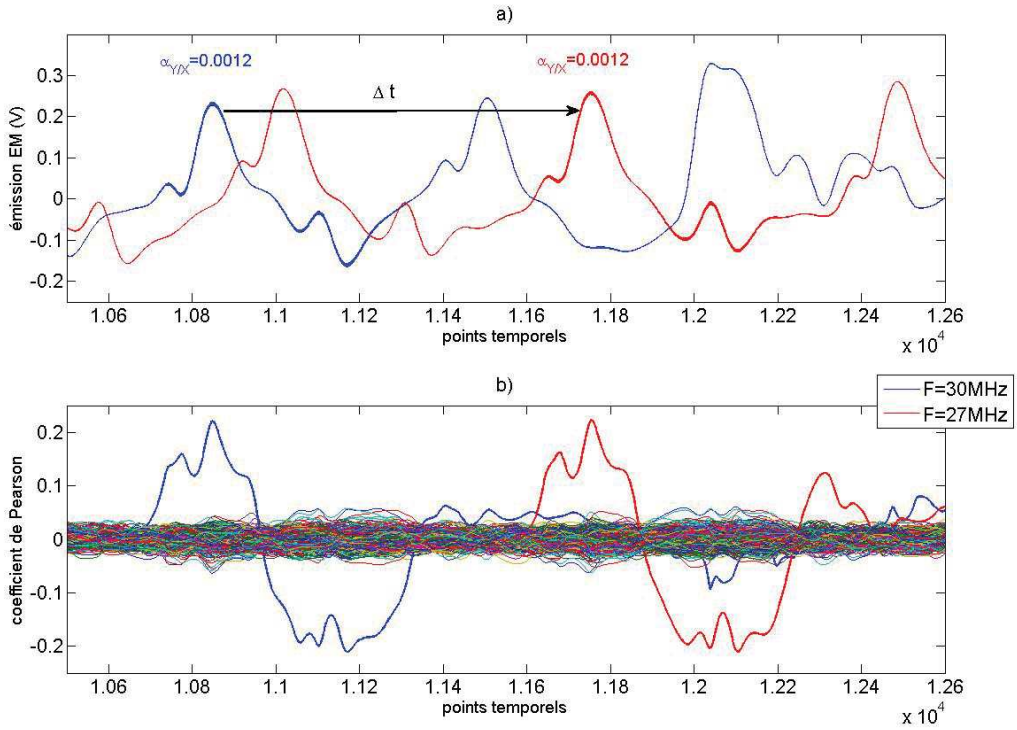

FIGURE 3.7: (a) Traces EM d'un AES pendant la fuite d'information avec deux valeurs différentes de F, (b) valeur de corrélation pour des attaques CPA avec deux valeurs différentes de F

La variation de fréquence a donc pour effet de distribuer la fuite d'information dans le temps tout comme la variation de tension lorsque celle-ci affecte la valeur de la fréquence d'horloge. La fréquence d'horloge est affectée lorsque la génération du signal d'horloge est interne au circuit, ce qui est un cas très fréquent dans le monde de la carte à puce. On peut donc en déduire que la variation de fréquence est utilisée pour des décalages dans le temps assez importants, tandis que la variation de tension peut décaler de manière plus fine et complémentaire la fuite d'information ; complémentaire dans le sens où il devient possible de créer plus de conditions de fonctionnement différentes, c'est à dire de valeurs de décalage temporel de la fuite.

3.4.3 Impact de la tension de polarisation de substrat sur la CPA

Dans cette partie, l'impact d'une variation de fréquence sur la CPA est étudié. Pour étudier cet effet, il est nécessaire de disposer d'un circuit dont la tension de polarisation de substrat est contrôlable. Le FPGA utilisé précédemment pour l'étude des effets des variations de tension et de fréquence n'offre pas la possibilité de contrôler la polarisation

de substrat. Un nouveau circuit a donc été utilisé pour mener ces expérimentations. Ce circuit est un micro-contrôleur 32bits conçues en technologie 90nm disposant d'un bloc AES implémenté matériellement. Afin d'évaluer son impact, trois valeurs différentes de polarisation de substrat positives (FBB) ont été utilisées (0mV, 200mV, 400mV).
Il est à noter que la tension de polarisation de substrat n'est pas effective sur la totalité du circuit. Le bloc *Phase Locked Loop* (PLL), qui a pour fonction de générer le signal d'horloge, a une tension de polarisation de 0mV qui ne peut pas être changée. Cela implique que le signal d'horloge du circuit ne sera pas affecté par le changement de la tension de polarisation du substrat.

La Fig. 3.8.a représente les traces EM de l'AES fonctionnant avec des valeurs de polarisation de substrat de 0mV, 200mV et 400mV. On peut observer que la polarisation de substrat crée un léger décalage temporel de 10 points (500ps) entre les traces EM. Le coefficients $\alpha_{Y/X}$ pour une polarisation de substrat de 400mV est de signe négatif tandis que pour une polarisation de substrat de 200mV et 0mV ceux-ci sont positifs. On peut donc en déduire que l'instant ou a lieu la fuite d'information a été affecté par ce changement.
Sur la Fig. 3.8.b, on peut observer les évolutions des courbes de corrélation dans le temps pour les trois valeurs de polarisation de substrat. On peut s'apercevoir que la fuite d'information pour une polarisation de substrat de 200mV et 0mV se produit au même moment sur les traces EM (en tenant compte de la légère désynchronisation naturelle du circuit probablement due à la gigue des PLL). Pour une polarisation de substrat de 400mV, l'instant ou se produit la fuite d'information n'est pas le même (lobe positif pour 400mV et lobe négatif pour 200mV et 0mV). L'explication de ce phénomène nous est inconnue et n'a pas pu être identifiée car nous ne disposons pas des informations nécessaires sur le design et le comportement du circuit (information confidentielle du fondeur du circuit).

3.4.4 RDVFS

Étant donné l'impact de changements de fréquence, de tension d'alimentation et de polarisation de substrat sur le fonctionnement des circuit, il devient donc possible de prédire que la contre-mesure RDVFS a pour effet d'altérer la fuite d'information en l'éparpillant dans le temps, mais elle ne la supprime en aucun cas.

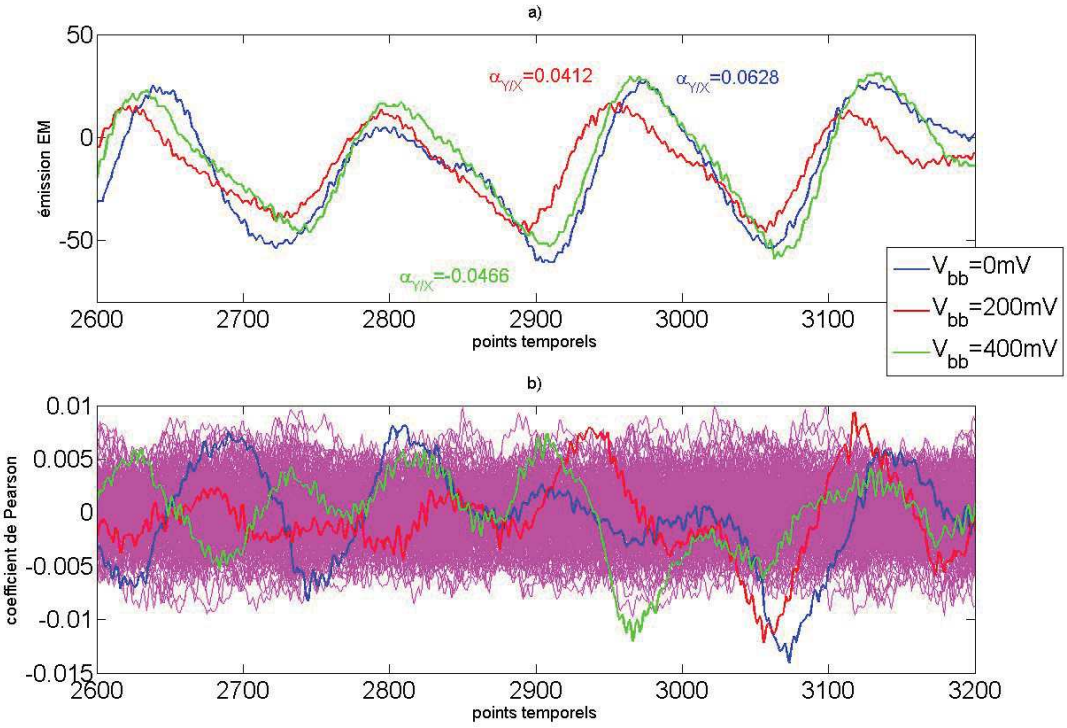

FIGURE 3.8: (a)Traces EM d'un AES pendant la fuite d'information pour trois valeurs différentes de V_{bb}, (b) corrélations considérées par la CPA pour trois valeurs différentes de V_{bb}

A partir du désalignement des traces de consommation introduit par un changement de tension ou de fréquence, l'analyse des courbes de corrélation obtenues avec des valeurs aléatoires de V et F fait apparaitre trois types de fuite d'information sur les traces EM.

– cas n°1 : c'est le cas où une fuite d'information, associée à un couple (V, F) ayant une corrélation positive ou négative, se produit au même moment qu'une fuite d'information associée à d'autres couples (V, F). On peut alors définir les mesures de corrélation dans le temps pour la totalité des couples (V, F) utilisés comme :

$$\rho(t) = f^n(\rho_p(t), \rho_n(t), \rho_{nc}(t)) \tag{3.4}$$

avec $\rho(t)$ l'évolution de la corrélation dans le temps lorsque tous les couples (V, F) sont utilisés. Chaque couple (V, F) apporte alors à l'instant t une fuite d'information corrélée positivement $(\rho_p(t))$ ou négativement $(\rho_n(t))$ ou non corrélée $(\rho_{nc}(t))$.

– cas n°2 : c'est le cas où pour l'ensemble des couples (V, F) utilisés, un seul couple véhicule une fuite d'information :

$$\rho(t) = f^n(\rho_p(t), \rho_{nc}(t)) \tag{3.5}$$

ou

$$\rho(t) = f^n(\rho_n(t), \rho_{nc}(t)) \tag{3.6}$$

la corrélation du couple (V, F) portant la fuite d'information est tant alors positive $(\rho_p(t))$ ou négative $(\rho_n(t))$. Il faut remarquer que ce cas apparait nécessairement à la fin ou au début de la fenêtre de chiffrement en présence de RDVFS et que les couples qui transportent l'information sont les couples en limite de fonctionnement définis par le concepteur du circuit ($\{V_{max}, F_{max}\}$ et $\{V_{min}, F_{min}\}$).

– cas n°3 : il s'agit du cas où pour la totalité des couples (V, F) utilisés, aucun d'eux ne véhicule de fuite d'information :

$$\rho(t) = \rho_{nc}(t) \simeq 0 \tag{3.7}$$

Afin de visualiser ces trois cas, un AES a été implémenté sur un FPGA. En configurant la tension d'alimentation et la fréquence du circuit, six couples (V, F) ont pu être utilisés. Pour chacun de ces couples, 10000 traces EM ont été collectées puis une attaque CPA a été effectuée sur chacun d'eux afin d'obtenir la trace de corrélation pour la bonne hypothèse de clé pour chaque couple. Le signal d'horloge de l'AES est généré en interne afin que celui-ci soit affecté par le changement de tension d'alimentation comme évoqué en 3.4.1. Les couples utilisés ont une fréquence de 65, 55, 54, 41, 39 et 29MHz.

Sur la Fig. 3.9a sont représentées les traces de corrélation pour toutes les hypothèses sur la valeur d'une sous-clé en considérant les couples (V, F) séparément. On peut ainsi y distinguer la bonne hypothèse pour chacun des couples (V, F). Afin de simuler le principe de la RDVFS, les traces EM collectées pour chaque couple (V, F) ont été mélangées afin d'obtenir un ensemble de 60000 traces EM correspondant à un fonctionnement RDVFS avec six couples (V, F) différents.

La Fig. 3.9b représente l'évolution des courbes de corrélation quand les 60000 traces EM sont utilisées pour une attaque CPA. On peut ainsi visualiser sur la Fig. 3.9b que l'évolution de la courbe de corrélation obtenue à partir d'une CPA avec l'ensemble des traces dépend de l'évolution des corrélations acquises pour chaque couple (V, F) utilisé. Il existe donc un lien entre les courbes de corrélation pour l'hypothèse de la bonne sous clé sur la Fig. 3.9a et celle que l'on observe sur la Fig. 3.9b. Ce lien est analysé dans la section suivante.

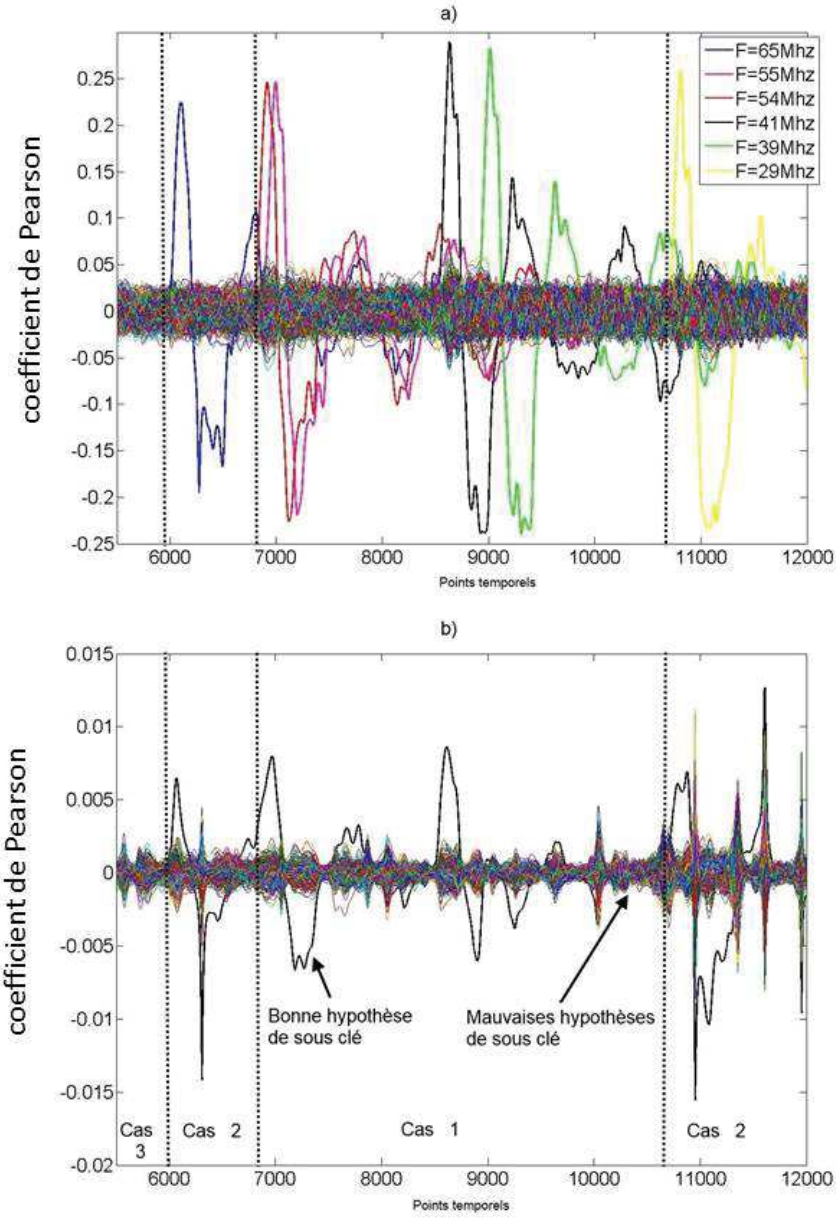

FIGURE 3.9: (a)Évolution de la corrélation associée à chaque hypothèse de sous clé pour les six couples (V, F) pris séparément, (b) évolution de la corrélation associée à chaque hypothèse de sous clé lorsque la RDVFS est activée avec les six couples (V, F)

3.4.5 Explication théorique

Comme cela a été évoqué, le principal atout de la RDVFS contre les attaques de type CPA est la dilution de la fuite d'information dans le temps par désynchronisation. Cette dernière peut être plus ou moins importante en fonction de la modification qui est effectuée. Cette dilution de la fuite d'information peut être induite par une modification de la tension d'alimentation (V_{dd}), de la Fréquence de fonctionnement (F) du circuit ou alors par la modification de la polarisation de substrat (V_{bb}). L'ensemble des échantillons temporels $\chi(t)$ d'un jeu de traces peut alors être exprimé de la façon suivante :

$$\chi(t) = \cup_{(i,j)}\chi_{(V_i,F_j)}(t) = \cup_I \chi_I(t) \tag{3.8}$$

avec (i,j) étant les index permettant de numéroter les couples (V_i, F_j) ou encore I l'indice des index (i,j).

Sachant que l'attaque CPA s'appuie sur le calcul du coefficient de corrélation de Pearson $\rho(X,Y)(t)$, nous avons calculé ce dernier dans le cas où les observations appartiennent à différents ensembles $\chi_{(V_i,F_j)}(t)$, sachant que les prédictions Y restent inchangées, ce qui est le cas lors de la RDVFS. Conformément aux eq. 2.11, ces calculs nous ont permis d'évaluer l'espérance $E(X(t)) = E(\cup_I X_I(t))$, la covariance $cov(X(t),Y) = cov(\cup_I X_I(t), Y)$ et la variance $var(X(t)) = var(\cup_I X_I(t), Y)$ de ce mélange de traces :

$$E(X(t)) = \sum_I \{p_I.E(X_I(t))\} \tag{3.9}$$

$$cov(X(t),Y) = \sum_I \{p_I.cov(X_I(t), Y_I)\} \tag{3.10}$$

$$\begin{aligned} Var(X(t)) &= \sum_{I=1}^{n} \{p_I.Var(X_I(t)) - E^2(X_I(t)).p_I(p_I-1)\} \\ &- \sum_{1\leq I<J}^{n} \{2.(p_I.p_J.E(X_I(t)).E(X_J))\} \end{aligned} \tag{3.11}$$

où p_I est la fréquence d'apparition (n_I/n) du couple de tension fréquence (V_i, F_i) et n le nombre de couples différents. Ceci conduit alors à l'expression du coefficient de corrélation ci-dessous. Cette dernière permet de calculer l'évolution du coefficient de Pearson dans le cas de la RDVFS.

$$\rho_{max}(X(t), Y) = \frac{\sum_I \{p_I.cov(X_I(t), Y_I)(t)\}}{\sqrt{var(X(t)).Var(Y)}} \tag{3.12}$$

Comme on peut le voir au dénominateur, la RDVFS atténue la fuite en moyennant les covariances d'échantillons $X_I(t)$ corrélées positivement avec Y ($cov(X_I(t), Y_I)(t) > 0$), négativement ($cov(X_I(t), Y_I)(t) < 0$) et ne portant pas de fuite d'information ($cov(X_I(t), Y_I) = 0$). Cette atténuation est essentiellement assurée par les décalages temporels introduits par les variations de fréquence et, dans une moindre limite, par celles de la tension qui affectent les temps de propagation des signaux.
On notera tout de même, que cette atténuation n'est effective que si et seulement si le choix des n couples (V_i, F_i) est tel qu'il n'existe aucun ensemble d'échantillon $X(t)$ tel qu'un grand nombre de covariances, $cov(X_I, Y_I)(t)$, soient de même signe a un instant t quelconque. C'est une condition qui, si elle n'est pas respectée, limite très significativement, voire annihile l'apport de la RDVFS. Sa satisfaction doit donc être garantie lors de la phase de conception par un choix judicieux des couples (V, F).

Toutefois, compte tenu du comportement temporel des portes logiques CMOS, et malgré le soin apporté à la conception, il existera toujours des échantillons pour lesquels un sous-ensemble de traces sera corrélé positivement ou bien négativement avec Y, tandis que le reste des échantillons ne portera que peu ou pas de fuites d'informations ($(cov(X_I(t), Y_I) \simeq 0)$). Ces échantillons correspondent aux décalages temporels minimal et maximal introduits par la RDVFS, i.e. aux couples (V_{max}, F_{max}) et (V_{min}, F_{min}). Si l'on suppose que le choix des (V_i, F_j) a été effectué pour que le dénominateur de l'eq. 3.12 soit nul ou alors très faible pour tous les autres types d'échantillons, alors les couples (V_{max}, F_{max}) et (V_{min}, F_{min}) fixent la limite en terme de robustesse de la contre-mesure RDVFS. La corrélation maximale qui est alors observable est égale à :

$$\rho(X(t), Y) = \frac{p_L.cov(X_L(t), Y_L)}{\sqrt{var(X(t)).Var(Y)}} \tag{3.13}$$

avec $L = \{V_{max}, F_{max}\}$ ou $\{V_{min}, F_{min}\}$ et $cov(X_M(t), Y_M)(t) = 0$ pour $M \neq L$ et avec t instants correspondants à la première ou dernière ronde

Compte tenu de cette limite et afin d'être plus explicite du point de vue de la robustesse de la RDVFS à la CPA, le nombre supplémentaire de traces de consommation permettant de retrouver la clé peut être estimé. Pour cela l'utilisation de l'eq. 3.14 de S. Mangard [87] permet d'effectuer une estimation du nombre S de courbes nécessaires pour retrouver la clé de chiffrement lors d'un chiffrement dit classique (V et F sont des constantes).

$$S = 3 + 8\left(\frac{Z_\alpha}{ln(\frac{1+\rho_{max}}{1-\rho_{max}})}\right)^2 \tag{3.14}$$

Ce calcul nous a permis d'aboutir à la définition du rapport suivant :

$$\sqrt{\frac{S_n}{S_1}} \approx \frac{ln(\frac{1+\rho_{max}}{1-\rho_{max}})}{ln(\frac{1+\frac{\rho_{max}}{n}}{1-\frac{\rho_{max}}{n}})} \tag{3.15}$$

où S_n est le nombre de courbes nécessaires pour retrouver la clé de chiffrement, k_0 en présence de la RDVFS avec n couples (V, F) et où S_1 est le nombre de courbes nécessaires pour retrouver la clé de chiffrement k_0 lorsque $n = 1$. Après un développement de Taylor, ce rapport peut être approximé par :

$$\sqrt{\frac{S_n}{S_1}} \approx \frac{3.n^2 + \frac{n^3.\rho_{max}^2}{3}}{3.n^2 + \rho_{max}^2} \propto n \tag{3.16}$$

on peut donc estimer que l'accroissement de robustesse ($\frac{S_n}{S_1}$) apporté par la contre-mesure RDVFS est proportionnel à n^2, où n est le nombre de couples (V, F) mis en jeux par la RDVFS.

3.5 Attaque CPA sur la contre-mesure RDVFS

Afin de vérifier la validité du raisonnement qui a été présenté précédemment, des attaques CPA ont été effectuées sur un circuit disposant de la contre-mesure RDVFS. Ce circuit est un FPGA spartan3 sur lequel un AES a été implémenté. Le régulateur de tension du FPGA qui se trouve sur la carte, a été supprimé afin de pouvoir contrôler la tension du cœur du FPGA à l'aide d'une alimentation stabilisée externe controlable par communication RS232. La plage de tension d'alimentation est comprise entre 0.96V et 1.5V avec un pas de 50mV. L'AES doit avoir une fréquence de fonctionnement qui doit être configurable. Pour cela un oscillateur en anneau (Fig. 3.10) fonctionnant avec plusieurs fréquences de fonctionnement différentes a été implanté. Les fréquences disponibles sont comprises entre 29MHz et 80 MHz. Afin de n'avoir aucun problème sur le chemin critique, l'AES a été conçu pour fonctionner à 100MHz. Sur ce FPGA, il n'est pas possible de modifier la tension de polarisation du substrat. Seules des variations de tension et de fréquence sont effectuées par ce circuit. Pour la communication avec le PC, il est nécessaire de définir un débit constant, cela n'est pas possible si la fréquence de fonctionnement est variable. Afin de résoudre ce problème, la machine d'état et la communication série implémentée sur le FPGA sont cadencées à une fréquence constante de 50MHz fournie par un quartz extérieur. L'AES est alors rendu asynchrone par rapport au reste du circuit.

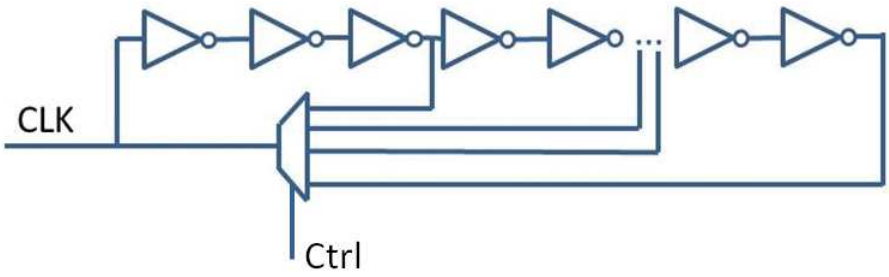

FIGURE 3.10: Oscillateur en anneau fournissant le signal d'horloge à l'AES.

Les traces EM utilisées pour les attaques CPA ont été collectées à l'aide du banc d'acquisition représenté sur la Fig. 2.5. L'amplificateur visible sur la figure est un amplificateur faible bruit (40dB) disposant d'une bande passante de $1MHz - 200MHz$. Le choix de cet amplificateur a été fait en suivant les recommandations relatives aux mesures de traces d'émissions EM dans [78]. La sonde utilisée pour l'acquisition des traces est une sonde faite maison composée d'un cœur de ferrite qui favorise la collecte des ondes EM

en basse fréquence. L'oscilloscope utilisé, dispose d'un taux d'échantillonnage de 20GS/s, d'une bande passante de 3.5GHz et d'une résolution verticale de 8 bits.

Pour chaque couple (V, F) pour lequel l'AES a été utilisé, 10.000 traces EM ont été acquises sur le banc d'acquisition. Les traces EM ainsi récupérées ont alors été mélangées de manière aléatoire afin de créer un jeu de données qui pourrait être obtenu lorsque la RDVFS est appliquée sur un circuit. Afin de vérifier que la robustesse de la RDVFS dépend du nombre de couples utilisés, 11 jeux de traces différents ont été constitués pour lesquels le nombre n de couples (V, F) est compris entre 1 et 11.

Des attaques CPA ont alors été lancées sur chacun de ces 11 jeux de mesures. Afin de valider l'approche théorique qui a été effectuée, le rapport de l'eq. 3.16 a alors été calculé à partir des résultats expérimentaux, puis à l'aide de l'eq. 3.12 et de l'estimation S (eq. 3.14) fournie par Mangard [87], une courbe d'estimation a été fournie.

La Fig. 3.11 représente l'évolution du rapport de robustesse ($\frac{S_n}{S_1}$) en fonction du nombre de couples (V, F) utilisés. On peut remarquer que la courbe bleue représentant l'évolution du coefficient de robustesse de la RDVFS est proche de la courbe noire représentant la fonction n^2. La courbe verte est l'application de l'eq. 3.14 qui confirme les résultats obtenus avec la RDVFS.

Afin de confirmer les conclusions obtenues en section 3.4.1, un AES fonctionnant avec une fréquence d'horloge fournie par un quartz a aussi été implémenté. La courbe rouge montre que le rapport de robustesse reste très proche de 1 pour n'importe quelle valeur de n. Cela étaye encore une fois les conclusions de la section 3.4.1.

Si les expérimentations qui ont été effectuées permettent de confirmer que la RDVFS augmente la robustesse d'un rapport n^2, dans le cas d'un AES implémenté sur un FPGA, une validation sur un micro-contrôleur de 32 bits a également été réalisée. Celui-ci est conçu en une technologie de 90nm. Il dispose d'un régulateur interne contrôlable qui permet d'affecter la tension d'alimentation à l'une des valeurs suivantes : 1.13V, 1.26V ou 1.32V. La fréquence de fonctionnement du circuit est contrôlée par une PLL configurable. Sur ce circuit, il est possible de modifier la tension de polarisation de substrat à partir de commandes prédéfinies par le concepteur du circuit. Les valeurs de polarisation

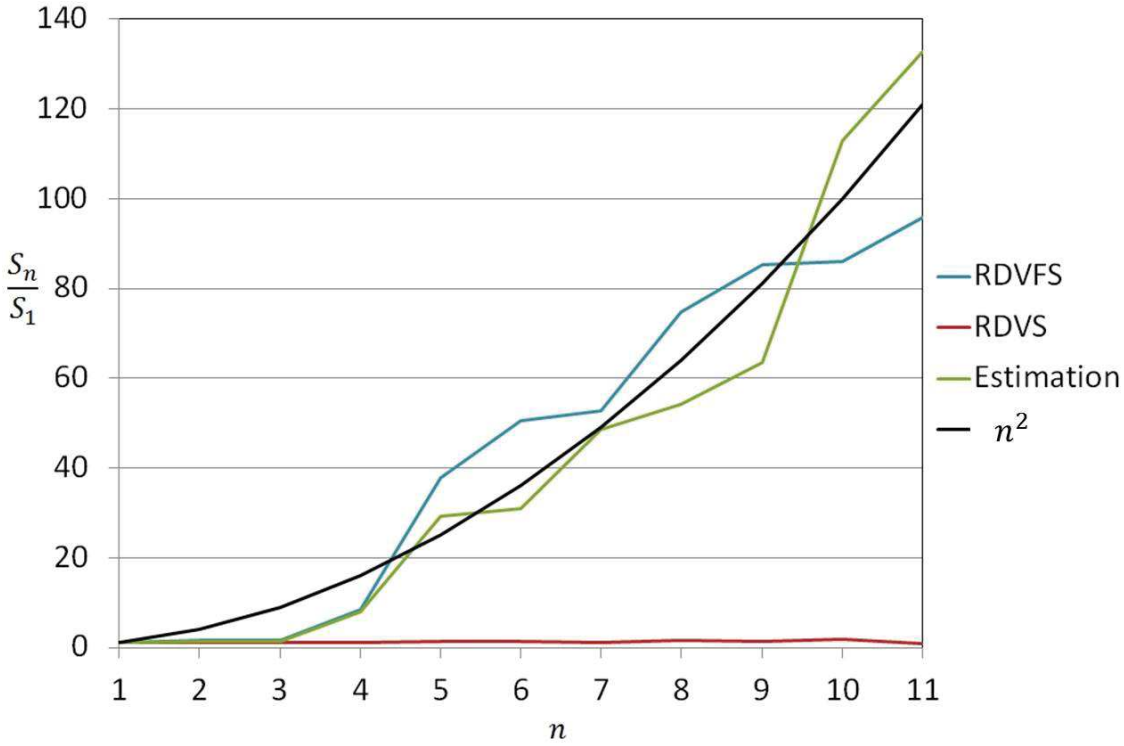

FIGURE 3.11: évolution du rapport de robustesse $\frac{S_n}{S_1}$ en fonction du nombre n de couples (V,F) utilisés sur FPGA

utilisables sont les suivantes : 0mV, 200mV ou 400mV. Ce circuit dispose aussi d'un AES matériel de 128 bits.

Une campagne d'acquisition sur cet AES sur micro-contrôleur a alors été effectuée. Comme pour le FPGA, 11 triplets de (V, F, V_{bb}) ont été utilisés et pour chacun de ces couples 200000 traces EM ont été collectées. Une gigue naturelle est présente sur ce circuit (2ns max). Afin d'être dans les mêmes conditions que pour le FPGA, une resynchronisation des traces a été effectuées après leur collecte.

Comme dans le cas du FPGA, la Fig. 3.12 représente l'évolution du rapport de robustesse $\frac{S_n}{S_1}$ en fonction du nombre de triplets (V, F, V_{bb}) sur le micro-contrôleur. Dans l'état de fonctionnement normal de ce circuit (V, F et V_{bb} constant), il est nécessaire d'obtenir 40.000 traces afin de retrouver la clé de chiffrement contre 1000 pour le FPGA. Cette robustesse naturelle du circuit explique qu'il n'y ait pas plus de 5 valeurs de n sur la Fig. 3.12. En effet, avec 40.000 traces nécessaires pour retrouver la clé lorsque $n = 1$, il faudrait au minimum 1.440.000 traces pour $n = 6$ alors que nous n'en disposons que de 1.200.000. En effet si $n > 5$, il n'est pas possible avec une simple CPA de retrouver la

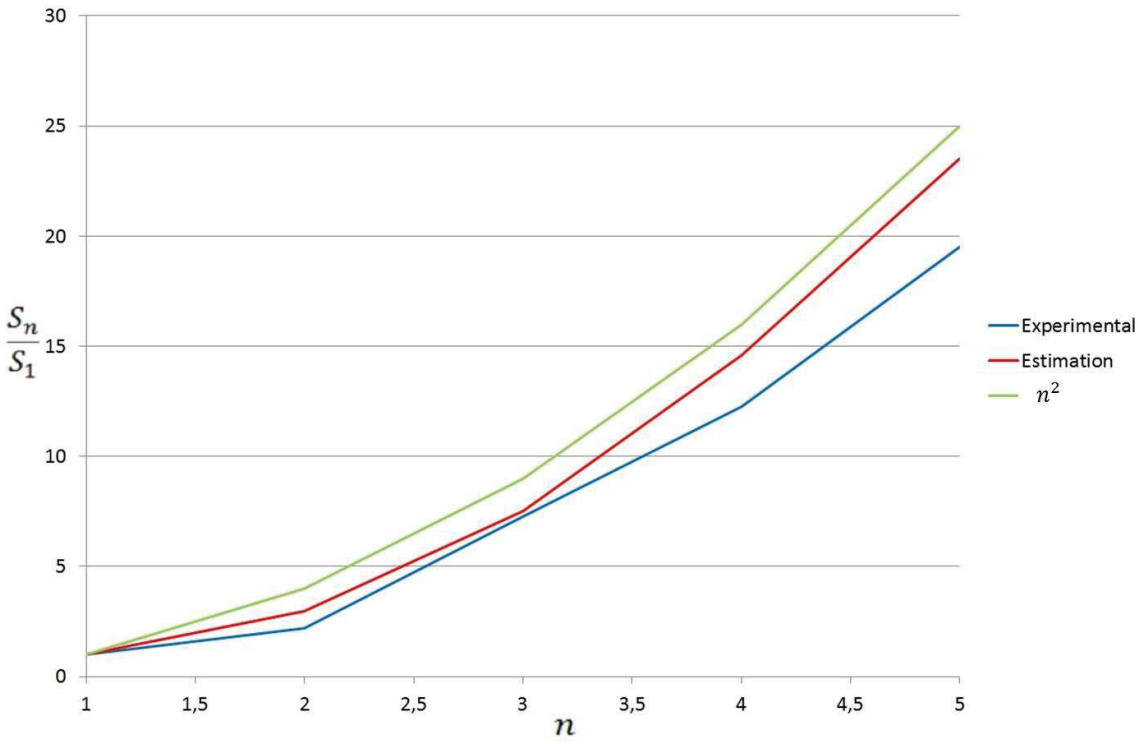

FIGURE 3.12: évolution du rapport de robustesse $\frac{S_n}{S_1}$ en fonction du nombre de triplets n utilisés sur un micro-contrôleur 32 bits

clé de chiffrement avec les traces EM disponibles pour le nombre n de triplets (V, F, V_{bb}) utilisés. Cependant il est tout de même possible de se rendre compte que la robustesse de la RDVFS sur un micro-contrôleur, est bien proportionnelle à n^2 comme attendu.

Les résultats obtenus sur micro-contrôleur nous permettent donc de confirmer les résultats obtenus sur FPGA et confirment que l'approche théorique qui a été effectuée est correcte. Il faut aussi remarquer que l'ajout de la variation de V_{bb} doit être considérée comme un paramètre permettant d'augmenter le nombre de couples disponibles et ainsi d'augmenter la robustesse.

3.6 Optimisation de la CPA

Il a été démontré dans les sections précédentes que la RDVFS permet d'augmenter la robustesse d'un circuit d'un facteur n^2 avec n le nombre de triplets (V, F, V_{bb}) qui sont utilisés. Cependant aucune solution n'a été présentée afin de réduire la robustesse apportée par la RDVFS. C'est l'objectif de cette section. Plusieurs solutions existent afin de réduire ce rapport de robustesse. Le nombre de triplets (V, F, V_{bb}) est limité

par le nombre de tensions différentes que le régulateur peut fournir, et par le nombre de fréquences de fonctionnement différentes auxquelles le circuit peut fonctionner. Il est alors possible à partir des jeux de données précédemment acquis de détecter à quel couple de (V, F, V_{bb}) appartient chaque trace. Puis il est alors possible de, soit resynchroniser la trace par rapport à une trace de référence, ou alors de lancer une CPA sur chaque paquet de traces et de fusionner les résultats.

3.6.1 Resynchronisation des traces EM

Lorsque l'on parle de désynchronisation due à des changements de fréquences, les méthodes les plus employées pour réaligner les traces sont les algorithmes de resynchronisation tel que le *Dynamic Time Warping* (DTW) [88] et le *Rapid Alignment Method* (RAM) [89]. Cependant ces algorithmes qui fonctionnent sur la détection des points d'intérêts ont un temps de calcul relativement long par trace (n^2 pour l'algorithme DTW, avec n le nombre de points dans les traces). Dans les attaques par canaux cachés sur circuit sécurisé, le nombre de traces traitées étant souvent supérieur au million, ces algorithmes ne sont pas viables en pratique à moins de disposer d'un supercalculateur.

Ne disposant pas de supercalculateur et afin de pouvoir resynchroniser les traces EM de manière rapide, nous proposons l'utilisation de l'algorithme ci-après. Cet algorithme se fonde sur les résultats obtenus sur la Fig. 3.11. On peut y observer que la courbe rouge (RDVS) représentant la variation de tension seule n'a aucun effet sur la CPA si le signal d'horloge n'est pas lui-même affecté par cette variation. Le seul effet de cette variation est la variation en amplitude sur les traces EM comme on peut le voir Fig. 3.4. L'algorithme développé ne va pas alors chercher à reconstruire les traces EM, mais seulement à supprimer des points afin que toutes les traces EM soit resynchronisées. Pour ne pas avoir à ajouter des points, les traces EM ayant la fréquence la plus forte servent de références. L'algorithme calcule la fréquence de la trace de référence puis de celle à resynchroniser et détermine un rapport entre ces fréquences. En fonction de la valeur du rapport obtenu, certains points sur la trace à resynchroniser sont supprimés de manière homogène (avec un rapport de 20%, l'algorithme supprimera un point tout les cinq points). Cet algorithme est décrit dans dans l'Algo. 2

Algorithm 2 *Resynchronisation*

$trace, trace_{ref}$;
$frequence_{ref} = freq(trace_{ref})$; {*Calcul de la fréquence de la trace de référence*}
$frequence_{cible} = freq(trace)$; {*Calcul de la fréquence de la trace à resynchroniser*}
$point = \frac{1}{1-\frac{frequence_{cible}}{frequence_{ref}}}$;
$cpt1 = 0; cpt2 = 0;$
for $i = 0 : taille(trace)$ **do**
  if $cpt1 == point$ **then**
    $cpt1 = 0;$
  else if
   then
    $trace_resync(cpt2) = trace(i);$
    $cpt2++;$
    $cpt1++;$
  end if
end for

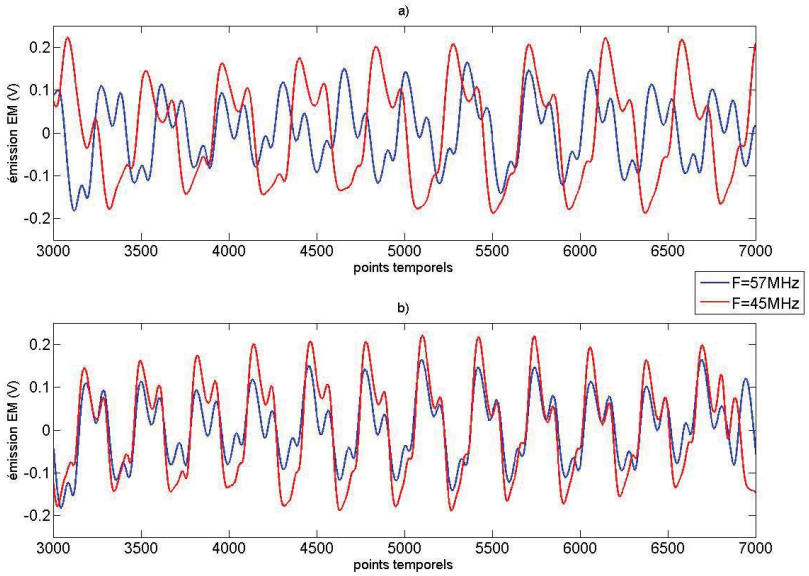

FIGURE 3.13: a) traces EM d'un chiffrement AES a deux fréquences différentes, b) traces EM d'un chiffrement AES resynchronisées

Sur la Fig. 3.13a, on peut voir deux traces de chiffrement AES, qui ont été acquises sur un FPGA, pour deux couples (V, F) différents qui ont une fréquence et une amplitude différentes. Après l'exécution de l'algorithme 2, on peut observer sur la Fig. 3.13b les traces resynchronisées. La trace traitée est maintenant synchronisée avec celle de référence sans qu'il y ait eu de modifications de forme ou d'amplitude.

3.6.2 Regroupement

Une autre méthode a été utilisée pour réduire la robustesse de la RDVFS. Sachant que le nombre de triplets (V, F, V_{bb}) est limité, le nombre de traces d'un même triplet sera alors égal à M/n avec M le nombre total de traces collectées et n le nombre de triplets. En cherchant à détecter à quel triplet (V, F, V_{bb}) appartient chaque trace puis en triant les traces en fonction de leur triplet d'appartenance, on peut alors lancer une CPA sur tous les triplets ainsi reconstitués.

Afin de distinguer à quel triplet (V, F, V_{bb}) chaque trace appartient, un distingueur très peu sensible au bruit doit être utilisé. Pour cela la cohérence spectrale $MSC(f)$ a été utilisée. Son expression est la suivante :

$$MSC(f) = \frac{|P_{xy}(f)|^2}{P_{xx}(f).P_{yy}(f)} \tag{3.17}$$

Dans l'eq. 3.17 le terme P représente la densité spectral de puissance. La valeur retournée permet de connaitre le taux de similarité entre deux signaux. Plus la valeur renvoyée est élevée plus les signaux sont similaires. Il est donc nécessaire de déterminer un seuil de manière judicieuse afin de ne pas affecter une trace a un triplet (V, F, V_{bb}) qui n'est pas correct. Le choix de ce seuil a été fait de manière expérimentale et fixé à une valeur de 0.9.
La méthode est décrite dans l'algorithme 3.

3.6.3 Contre-mesure RDVFS contre les attaques CPA améliorées

Les méthodes de resynchronisation et de regroupement ont été appliquées. Pour cela, une nouvelle campagne d'acquisition a été effectuée avec 11 nouveaux couples (V, F) sur la carte FPGA. Les résultats obtenus avec une CPA standard et avec les deux méthodes proposées sont représentées sur la Fig. 3.14. En utilisant la resynchronisation ou le regroupement, la robustesse de la RDVFS est ainsi passée d'un facteur n^2 à un facteur n. La méthode de resynchronisation utilisée est celle décrite dans la section 3.6.1. La resynchronisation a permis de réduire le rapport de robustesse d'un facteur n^2 à un facteur n cependant, la diminution de ce rapport est difficile à quantifier théoriquement. En effet,

Algorithm 3 *Regroupement*

```
trace, ref;
ref[0] = trace[0]; {La première trace est une référence}
triplet[0, 0] = trace[0]; {Stockage de la trace en mémoire}
Nbrgroupe = 1;
for i = 1 : nbrtrace do
  Validgroupe = 0
  for cptgroupe = 0 : Nbrgroupe − 1 do
    if MSC(trace[i], ref[cptgroupe]) > 0.9 then
      triplet[cptgroupe, cpttrace[cptgroupe]] = trace[i]; {Stockage de la trace en
      mémoire}
      if (cpttrace[cptgroupe]%100) == 1 then
        CPA(triplet[cptgroupe, cpttrace[cptgroupe]]); {Exécution d'une CPA toute
        les 100 traces dans un groupe}
      end if
      cpttrace[cptgroupe] + +;
      Validgroupe = 1;
    end if
  end for
  if Validgroupe == 0 then
    ref[Nbrgroupe] = trace[i]; {Ajout de la trace en référence si elle n'appartient a
    aucun des autres groupes}
    Nbrgroupe + +;
  end if
end for
```

il est possible qu'en utilisant d'autres algorithmes de resynchronisation, la robustesse de la RDVFS puisse être inférieure à n ou alors bien supérieure. Le regroupement des traces permet lui aussi de passer d'une robustesse de n^2 à n cependant ce nombre peut être plus faible si le choix des couples (V, F) n'est pas équiprobable lors de l'utilisation de la RDVFS. En effet, lors de cette expérimentation, il y avait le même nombre de traces pour chaque couple et ces traces ont été mélangées de manière aléatoire. Il est donc logique qu'avec la technique du regroupement l'accroissement de la robustesse soit de n. Si par la conception du circuit, un couple (V, F) est utilisé plus fréquemment que les autres, cela a pour effet de réduire encore plus la robustesse de la RDVFS car en effectuant une attaque CPA avec regroupement sur le couple (V, F) contenant le plus grand nombre de traces, l'accroissement de la robustesse sera inférieur à n.

Le regroupement a aussi été utilisé sur les traces provenant du micro-contrôleur utilisé précédemment. Les résultats obtenus ont confirmé ceux acquis sur FPGA. La resynchronisation n'a cependant pas été utilisée, car le temps de resynchronisation des traces

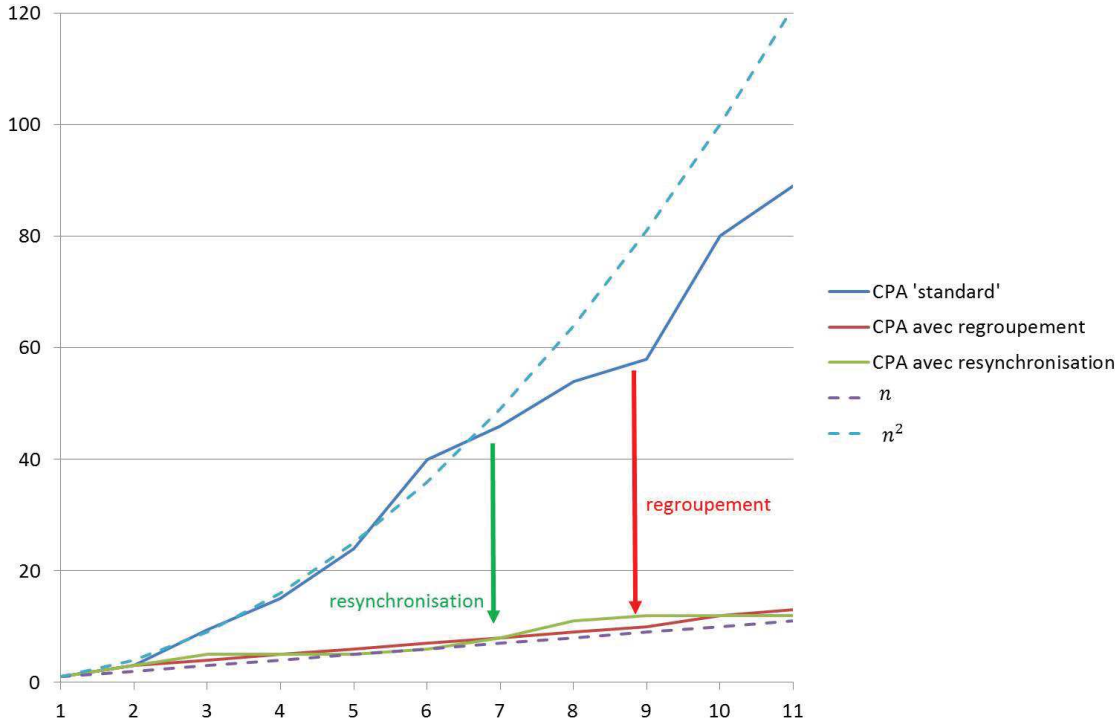

FIGURE 3.14: Evolutions du rapport de robustesse $\frac{S_n}{S_1}$ en fonction du nombre n de couples utilisés avec une CPA 'standard', une CPA avec resynchronisation et une CPA avec regroupement

(> 2Millions) était bien trop important devant celui nécessaire pour effectuer le regroupement.

3.7 Conclusion

L'objectif des travaux reportés dans cette partie était d'évaluer l'impact des technologies faible consommation sur la sécurité des circuits. Parmi celles ci, la technique nommée DVFS est de plus en plus répandue dans les circuits. Elle permet de faire des économies substantielles d'énergie en rendant possible une gestion efficace du compromis consommation/performance. Afin d'évaluer le gain en robustesse sur la CPA de cette technique, qui revient à faire varier la fréquence et la tension d'alimentation du circuit, une étude de l'effet de chaque paramètre pris séparément a été effectuée pour connaitre l'impact de chacun d'eux.

Il a été montré que les variations de la tension produisent un effet sous certaines conditions. Ces variations ont un effet que si la génération du signal d'horloge est elle-même affectée par ces variations. Si le signal d'horloge est fourni par un système non affecté par

ces variations (exemple : un quartz extérieur au circuit), alors l'efficacité de la CPA est nullement affectée. Par contre, si le signal est affecté (exemple : une PLL), ces variations affectent les résultats obtenus avec la CPA.

Une analyse a permis de démontrer théoriquement que la robustesse amenée par la RDVFS contre la CPA est proportionnelle à n^2 avec n le nombre de couples (V, F) utilisés. Cette estimation théorique a été confirmée en pratique par l'implémentation de la RDVFS sur un FPGA et sur un micro-contrôleur 32bits. Toutefois, à l'aide de méthodes simples à mettre en place, il est possible de diminuer ce rapport. La méthode de regroupement qui revient à trier les traces de consommation de sorte à regrouper les traces associées à un même couple (V, F) a permis de diminuer le rapport de robustesse de n^2 à n. La méthode de la resynchronisation permet elle aussi de diminuer le rapport de robustesse. Cependant celui-ci est difficilement quantifiable car il dépend de l'algorithme de resynchronisation utilisé.

Chapitre 4

Les impulsions EM comme moyen d'injection de fautes

Dans ce chapitre, un état de l'art sur les effets de l'injection EM est présenté. Puis un test expérimental est présenté afin de prouver qu'il est possible de générer des fautes de type bitset et bitreset avec l'injection EM. D'autres tests expérimentaux sont également présentés afin de déterminer le modèle de faute que suit l'injection EM. Ce modèle, que l'on nomme modèle 'faute d'échantillonnage', est présenté en fin de chapitre. Ce chapitre reporte des résultats publiés à CARDIS2014 et FDTC2015.

4.1 Généralités

L'utilisation des ondes électromagnétiques comme canal auxiliaire d'attaque [81] est très répandue de nos jours. Comme évoqué dans le chapitre 3, les SCA sont un type d'attaque très efficaces. Cependant, un autre type d'attaques, très efficace également, est lui aussi très répandu. Il s'agit des attaques par fautes. Elles consistent à injecter une erreur dans le circuit afin de récupérer des informations secrètes. Parmi les moyens utilisés pour injecter des fautes dans les circuits cryptographiques, le laser reste la méthode la plus populaire en raison de ses précisions spatiale et temporelle. Cependant, l'injection de fautes à l'aide d'un laser est confrontée à plusieurs difficultés.
La première est le nombre croissant de couches métalliques (jusqu'à 12 niveaux de

métaux) qui sont utilisées pour distribuer des signaux dans le circuit. Cette particularité peut avoir pour effet d'empêcher l'utilisation d'un laser pour injecter une faute par la face avant des circuits. La seconde difficulté, est due au fait que le laser est utilisé depuis plus de 20 ans comme moyen d'injection de fautes. Cela a permis le développement de contre-mesures embarquées de plus en plus efficaces comme le détecteur de tir laser [90]. Les attaquants se doivent donc de développer de nouvelles méthodes d'injection de fautes.

Deux nouveaux moyens d'injection de fautes sont apparus récemment [46, 80]. Le premier est l'injection d'un pic de tension directement dans le substrat du circuit (attaque par *Body-Bias Injection* (BBI)). Cela peut créer deux types d'effets : un pic de tension sur la masse du circuit ou une chute de tension dans le circuit. L'effet qui est produit dépend de la polarité du pic de tension qui est utilisée [46]. Le second moyen d'injection de fautes récemment apparu est l'injection EM [80, 91].

4.2 Etat de l'art sur l'injection EM

L'utilisation des ondes EM comme médium pour injecter des fautes est assez récent. La première publication [91] date de 2002 dans laquelle il est affirmé qu'il est possible de perturber le comportement d'une mémoire embarquée à l'aide d'une injection EM. Il a été signalé que cette méthode d'injection de fautes possède un avantage non négligeable sur les tirs laser ou la BBI. Il s'agit de sa capacité à injecter des fautes à travers le boitier du circuit aussi bien en face avant que face arrière. Grâce à cet avantage, d'autres travaux ont depuis été menés. En 2007, Schmidt [52] présente un système produisant une forte impulsion EM, à base d'un allume-gaz astucieusement détourné de sa fonction principale, de sorte à générer des arcs électriques. Lorsqu'un arc électrique se produit, celui-ci génère un fort champ EM, de brève durée, qui est capable de perturber un micro-contrôleur exécutant une opération RSA.

Deux types de plateformes d'injection EM existent. La première que l'on nomme plateforme d'injection EM harmonique, génère des ondes EM sinusoïdales, qui peuvent être modulées en amplitude afin de produire des fautes. Ce type de plateforme a été utilisée par F. Poucheret dans [82] afin de perturber la fréquence d'oscillation d'un générateur de signal d'horloge interne. P. Bayon [92] a, quant à lui, utilisé cette plateforme afin

de perturber un générateur de nombres aléatoires (*True Random Number Generator* (TRNG)) afin que les valeurs fournies par le TRNG soient biaisées.

Le second type de plateforme que l'on nomme plateforme d'impulsion EM (EMP), est celle qui a été utilisée pendant cette thèse. Elle produit une courte mais très puissante impulsion électromagnétique, tout comme [80, 91], qui crée soudainement un flux de courant dans le réseau d'alimentation et/ou de masse du circuit. Cela a pour effet de générer une chute de tension sur le réseau d'alimentation et/ou un pic de tension sur le réseau de masse. Ce type de plateforme a été utilisée par A. Dehbaoui [83] afin d'injecter des fautes dans un ancien micro-contrôleur (350nm). En analysant les fautes obtenues, l'auteur a conclu dans [93] que l'injection de fautes par impulsion EM produit des fautes de timing et plus précisément des violations de la contrainte de temps de setup. A partir de ces observations, un détecteur de glitch EM a été défini et évalué dans [72] où est mise en lumière son efficacité partielle.

Les résultats fournis dans [93] sont intéressants, cependant, ils ont un intérêt très limité pour l'injection EM de fautes sur les cartes à puce. En effet, de nos jours, les cartes à puce sont conçues en technologie de 90nm et fonctionnent à une faible fréquence d'horloge ($< 40MHz$). Cela implique qu'elles sont caractérisées par de grands timing slacks (marges temporelles de fonctionnement avant apparition d'une violation de temps setup). Elles sont donc naturellement très robustes aux injections EMP si ce type d'injection ne produit que des fautes de timing. Le contexte de ce chapitre de thèse est de démontrer qu'il est possible de générer d'autres types de fautes avec une injection EMP que celles présentées dans la littérature et plus particulièrement dans [93].

4.3 Mise en place d'un banc d'injection EMP

Dans la littérature, de brèves descriptions des plateformes d'injection EM harmonique et pulsée sont données dans [94]. Dans cette section, une description plus détaillée de la plateforme d'injection EMP et des différentes sondes d'injection utilisées durant cette thèse est fournie.

4.3.1 Plateforme d'injection EMP

L'objectif d'une plate-forme d'injection EMP est de générer, à proximité immédiate de l'appareil ciblé, une variation intense et soudaine du champ magnétique. Cette variation du flux magnétique est ensuite capturée par une partie des antennes présentes dans le circuit. Les antennes présentes dans un circuit sont formées par les réseaux d'alimentation et de masse ou les interconnexions véhiculant des signaux. La variation du flux magnétique a pour effet de créer une variation soudaine et intense du courant dans le circuit. Cela induit alors des chutes ou des pics de tension sur les différents signaux du circuit. Du fait de ces perturbations, le circuit ne fonctionne pas dans des conditions normales et des fautes peuvent apparaitre.

La plateforme utilisée durant cette thèse est représentée sur la Fig. 4.1. Elle est composée d'un ordinateur qui a pour fonction de contrôler toute la plateforme à l'aide de différents ports séries. Un système de positionnement sur 3 axes avec une précision de 5μm est utilisée pour positionner les sondes d'injection EM au dessus de la cible. Il est couplé avec un système de vision sur 3 axes permettant au système de positionnement d'être précis. Un oscilloscope à échantillonnage numérique (*Digital Sampling Oscilloscope* (DSO)) est utilisé pour contrôler la synchronisation de l'injection EMP au fonctionnement du circuit. Le générateur d'impulsions est l'élément principal de la plateforme. Il délivre à la sonde d'injection une impulsion de tension pouvant aller jusqu'à 200V (courant de 8A), pendant une durée comprise entre 5ns et 100ns. Les temps de montée et de descente de l'impulsion sont de 1.5ns.

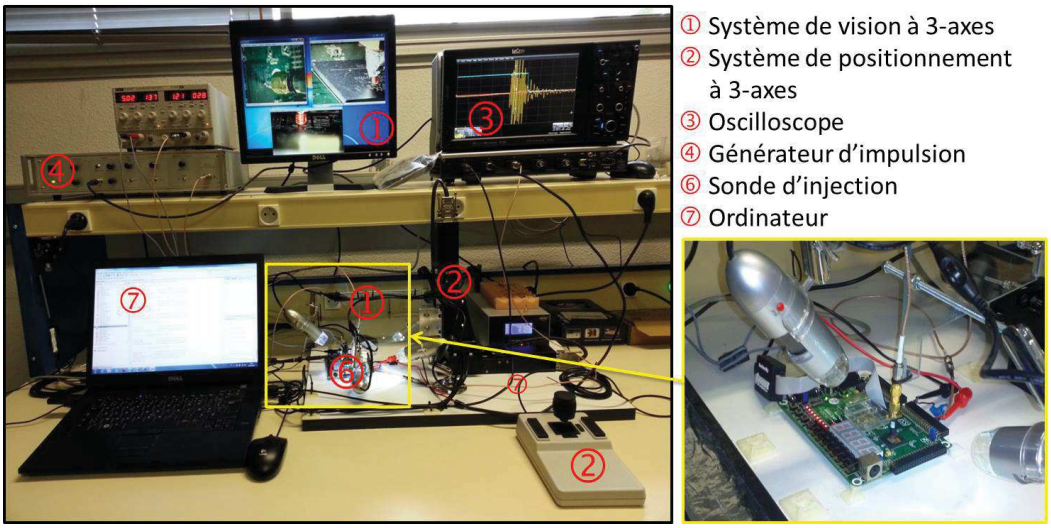

FIGURE 4.1: Plateforme d'injection EMP du LIRMM

L'injection EMP se doit d'avoir un effet local. L'attaquant a en effet pour but d'injecter des fautes dans des zones spécifiques du circuit sans que les autres zones du circuit ne soient affectées par l'injection. Il est donc nécessaire que la zone d'injection soit la plus petite possible. Pour cela, les sondes d'injection doivent être miniaturisées.

4.3.2 Sondes d'injection EMP

Il existe plusieurs types de sondes d'injection EM qui sont utilisées en fonction des zones visées ou de la précision du champ émis. La Fig. 4.2 montre trois types de sondes qui ont été utilisées durant cette thèse. Toutes les sondes ont été réalisées à la main. Elles sont conçues autour d'un cœur en ferrite pour guider les lignes de champ magnétique vers la cible. Chaque sonde a une taille différente. Les sondes plates (Fig. 4.2a) ont un cœur de ferrite dont la taille est comprise entre 750μm et 300μm. Les sondes appointées visibles sur la Fig. 4.2b ont un cœur de ferrite de même taille que les sondes plates. Cependant, la pointe a été affinée jusqu'à 50μm [95] afin de concentrer le champ EM dans un petit volume. Le dernier type de sondes utilisées sont les sondes dites 'oméga' (Fig. 4.2c). Elles sont constituées d'un cœur de ferrite en forme de demi-cercle dont les deux extrémités séparées d'une distance s, sont appointées.

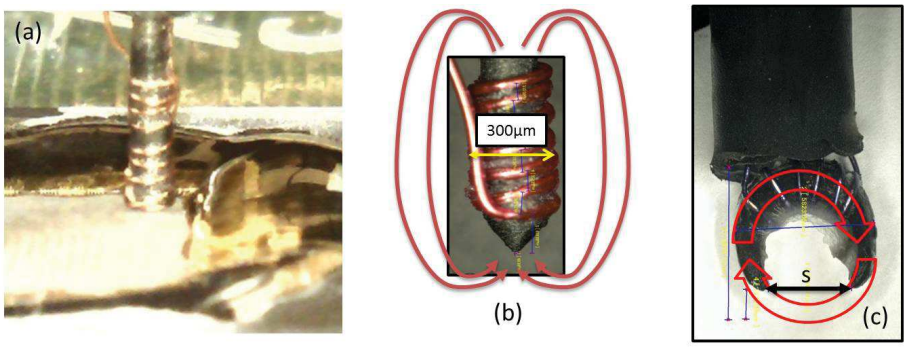

FIGURE 4.2: (a) Sondes d'injection plate, (b) Sonde d'injection appointée, (c) Sonde d'injection oméga

Les sondes plates et appointées sont conçues pour focaliser le champ magnétique sous l'extrémité de la pointe de ferrite. Dans ce cas, une sonde appointée (Fig. 4.2b), comme proposé dans [95], permet de concentrer davantage le champ magnétique dans un plus petit volume et donc d'augmenter la résolution spatiale. Il est à noter que contrairement aux résultats obtenus par simulation dans [95], la pratique a montré que 4 à 7 spires autour de la ferrite fournissent de meilleurs résultats que 1 ou 2.

Bien que les sondes plates et appointées soient efficaces, elles ont tout de même un inconvénient. Les lignes de champs créées par celles-ci vont d'une extrémité à l'autre de la ferrite avec une forme ellipsoïdale comme représentée par les flèches rouges sur la Fig. 4.2b. Cela a pour effet de limiter la résolution spatiale de ce type de sondes, même si le champ magnétique est extrêmement fort sous la pointe.

Afin de contourner cette limitation, des sondes oméga ont été réalisées. L'idée est de créer un champ magnétique circulaire afin de concentrer celui-ci entre les deux extrémités de la ferrite en forme d'arc de cercle. Ce type de sonde devrait éviter (ou pour le moins limiter) toute pollution magnétique autour de l'espace séparant les deux extrémités de la ferrite. Les lignes de champ magnétique devraient en effet sortir d'une extrémité, puis traverser les couches supérieures du circuit (réseaux d'alimentation et de masse) et enfin revenir dans la ferrite par l'autre extrémité. De plus, en raison de leur géométrie, les sondes d'injection oméga ont une propriété intéressante : elles sont directionnelles. En effectuant une rotation autour de l'axe Z, la direction des lignes de champ magnétique vont également tourner du même angle que la sonde. Cela peut ainsi modifier les propriétés de couplage entre la sonde et le circuit ciblé. Cette particularité n'existe pas pour les sondes plates ou appointées à cause de leur géométrie cylindrique.

4.4 Sources de défaillance des circuits synchrones

De nos jours, la majorité des circuits intégrés sont synchrones, c'est à dire des circuits dont les opérations sont cadencées par un signal global qui est l'horloge (clock). Dans cette section, des rappels sur la structure des circuits (éléments constitutifs et principe de fonctionnement) sont fournis. Ces rappels sont un préambule à l'identification des divers mécanismes qui peuvent expliquer l'apparition des fautes dans un circuit soumis à une injection EMP de forte amplitude. Enfin, des tests permettant de discriminer au cours d'expériences les sources d'erreurs sont définis.

4.4.1 Structure d'un circuit synchrone

Un circuit intégré synchrone est un circuit dans lequel les échanges de données entre les différents blocs sont synchronisés par un signal global. Ce signal, l'horloge, commande l'échange d'informations entre les blocs et l'échantillonnage des résultats des calculs à

intervalles de temps réguliers.

Les calculs sont effectués par des portes logiques, habituellement en technologie CMOS, qui sont positionnées entre deux registres, généralement des bascules D flip-flops (DFF), qui permettent d'assurer à la fois l'échantillonnage et le transfert des résultats entre les différents blocs. Compte tenu de cette structure, un IC synchrone peut être schématisé par la Fig. 4.3 dans laquelle les registres sont représentés par deux DFF (avec un signal d'initialisation à '0' asynchrone actif sur niveau bas (reset) et un signal d'initialisation à '1' asynchrone actif sur niveau haut (set)) qui entourent un bloc combinatoire de portes logiques CMOS assurant le calcul.

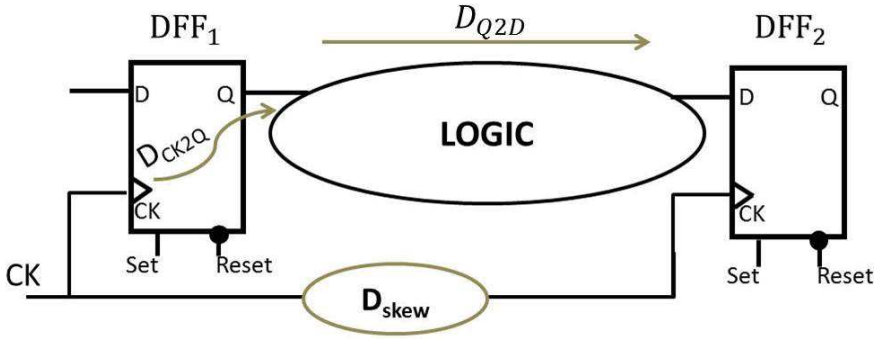

FIGURE 4.3: Schéma d'un circuit synchrone

4.4.2 Contraintes de fonctionnement des portes logiques

Si le comportement des portes combinatoires utilisées afin d'intégrer sur silicium toutes fonctions booléennes, est assez simple, les DFF ont un comportement plus complexe et certaines contraintes analogiques doivent être satisfaites afin d'assurer leurs bon fonctionnement. Pour rappel, une DFF copie le signal présent sur l'entrée D depuis un temps $D2CK$ avant le front d'horloge, sur sa sortie Q, lors du front montant de l'horloge. Cette copie n'est effective qu'après une durée de $CK2Q$ qui correspond au délai de propagation de D à travers la bascule. Cependant, comme cela est représenté sur la Fig. 4.4, pour qu'une copie correcte de D sur Q soit effectuée, le signal D doit théoriquement être stable t_{setup} ps avant le front montant de l'horloge et doit rester inchangé pendant une durée t_{hold} ps après celui-ci. Cela peut s'expliquer par le fait que lorsque la donnée D arrive $(t_{setup}\epsilon)$ps avant le front montant de l'horloge, la valeur de $CK2Q$ croit avec ϵ et peut devenir très grande et théoriquement ∞. Il est alors courant de prévoir une marge lors de la conception des circuits intégrés et plus précisément de prendre pour temps

de setup la valeur pratique t^p_{setup} (et t^p_{hold} pour le temps de hold), qui correspond à une dégradation de 10% du délai $CK2D$. Cela permet de prévenir une arrivée tardive du signal D.

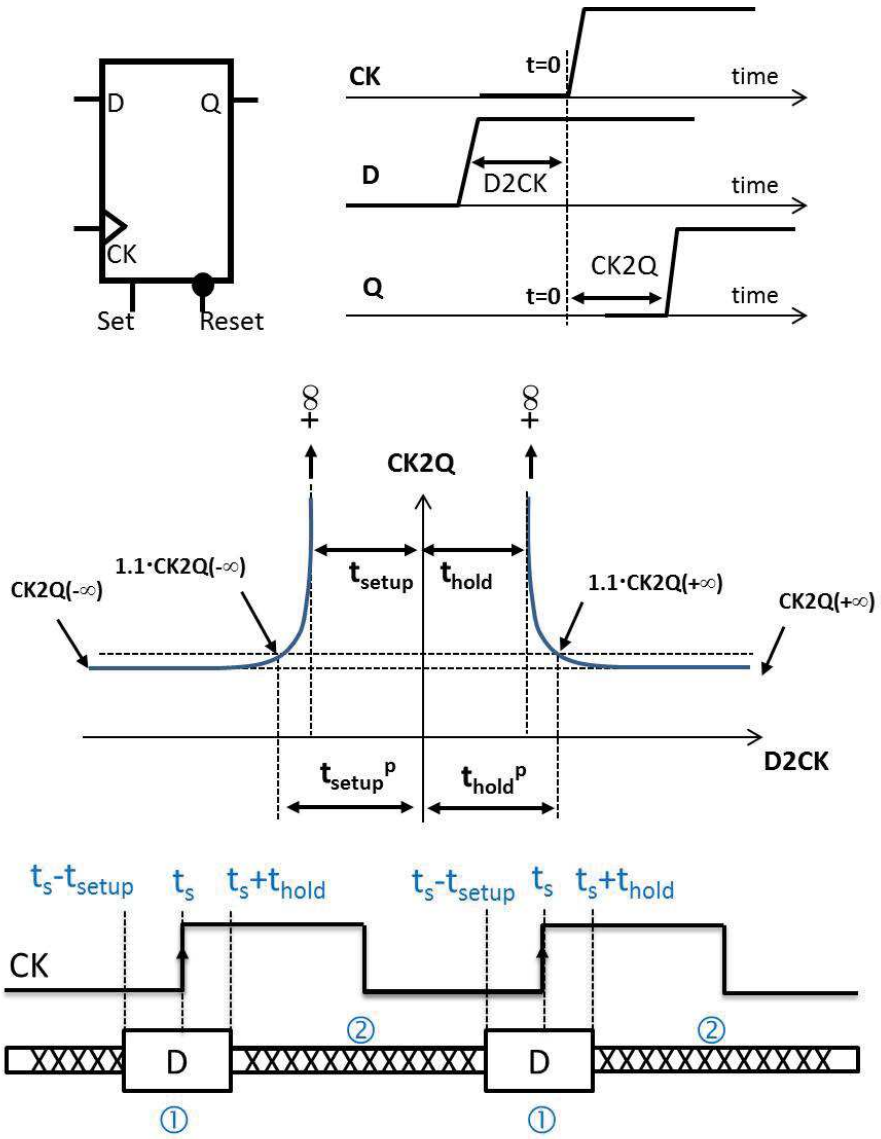

FIGURE 4.4: Symbole d'une DFF et définition du temps de setup (t_{setup}) et du temps de hold (t_{hold})

La stabilité du signal D lors d'un changement d'état d'une DFF est une contrainte au niveau porte. Cette stabilité, si elle n'est pas respectée, peut générer des fautes de types bitset, bitreset ou bitflip. A l'aide de l'injection EMP, un fort courant peut être induit dans le circuit, ce qui a pour effet de modifier la tension du réseau d'alimentation ou de l'interconnexion transportant le signal D, et ainsi de produire un mauvais fonctionnement d'une DFF. Ce type de fautes sera désigné ultérieurement comme une faute d'échantillonnage.

A partir du raisonnement ci-dessus selon lequel une injection EMP peut modifier de manière significative un signal dans un circuit, il est également probable qu'une injection EMP puisse produire des bitsets ou bitresets dans une DFF en modifiant tout simplement les potentiels des signaux de set ou reset d'une DFF ou en réduisant la différence de potentiel $V_{dd} - Gnd$ à zéro temporairement. Il semble alors possible de générer ce type de fautes, même lorsque il n'y a pas de commutation de la DFF, si les signaux de set et reset sont conçus pour être asynchrones. Si cette dernière hypothèse est correcte, l'injection EMP doit également être capable de produire la commutation d'une DFF en créant une perturbation sur le signal d'horloge ce qui génère un front d'horloge parasite, ou qui masque (inhibe) le front montant de l'horloge.

Si ce qui précède est correct, il apparait donc à ce stade que les DFFs constituent un chemin pour l'injection de fautes par impulsion EM.

4.4.3 Contraintes de fonctionnement au niveau circuit

Les contraintes de fonctionnements des bascules DFF imposent des contraintes bien connues au niveau circuit qui doivent être satisfaites lors de la phase de conception. Elles sont imposées lors de la conception en utilisant des outils d'analyse des délais (*static timing analysis*). Parmi les contraintes les plus exigeantes, on peut identifier la contrainte de temps de hold et la contrainte du temps de setup. Il a été mis en évidence dans [93] que le temps de setup peut être un moyen d'introduction de fautes pour l'injection EMP. Afin de mieux en comprendre les raisons, voici un rappel sur la contrainte du temps de setup.
La contrainte du temps de setup au niveau circuit est définie par l'inégalité suivante :

$$T_{CK} > D_{CK2Q} + D_{Q2D} + t_{setup} + D_{Skew} \tag{4.1}$$

avec T_{CK} la période du signal d'horloge, D_{CK2Q} et D_{Q2D} les délais de propagation de la DFF (voir Fig. 4.3 et Fig. 4.4) et des blocs combinatoires, t_{setup} le temps de setup de la DFF_2, et D_{Skew} le décalage d'horloge (skew d'horloge).

Lors de la conception, le travail du concepteur est de forcer tous les chemins logiques à avoir des retards D_{Q2D} satisfaisant l'eq. 4.1 pour une valeur ciblée de T_{CK}. Il est

aussi nécessaire que l'eq. 4.1 soit respectée pour une plage de température définie par l'application pour laquelle le circuit est conçu (-40^oC à $+125^oC$ pour les applications militaires), mais aussi pour une gamme de tension comprise entre : $0.9V_{dd}$ et $1.1V_{dd}$ (V_{dd} étant la tension d'alimentation nominale du circuit). La valeur de cette tension est imposée par la technologie (1.2V pour la technologie 90nm). En dehors de ces deux plages, le fonctionnement du circuit n'est pas garanti.

Dans [93], il est mis en évidence que la contrainte du temps de setup au niveau circuit est un moyen d'injection de fautes pour l'injection EMP. En effet, il est suggéré que l'injection EMP modifie localement et temporairement la tension d'alimentation des portes logiques, ce qui a pour effet d'augmenter les délais D_{Q2D} de telle sorte que la contrainte de temps de setup n'est plus respectée, ce qui a alors pour résultat de produire une faute de timing. Si cette explication est correcte, il est alors difficile de déterminer si l'injection EMP induit des violations sur le temps de setup au niveau des portes logiques ou au niveau circuit. Afin de déterminer cela, nous allons définir des tests pour déterminer si l'injection EMP induit des violations de contraintes au niveau portes ou au niveau du circuit, ce qui revient à déterminer si l'injection EMP induit des fautes d'échantillonnage (niveau portes logiques) ou des fautes de timing (niveau circuit).

4.4.4 Tests de discrimination

Nous avons donc cherché des tests permettant de vérifier si le modèle 'fautes de timing' est un meilleur modèle que le modèle 'fautes d'échantillonnage' pour l'injection EMP.

D'après l'eq. 4.1, plusieurs critères ou tests peuvent être définis pour déterminer expérimentalement si l'injection EMP suit le modèle 'faute de timing'. En effet, selon l'eq. 4.1, un premier test pourrait consister à essayer d'éviter l'apparition d'une violation de la contrainte du temps de setup en réduisant la fréquence d'horloge, soit en augmentant T_{CK}.

Un second test peut consister à produire la même injection EM durant une même période d'horloge, mais a des instants différents (t_{pulse}), puis à vérifier que la faute survenue est indépendante de ce paramètre. En effet, indépendamment de l'instant auquel une augmentation de D_{Q2D} est produite (début, milieu ou fin de la période d'horloge), si l'augmentation est suffisante alors une faute apparait.

Il est sans doute possible de définir d'autres tests. Cependant, ces deux tests ont été jugées suffisants pour vérifier si l'injection EMP produit des fautes de timings ou non. De même que ce que nous avons fait pour le modèle 'fautes de timing', nous avons analysé les diverses implications du modèle 'faute d'échantillonnage'. Parmi celles-ci on peut observer que si l'injection EMP produit de telles fautes, alors ces fautes peuvent uniquement apparaître lorsque l'injection EMP est produite juste avant l'apparition d'un front montant du signal d'horloge et plus précisément pendant les "fenêtres de stabilité" (zone 1 de la Fig. 4.4) correspondant au changement d'état d'une DFF. En outre, si ce modèle de faute EM est validé, ces fenêtres de temps au cours desquelles l'injection EMP est capable de produire des fautes, sont :

– périodiques avec une période égale à T_{CK} et ont une largeur indépendante de la fréquence d'horloge. En effet, t_{setup} et t_{hold} ne dépendent que de paramètres intrinsèques liés à la conception des bascules DFF (schématique, placement, technologie ou tension d'alimentation,...) et sur les temps de transition de l'horloge et du signal D.
– nécessairement séparées par des intervalles de temps au cours desquels la probabilité de produire une faute est nulle. Ces intervalles correspondent au moment ou l'injection EMP n'est pas produite durant la fenêtre de stabilité des DFFs.

Toutes ces implications du modèle d'échantillonnage seront utilisées pour vérifier si l'injection EMP produit des fautes d'échantillonnage lors de nos expérimentations. Toutefois, avant d'appliquer ces tests de discrimination, nous avons souhaité évaluer s'il est possible d'induire des fautes de type bitset ou bitreset en perturbant les signaux de set et de reset des DFF au repos.

4.5 Production de bitset et bitreset sur DFF au repos

Cette section vise à démontrer expérimentalement qu'il est possible de produire des fautes de type bitset ou bitreset avec l'injection EMP en perturbant les signaux de set et de reset. Pour cela, un circuit de test a été conçu.

4.5.1 Description de la procédure et du circuit de test

Notre intention était de pouvoir facilement écrire et lire le contenu de DFFs pour détecter, par simple comparaison, l'apparition de fautes de type bitset ou bitreset. Pour cela, une grande FIFO (*First In First Out*) a été réalisée avec 5120 DFFs regroupés par 8 (afin de réaliser un octet). Le placement de ces paquets de 8 DFFs a été effectué sur 10 lignes afin d'obtenir 64 registres de 8 bits par ligne. Cette structure a été implémentée sur un FPGA Xilinx spartan 3-1000 (technologie de 90nm). La Fig. 4.5 montre l'implémentation sur le FPGA. Il est à noter que pour le reste de ce chapitre, toutes les DFFs ont un signal de reset actif sur niveau bas et un signal de set actif sur niveau haut. Deux autres blocs ont aussi été implémentés, une machine d'état (FSM) et un bloc de communication (RS232) afin de pouvoir communiquer avec l'utilisateur.

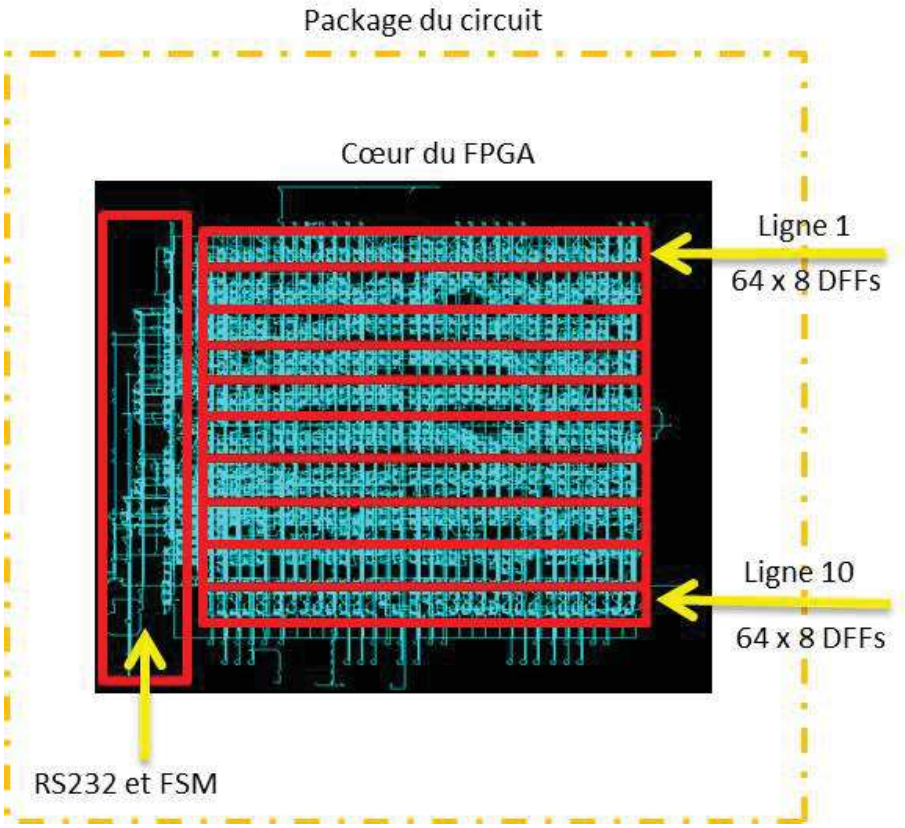

FIGURE 4.5: FIFO de 640x8 DFF implémentées sur FPGA pour démontrer l'occurrence des fautes de type bitset et bitreset

Ce circuit de test a été exposé à des injections EMP dans le but d'établir une cartographie et de déterminer les zones sensibles à l'injection EMP. La procédure automatisée qui a été adoptée pour détecter l'apparition de fautes de type bitset et bitreset est décrite ci-dessous :

- $1^{ère}$ étape : la sonde d'injection EM est placée à une position (X,Y) (valeur initiale (0,0)) au dessus du circuit de test. Dans le but de maximiser la résolution spatiale de l'injection, la sonde est placée au plus proche possible du circuit (le boitier a été retiré chimiquement).
- $2^{ème}$ étape : le contenu de chaque octet de la FIFO est réglée à la valeur hexadécimale 'AA' ('10101010' en binaire).
- $3^{ème}$ étape : le signal d'horloge est stoppé afin d'éviter l'apparition de faute de timing.
- $4^{ème}$ étape : une injection EMP est réalisée, avec une tension V_{pulse} d'amplitude comprise entre -200V et 200V.
- $5^{ème}$ étape : le signal d'horloge est réactivé (plusieurs μs après l'injection) et le contenu de la FIFO est récupéré.
- $6^{ème}$ étape : le contenu initial et final de la FIFO sont comparés (avec une opération xor) afin de détecter l'apparition d'une faute de type bitset ou bitreset. Les données comparées sont stockées dans un fichier de résultats.
- $7^{ème}$ étape : les étapes de 2 à 6 sont répétées 9 fois (10 injection au total) afin de pouvoir estimer la probabilité d'obtenir une faute de type bitset ou bitreset à la position (X,Y).
- $8^{ème}$ étape : toute la procédure est répétée à chaque nouvelle position (X,Y) afin d'obtenir une cartographie des zones sensibles.

4.5.2 Occurence de fautes de type bitset et bitreset

A partir de la procédure décrite dans la section 4.5.1, beaucoup de zones de sensibilités à l'injection EMP ont été établies pour des valeurs de V_{pulse} comprise entre -200V et 200V. Plusieurs sondes d'injection on également été utilisées. Cependant, seuls les résultats obtenus avec une sonde d'injection oméga (ayant un s=450μm) sont reportés car ces résultats sont meilleurs au niveau de la résolution spatiale. Au cours de cette expérience, quatre types de comportements du circuit ont été observés :

- l'injection a produit des fautes de type bitset dans un certain nombre de DFFs,
- l'injection a produit des fautes de type bitreset dans un certain nombre de DFFs,
- le circuit est devenu 'muet' ou le bloc de communication (RS232) a été affecté,
- aucune faute n'a été produite et le circuit fonctionne correctement.

La Fig. 4.6 montre trois cartographies obtenues avec un pas de déplacement de la sonde d'injection de 300μm. La surface du circuit (5500μm x 5000μm) a été scannée. Les

cartographies résultantes sont de plus petite taille (de taille 4000μm x 2400μm) en raison de la forme de la sonde d'injection et d'une marge spatiale de positionnement prise afin d'éviter toute collision avec les fils de bondings du circuit. Ces cartographies ont été obtenues avec les paramètres suivants : $V_{pulse} = +170V$ et une largeur d'impulsion $PW = 8ns$. La Fig. 4.6a montre la probabilité d'avoir des fautes de n'importe quel type. La Fig. 4.6b montre la probabilité de générer une faute de type bitset tandis que la Fig. 4.6c montre la probabilité de rendre le circuit 'muet'. Enfin, la Fig. 4.6d montre l'orientation de la sonde d'injection au dessus de la surface du circuit, la pertinence de ce paramètre sera discuté ultérieurement. Deux types de fautes de type 'muet' ont été observés. La première catégorie est caractérisée par l'absence de réponse du circuit mais dont il n'est pas nécessaire de reprogrammer le circuit pour que celui-ci fonctionne à nouveau. Ceci suggère l'apparition d'une faute dans l'une des DFF de la machine d'état du circuit. La seconde catégorie est plus inquiétante. En effet, afin de pouvoir faire fonctionner à nouveau le circuit, il est nécessaire de le reprogrammer. Ceci suggère que le bitstream (fichier de programmation implémenté dans le FPGA) a été corrompu par l'injection EMP tout comme il est possible de le faire avec un laser [96].

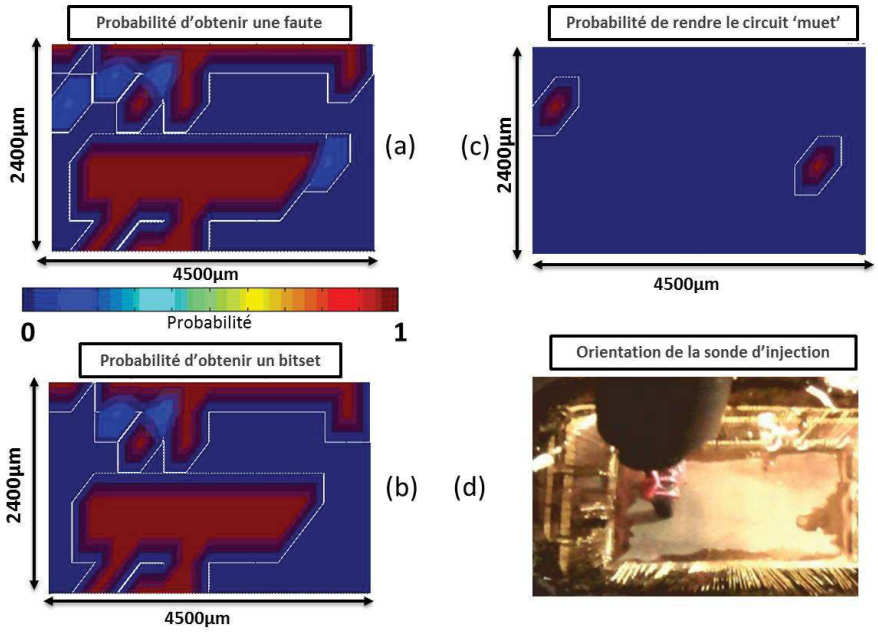

FIGURE 4.6: Probabilité de produire (a) une faute de n'importe quel type, (b) une faute de type bitset, (c) une faute de type 'muet'. (d) orientation de la sonde d'injection oméga

L'obtention de ces cartographies a permis de déterminer des zones de sensibilité, en particulier celles de la Fig. 4.6b, qui constitue une démonstration expérimentale que l'injection EMP, menée avec des sondes d'injection améliorées, est capable de produire

des fautes de type bitset. Ceci étant l'un de nos objectifs. En outre, on peut observer que l'injection EMP est locale et reproductible.

4.5.3 Effet de la polarité de l'injection EMP

En dépit d'être une preuve expérimentale que l'injection EMP peut produire des fautes, dans des registres, qui ne sont pas des violations de timing, les expériences reportées dans la section 4.5.2 n'ont jamais permis de réaliser des fautes de type bitreset. En considérant que le signal de set des DFF est actif sur niveau haut, et que le signal de reset est actif sur niveau bas, plusieurs expériences similaires ont été réalisées pour les deux polarités de l'injection EMP : avec V_{pulse}=-140V et +140V au lieu de +170V seulement. L'idée qui a motivé cette expérience était l'hypothèse qu'une impulsion d'une polarité donnée peut affecter plus le réseau de masse que le réseau d'alimentation (ou vice-verca) ou augmenter ou réduire la polarisation d'un signal d'interconnexion. Par conséquent, il peut être plus facile de produire une faute de type bitset que de type bitreset (ou l'inverse) en fonction de la polarité de l'injection EMP. Il est toutefois à noter que la polarité est ici une notion arbitraire qui dépend dans notre cas à la fois de l'orientation de la sonde d'injection et du signe du pic de tension émis par le générateur d'impulsion et d'autres paramètres comme le sens de bobinage des sondes. Par souci de simplicité, il a été choisi de définir la polarité positive lorsque l'impulsion affecte plus le signal de set qui est actif sur niveau haut que le signal de reset qui est actif sur niveau bas.

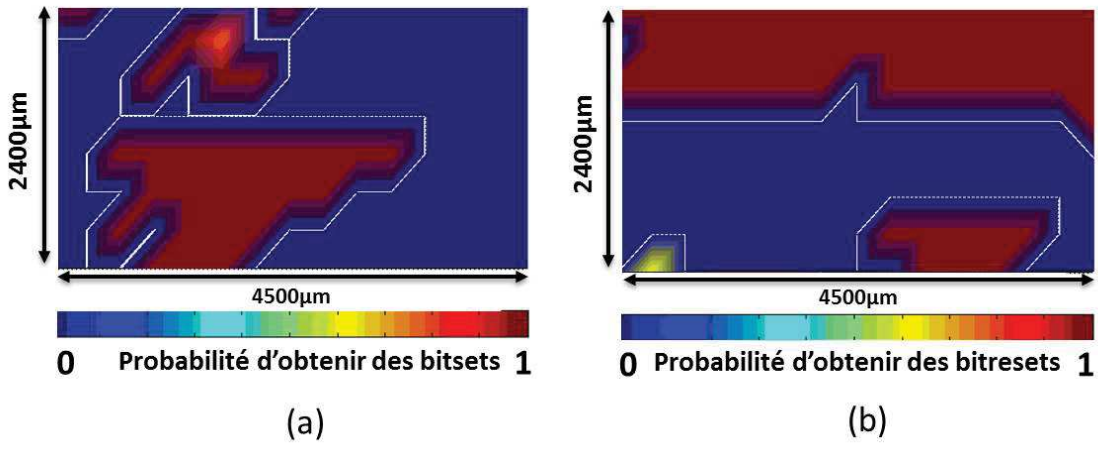

FIGURE 4.7: Probabilité de produire (a) une faute de type bitset avec un V_{pulse}=+140V et (b) une faute de type bitreset avec un V_{pulse}=-140V

La Fig. 4.7a donne la probabilité d'obtenir des fautes de type bitset lors d'une injection EMP positive d'amplitude de +140V au lieu de +170V pour la Fig. 4.6b. En comparant ces deux figures (Fig. 4.7a et Fig. 4.6b), on peut observer que la réduction de V_{pulse} permet de réduire les zones de sensibilité du circuit. Il est à noter cependant que les cartographies restent semblables dans la forme. Ceci indique que l'amplitude V_{pulse} peut être considérée comme un paramètre de contrôle efficace de la puissance de l'injection EMP, comme on pouvait s'y attendre.

La Fig. 4.7b donne la probabilité d'obtenir des fautes de type bitreset lors d'une injection EMP négative d'amplitude de -140V. Au cours de cette expérience, aucune faute de type bitset n'a pu être obtenue. On peut observer que les cartographies sont complètement différentes indiquant que la susceptibilité d'un circuit à une impulsion positive ou négative peut être radicalement différente.

Néanmoins, la principale conclusion qui peut être tirée de ces expériences est que la polarité de l'impulsion (et l'orientation de la sonde d'injection) est un facteur clé dans le contrôle du type de fautes induit par l'injection EMP. Il semble que pour créer une perturbation sur le réseau de masse ou d'alimentation la topologie du circuit et la tension de polarisation sont importantes. Ces résultats suggèrent également que, selon leurs occurrences, les fautes de type bitset et bitreset sont liées à la manière dont sont conçues les DFF (signal de set/reset actif sur niveau haut/bas). Cependant, afin de valider définitivement cette hypothèse, d'autres investigations sont nécessaires.

4.6 Injection EMP sur un circuit en fonctionnement

A ce stade du chapitre, il a été montré que l'injection EMP a un effet local, mais surtout qu'elle peut produire des fautes de types bitset ou bitreset dans un circuit au repos. Ce résultat suggère que l'injection EMP suit le modèle 'faute d'échantillonnage' (perturbation des bascules) plutôt que le modèle 'faute de timing'. Cependant, les attaques en fautes sont menées sur des circuits en fonctionnement et non au repos. Par conséquent, le but de cette section est d'identifier sur un circuit en fonctionnement, et non au repos, le modèle de faute le plus adéquat entre le modèle 'faute d'échantillonnage' et le modèle 'faute de timing'. A cet effet, un nouveau circuit de test a été conçu.

4.6.1 Circuit de test en fonctionnement

Le circuit de test utilisé pour mener nos expériences est un FPGA (Xilinx Spartan 3-1000), conçu en technologie de 90nm, sur lequel quatre blocs fonctionnels ont été conçus et placés. Le premier est une machine d'état fonctionnant à une fréquence de 50MHz. Elle contrôle l'ensemble des évènements et contient les registres stockant le résultat du chiffrement ou déchiffrement ainsi que la clé de chiffrement. Le second est un gestionnaire numérique du signal d'horloge (DCM) qui permet de fournir sur commande un signal d'horloge de fréquence 100MHz, 50MHz ou 25MHz au troisième bloc. Le troisième bloc est un AES 128bits. Il chiffre un texte clair en 10 rondes à la fréquence fournie par le DCM. Enfin, le quatrième bloc est une interface RS232 permettant la communication entre la machine d'état et l'utilisateur. Le placement sur le circuit de ces différents blocs a été contraint afin de les séparer. Le placement est visible sur la Fig. 4.8. Ces contraintes ont été imposées pour permettre l'analyse spatiale des effets de l'injection EMP.

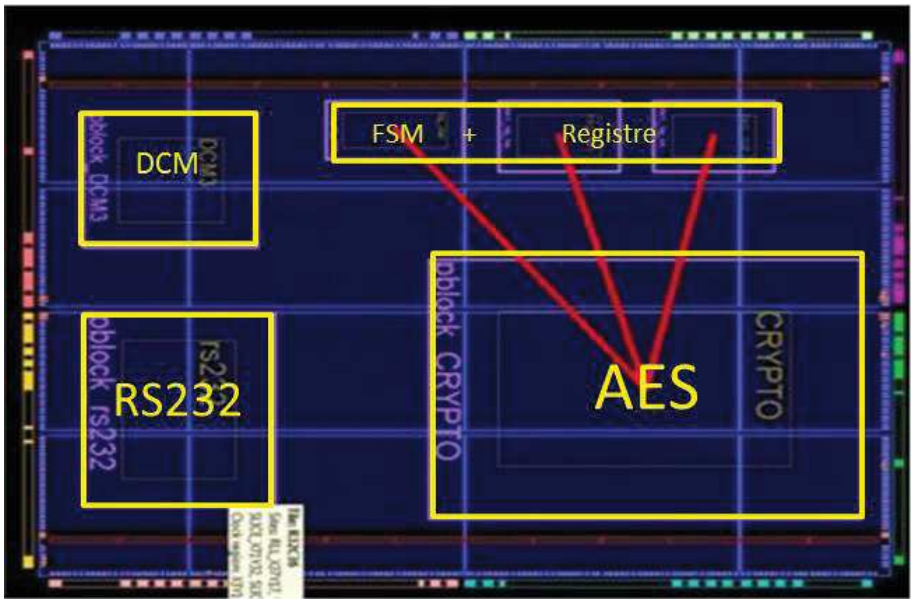

FIGURE 4.8: Placement des différents blocs du circuit de test

4.6.2 Objectifs du test

Dans les sections précédentes, l'accent a été mis sur les différents modèles de fautes. Cependant, l'une des premières questions qui a été abordée est la localisation des fautes

produites. Pour répondre à cette question, des cartographies révélant la probabilité d'induire des fautes ont été réalisées sur le circuit de test décrit dans la section 4.6.1. L'injection EMP a été réalisée à un moment précis du chiffrement de l'AES : la neuvième ronde. Les fautes obtenues ont été analysées pour révéler leur nature multibits ou monobits (plusieurs bits, un seul bit), le nombre d'octets fautés ou encore la position de la sonde d'injection permettant de perturber chacun des seize octets manipulés par l'AES.

Suite à ces expériences préliminaires, une seconde expérience a été menée. Pour cela, 100 injections ont été effectuées à plusieurs positions (positions où des fautes sont apparues lors des expériences précédentes) et ce pour plusieurs instants d'injection (t_{pulse}), permettant de couvrir la totalité du chiffrement AES avec un pas de temps Δt_{pulse} égal à $1ns$. Cette expérience a été effectuée pour les trois valeurs différentes de la fréquence du signal d'horloge délivré par le DCM. Au cours de ces injections, l'AES a effectué les chiffrements de 100 messages clairs choisis aléatoirement. Ces dernières expériences ont été menées afin de déterminer si les fautes obtenues sont des fautes de timing ou des fautes d'échantillonnage selon les tests de discrimination introduits dans la section 4.4.4.

4.6.3 Résultats expérimentaux

Cette section décrit les résultats expérimentaux obtenus et les protocoles qui ont été suivis pour les obtenir.

4.6.3.1 Cartographie et localité des fautes lors d'une injection EMP

Les cartographies de la Fig. 4.9 révèlent la probabilité d'induire une faute dans le circuit, avec deux types de sonde d'injection (plate et oméga). Les cartographies ont été obtenues en effectuant à chaque coordonnées (X,Y) 100 injections avec 10 textes clairs choisis aléatoirement (soit 10x10 injections) avant de lancer les expériences. Pour chaque position les textes clairs utilisés sont identiques. Au cours de ces injections, l'impulsion de tension fournie par le générateur d'impulsion est d'une amplitude $Vpulse = 44V$ et d'une durée de $PW = 8ns$. Les extrémités en ferrite des sondes étaient en contact avec la surface du circuit. La fréquence du signal d'horloge fourni à l'AES a été fixée à 100MHz et l'alimentation du circuit a été fixée à $V_{dd} = 1.2V$, sa valeur nominale.

Les cartographies réalisées avec la sonde d'injection plate ont été obtenues avec un pas de déplacement de $\Delta X = \Delta Y = 200\mu m$. Celles effectuées avec la sonde d'injection oméga ont quant à elles été obtenues avec un pas de déplacement de $\Delta X = \Delta Y = 100\mu m$. Les Fig. 4.9a et 4.9b donnent la probabilité d'introduire une faute lors d'une injection EMP. Dans le cas de la sonde d'injection plate, deux types de fautes ont été observées : certains messages chiffrés étaient erronés et dans d'autres cas le circuit était muet. Ce dernier cas correspond à la situation dans laquelle le FPGA cesse de fonctionner correctement et ne donne aucune réponse, quelle soit bonne ou mauvaise. La Fig. 4.9c montre les coordonnées auxquelles le circuit est muet. Il est à noter qu'avec la sonde d'injection oméga, le circuit n'est jamais devenu muet et seules des fautes de chiffrements sont apparues.

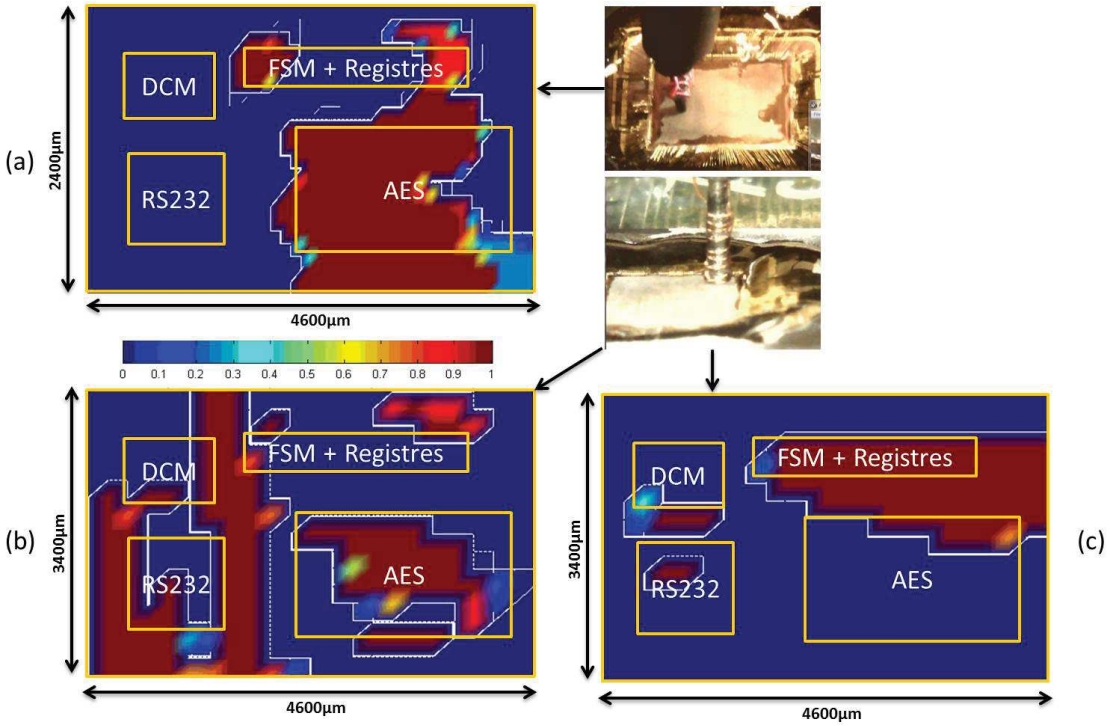

FIGURE 4.9: Probabilité de générer (a) un texte chiffré fauté avec la sonde d'injection oméga, (b) un texte chiffré fauté avec la sonde d'injection plate et (c) que le circuit soit muet avec la sonde d'injection plate

Comme le montre le Fig. 4.9a, l'injection EMP avec la sonde d'injection oméga a un effet local. En effet, les fautes obtenues qui ont un fort niveau de probabilité sont dans des zones correspondant approximativement au placement des différents blocs constituants le circuit. Ces régions correspondent en effet aux placements de l'AES, des registres contenant la clé de chiffrement et le message chiffré, mais également au placement de la machine d'état (FSM). Il est intéressant de remarquer que les fautes produites avec la

sonde d'injection oméga placée au dessus de la machine d'état ne sont pas des mutes, mais des chiffrés fautés.

De même, on peut observer sur la Fig. 4.9b que les injections EMP réalisées avec une sonde d'injection plate sont également locales, mais les zones qui ont un fort taux de probabilité sont très différentes de celles observées sur la Fig. 4.9a. En effet, la zone de l'AES ayant un texte chiffré fauté est beaucoup plus petite et des zones additionnelles apparaissent, principalement autour de la machine d'état (FSM) et du gestionnaire de fréquence du signal d'horloge (DCM). En plus de ces différences spatiales qui peuvent probablement être expliquées par la différence des champs émis par les sondes d'injection comme évoqué section 4.3.2, la principale différence entre les résultats obtenus avec les deux sondes d'injection est l'apparition d'état ou le circuit est muet. Beaucoup d'injections effectuées avec la sonde d'injection plate produisent un effet de circuit muet tandis que cela ne se produit pas avec la sonde d'injection oméga.

Si ces cartographies mettent en valeur la nature locale des injections EMP, cette caractéristique est beaucoup plus évidente lorsque le lien entre la position de la sonde d'injection et les octets fautés est analysé. La Fig. 4.10 donne dans le cas d'une sonde d'injection oméga, la probabilité de générer une faute dans chacun des 16 octets traités par l'AES en fonction de la position de la sonde d'injection. Comme le montre la Fig. 4.10, le positionnement de la sonde d'injection a une influence sur le taux de fautes d'un octet donné, et les positions auxquelles il est facile de provoquer une faute dans un octet donné sont différentes pour chaque octet. Il existe toutefois des positions où il est possible de générer des fautes sur plusieurs octets.

Le caractère local de l'injection EM a une nouvelle fois était mis en évidence. Les coordonnées (X,Y) associées à une forte probabilité de générer une faute étant connue, les expérimentations visant à identifier le modèle de faute le plus adéquat pour l'injection EMP ont pu être réalisées.

4.6.3.2 Modèle de faute de l'injection EMP ?

Afin de connaitre quel modèle suit l'injection EMP, plusieurs campagnes d'injection ont été réalisées avec la sonde d'injection oméga positionnée à trois coordonnées distinctes qui ont une forte probabilité de produire des fautes (coordonnées connues grâce à la

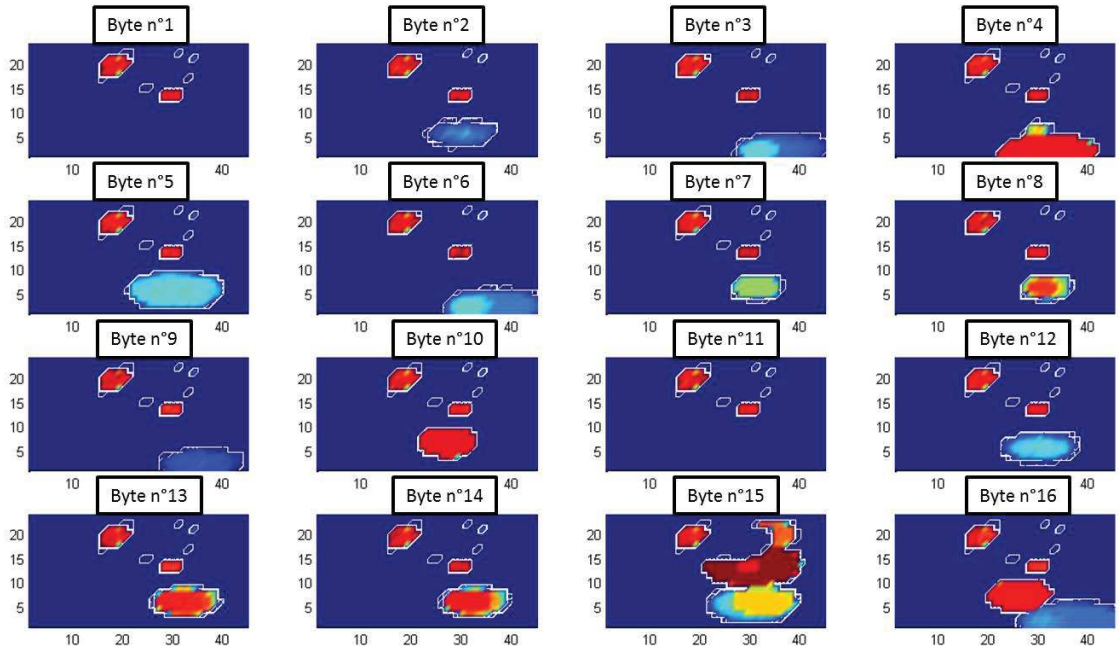

FIGURE 4.10: Probabilité de générer une faute pour chaque octet de l'AES en fonction de la position de la sonde d'injection (oméga)

Fig. 4.9). Au cours de ces campagnes d'injection deux variables expérimentales ont été examinées.

La première est la fréquence du signal d'horloge qui cadence l'AES et qui peut être fixée à trois valeurs différentes : $F_{AES} = 25MHz$, $50MHz$ et $100MHz$. La seconde variable expérimentale est l'instant (t_{pulse}) auquel les 100 injections EM sont produites (toujours avec les mêmes textes clairs). La plage de valeurs de t_{pulse} a été choisie en fonction de F_{AES} de sorte à balayer la totalité du chiffrement de l'algorithme AES (11 cycles d'horloge). Il est à noter qu'au cours de ces campagnes expérimentales, les autres paramètres de l'injection EMP ont été maintenus constants aux valeurs suivantes : $V_{pulse} = 44V$ et $PW = 8ns$.

Les résultats obtenus ont permis de créer la Fig. 4.11 qui rend compte de l'évolution du nombre d'octets fautés, pour une fréquence de F_{AES} de 100MHz, en fonction du moment d'injection. Comme on peut le voir, des intervalles de temps durant lesquels il est possible de générer des fautes apparaissent. Celux-ci sont régulièrement espacés de 10ns, valeur qui correspond à la période d'horloge de l'AES. Ces intervalles d'une durée égale à 6ns sont désignées par le terme de fenêtre de susceptibilité EM dans le reste de cette thèse. Ils sont séparés par des intervalles de temps durant lesquels aucune faute n'est créée avec l'injection EMP.

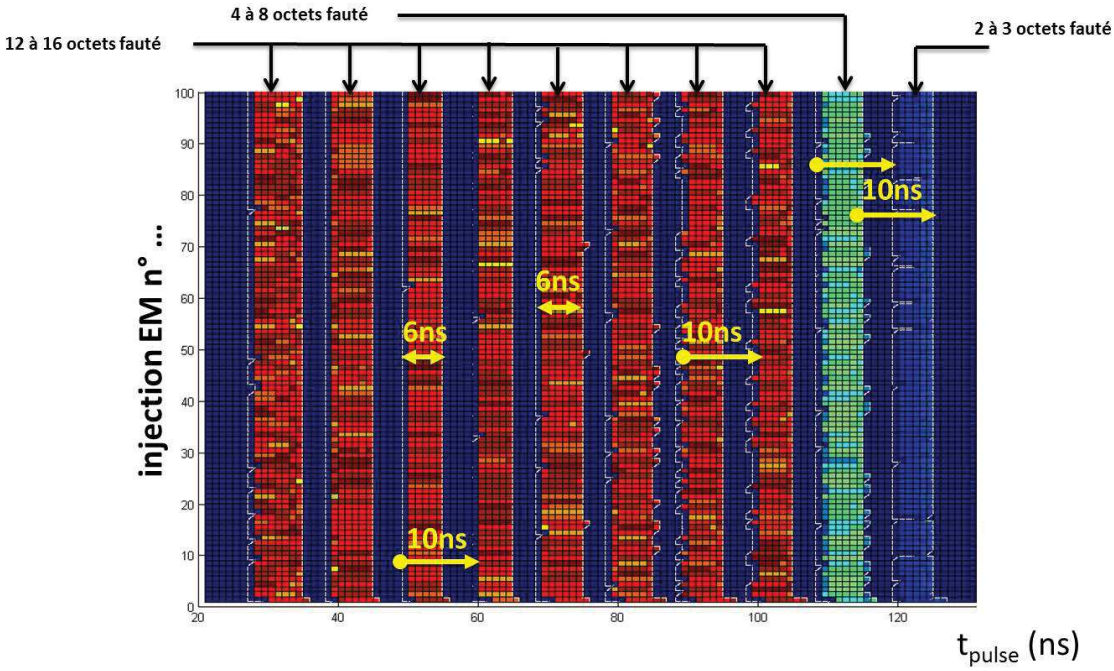

FIGURE 4.11: Nombre d'octets fautés à une position (X,Y) fixe en fonction du moment d'injection (t_{pulse}) pour 100 injections avec $F_{AES} = 100MHz$ et une sonde d'injection oméga

Compte tenu de ces résultats, et des tests de discrimination établis dans la section 4.4.4, il semble donc que le modèle le plus réaliste pour l'injection EMP est le modèle 'faute d'échantillonnage' et non le modèle 'faute de timing'. En effet, si les fautes qui ont été observées étaient des fautes de timing, il n'y aurait pas d'intervalles de temps au cours desquels aucune faute n'est générée car le moment où l'augmentation du délai provoquée par l'injection EMP ne conditionne pas l'apparition d'une faute.

Toutefois, afin de mieux soutenir ce résultat, ces expériences ont été répétées sur les trois dernières rondes de l'AES successivement cadencées à $F_{AES} = 100MHz$, $50MHz$ et $25MHz$. La Fig. 4.12 montre, pour ces trois valeurs de fréquence, la probabilité de générer une faute. A noter que l'échelle en abscisse de ces trois figures n'est pas la même afin d'avoir une meilleur visualisation des résultats. L'observation de ces trois évolutions montre clairement que l'apparition des fenêtres de susceptibilité EM est indépendante de la fréquence du signal d'horloge et que la largeur de cette fenêtre est constante : 6ns. En outre, on peut observer que la durée des intervalles de temps au cours desquels aucune faute n'est générée augmente de façon linéaire avec la période d'horloge (34ns pour $F_{AES} = 25MHz$, 14ns pour $F_{AES} = 50MHz$ et 4ns pour $F_{AES} = 100MHz$). Ces expérimentations confirment bien que le modèle de faute le plus réaliste pour l'injection EMP est bien le modèle 'faute d'échantillonnage'.

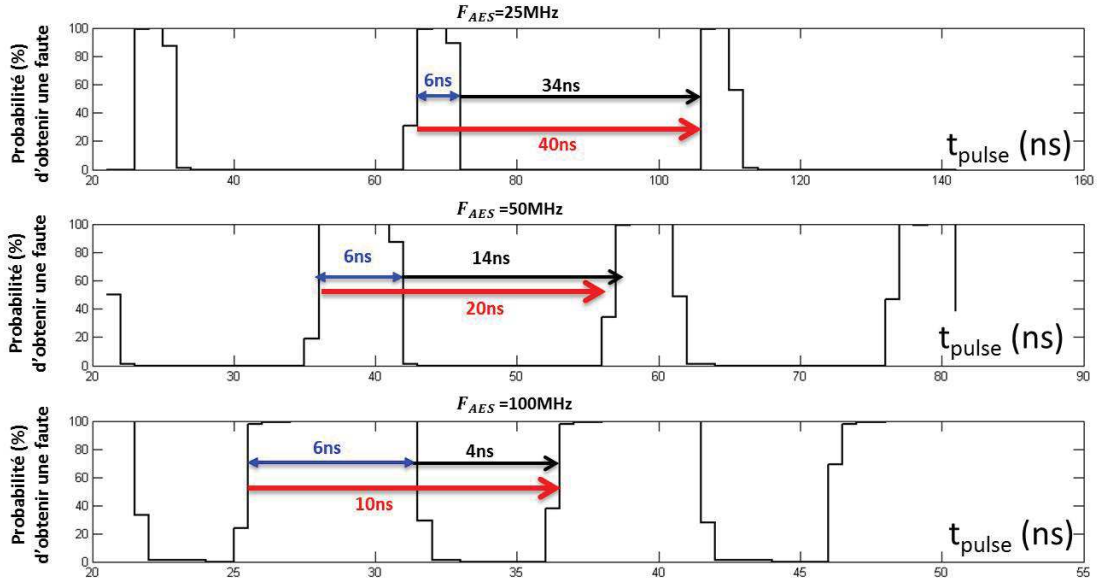

FIGURE 4.12: Probabilité de générer une faute sur un AES hardware implémenté sur un FPGA spartan3-1000 en fonction du moment de d'injection (t_{pulse}) pour 3 valeurs de fréquences différentes et avec une sonde d'injection oméga

Si ces expérimentations sont suffisantes pour démontrer que les fautes obtenues sont des fautes d'échantillonnage, dans le cas d'un AES implémenté sur un FPGA, des expérimentations similaires ont été menées sur un micro-contrôleur de 32 bits moderne. L'objectif était de vérifier que le modèle 'faute d'échantillonnage' n'est pas spécifique au FPGA. Ce micro-contrôleur est conçu en technologie de 90nm, comporte un régulateur interne pour maintenir la tension d'alimentation du circuit à 1.2V. Son principal bloc est un processeur ARM Cortex M4 fonctionnant à une fréquence de 30MHz. Ce micro-contrôleur intègre aussi un AES 128bits matériel cadencé a une fréquence configurable. Pour cette expérimentation, l'AES fonctionne a une fréquence de 120MHz (T_{clk}=8.3ns).

La Fig. 4.13 donne la probabilité de générer une faute pour trois valeurs de V_{pulse} : +120V, +160V et +190V. L'intervalle de temps sur lequel les injections EMP ont été effectuées correspond au trois dernières rondes de l'AES. La sonde d'injection EMP a été placée au dessus de l'AES lors de ces expérimentations afin que les fautes produites soit des fautes de chiffrement. Comme on peut le voir, le comportement observé est similaire a celui trouvé dans le cas du FPGA. Les trois fenêtres de susceptibilités sont espacées de 8.3ns, ce qui correspond à la fréquence de l'AES ($F_{AES} = 120MHz$). Cependant, la durée de ces fenêtres de susceptibilité varie de 2.1ns à 4.25ns en fonction de la valeur de V_{pulse}. Ces durées sont plus faibles que dans le cas du FPGA (6ns). Une explication probable peut être la valeur typique du délai de propagation de D_{CK2Q} d'une DFF qui

est significativement plus court dans le cas d'un ASIC (350ps) que dans le cas d'un FPGA (1ns). Enfin, ces fenêtres sont plus arrondies que dans le cas de l'AES embarqué sur un FPGA. Cela peut s'expliquer par la présence d'une faible gigue sur le signal de synchronisation qui permet le déclenchement de l'injection. Cette gigue n'est pas présente sur le FPGA car le signal d'horloge est généré par un quartz externe, tandis que pour le micro-contrôleur, le signal d'horloge est généré par une PLL interne.

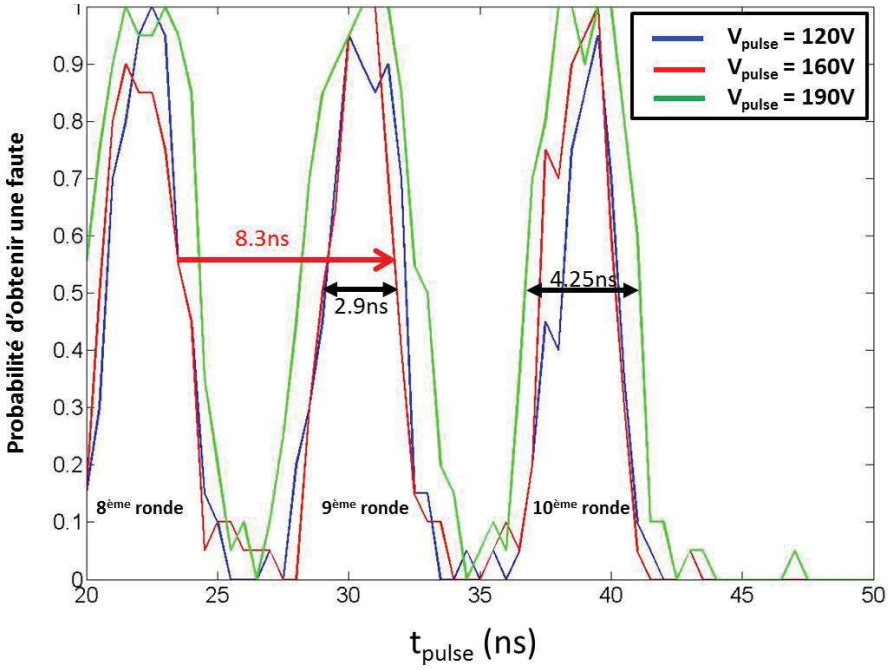

FIGURE 4.13: Probabilité de générer une faute sur un AES matériel implémenté sur un micro-contrôleur 32bit en fonction du moment de d'injection (t_{pulse}) pour 3 valeurs de V_{pulse} et avec une sonde d'injection oméga

4.7 Modèle 'faute d'échantillonnage'

Compte tenu des expériences et des observations décrites dans ce chapitre, il semble que le modèle de faute associé à l'injection EMP soit le modèle 'faute d'échantillonnage', qui correspond à une perturbation du processus de commutation des DFFs. Un tel évènement peut être généré à chaque front montant du signal d'horloge, ou a tout moment si les DFFs disposent de signaux de set et reset asynchrone. Cependant, il semble plus difficile de perturber les signaux de set et reset des DFFs au repos lorsque on observe les valeurs de V_{pulse} dans la section 4.5 (140V pour produire des bitset et bitreset) et dans la section 4.6 (44V pour générer des fautes lors de la commutation des DFFs). Cette

section propose donc une description de ce qu'est le modèle 'faute d'échantillonnage', qui correspond le plus à l'injection EMP.

La Fig. 4.14 montre des impulsions électromagnétiques générées par le système décrit dans la section 4.3.1 pour des valeurs croissantes de V_{pulse}. Ces émissions électromagnétiques ont été mesurées avec une sonde Langer. Comme on peut le voir, un pic de tension produit deux émissions électromagnétiques : une positive et une négative associées aux fronts montant et descendant du pic de tension. La première impulsion a généralement une amplitude plus élevée (en valeur absolue) que la seconde. On peut également observer qu'augmenter V_{pulse} équivaut à augmenter l'amplitude de l'impulsion électromagnétique sans pour autant augmenter sa largeur. Il est supposé pour plus de facilité ci-après, que V_{pulse} est une mesure directe de l'amplitude de l'impulsion électromagnétique. Cela revient alors à considérer un couplage électromagnétique idéal entre la sonde d'injection et le circuit ciblé par l'injection.

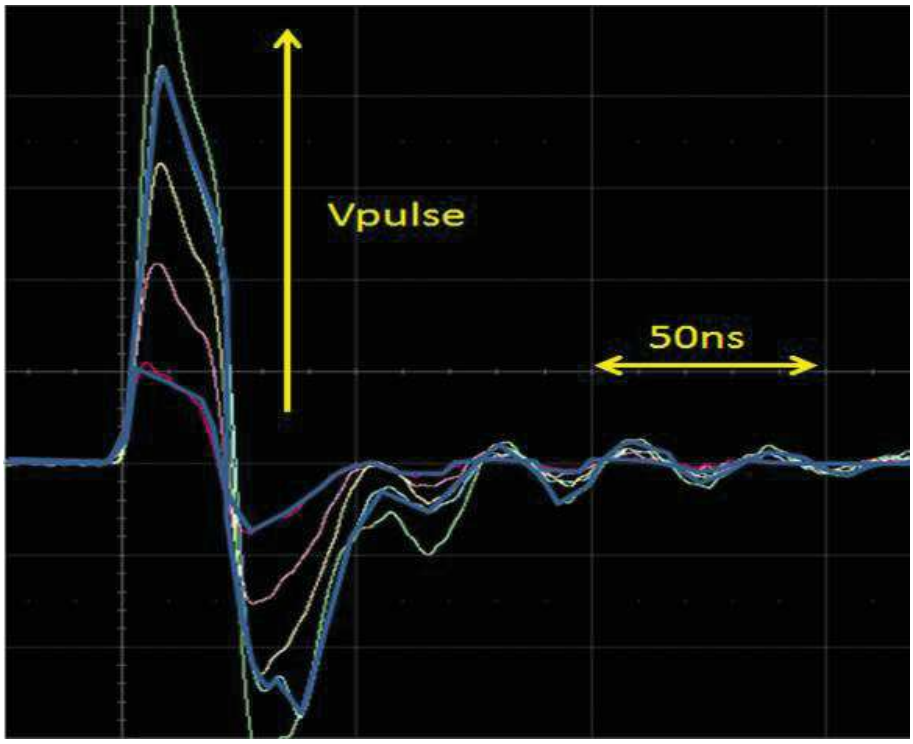

FIGURE 4.14: Image d'un champ EM émis par une sonde d'injection lors d'une injection EMP

Sur la Fig. 4.15, sont reportées deux valeurs de tension de seuil, $V_{thhaute}$ et $V_{thbasse}$, associées à la susceptibilité électromagnétique d'une DFF. $V_{thhaute}$ est l'amplitude minimale que l'injection EMP doit avoir pour générer une faute à n'importe quel moment, c'est à dire pour produire une faute de type bitset ou bitreset. $V_{thbasse}$ représente quant

à elle l'amplitude minimale que l'injection EMP doit avoir pour générer une faute lors de la commutation d'une DFF. Bien entendu, ces valeurs de tension de seuil dépendent de nombreux paramètres de conception de la DFF, mais aussi du circuit ciblé par l'injection EMP qui définit la qualité du couplage EM entre la sonde d'injection et le circuit. Pour une DFF donnée dans un circuit intégré, la position de la sonde d'injection est aussi un critère important. De plus, il est évident que $V_{thhaute} > V_{thbasse}$.

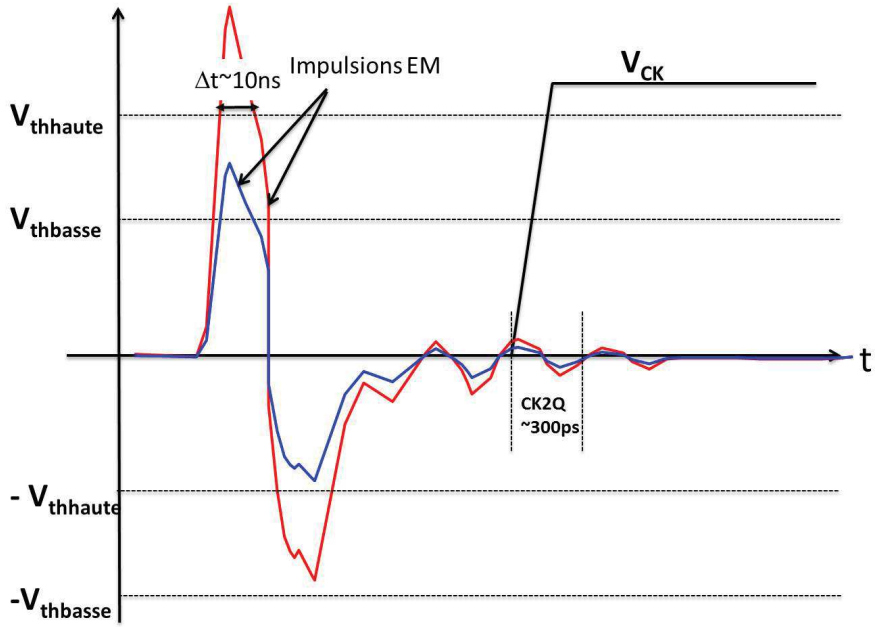

FIGURE 4.15: Image d'un champ EM émis par une sonde d'injection lors d'une injection EMP

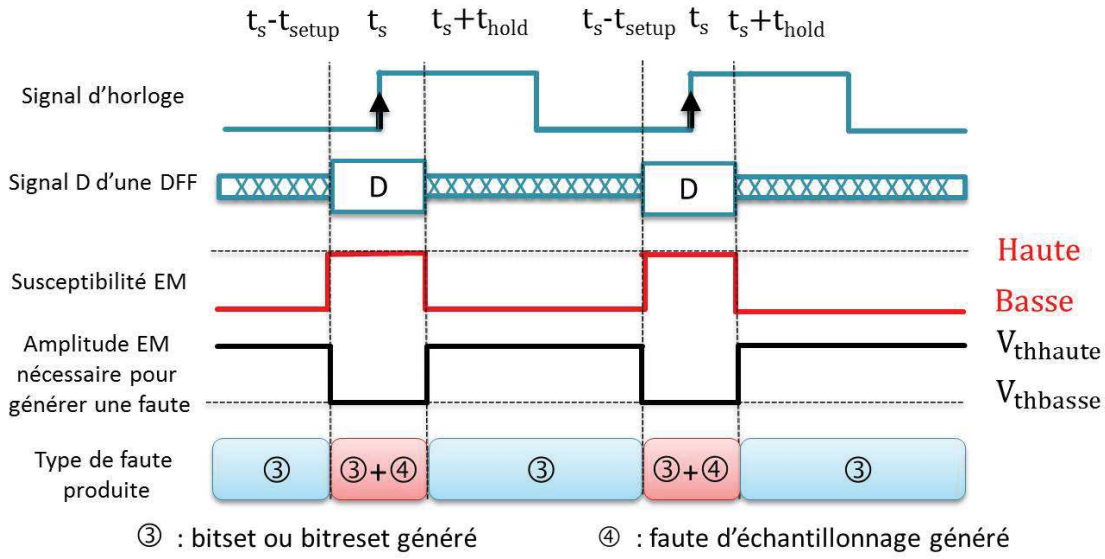

FIGURE 4.16: Modèle 'faute d'échantillonnage'

A partir des figures précédentes, il est possible de résumer le modèle de faute à la Fig. 4.16. La fenêtre de susceptibilité électromagnétique apparait lorsque l'amplitude du signal d'injection est modéré ($V_{thhaute} > V_{pulse} > V_{thbasse}$). Ainsi si l'injection EMP se produit durant la fenêtre de susceptibilité (qui correspond à la fenêtre de stabilité de la Fig. 4.4) une faute apparait. Tandis que si l'injection se produit en dehors de la fenêtre de susceptibilité, alors aucune faute n'est générée. Par contre, si l'amplitude de l'EMP est réduite jusqu'à atteindre $V_{thhaute} > V_{thbasse} > V_{pulse}$, alors aucune ne sera produite même pendant la fenêtre de susceptibilité.
Maintenant, si les amplitudes des EMP ont des valeurs assez élevées ($V_{pulse} > V_{thhaute} > V_{thbasse}$), des fautes apparaissent indépendamment du moment de l'injection t_{pulse}, c'est à dire même si le signal d'horloge est désactivé des fautes apparaissent (comme montré dans la section 4.5). Dans ce cas, la probabilité de générer une faute est constante au cours du temps et ne dépend, dans la pratique, que de l'existence d'un couplage électromagnétique suffisant entre la sonde d'injection et le circuit ciblé par l'attaque.

4.8 Conclusion

Dans ce chapitre, une description de la plateforme d'injection EMP et plusieurs expérimentations effectuées sur FPGA et sur un micro-contrôleur moderne on été présentées. Les expérimentations menées ont permis de mettre de évidence l'effet local de l'injection EMP. Ces expérimentations ont aussi permis d'identifier le phénomène expliquant au mieux, et à ce jour, le type de fautes obtenues. Dans les anciennes publications, il a été suggéré que les fautes générées par l'injection EMP étaient des fautes de timing. Cependant, après une analyse des différentes sources probables d'erreur sur un circuit en présence d'une injection EMP, certaines expérimentations ont été définies et utilisées de manière à identifier le modèle de faute le plus réaliste pour l'injection EMP. Les résultats obtenus ont montré que le modèle 'faute de timing' n'explique pas tous les résultats obtenus, tandis que le modèle 'faute d'échantillonnage', qui est présenté dans ce chapitre, correspond mieux aux résultats obtenus. Ce modèle suggère que l'injection EMP, menée avec des sondes d'injection améliorées, est suffisamment puissante pour perturber le processus de commutation d'une DFF et même de déclencher les signaux de set et reset d'une DFF en émettant une injection EMP encore plus forte.

Chapitre 5

Etude des effets de la gestion dynamique aléatoire de V_{dd}, F, V_{bb} sur l'injection EMP et BBI

Dans ce chapitre, une analyse expérimentale des effets de variations de tension, fréquence et polarisation de substrat sur les méthodes d'injection est présentée.

5.1 Généralités

L'un des objectifs de cette thèse, est de connaitre les effets des variations de tension d'alimentation, de la fréquence de fonctionnement et de la polarisation du substrat, paramètres importants pour la maitrise des performances et de la consommation des circuits. Dans le chapitre 3, une analyse des effets de ces variations sur les attaques par observation a été effectuée. Dans ce chapitre, une analyse des effets de la RDVFS sur des méthodes d'injection de fautes est réalisée. Les méthodes d'injection de fautes considérées sont l'injection EMP, qui a été décrite dans le chapitre 4, et la *Body Bias Injection* (BBI) décrite dans [46]. L'injection de fautes par tir laser n'a pas pu être réalisée car aucune plateforme d'injection laser n'était à disposition durant cette thèse au LIRMM. En outre, ce travail était dévolu au Centre Microelectronique de Provence (CMP) dans le cadre du projet FSN MAGE. Avant d'étudier les effets de la RDVFS sur

ces deux méthodes d'injection, une comparaison entre ces deux méthodes a tout d'abord été réalisée.

Pour effectuer ces expérimentations, un micro-contrôleur conçu en technologie de 90nm a été utilisé comme cible d'attaque. Il comporte un régulateur interne qui permet de maintenir la tension d'alimentation du circuit à l'une des valeurs suivantes : 1.1V, 1.2V ou 1.3V. Le principal bloc du micro-contrôleur est un processeur ARM Cortex M4 fonctionnant à une fréquence de 30MHz. Ce micro-contrôleur intègre aussi un AES 128bits matériel cadencé à une fréquence fournie par une PLL configurable. Le placement des différents blocs est représenté sur la Fig. 5.1. De plus, il est possible de fixer la polarisation du substrat du circuit à des valeurs prédéfinies : 0mV, 200mV et 400mV.

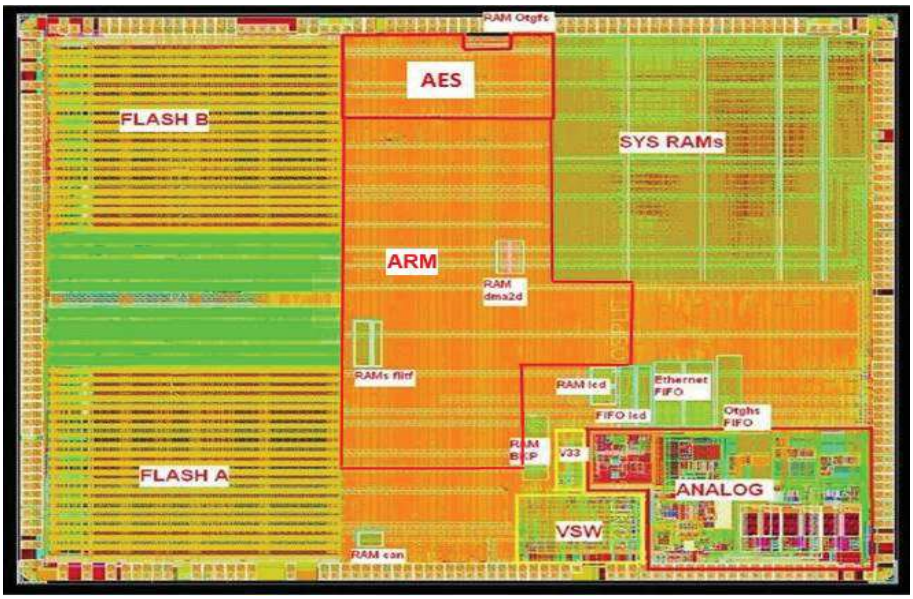

FIGURE 5.1: Placement des différents blocs du micro-contrôleur

Pour étudier les effets de toutes ces variations, les mêmes tests qui ont été précédemment décrits dans la section 4.6 sont utilisés. Ils permettent ainsi de déterminer si les variations de tension d'alimentation, de fréquence et de polarisation de substrat ont un effet sur les capacités d'injection EMP et BBI. Les effet recherchés peuvent être le changement des zones de susceptibilité pour la variation d'un même paramètre ou la modification du moment d'injection (si l'on souhaite effectuer une injection à un moment précis). Ces expérimentations ont été effectuées avec le boitier du circuit ouvert. Pour ces deux méthodes d'injection, les paramètres du générateur d'impulsion ont été fixés aux valeurs $V_{pulse} = 130V$ et $PW = 8ns$. Le choix de ces valeurs a été effectué d'après les expérimentations réalisées avec l'injection EMP.

La BBI injecte une impulsion dans le substrat du circuit. Il est donc nécessaire d'avoir accès à la face arrière du circuit. Ainsi toutes les expérimentations (injection EMP comme BBI), ont été effectuées sur la face arrière du circuit afin de pouvoir les comparer.

5.2 Comparaison entre l'injection EMP et BBI

Comme signalé en section 2.6.2, seuls trois moyens d'injection de fautes sont généralement utilisés. En analysant la méthode d'injection par pic de tension dans le substrat (*Body Bias Injection* (BBI)), décrite dans [46], on peut se rendre compte qu'elle dispose de plusieurs éléments en commun avec l'injection EMP. En effet, la seule différence entre ces deux méthodes vient des sondes d'injection utlisée.

5.2.1 Mise en place des expérimentations

Afin de pouvoir comparer les méthodes d'injection EMP et BBI, et de déterminer les avantages et les inconvénients de l'une sur l'autre, la sonde du banc d'injection EMP, présenté par la section 4.3.1, a été remplacée afin que l'injection BBI puissent être effectuée.
La Fig. 5.2 montre les sondes utilisées pour effectuer la comparaison entre l'injection EMP et BBI. La Fig. 5.2a montre la sonde BBI utilisée. Elle est en tungstène et a un diamètre de $200\mu m$. Sa pointe a quant à elle un diamètre de $20\mu m$. La Fig. 5.2b montre une sonde d'injection EMP plate dont le diamètre (ferrite + fil) est de $800\mu m$.

Afin de pouvoir comparer l'injection EMP et la BBI, les mêmes paramètres d'injection sont utilisés pour ces deux méthodes. Ainsi, la tension de l'impulsion fournie par le générateur d'impulsion est de $V_{pulse} = 130V$ et la durée de l'impulsion fixée à $PW = 8ns$. Le circuit est lui aussi configuré à l'identique pour ces deux méthodes. La fréquence de chiffrement de l'AES est fixée à $F = 50MHz$ (20ns). Le régulateur du circuit est paramétré à $V_{dd} = 1.2V$. Aucune polarisation de substrat n'est appliquée $V_{bb} = 0mV$.

Afin de connaitre les différentes zones sensibles du circuit en fonction de la méthode d'injection, des cartographies représentant le probabilité de générer une faute pour une position (X,Y) ont été réalisées avec ces deux méthodes. Le pas entre chaque position

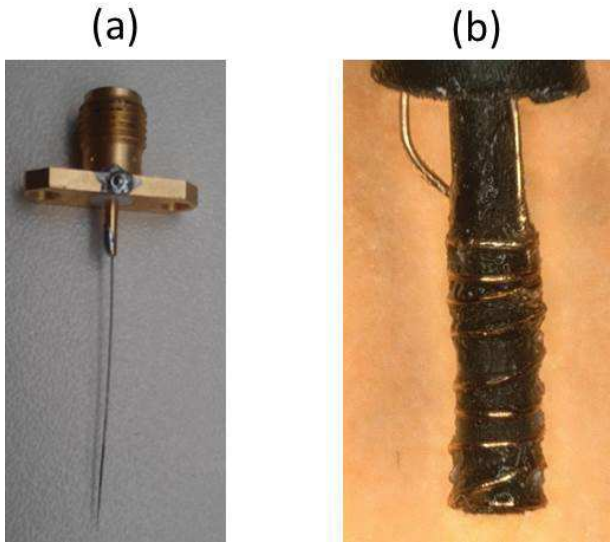

FIGURE 5.2: Sondes d'injection utilisées (a) sonde BBI et (b) sonde EMP

de ces cartographies a été fixé à $200\mu m$. Le moment de l'injection a été paramétré pour que celle-ci se produise pendant la 9ème ronde du chiffrement de l'AES.

5.2.2 Analyse des résultats obtenus

Les résultats de ces expérimentations sont représentés sur la Fig. 5.3. La Fig. 5.3a représente la cartographie du circuit lorsque n'importe quel type d'erreur a été généré avec l'injection EMP. L'injection EMP a générée un grand nombre de fautes sur les mémoires FLASH du circuit et sur la partie centrale qui correspond au placement du processeur ARM. En analysant les fautes obtenues, il apparait qu'un grand nombre de celles-ci sont des 'mutes' : le circuit ne répond plus. La Fig. 5.3b représente la cartographie du circuit lorsqu'une faute sur le chiffrement s'est produite avec l'injection EMP. On peut ainsi se rendre compte que les meilleures positions pour générer des fautes sur le message chiffré sont celles au dessus de l'AES.

La Fig. 5.3c donne la probabilité d'induire n'importe quel type d'erreur avec la méthode BBI. La différence est flagrante avec celle obtenue pour l'injection EMP (Fig. 5.3a). On peut ainsi remarquer que lorsqu'on produit une injection BBI au dessus du processeur ARM, aucune faute n'apparait. Seules quelques zones au dessus des mémoires FLASH, de la partie analogique et de l'AES sont sensibles à la BBI. En se focalisant sur les fautes générées dans les messages chiffrés, qui sont visibles sur la Fig. 5.3d, on remarque que la zone la plus propice est celle au dessus de l'AES. Cependant cette zone est différente

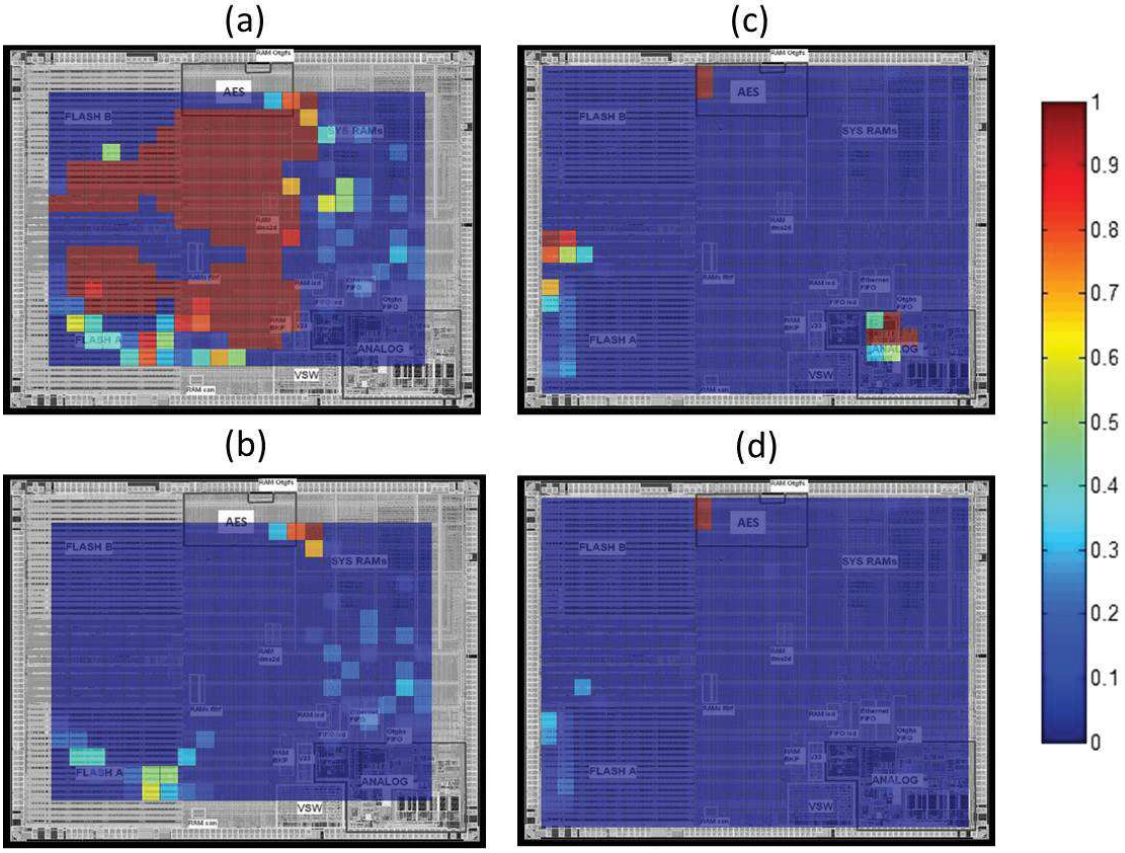

FIGURE 5.3: Probabilité d'induire : (a) et (c) des fautes de nature quelconque avec l'injection EMP (a) et BBI (c), (b) et (d) des fautes de chiffrement avec l'injection EMP (b) et BBI (d)

de celle obtenue avec l'injection EMP.

Il est fort probable que cette différence soit due aux tailles des sondes d'injection EMP et BBI qui ont un diamètre fortement différent. De plus, il est possible qu'il y ait un meilleur couplage entre la sonde d'injection EMP et le circuit sur une zone différente que celle où les fautes apparaissent avec la méthode BBI.

En connaissant les zones de susceptibilité du circuit pour ces deux méthodes d'injection, les sondes d'injection ont été placées aux endroits les plus sensibles pour chacune de ces deux méthodes puis une variation de l'instant d'injection t_{pulse} a été effectuée. Cette expérience a été effectuée dans le but de connaitre si ces deux méthodes suivent le même modèle de faute. La Fig. 5.4 reporte les résultats obtenus lors de cette expérience. On peut ainsi s'apercevoir que l'injection EMP suit bien le modèle 'faute d'échantillonnage' défini dans la section 4.7. On peut aussi remarquer que la méthode BBI semble suivre le même modèle. Cependant, des différences entre ces deux méthode d'injection apparaissent. La première est que pour chaque front montant d'horloge du circuit l'injection

EMP génère une faute, ce qui n'est pas le cas pour la méthode BBI. Il apparait donc que certaine ronde soit plus robuste à la méthode BBI. Il n'a pas était possible d'expliquer ce phénomène car il aurait été nécessaire de connaitre tous les paramètres de la conception du circuit, ce qui n'a pas été possible pour des aspects de confidentialité.

Le second effet visible est la durée des fenêtres de susceptibilité. Pour l'injection EMP celles-ci sont d'une durée de 4ns, tandis que pour la BBI certaines fenêtres ont une durée de 4ns et d'autres d'une durée de 16ns. Il est difficile de connaitre l'origine de cette différence entre les fenêtres de susceptibilité en fonction des différentes rondes de l'AES. Cependant, il est possible que cette différence entre ces deux méthodes d'injection soit due à l'impulsion fournie par le générateur pour perturber le circuit. La Fig. 5.5 représente l'image de l'impulsion perturbant le circuit pour l'injection EMP et BBI. La sonde d'injection BBI est connectée directement au circuit par le substrat. L'impulsion émise au circuit est alors celle fournie par le générateur d'impulsion. Pour l'injection EMP la perturbation émise par la sonde d'injection est définie par la dérivée du signal fourni par le générateur d'impulsion. Ainsi, la perturbation pour l'injection EMP sera générée durant le front montant de l'impulsion (qui est de 1.5ns), tandis que pour la BBI elle est de la durée de l'impulsion (8ns).

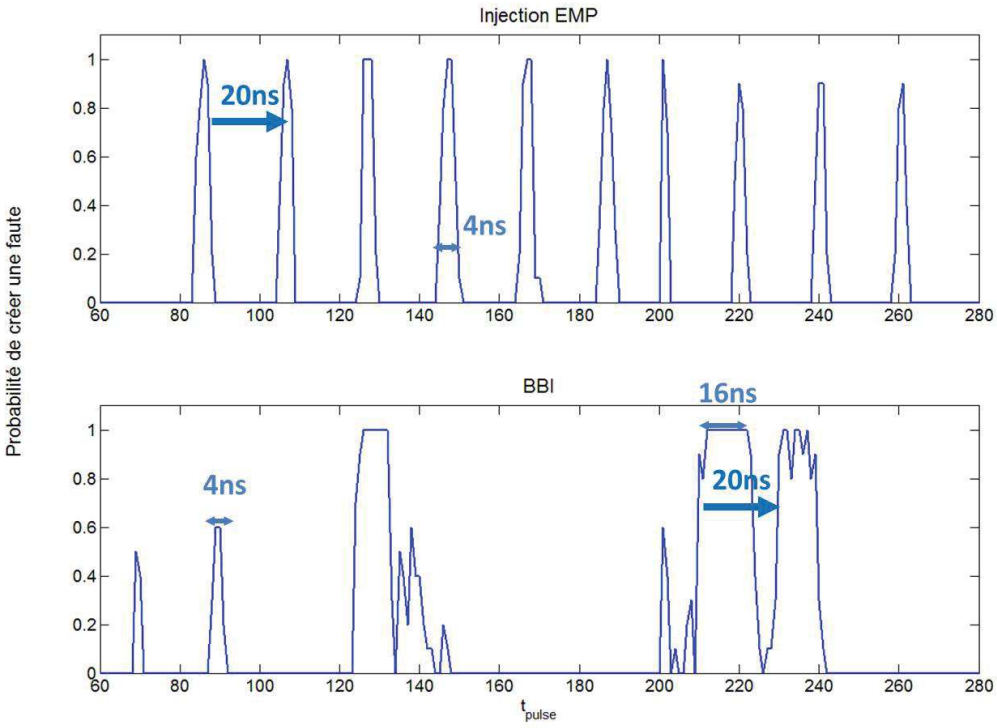

FIGURE 5.4: Probabilité de générer une faute en fonction de l'instant d'injection t_{pulse} de l'EMP et du pic de tension (BBI)

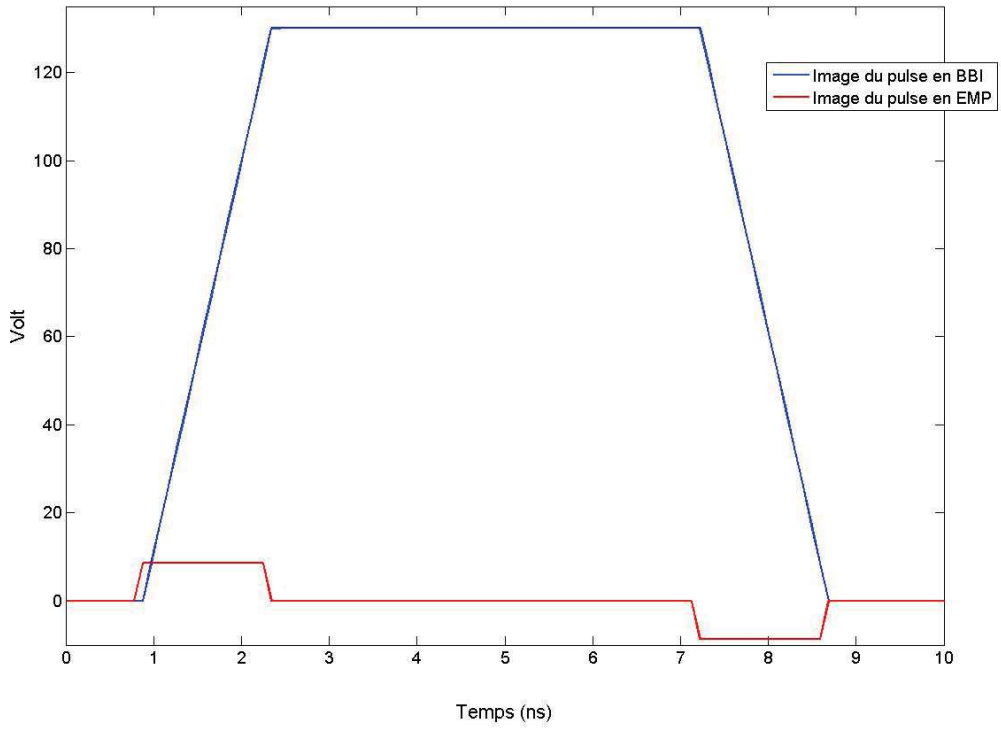

FIGURE 5.5: Image de l'impulsion perturbant le circuit pour l'injection EMP et BBI

A partir des expérimentations effectuées, on peut en conclure que l'injection BBI a un effet beaucoup plus local que l'injection EMP. Ceci peut s'expliquer par le fait que la sonde d'injection EMP utilisée pour ces expériences est huit fois plus grande que celle utilisée par la méthode BBI et que donc son rayonnement s'étend largement au dessus de la surface. Cependant, pour pouvoir utiliser la BBI, l'attaque doit s'effectuer sur la face arrière du circuit et il est nécessaire d'avoir un accès au substrat du circuit. Cette contrainte n'existe pas pour l'injection EMP qui peut fonctionner aussi bien sur la face avant que la face arrière, et à travers le boitier du circuit.
De plus, les fautes qui sont produites par ces deux méthodes d'injection semblent suivre le même modèle 'de faute d'échantillonnage' défini dans la section 4.7. Toutefois, il est nécessaire d'effectuer plus de travaux avant de pouvoir conclure de manière définitive que la BBI suit bien ce modèle.

5.3 Effet de la RDVFS sur les méthodes d'injection

Dans cette section, une étude des effets de la RDVFS sur les capacités d'injection EMP et BBI est effectuée. Afin d'étudier les effets d'une variation de tension, l'AES matériel

implémenté dans le circuit est ciblé. Le moment de l'injection est réglé de manière à ce que l'injection se produise durant la $9^{ème}$ ronde de l'AES. Les mêmes tests qui ont été décrit dans la section 4.6 ont été effectués.

5.3.1 Effet d'une variation de tension sur l'efficacité de l'injection EMP

La Fig. 5.6 donne les cartographies des probabilités d'injecter n'importe quel type de fautes, ou des fautes de chiffrement, dans le circuit en fonction de la tension d'alimentation. Les cartographies Fig. 5.6a, b et c donnent les zones de susceptibilité du circuit lorsqu'on produit n'importe quel type de faute. On peut ainsi remarquer une forte ressemblance entre les trois cartographies. Les zones les plus sensibles se situent sur le processeur ARM, les mémoires FLASH et l'AES matériel du circuit. On remarque tout de même un léger décalage des zones de susceptibilité. Ces différences peuvent s'expliquer partiellement par un léger décalage entre chaque cartographie, due au positionnement de la sonde. Le concepteur du circuit, n'a pas pu fournir de plus amples informations sur ce circuit pour cause de confidentialité. Du coup, il n'est pas possible de chercher ou de fournir d'autres explications.

Sur les Fig. 5.6d, e et f sont représentées les zones de susceptibilité du circuit permettant d'induire des fautes sur le texte chiffré de l'AES. On peut s'apercevoir que les zones ayant une forte probabilité de faute sont les mêmes pour toutes les tensions d'alimentation. Elles se situent essentiellement au dessus de l'AES. A partir de ces zones, la sonde d'injection EMP a été placée sur les coordonnée (X,Y) fournies par les cartographies 5.6d, e et f, puis des analyses temporelles ont été effectuées.

La Fig. 5.7 représente la probabilité de générer une faute en fonction de l'instant d'injection (t_{pulse}) pour les trois tensions d'alimentation du circuit fonctionnant à une fréquence de 120MHz. On peut observer que le principal effet d'une variation de tension est une variation de la durée de la fenêtre de susceptibilité (définis en section 4.6.3.2). En effet, plus la tension est élevée, plus la durée de cette fenêtre est courte. Deux explications différentes peuvent être avancées.
La première est que les valeurs du temps de hold et de setup d'une bascule sont dépendantes de la valeur de la tension d'alimentation du circuit. Dans [97], l'auteur montre clairement cette dépendance. Pour la seconde explication, ce sont les valeurs de $V_{thhaute}$ et $V_{thbasse}$, définies en section 4.7, qui expliquent cela. En effet, ces valeurs

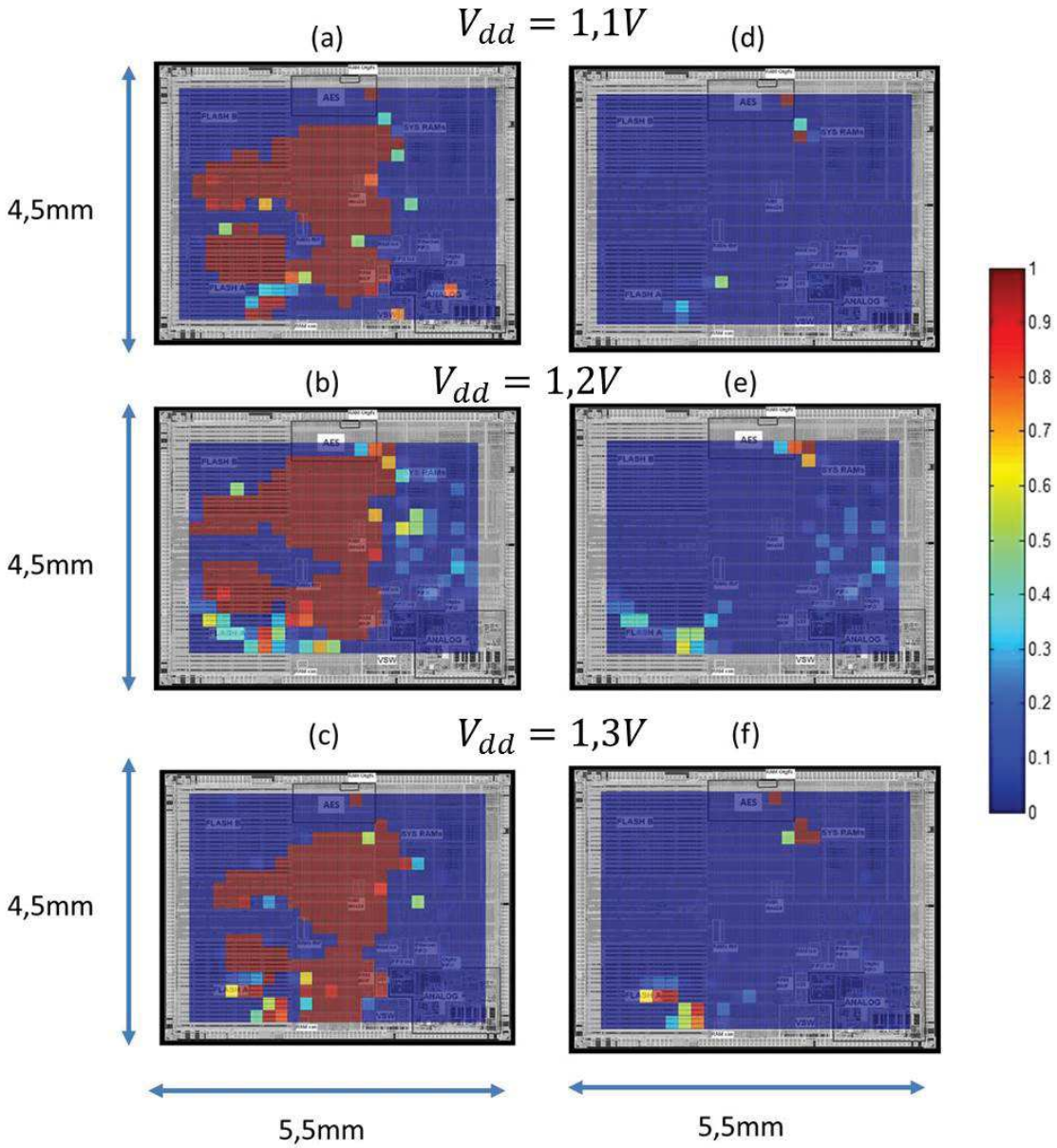

FIGURE 5.6: Cartographie de la probabilité d'induire (a,b,c) n'importe quel type de fautes avec une injection EMP lorsque le circuit est alimenté sous 1.1V(a), 1.2V(b) et 1.3V(c), (d,e,f) des fautes de chiffrement dans l'AES matériel alimenté sous 1.1V(d), 1.2V(e) et 1.3V(f)

sont dépendantes d'un grand nombre de paramètres parmi lesquels on trouve la tension d'alimentation du circuit.

5.3.2 Effet d'une variation de tension sur l'efficacité de l'injection BBI

Les mêmes expérimentations que celles reportées dans la section précédente ont été réalisées avec la méthode BBI. La Fig. 5.8 reporte les cartographies de la probabilité

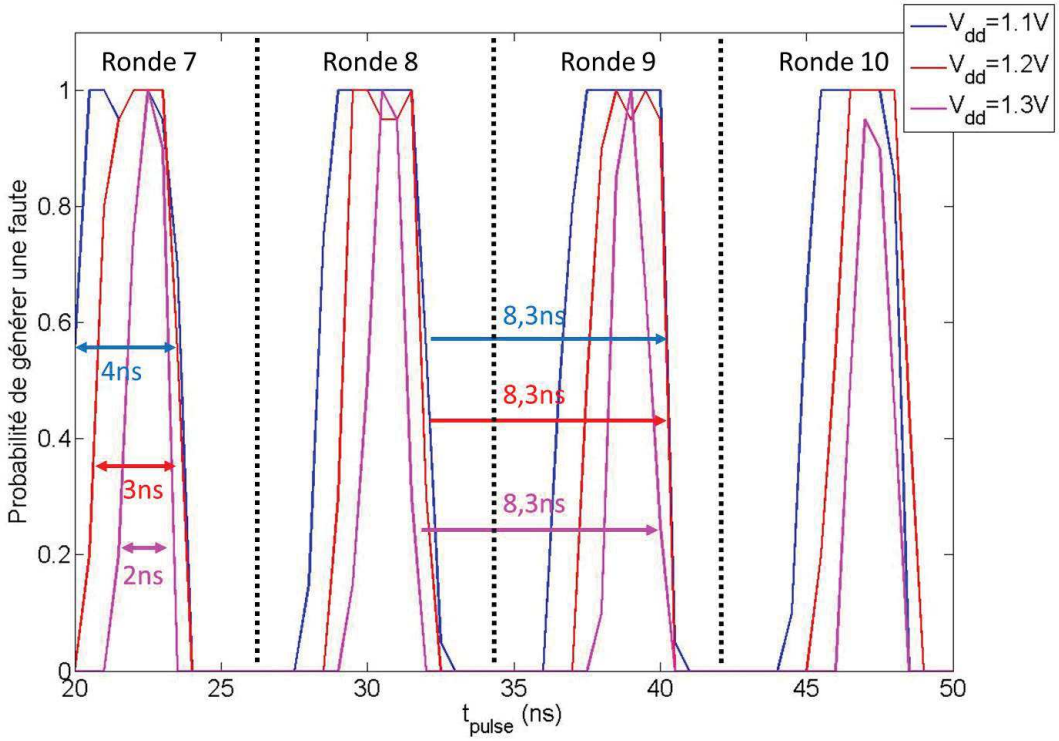

FIGURE 5.7: Probabilité de générer une faute sur un AES hardware implémenté sur un micro-contrôleur 32bit en fonction du moment de d'injection (t_{pulse}) pour 3 valeurs de tension d'alimentation et avec une sonde d'injection plate

d'injecter des fautes en fonction de la tension d'alimentation du micro-contrôleur. Les cartographies Fig. 5.8a, b et c donnent les zones de susceptibilité du circuit permettant de produire n'importe quel type de fautes. On peut remarquer que pour les tensions d'alimentation de $1.2V$ et $1.3V$, les zones de susceptibilité sont très similaires. Cependant, pour la tension d'alimentation $V_{dd} = 1.1V$, des zones de susceptibilité sur la RAM et les parties analogiques du circuit apparaissent. Ces zones de susceptibilité apparaissent seulement pour une tension d'alimentation de $V_{dd} = 1.1V$. Il est probable que le seuil de tension nécessaire pour injecter une faute dépende de la tension d'alimentation du circuit. Ainsi, si l'on augmente la tension d'injection pour des tensions d'alimentation du circuit de $V_{dd} = 1.2V$ et $V_{dd} = 1.3V$, ces zones de susceptibilité du circuit devraient elles apparaitre. Cette idée a été vérifiée expérimentalement pour un $V_{dd} = 1.2V$. Des fautes ont été produites avec une tension $V_{pulse} = 160V$ dans ces zones là.

Sur les Fig. 5.8d, e et f sont représentées les zones de susceptibilité du circuit permettant de générer des fautes sur le texte chiffré. On peut s'apercevoir que les zones ayant un fort taux de probabilité de générer une faute se situent sur l'AES du circuit. Ainsi cette

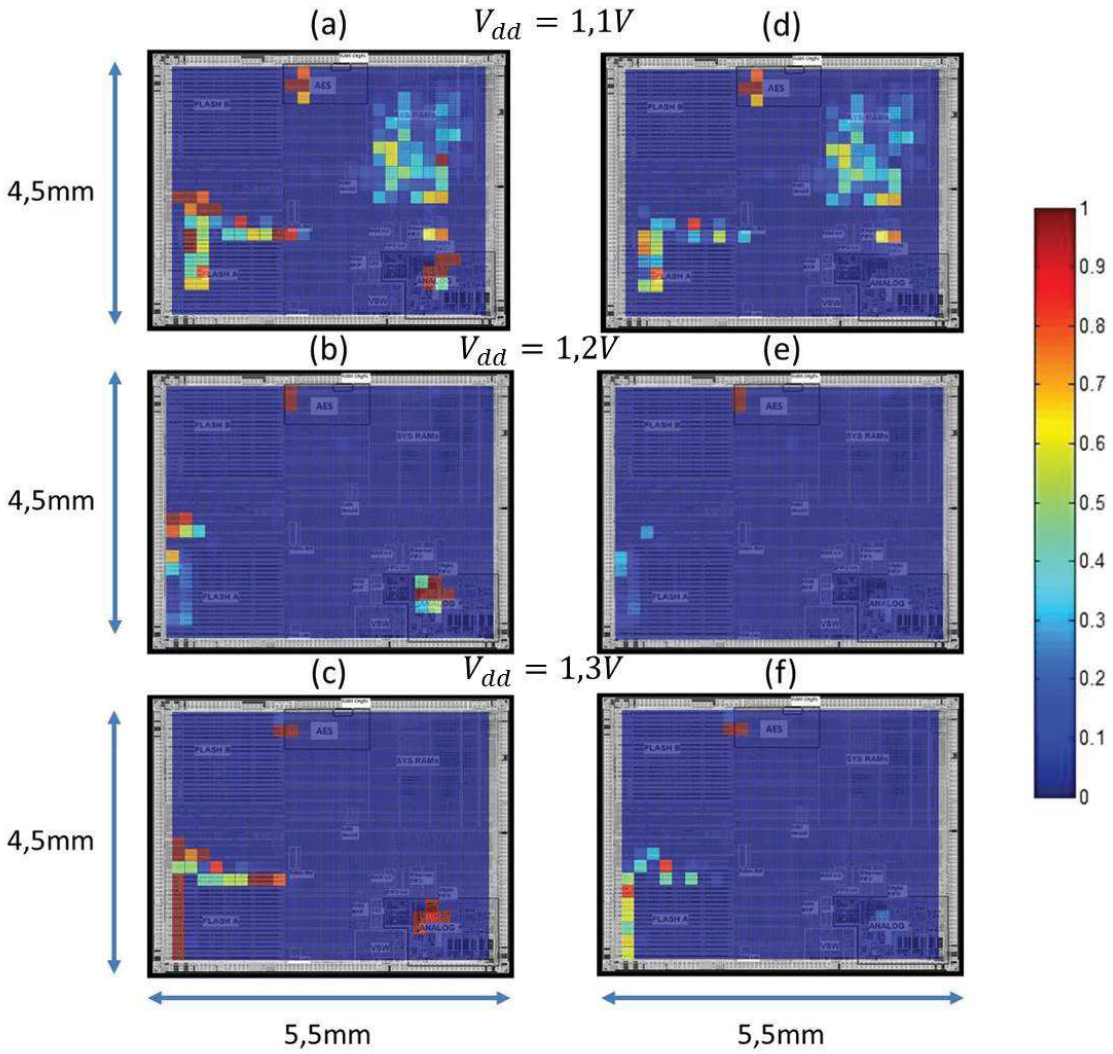

FIGURE 5.8: Cartographies (a,b,c) de la probabilité d'induire un comportement erroné quelconque lorsque le circuit est alimenté à 1.1V(a), 1.2V(b) et 1.3V(c). Cartographies (d,e,f) de la probabilité de générer un chiffré fauté lorsque le circuit est alimenté à 1.1V(d), 1.2V(e) et 1.3V(f)

zone de faute n'a pas été affectée par la variation de tension. La sonde d'injection a alors été conservée sur cette zone pour l'expérimentation suivante.

La Fig. 5.9 représente la probabilité de générer une faute en fonction de l'instant où est délivrée l'injection (t_{pulse}) pour les trois tensions d'alimentation du circuit. On peut ainsi s'apercevoir que la tension d'alimentation a un effet sur le choix de t_{pulse} à travers la durée des fenêtres durant lesquelles des fautes apparaissent. En effet, pour une tension d'alimentation de $1.1V$, on peut distinguer que les fenêtres de susceptibilité apparaissent pour chaque front montant d'horloge du circuit. Pour une tension d'alimentation de $1.2V$, les résultats sont légèrement similaires, cependant sur certaine ronde de l'AES aucune

faute n'apparait.

Pour une tension d'alimentation de $1.3V$, une différence apparait. Les instants d'injection permettant de produire des fautes, sont bien moins nombreux que pour les deux autres tensions d'alimentation (seul une fenêtre de quelques point lors de la 9^{eme} ronde de l'AES apparait). Cet effet s'explique par le fait que la tension V_{pulse} a été réglée de sorte à être proche du seuil requis pour générer une faute à $1.2V$. Augmenter la tension d'alimentation modifie donc légèrement la susceptibilité du circuit au injection BBI. Toutefois, en augmentant la tension V_{pulse} à 190V, les mêmes résultats que pour les deux autres tensions d'alimentation ont été obtenus.

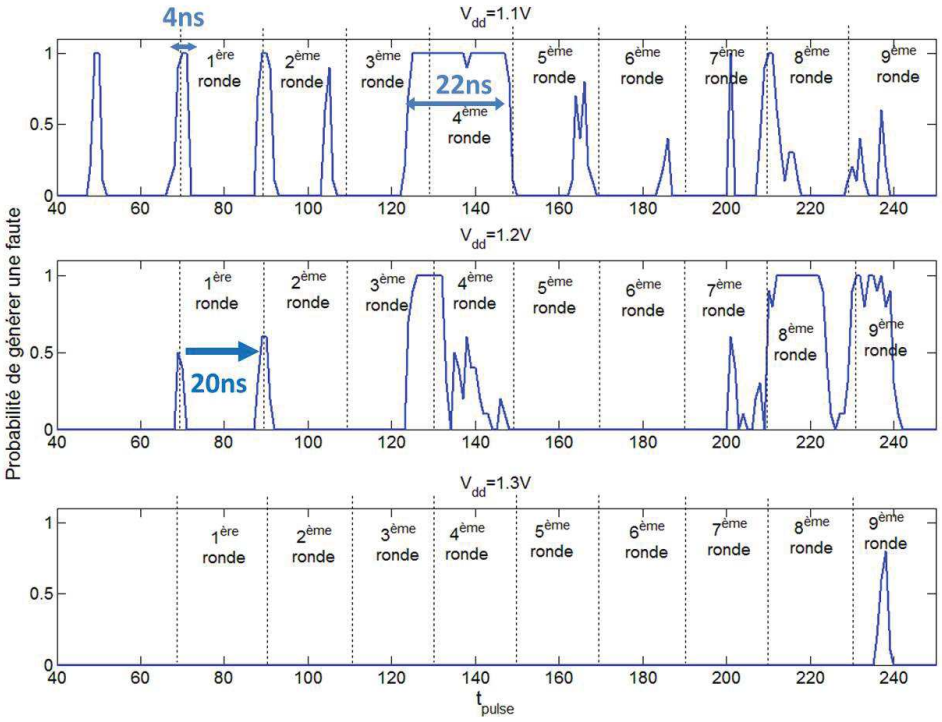

FIGURE 5.9: Evolution avec t_{pulse} de la probabilité d'induire une faute de chiffrement dans l'AES matériel du microcontrôleur et ce pour trois valeurs de tension d'alimentation

Pour conclure, une variation de la tension d'alimentation du circuit produit différents effets sur la capacité à induire des fautes avec la BBI. Ces effets sont dus probablement à la modification de la tension de seuil minimale permettant de générer des fautes. L'attaquant peut toutefois aisément contrecarrer les effets d'une variation de tension en augmentant la valeur de V_{pulse}. Il est cependant nécessaire de ne pas mettre une tension V_{pulse} trop forte sous peine de détruire le circuit.

5.3.3 Effet d'une variation de fréquence sur l'injection EMP

Lors d'une variation de fréquence, l'un des effets qui est à prévoir est un déplacement des fenêtres de susceptibilité EM du circuit ; celles-ci étant centrées sur les fronts d'horloge. Cependant, il est difficile de prédire les autres effets sur l'injection EMP. La Fig. 5.10 représente les cartographies de la probabilité d'induire des fautes dans le circuit en fonction de sa fréquence. Les cartographies Fig. 5.10a, b et c donnent les zones de susceptibilité du circuit. On peut observer que les zones de fortes probabilités sont très similaires entre ces trois cartographies. On peut en conclure que le changement de fréquence n'a aucun autre effet que celui de modifier la position dans le temps des fenêtres de susceptibilité.

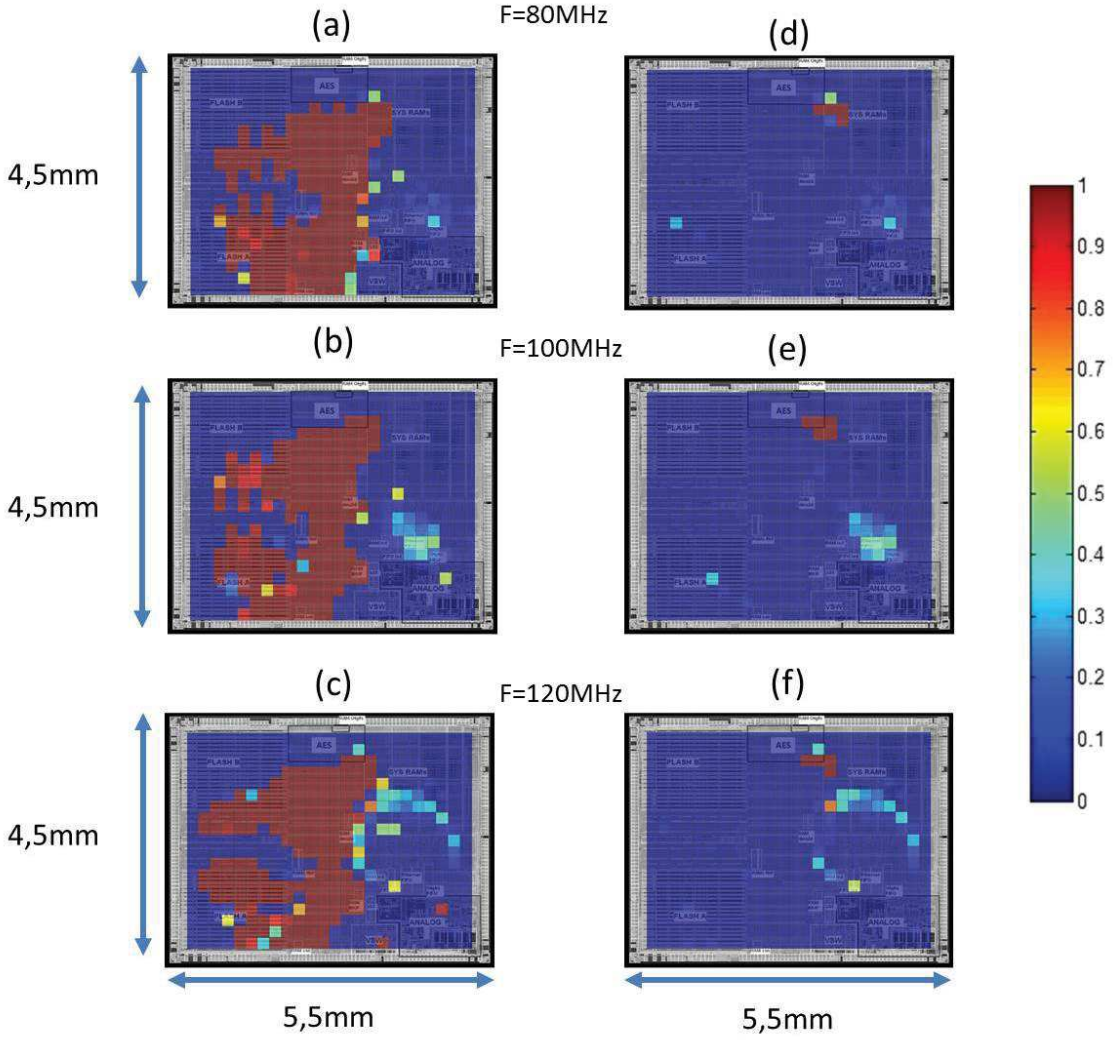

FIGURE 5.10: Cartographies de la probabilité, (a,b,c) d'induire un comportement erroné quelconque avec une impulsion EM et (d,e,f) une faute de chiffrement

Les Fig. 5.10d, e et f donnent les zones de susceptibilité du circuit conduisant à la production d'un chiffré fauté. Ainsi les zones ayant un fort taux de probabilité de faute se situent à droite de l'AES pour les trois fréquences. Des zones caractérisées par de faibles probabilités apparaissent lorsque la fréquence du circuit est élevée. Cependant ces fautes ne peuvent être considérées comme exploitables d'après l'attaque DFA de Piret [38] car pour cette attaque, qui se déroule sur la 9^{eme} ronde de l'AES, il est nécessaire de n'avoir que 4 octets de fautés. Ce qui n'est pas le cas sur ces zones de susceptibilité, où les 16 octets sont fautés lors d'une injection EMP pour n'importe quelle fenêtre de susceptibilité.

La sonde d'injection a ensuite été placée au dessus d'une zone de forte susceptibilité associée à l'induction de fautes de chiffrement, puis des injections ont été faites à différents instant t_{pulse}, afin de couvrir les trois dernières rondes de l'AES. La Fig. 5.11 représente cette expérimentation. Un décalage temporel a du être ajouté afin de pouvoir superposer les courbes associées à des fréquences différentes. Ainsi pour une fréquence de 100MHz un décalage de 110ns, par rapport à la fréquence de 120MHz, tandis que pour la fréquence de 80MHz, un décalage de 260ns a du être ajouté. On peut observer sur la Fig. 5.11, l'apparition des fenêtres de susceptibilité d'une durée de 6ns pour les trois valeurs de fréquence. Cette durée est donc indépendante de la fréquence du circuit. On peut aussi observer que les fenêtres de susceptibilité sont répétées à une fréquence correspondant à la fréquence du circuit comme étant attendu. Ainsi, les résultats observés suivent bien le modèle de faute d'échantillonnage décrit dans la section 4.7

A partir de ces résultats, on peut en conclure que des variations de fréquence n'ont aucun effet sur l'injection EMP hormis le déplacement des fenêtres de susceptibilité.

5.3.4 Effet d'une variation de fréquence sur la BBI

Les mêmes expérimentations que celles décrites dans la section précédente ont été réalisées mais avec la méthode BBI. La Fig. 5.12a, b et c donnent les zones de susceptibilité associées à l'apparition de n'importe quel type de comportement erroné pour des fréquences de 50MHz, 80MHz et 100MHz du circuit. Pour ces trois cartographies, les zones de susceptibilité sont similaires. Cependant, on peut observer que pour une fréquence de 50MHz, la probabilité de générer une faute est moins importante que pour des fréquences de 80MHz et 100MHz.

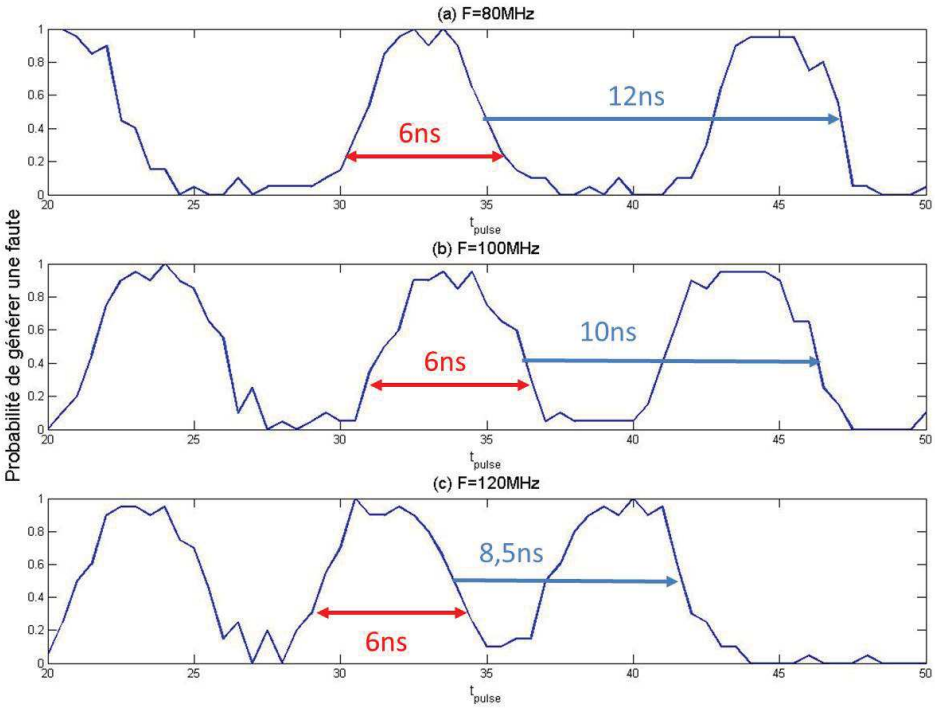

FIGURE 5.11: Probabilité de générer une faute sur un AES matériel implémenté sur un micro-contrôleur 32bit en fonction du moment d'injection (t_{pulse}) pour 3 valeurs de fréquence de fonctionnement

Sur les Fig. 5.12d, e et f, sont représentées sur des cartographies la probabilité d'induire une faute de chiffrement pour des fréquences de 50MHz (d), 80MHz (e) et 100MHz (f). Les zones de susceptibilité se situent aux mêmes emplacements sur le circuit. Cependant, la probabilité de générer une faute à l'aide de la méthode BBI diminue pour une fréquence de 50MHz. Cette diminution est due au choix du moment d'injection qui n'a pas été choisi de manière optimale pour cette valeur de fréquence. En modifiant légèrement (1ns) l'instant d'injection, une probabilité de 1 apparait sur la zone de l'AES.

La sonde d'injection a été fixée au dessus de l'AES, à une position caractérisée par une forte probabilité de générer une faute sur le message chiffré. Des injections BBI ont ensuite été produites pour différentes valeurs de t_{pulse} afin d'évaluer un lien, s'il existe, entre la fréquence du circuit et la probabilité de générer une faute. Les résultats de cette expérimentation sont reportés sur la Fig. 5.13. Il y apparait alors très clairement que la probabilité de générer une faute est indépendante de la fréquence du circuit. En effet, on peut remarquer que pour chacune des trois fréquences, les instants d'injection où une faute est générée sont communs. On peut ainsi observer que les fautes de chiffrement

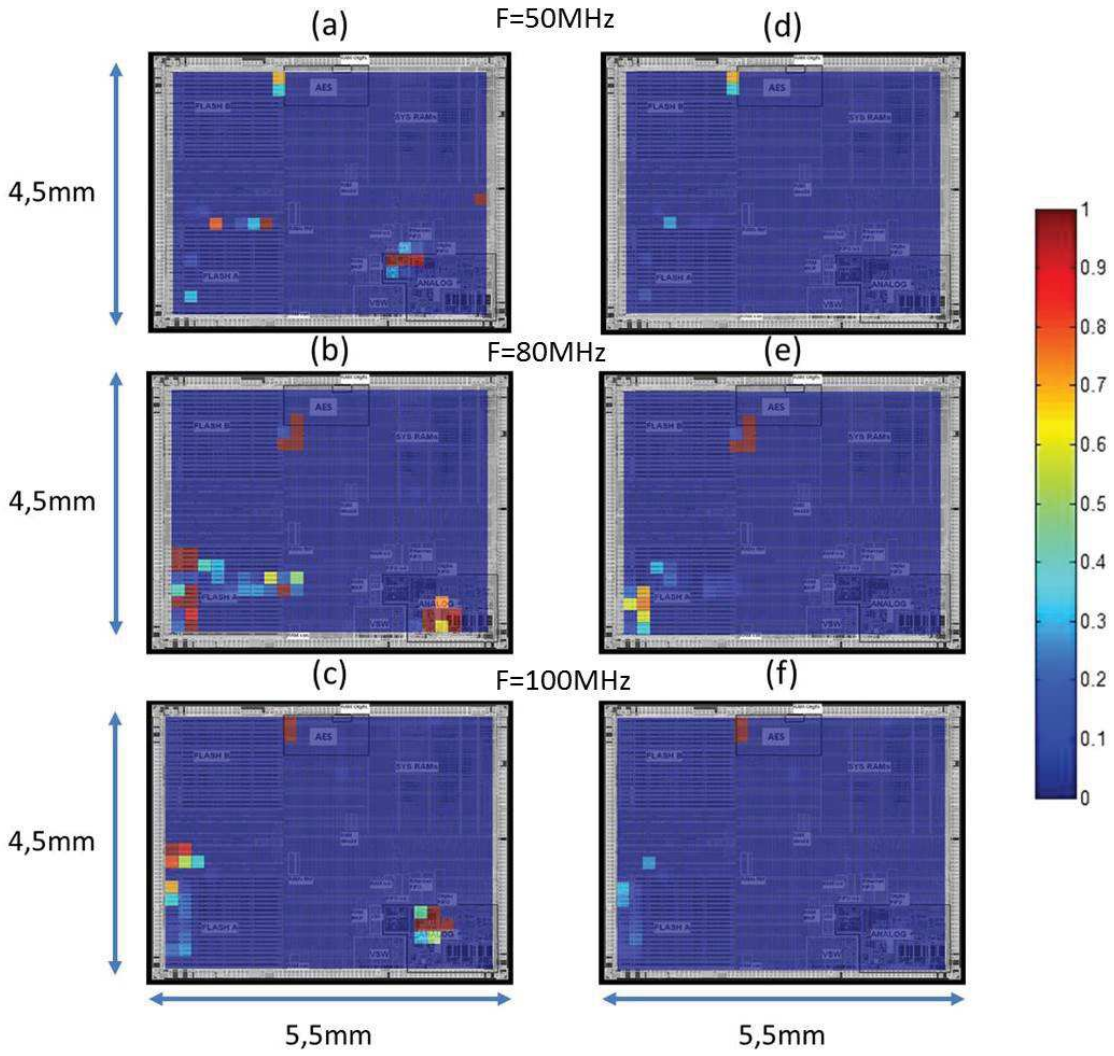

FIGURE 5.12: Cartographies de la probabilité (a,b,c) d'induire n'importe quel comportement erronée avec l'injection BBI lorsque le circuit fonctionne à 50MHz(a), 80MHz(b) et 100MHz(c) ; (d,e,f) d'induire des fautes de chiffrement avec l'injection BBI lorsque le circuit fonctionne à 50MHz(d), 80MHz(e) et 100MHz(f)

apparaissent principalement durant les rondes 3, 4, 7, 8 et 9 de l'AES. Il est à noter que pour chacune des trois figures l'échelle de temps n'est pas la même afin de pouvoir visualiser seulement le chiffrement de l'AES. Ainsi pour les fréquences 50MHz et 80MHz, on peut distinguer les différentes fenêtres de susceptibilité. Cependant pour une fréquence de 100MHz, ces fenêtres ont fusionné pour ne fournir qu'une seule fenêtre.

A partir de ces résultats, il apparait que la BBI semble suivre le même modèle de faute que l'injection EMP qui est le modèle 'faute d'échantillonnage'. Cependant une différence apparait entre ces deux méthodes qui est la durée des fenêtres de susceptibilité.

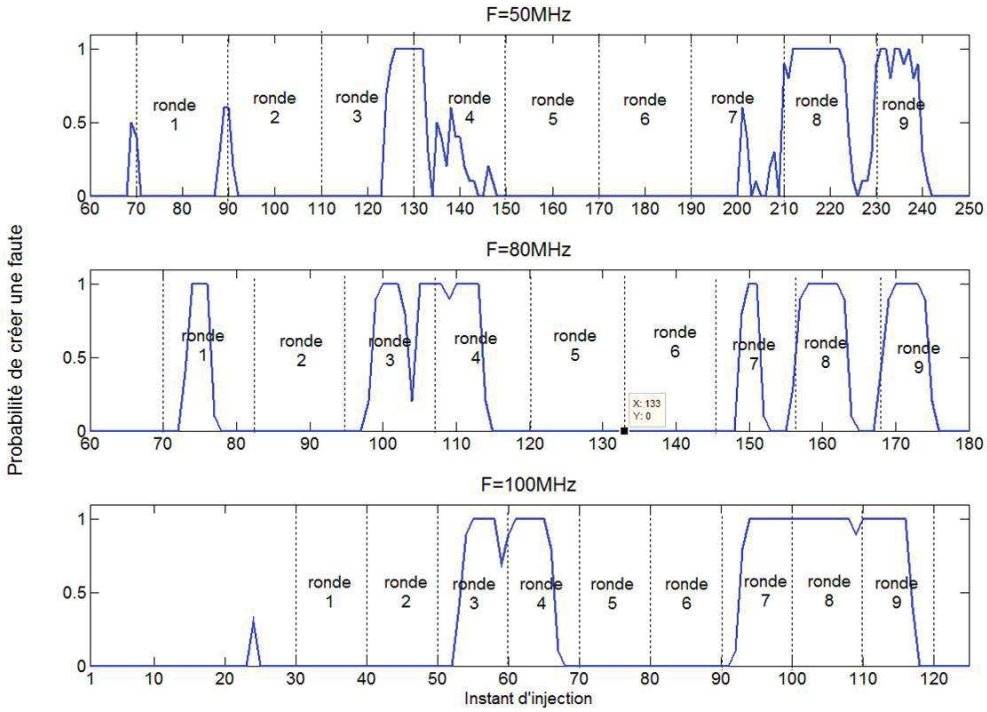

FIGURE 5.13: Probabilité de générer une faute sur un AES hardware implémenté sur un micro-contrôleur 32bit en fonction du moment d'injection (t_{pulse}) pour 3 valeurs de fréquence de fonctionnement et avec une sonde d'injection plate

5.3.5 Effet d'une variation de la polarisation de substrat sur les capacités d'injection EMP

Pour cette section, une variation de la tension de la polarisation du substrat a été appliquée sur le micro-contrôleur 32bits afin d'en connaitre les effets lors d'une injection EMP. Les valeurs de la polarisation du substrat que nous avons considérées sont : $V_{bb} = 0mV$, $200mV$ et $400mV$. La Fig. 5.14 représente les cartographies du circuit en fonction des tensions de polarisation du substrat. Les cartographies Fig. 5.6a, b et c donnent les zones de susceptibilité du circuit conduisant à l'apparition de n'importe quel type de comportement erroné avec l'injection EMP. On peut observer que, pour ces trois cartographies, plusieurs zones sont caractérisées par de fortes probabilités (mémoire FLASHs, AES, processeur).

Cependant, en augmentant la tension de la polarisation du substrat, une nouvelle zone de susceptibilité apparait. Cette zone, qui se situe au dessus du bloc analogique, a une susceptibilité à l'injection EMP faible lorsque la polarisation du substrat est de 0mV.

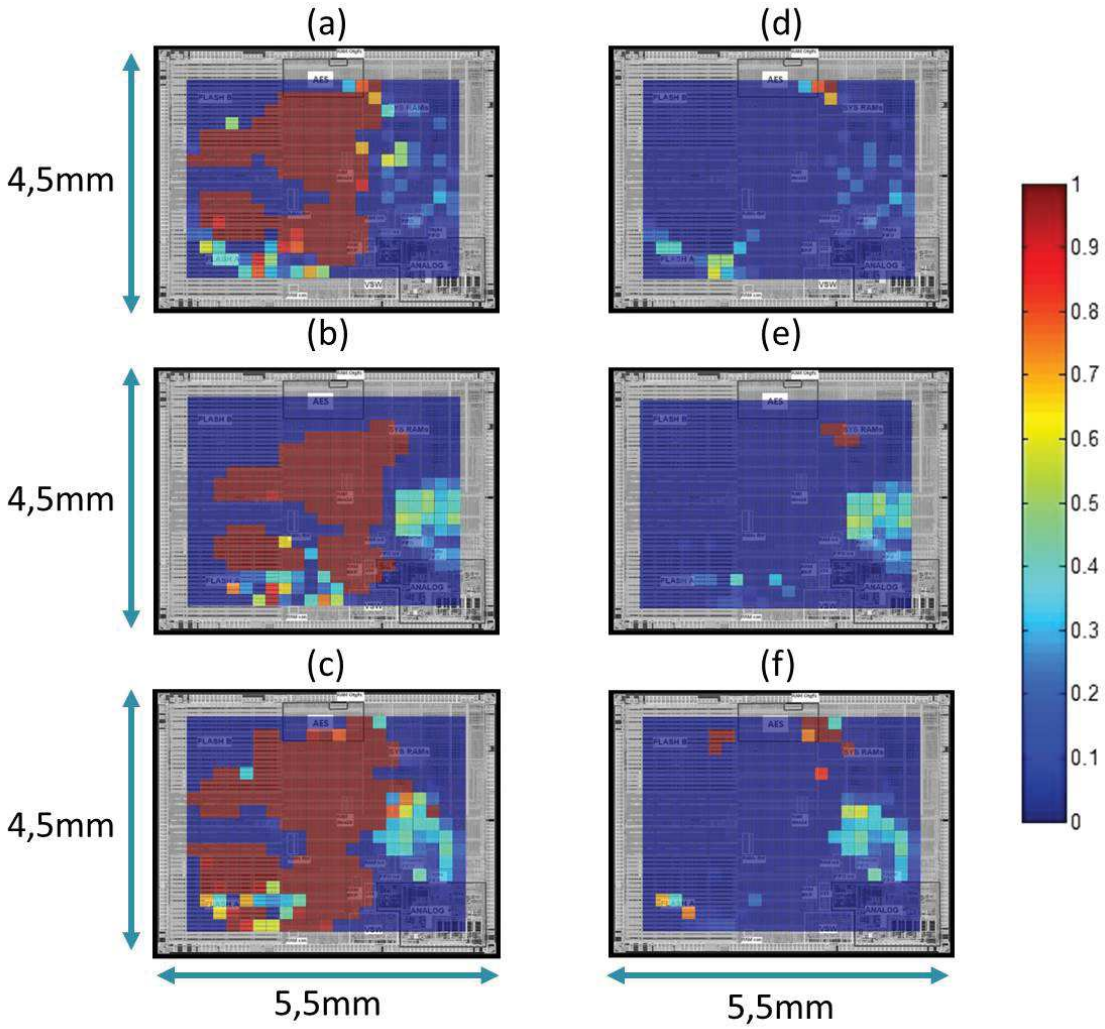

FIGURE 5.14: Cartographies (a,b,c) de la probabilité d'induire un comportement erroné quelconque lorsque le circuit a une polarisation de substrat de 0V(a), 200mV(b) et 400mV(c). Cartographies (d,e,f) de la probabilité de générer un chiffré fauté lorsque le circuit a une polarisation de substrat de 0V(d), 200mV(e) et 400mV(f)

Puis en augmentant la tension de la polarisation du substrat, la probabilité de générer une faute augmente, lorsque une injection est produite sur cette zone.

Sur les Fig. 5.6d, e et f sont représentées les zones de susceptibilité du circuit lorsqu'une faute de chiffrement est produite. On peut observer une zone ayant une forte probabilité de faute. Celle-ci est commune aux trois cartographies. Cette zone, qui se situe à droite de l'AES, n'est donc pas affectée par le changement de tension de polarisation. Cependant, une nouvelle zone ayant une probabilité de 0.5 apparait pour des tensions de polarisation de substrat de 200mV et 400mV. En analysant les fautes du message chiffré lorsqu'une injection est effectuée sur cette dernière zone, on se rend compte que les fautes suivent le modèle de faute d'échantillonnage présenté dans la section 4.7. Cependant les

fautes produites affectent les 16 octets du message chiffré indépendamment de la ronde de l'algorithme AES. Ces fautes ont donc été considérées comme non exploitables car l'attaque DFA utilisée durant cette thèse est celle décrite dans [38] et nécessite que 4 octets soient fautés lorsqu'on injecte une faute durant la 9^{eme} ronde de l'AES. Or dans cette zone, 16 octets sont fautés lors de l'injection sur la 9^{eme} ronde.

La Fig. 5.15 représente la probabilité de générer une faute en fonction de l'instant de l'injection (t_{pulse}) pour les trois valeurs de polarisation du substrat lors des trois dernières ronde de l'AES. On peut ainsi observer que les fautes générées suivent le modèle 'faute d'échantillonnage'. La durée de la zone de susceptibilité varie en fonction de la tension de polarisation du substrat. Cet effet a probablement pour même origine la dépendance entre la tension de polarisation du substrat et les temps de hold et setup d'une bascule DFF.

On peut donc en conclure qu'une variation de la tension de polarisation du substrat génère le type même d'effet qu'une variation de tension d'alimentation.

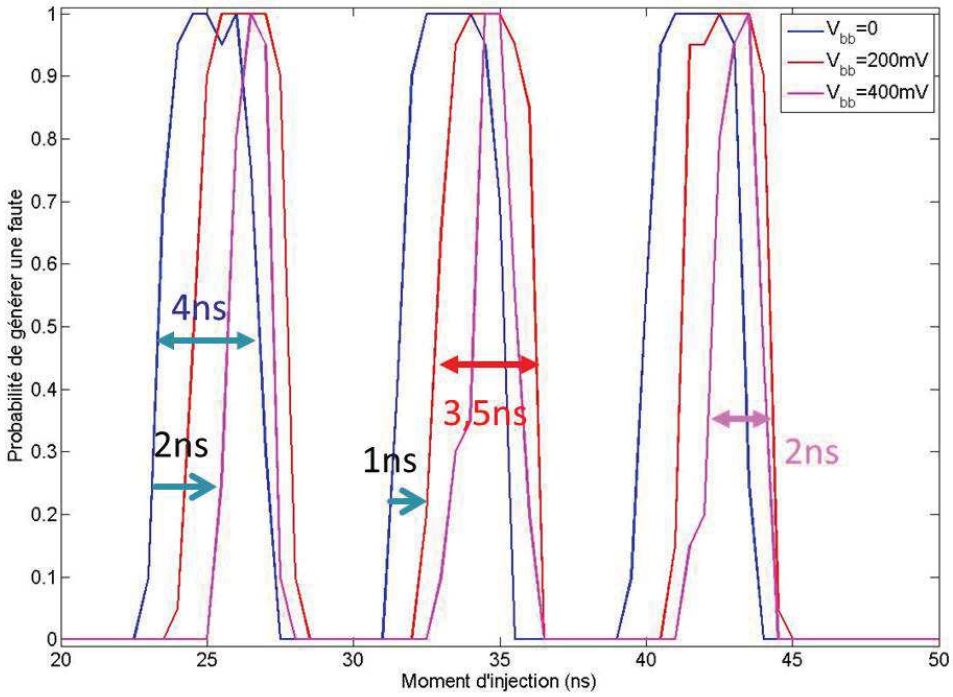

FIGURE 5.15: Probabilité de générer une faute sur un AES hardware implémenté sur un micro-contrôleur 32bit en fonction du moment d'injection (t_{pulse}) pour 3 valeurs de tension de polarisation du substrat et avec une sonde d'injection plate

5.3.6 Effet d'une variation de polarisation de substrat sur la BBI

Dans cette section, l'étude de la variation de polarisation de substrat sur la capacité d'injection BBI est considérée. Les mêmes expérimentations, que celles effectuées dans la section précédente ont été réalisées. La Fig. 5.16 donne les cartographies de la probabilité d'induire des fautes en fonction des tension de polarisation du substrat appliquées. Les cartographies Fig. 5.16a, b et c donnent les zones de susceptibilité du circuit lorsqu'on génère n'importe quel type de faute à l'aide de la méthode BBI. On peut ainsi observer que différentes zones ayant une forte probabilité de faute apparaissent. Ces zones se situent au dessus de l'AES et d'une mémoire FLASH. Cependant, un effet intéressant se produit. Pour des polarisation de substrat de 0mV et 400mV une zone de susceptibilité apparait au dessus de la partie analogique du circuit. Or, celle-ci n'apparait pas pour une polarisation du substrat de 200mV. N'ayant pas accès aux caractéristiques du circuit, il nous est impossible d'expliquer cette observation.

Sur les Fig. 5.16d, e et f sont représentées les zones de susceptibilité du circuit lorsqu'une faute sur le texte chiffré est produite. Une zone commune à ces trois cartographies caractérisée par un fort taux de probabilité apparait. Cette zone, qui se situe au dessus de l'AES, permet de générer une faute facilement lors d'un chiffrement AES. Sur chacune de ces trois cartographies, différentes zones apparaissent notamment autour de la mémoire FLASH A. En examinant les fautes générées, il s'est avéré que celles-ci ne sont pas exploitables selon l'inventeur de l'attaque de Piret [38].

La Fig. 5.17 représente la probabilité de générer une faute en fonction du moment de l'injection (t_{pulse}) pour deux valeurs de polarisation du substrat. En effet, suite à des problèmes techniques (destruction du circuit due à un tir trop puissant), cette expérimentation n'a pu être effectuée avec une tension de polarisation du substrat de 200mV. On peut ainsi observer que pour une tension de polarisation du substrat de 400mV des fenêtres de susceptibilité apparaissent. La variation de substrat semble donc avoir les mêmes conséquences qu'une variation de tension. Cette conséquence est la modification des tensions de seuil $V_{thhaute}$ et $V_{thbasse}$.

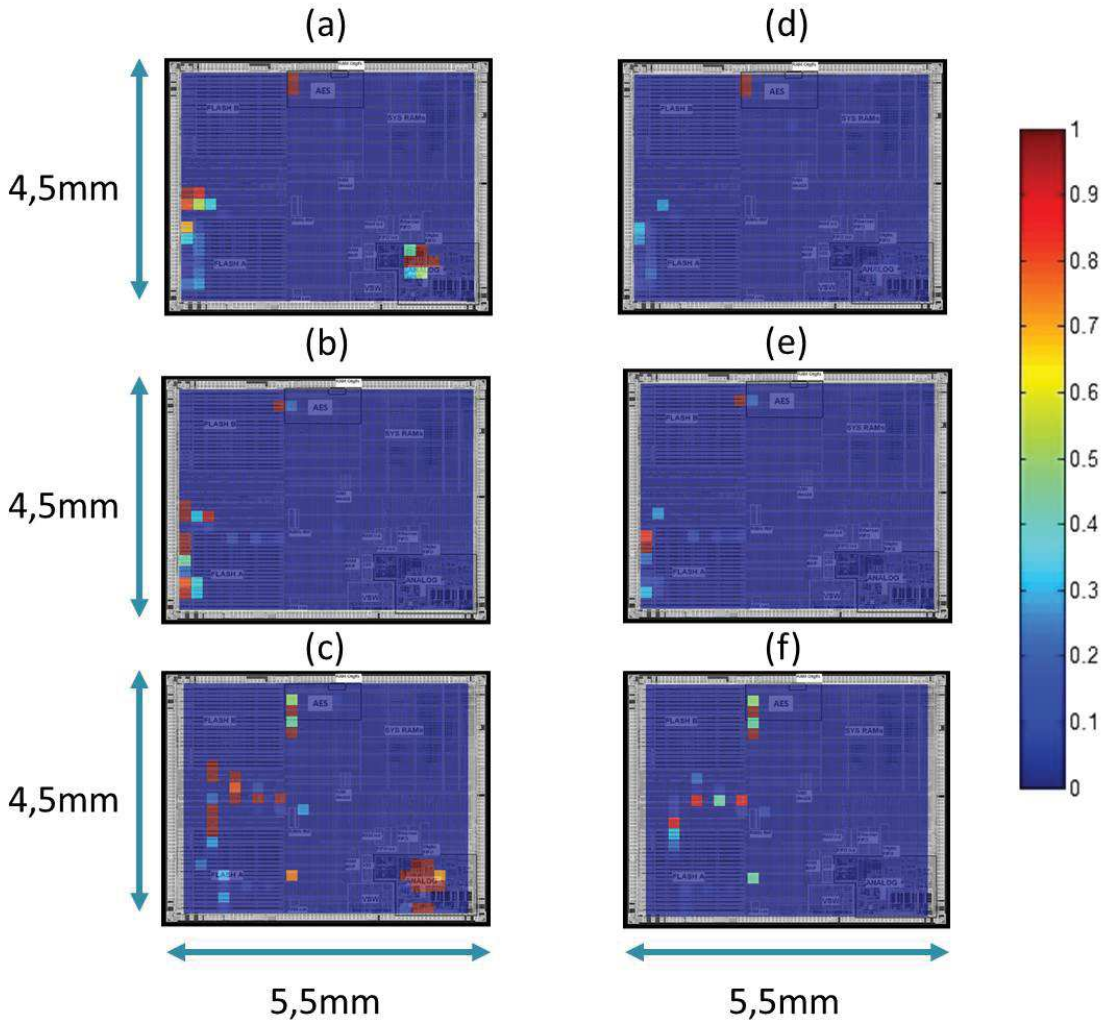

FIGURE 5.16: Zones de susceptibilité du micro-contrôleur pour n'importe quel type d'erreur avec des tension de polarisation du substrat de (a) 0mV, (b) 200mV et (c) 400mV. Zones de susceptibilité du micro-contrôleur pour une erreur sur le texte chiffré avec des tension d'alimentation de (d) 0mV, (e) 200mV et (f) 400mV

5.4 Conclusion

Ce chapitre a permis d'étudier expérimentalement les effets des variations de tension d'alimentation, de fréquence et de polarisation du substrat sur sur l'efficacité de deux méthodes d'injection de fautes. Ces méthodes sont la BBI et l'injection EMP. Tout d'abord, une comparaison entre ces deux méthodes a été effectuée à l'aide d'un micro-contrôleur 32 bits. Il est apparu que la BBI a un effet beaucoup plus localisé que l'injection EMP. Cette différence est principalement due aux contraintes de dimensionnement des sondes d'injection. En effet, la sonde d'injection EMP utilisée pour cette comparaison a un diamètre 40 fois plus grand que la sonde utilisée pour la BBI. Cependant,

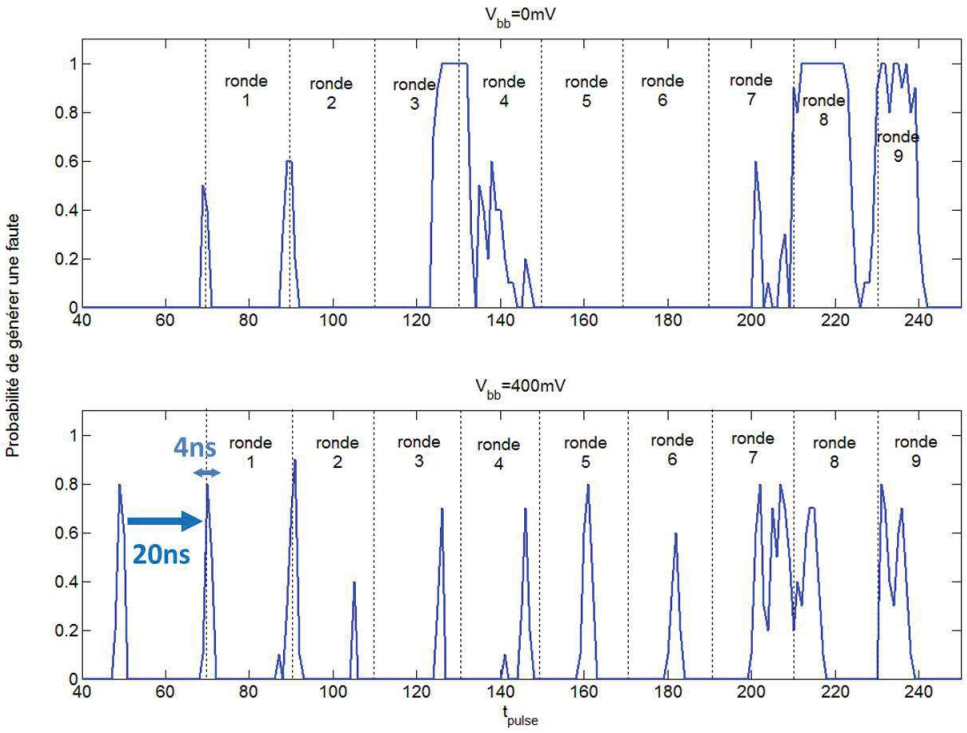

FIGURE 5.17: Probabilité de générer une faute sur un AES hardware implémenté sur un micro-contrôleur 32bit en fonction du moment d'injection (t_{pulse}) pour 2 valeurs de tension de polarisation du substrat

l'injection EMP dispose d'un avantage non négligeable sur la BBI. L'injection EMP peut générer une faute à travers le boitier du circuit, tandis que la BBI nécessite un accès direct au substrat du circuit. Toutefois, aucune préparation du substrat n'est nécessaire. De plus le modèle de faute que suivent ces méthodes semble être le même. En effet, l'injection EMP et la BBI suivent le modèle 'faute d'échantillonnage' décrit dans la section 4.7. Toutefois d'autres expérimentations sont requises pour la BBI afin d'étayer plus fortement ce résultat.

Pour analyser les effets de ce type de variations sur l'efficacité de ces deux méthodes d'injection, les tests décrits dans la section 4.4.4 ont été utilisés. A partir de ces tests, il est apparu que ce type de variations n'a que peu d'impact sur la BBI. En effet les variations de tension d'alimentation ont pour effet de modifier légèrement la tension de seuil nécessaire pour générer une faute. L'étude de la variation de fréquence à quant à elle permis de mettre en évidence que cette variation a seulement pour effet de déplacer les fenêtres de susceptibilité dans le temps. La modification de la polarisation de substrat n'a fait apparaitre aucun effet sur la BBI. Cependant, il est fort probable que ce type

de variation ait le même type d'effets que ceux produits par une variation de tension, mais de manière plus limitée.
Pour l'injection EMP, les variations de tension d'alimentation, de fréquence et de polarisation du substrat, ont aussi un impact. En effet, les variations de tension d'alimentation et de polarisation de substrat ont un impact sur la durée des fenêtres de susceptibilité EM décrites dans le modèle de faute d'échantillonnage. Cet effet est probablement du au temps de *hold* et de *setup* d'une DFF qui dépendent de la tension d'alimentation et de polarisation du substrat du circuit. La variation de fréquence, n'a que peu d'effet sur l'injection EMP. Cette variation a pour seul effet de modifier le moment de l'injection.

A partir de ces résultats, il apparait que les augmentations de la tension d'alimentation, de la fréquence et de la polarisation du substrat, augmentent très légèrement la robustesse des circuits contre les attaques par faute conduites avec ces méthodes d'injection. Cependant cet apport peut facilement être anticipé en effectuant une injection assez forte afin de ne pas être impacté par des variations de tension d'alimentation et de polarisation du substrat. Le seul apport sécuritaire non compensable est la modification du moment d'injection, pour une variation de la fréquence, si l'on souhaite injecter une faute dans la 9^{eme} ronde de l'AES pour effectuer l'attaque DFA de Piret [38].

Chapitre 6

Conclusion

Avec la démocratisation des objets connectés, la consommation des circuits intégrés est devenue un enjeu majeur. Pour cela, les concepteurs de circuits ont du développer des méthodes pour diminuer cette consommation. Cependant, certain circuits peuvent avoir à traiter des données confidentielles. Il est donc nécessaire de connaitre les effets des méthodes de diminution de la consommation sur la sécurité du circuit.
Dans ce contexte, les différents chapitres de cette thèse ont présenté les effets sur différentes attaques de deux méthodes de diminution de la consommation, la DVFS (*Dynamic Voltage and Frequency Scaling*) et le *Body-Biasing*.

La première étude a été effectuée sur l'attaque par canal auxiliaire la plus répandue : la CPA. Afin d'effectuer l'étude sécuritaire l'utilisation de la contremesure RDVFS a été utilisée. Elle a pour effet de modifier de manière aléatoire la tension d'alimentation et la fréquence du circuit, ce qui correspond à la DVFS. Il a également été ajouté à cette contremesure une variation aléatoire de la tension de polarisation du substrat, lorsque cela était possible, afin d'étudier également les effets du *Body-Biasing*.
Il est apparu que ces méthodes de diminution de la consommation ne supprime pas la fuite d'information mais la dilue dans le temps. L'utilisation de ces méthodes ont pour conséquence d'augmenter la robustesse du circuit aux attaques CPA d'un facteur n^2 avec n le nombre de triplet (V_{dd}, F, V_{bb}) utilisés. Cependant, ce rapport de robustesse peut facilement diminuer à un facteur n en utilisant des méthodes simples comme la resynchronisation ou le regroupement des traces de consommation.

La seconde étude a été effectuée sur l'attaque par faute. Les moyens d'injection de fautes utilisés sont l'injection EMP et BBI (*Body Biasing Injection*). Cependant, avant d'effectuer cette étude, il a été nécessaire d'étudier les effets de l'injection EMP sur les circuits. Il est apparu qu'il est possible de générer des fautes de type bitset et bitreset à l'aide de l'injection EMP si une forte impulsion est générée. Toutefois, il est possible de générer des fautes avec une impulsion beaucoup plus faible lors des fenêtres de susceptibilité des bascules DFF. Les fautes générées suivent un modèle que nous nommons modèle 'faute d'échantillonnage'. Après plusieurs expérimentations, il est apparu que l'injection BBI suit le même modèle que l'injection EMP.

Une fois le modèle défini pour l'injection EMP et BBI, une étude des effets de variation de tension d'alimentation, fréquence et polarisation de substrat a pu être effectuée. Il est ainsi apparu que ces variations n'ont qu'un seul effet gênant sur ces méthodes d'injection. Cet effet est le déplacement potentiellement aléatoire comme pour la RDVFS, dans le temps des fenêtres de susceptibilité. Ainsi, il est nécessaire de modifier l'instant d'injection pour générer une faute. Tous les autres effets peuvent être facilement compensable en augmentant la puissance de l'injection.

Il apparait donc que les méthodes DVFS et *Body-Biasing* permettent de diminuer la consommation du circuit en augmentant légèrement la sécurité de ceux-ci. Cependant, ces méthodes ne doivent pas être considérées comme des contremesures efficaces contres les différentes attaques. En effet, bien que ces méthodes permettent d'augmenter sensiblement la robustesse contre les attaques par canaux auxiliaire, elles n'ont en revanche qu'un effet très limité sur les attaques en faute.

Annexe A

Modèle de fuite dans le domaine fréquentiel

Durant cette thèse, plusieurs collaborations avec d'autres doctorants ont été effectuées. Ce chapitre présente très brièvement la collaboration la plus importante qui a été effectuée durant cette thèse en dehors du sujet principale. La grande majorité des travaux ont été réalisés par Sébastien Tiran et ont permis de publier plusieurs articles [98][78][99].

A.1 Introduction

Les travaux réalisé par Sébastien Tiran sont basés sur une constatation assez simple. De bonne traces de consommation sont nécessaire pour réaliser une attaque par canal auxiliaire. Afin d'améliorer la qualité des traces de consommation, il est possible de les filtrer. Cependant, il est nécessaire de connaitre la gamme de fréquence qui porte le plus d'information. Les travaux présentés dans ce chapitre sont ceux réalisés en collaboration avec Sébastien Tiran et ont pour but de déterminer la meilleure gamme de fréquence à utiliser pour filtrer les traces de consommation. La contribution apporté à ces travaux est également décrite.

Afin de connaitre les fréquences transportant le plus d'information, un modèle de fuite dans le domaine fréquentiel a été proposé. Ce modèle décrit dans la thèse de Sébastien Tiran [100], montre que la fuite d'information dans le domaine fréquentiel se situe dans les basses fréquences. Ainsi, un critère permettant de localiser la fuite d'information dans

le domaine fréquentiel a pu être proposé. Ce critère se base sur le fait qu'il est possible de calculer le rapport signal à bruit de chaque fréquence pour un jeu de trace brut. Le résultat obtenu peut alors être divisé par la fréquence afin de prendre en compte la conclusion du modèle de fuite : les fuites EM s'étalent en $\frac{1}{f}$ dans le spectre. Le rapport signal à bruit utilisé correspond à la moyenne du signal divisé par son l'écart type qui est une méthode très répandu dans le traitement d'image [101]. Cette méthode est alors transposé dans le domaine fréquentiel à l'aide du module de la transformé de Fourier de traces au lieu d'être calculé directement sur des traces. Il en résulte un critère exprimé à partir du rapport signal à bruit ($SNR(f)$). Ce critère (equ. A.1) permet ainsi de d'identifier les fréquences où la fuite d'information est potentiellement le plus important.

$$LNR_{EM}(f) = \frac{1}{f}.\frac{< A_{signal(f)} >}{\sigma_{A_{signal(f)}}} = \frac{1}{f}.SNR(f) \tag{A.1}$$

où $A_{signal(f)}$ est la densité spectrale de puissance à f du signal moyen et $\sigma_{A_{signal(f)}}$ son écart-type. Ce critère est empirique et permet de déterminer les fréquences qui fuient le plus au premier ordre.

A.2 Contribution

A.2.1 Validation du critère LNR

Afin de valider le modèle proposé, des expérimentations ont été menées. La contribution aux travaux réalisés se situe sur ces expérimentations. Pour valider le modèle, un circuit cible a été réalisé. Ce circuit est un FPGA sur lequel un AES, un bloc de communication RS232 et une machine d'état ont été implémentés. Tous ces éléments sont synchronisés par un signal d'horloge fournis par un quartz à une fréquence de 50MHz. Pour effectuer les acquisitions des traces EM le banc d'acquisition est composé d'une sonde EM d'un diamètre de $300\mu m$, d'un amplificateur faible bruit ayant un gain de 40dB et d'un oscilloscope Lecroy ayant un taux d'échantillonnage de 20GS/s. La bande de fréquence de ces appareils sont respectivement de $[30MHz, 3.5GHz]$, $[100MHz, 1GHz]$ et de $[0Hz, 3.5GHz]$. Afin de diminuer le bruit ambiant, chaque trace EM a été obtenue en effectuant une moyenne de 20 traces.

SR / Freq	CPA 20%	CPA 80%	DPASum 20%	DPASum 80%
0HZ - 10GHz	530	980	1260	2540
100MHZ - 10GHz	1940	4070	2430	3600
200MHZ - 10GHz	4310	Échec	3610	4560
500MHZ - 10GHz	Échec	Échec	Échec	Échec
1GHZ - 10GHz	Échec	Échec	Échec	Échec
2GHZ - 10GHz	Échec	Échec	Échec	Échec
3GHZ - 10GHz	Échec	Échec	Échec	Échec
4GHZ - 10GHz	Échec	Échec	Échec	Échec
5GHZ - 10GHz	Échec	Échec	Échec	Échec
7GHZ - 10GHz	Échec	Échec	Échec	Échec
8GHZ - 10GHz	Échec	Échec	Échec	Échec

TABLE A.1: Nombre de traces EM traitées pour atteindre un taux de réussite de 20% ou 80% pour des attaques CPA et DPA

Afin d'estimer le niveau de robustesse de l'AES non protégé, les attaques CPA et DPA-Sum [102] ont été utilisées. Lors de l'attaque, les traces EM ont été filtrées numériquement sur plusieurs bandes de fréquences. Les résultats obtenues sont représentés sous la forme d'un taux de réussite (*Success Rate*) dont la méthode de calcul est décrite dans [103]. Les Tab. A.1 et A.2 donnent le nombre de courbes nécessaires pour obtenir un taux de réussite des attaques CPA et DPASum de 20% et 80% pour différentes bandes de fréquences. Les résultats obtenus sont en concordance avec les prédictions du modèle de fuite établi par Sébastien Tiran. En effet, comme cela est visible sur le Tab. A.1, la suppression des basses fréquences a pour effet d'augmenter le nombre de traces nécessaire à la réussite de l'attaque ou éventuellement de conduire à l'échec de l'attaque.
De plus, comme le prédit le modèle, la suppression des hautes fréquences n'a pas d'impact sur l'efficacité de la CPA et la DPASum car la majorité de la fuite d'information est localisée dans les faibles fréquences. Cela est observable dans le Tab. A.2. Les mêmes expérimentations ont été menées sur les traces du *DPA contest* v1 et v2 [104] et des résultats similaires ont été observés.

Toutes les expérimentations réalisées ont permis de confirmer que la fuite d'informations n'est pas présente sur toutes les fréquences, mais sur une bande plus ou moins large située dans les basses fréquences. Cependant, toutes ces expérimentations ont été réalisées sur un circuit générant que très peu de bruit ambiant. Ainsi, un microcontrôleur 32bits embarquant un AES matériel conçu en technologie 90nm a été utilisé. Pour collecter les traces EM, les mêmes équipements que précédemment ont été utilisés. La sonde

SR / Freq	CPA 20%	CPA 80%	DPASum 20%	DPASum 80%
0HZ - 70MHz	520	820	840	1200
0HZ - 100MHz	500	1060	1010	1810
0HZ - 200MHz	480	850	1650	2610
0HZ - 300MHz	500	860	1310	2450
0HZ - 400MHz	520	870	1290	2460
0HZ - 500MHz	540	860	1390	2590
0HZ - 800MHz	510	910	1320	2610
0HZ - 1GHz	510	940	1320	2610
0HZ - 2GHz	510	970	1310	2610
0HZ - 5GHz	540	970	1320	2630
0HZ - 10GHz	530	970	1360	2610

TABLE A.2: Nombre de traces EM traitées pour atteindre un taux de réussite de 20% ou 80% pour des attaques CPA et DPA

d'analyse a été placée au dessus de l'AES matériel afin de ne pas capter les émissions EM des autres blocs du circuit. Malgré cela, les traces EM acquises sont bruitées à cause de la pompe de charge du circuit qui se déclenche de manière intempestive. Pour limiter ce bruit, chaque trace EM, pour un message donné, a été acquise en effectuant un moyennage de 10 traces EM d'un même message. Ainsi, avec les 54000 traces EM (540000 acquisitions) une attaque CPA a été effectuée et la clé de chiffrement n'a pas pu être retrouvée.

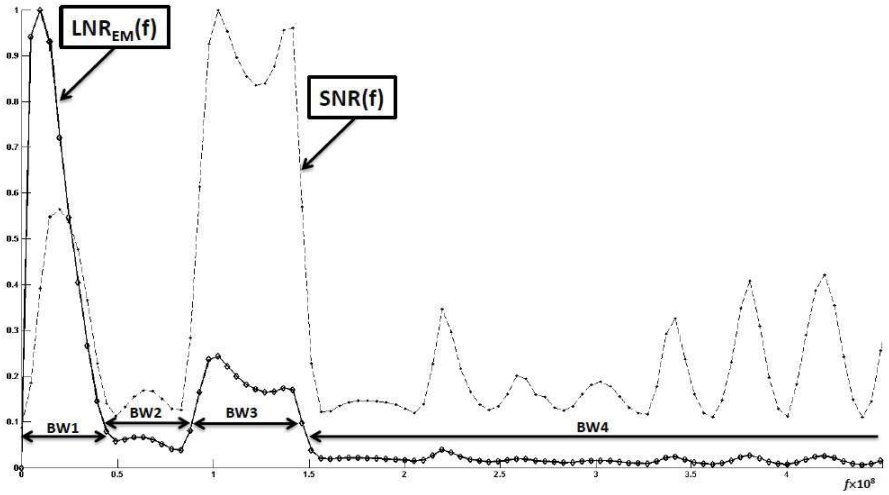

FIGURE A.1: Evolution du $LNR_{EM}(f)$ et du $SNR(f)$

Afin d'identifier les fréquences portant l'information, le $LNR_{EM}(f)$ et le $SNR(f)$ définis par l'equ. A.1 ont été appliqués à ce jeu de traces. La Fig. A.1 donne l'évolution de

Bande de fréquence	Nombre de traces	Nombre de sous-clé
Toutes	Échec	11
1MHZ - 200MHz	Échec	12
4MHZ - 160MHz	27700	16
BW1	28900	16
BW2	Échec	3
BW3	49900	16
BW4	Échec	0
BW1 $\cup$ BW3	22100	16

TABLE A.3: Résultat d'attaque CPA sur les traces EM du micro-contrôleur pour différente bande de fréquences

ces deux critères en fonction de la fréquence comprise entre 0Hz et 450MHz. Ainsi, il apparait que le critère $LNR_{EM}(f)$ pointe une bande de fréquence nommé BW1 ($[4MHz, 48MHz]$) tandis que le critère $SNR(f)$ pointe lui vers une autre bande de fréquence nommé BW3 ($[83MHz, 160MHz]$). Dans ce cas, le $SNR(f)$ est induit en erreur par le bruit algorithmique identifié comme important autour des harmoniques du signal d'horloge (cadencé a une fréquence de 120MHz). On peut également observer que dans la bande de fréquence BW4 ($[160MHz, 450MHz]$), le $LNR_{EM}(f)$ est quasi nul tandis que le $SNR(f)$ dispose de plusieurs oscillations.

Le Tab. A.3 donne le nombre de trace nécessaire a une attaque CPA pour retrouver la clé de chiffrement de l'AES implémenté dans le micro-contrôleur pour différentes bandes de fréquences. On peut y observer que lorsque aucun filtrage n'est appliqué et pour des bandes de fréquences $[1MHz, 200MHz]$, l'attaque n'arrive pas a retrouver les 16 sous-clés. On peut également observer que pour la bande de fréquence BW1 ($[4MHz, 48MHz]$), l'attaque a retrouvé la totalité des sous-clés en 28900 traces EM, tandis que pour la bande de fréquence BW3 49900 traces sont nécessaire pour retrouver les 16 sous-clés. Cependant lorsque l'attaque prend les 2 bandes de fréquences où l'attaque réussie séparément ($BW1 \cup BW3$), le nombre de traces nécessaire diminue pour retrouver les 16 sous-clés.

Ces expérimentations ont permis de démontrer l'efficacité du critère $LNR_{EM}(f)$ et indirectement de valider le modèle de fuite dans le domaine fréquentiel.

A.2.2 Optimisation du matériel d'attaque

A partir modèle de fuite établi par Sébastien Tiran, il semble que la fuite d'information se situent principalement dans les basses fréquences. Le critère $LNR_{EM}(f)$ a été proposé afin de pouvoir trouver les fréquences portant le plus de fuite d'information afin d'améliorer le filtrage des traces et donc l'efficacité des attaques. Toutefois, la première étape lors d'une attaque est l'acquisition des traces. Il est donc crucial de choisir la sonde d'acquisition et l'amplificateur de manière pertinente. Avant la conclusion de ces travaux, le banc d'analyse était composé de l'équipement suivant. Une sonde avec une bande passante de $[30MHz, 1GHz]$ (Fig. A.2b) et d'un amplificateur 48dB ayant une bande passante de $[100MHz, 1GHz]$ (Fig. A.2a). Bien que ces deux dispositifs dispose d'une large bande passante, celle-ci ne comprend pas les basses fréquences. En effet la bande passante de l'amplificateur commence à 100MHz, ce qui est trop élevée et peut avoir pour conséquence de filtrer les fréquences portant la fuite d'information.

Du nouveau matériel a ainsi été acquis à partir des conclusions de ces travaux. L'amplificateur a été remplacé par un amplificateur ayant une bande passante comprise entre $[1KHz, 200MHz]$ (Fig. A.2c). Ne trouvant pas de sonde d'acquisition correspondant aux spécificités désirées, il a été décidé de réaliser les sondes d'analyse au laboratoire. Celles-ci ont été réalisées par Ludovic Guillaume-Sage et sont constituées d'un noyau en ferrite qui est un élément qui a pour propriété de ne pas filtrer les basses fréquences (Fig. A.2d). Ne disposant pas de matériel de caractérisation, ils nous a été impossible de caractériser les sondes produites au sein du LIRMM. Toutefois, ceci a été fait dans le cadre de l'ANR E-Matahari.

Afin de vérifier le gain apporté par ces nouveaux équipements, une expérimentation a été effectuée en comparant les différents équipements. Cette expérimentation est décrite dans la section suivante.

A.2.3 Comparatif entre les différents matériels

Afin d'effectuer ce comparatif, plusieurs ensembles de traces d'un AES implémenté dans un FPGA ont été recueillies avec différentes sondes et amplificateurs. Deux sondes ont été utilisées avec trois amplificateur différents. Les sondes d'acquisition ont été placé a la même position à l'aide de la table XYZ motorisée ayant une précision de $5\mu m$. Le

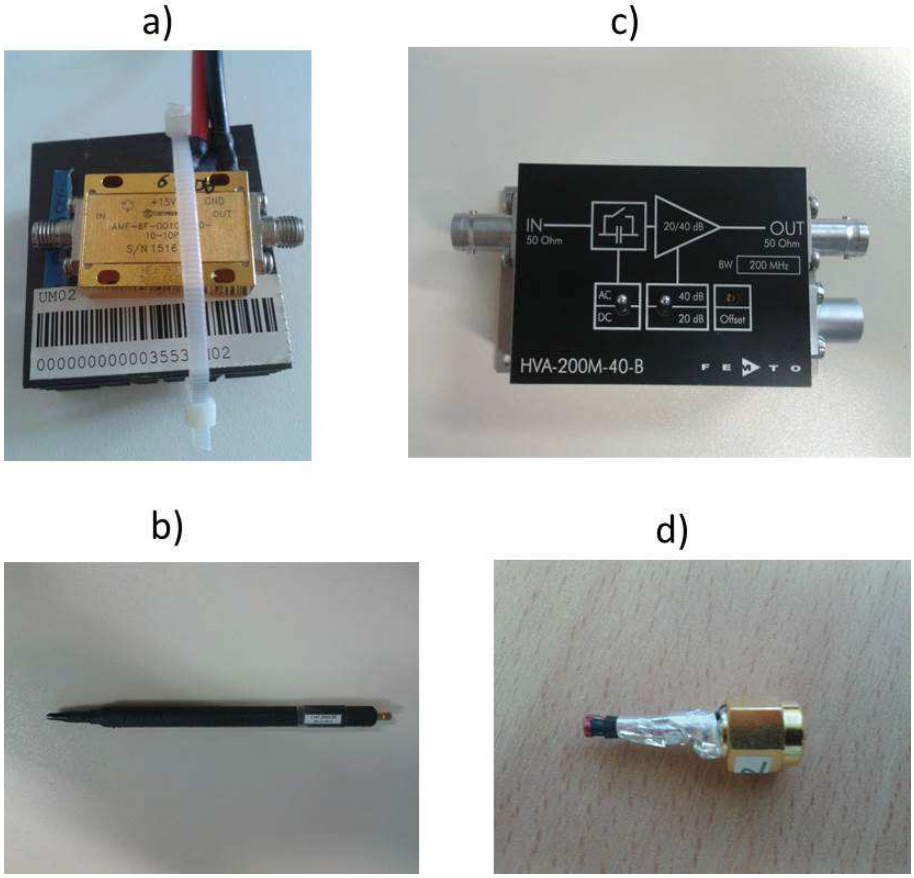

FIGURE A.2: Ancien et nouveau matériels du LIRMM. a) Amplificateur [100MHz,1GHz], b) sonde d'acquisition [30MHz,1GHz], c) amplificateur [10KHz,200MHz] et d) sonde d'analyse avec un cœur de ferrite

premier amplificateur (A1) a un gain de 40dB et une bande passante de [1KHz,200MHz]. Le second (A2) a un gain de 40dB et une bande passante de [20MHz, 500MHz] et le dernier (A3) dispose d'un gain de 48dB et d'une bande passante de [100MHz,1GHz]. La première sonde d'analyse (S1) dispose d'une bande passante de [30MHz,1GHz] et la seconde (S2) est constituée d'un cœur en ferrite filtrant naturellement les fréquences au delà de 110MHz.

Pour cette expérimentation, la mesure du taux de réussite de la CPA a été effectué sur 5000 traces EM. Le Tab. A.4 montre le nombre de traces nécessaires à la CPA pour avoir un taux de réussite de 80% pour chaque jeu de trace. Celui-ci montre clairement le fait que l'équipement adapté aux basses fréquence fournis de bien meilleurs résultats. En effet, seulement 850 traces sont nécessaires pour atteindre un taux de réussite de 80% lorsque les traces sont acquises avec cet équipement tandis que 5000 traces ne sont pas suffisantes avec une sonde et un amplificateur qui ont respectivement une bande passante

Amplificateur \ Sonde	S1 [30MHz,1GHz]	S2
A1 [1KHz,200MHz]	2700	850
A2 [20MHz,500MHz]	3400	1570
A3 [100MHz,1GHz]	Échec	2910

TABLE A.4: Nombre de traces d'un AES nécessaire à la CPA pour obtenir un taux de réussite de 80%

commençant à 30MHz et 100MHz. On peut aussi remarquer que plus l'équipement choisi a une fréquence de coupure basse de faible valeur plus les traces sont adaptées aux attaques.

Ces résultats sont une nouvelle confirmation que le modèle proposé par Sébastien Tiran est correcte.

A.3 Conclusion

Les travaux réalisés par Sébastien Tiran décrits en A.1 ont permis de définir un modèle de fuite dans le domaine fréquentiel. Ce modèle montre que la majorité de la fuite d'information se situe dans les basses fréquences. Afin de valider ce modèle une contribution a été amenée afin de le valider de manière expérimentale. Pour cela, des campagnes d'acquisitions de traces EM sur un FPGA et un micro-contrôleur ont permis de démontrer qu'en ne gardant que les basses fréquences pour l'attaque, les résultats d'attaques sont meilleurs. Ces résultats ont donc permis de confirmer de manière expérimentale le modèle de fuite dans le domaine fréquentiel.

A partir de ces résultats, un nouvel amplificateur et de nouvelles sondes d'analyse ont été acquis pour le banc d'analyse E-Sense du LIRMM. Ces nouveaux équipements, qui suivent les recommandations du modèle de fuite dans le domaine fréquentiel sont désormais utilisés systématiquement pour les expérimentations d'analyse au LIRMM.

Liste des publications

S. Ordas, L. Guillaume-Sage, P. Maurine, ''EM Injection : fault model and locality" FDTC 2015

Sébastien Tiran, Sébastien Ordas, Yannick Teglia, Michel Agoyan, Philippe Maurine : A model of the leakage in the frequency domain and its application to CPA and DPA. J. Cryptographic Engineering 4(3) : 197-212 (2014)

Sébastien Ordas, Ludovic Guillaume-Sage, Karim Tobich, Jean-Max Dutertre, Philippe Maurine : Evidence of a Larger EM-Induced Fault Model. CARDIS 2014 : 245-259

Mathieu Carbone, Sébastien Tiran, Sébastien Ordas, Michel Agoyan, Yannick Teglia, Gilles R. Ducharme, Philippe Maurine : On Adaptive Bandwidth Selection for Efficient MIA. COSADE 2014 : 82-97

Sébastien Ordas, Mathieu Carbone, Sébastien Tiran, Philippe Maurine : Efficiency of the RDVFS countermeasure. FTFC 2014

Sébastien Tiran, Sébastien Ordas, Yannick Teglia, Michel Agoyan, Philippe Maurine : A frequency leakage model for SCA. HOST 2014 : 97-100 2013

Sébastien Tiran, Sébastien Ordas, Yannick Teglia, Michel Agoyan, Philippe Maurine : A Frequency Leakage Model and its application to CPA and DPA. IACR Cryptology ePrint Archive 2013 : 278 (2013)

Bibliographie

[1] A. Kerckhoffs and George Fabyan Collection (Library of Congress). *La cryptographie militaire, ou, Des chiffres usités en temps de guerre : avec un nouveau procédé de déchiffrement applicable aux systèmes à double clef*. Extrait du Journal des sciences militaires. Librairie militaire de L. Baudoin, 1883. URL http://books.google.fr/books?id=VbQBAAAAYAAJ.

[2] PUB FIPS. 46-3 : Data encryption standard (des). *National Institute of Standards and Technology*, 25(10), 1999.

[3] Claude Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28 :656–715, 1949.

[4] Praphul Chandra. *Bulletproof Wireless Security : GSM, UMTS, 802.11, and Ad Hoc Security*. Newnes, 2005.

[5] Marc Briceno, Ian Goldberg, and David Wagner. A pedagogical implementation of the gsm a5/1 and a5/2 "voice privacy" encryption algorithms. In *voice privacy*, 1999. URL https://edipermadi.files.wordpress.com/2008/03/pedagogical_implementation_of_a5_cipher.pdf.

[6] Juha T. Vainio. Bluetooth security. 2000. URL http://www.yuuhaw.com/bluesec.pdf.

[7] P. Prasithsangaree and P. Krishnamurthy. Analysis of energy consumption of RC4 and AES algorithms in wireless LANs. In *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, volume 3, pages 1445–1449 vol.3. IEEE, December 2003. ISBN 0-7803-7974-8. doi : 10.1109/glocom.2003.1258477. URL http://dx.doi.org/10.1109/glocom.2003.1258477.

[8] Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. *IEEE Trans. Inf. Theor.*, 22(6) :644–654, September 1976.

[9] M. Bellare and P. Rogaway. The Exact Security of Digital Signatures - How to Sign with RSA and Rabin. *Lecture Notes in Computer Science*, 1070 :399–416, 1996.

[10] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A Digital Signature Scheme Secure against Adaptive chosen-message Attacks. *SIAM J. Comput.*, 17(2) :281–308, April 1988.

[11] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM*, 21 :120–126, 1978.

[12] Taher ElGamal. A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 31 :469–472, 1985.

[13] National Institute of Standards and Technology. Digital Signature Standard (DSS). FIPS Publication 186, May 1994.

[14] Don Johnson and Alfred Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). Technical report, 1999.

[15] le lapin intelligent attention au piratage. 2013. URL http://www.cnetfrance.fr/news/karotz-le-lapin-intelligent-attention-au-piratage-39793818.htm.

[16] le premier frigo pirate au monde. 2013. URL http://www.panoptinet.com/cybersecurite-decryptee/le-premier-frigo-pirate-au-monde.

[17] Randy Torrance and Dick James. The state-of-the-art in ic reverse engineering. In *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '09, pages 363–381, Berlin, Heidelberg, 2009. Springer-Verlag. ISBN 978-3-642-04137-2. doi : 10.1007/978-3-642-04138-9_26. URL http://dx.doi.org/10.1007/978-3-642-04138-9_26.

[18] Sergei P. Skorobogatov and Ross J. Anderson. Optical fault induction attacks. pages 2–12. Springer-Verlag, 2002.

[19] S. P. Skorobogatov. Semi-Invasive Attacks - A New Approach to Hardware Security Analysis. Technical report, University of Cambridge, Computer Laboratory, 2005. URL http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf.

[20] Thomas Ordas, Mathieu Lisart, Etienne Sicard, Philippe Maurine, and Lionel Torres. Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits. In *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation, 18th International Workshop, PATMOS 2008, Lisbon, Portugal, September 10-12, 2008. Revised Selected Papers*, pages 229–236, 2008. doi : 10.1007/978-3-540-95948-9_23. URL http://dx.doi.org/10.1007/978-3-540-95948-9_23.

[21] Sébastien Ordas, Mathieu Carbone, Sébastien Tiran, Gilles Ducharme, and Philippe Maurine. Efficiency of the RDVFS countermeasure. In *IEEE Low Voltage Low Power Conference*, 2014.

[22] Shivam Bhasin, Sylvain Guilley, Laurent Sauvage, and Jean-Luc Danger. Unrolling cryptographic circuits : A simple countermeasure against side-channel attacks. In *Topics in Cryptology - CT-RSA 2010, The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, USA, March 1-5, 2010. Proceedings*, pages 195–207, 2010. doi : 10.1007/978-3-642-11925-5_14. URL http://dx.doi.org/10.1007/978-3-642-11925-5_14.

[23] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology - CRYPTO'96*, pages 104–113, 1996. URL http://www.springerlink.com/index/4el17cvre3gxt4gd.pdf.

[24] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA) : Measures and Counter-Measures for Smart Cards. In Isabelle Attali and Thomas P. Jensen, editors, *E-smart*, LNCS, pages 200–210. Springer, 2001.

[25] Christophe Clavier and Marc Joye. Universal exponentiation algorithm. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, number Generators, pages 300–308, 2001. doi : 10.1007/3-540-44709-1_25. URL http://dx.doi.org/10.1007/3-540-44709-1_25.

[26] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, volume 1666 of *CRYPTO '99*, pages 388–397, London, UK, UK, 1999. Springer-Verlag. URL http://www.springerlink.com/index/kx35ub53vtrkh2nx.pdf.

[27] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In *CHES*, volume 3156 of *LNCS*, pages 16–29, Cambridge, MA, USA, August 2004. Springer, Heidelberg.

[28] Thanh-Ha Le, Jessy Clédière, Cécile Canovas, Bruno Robisson, Christine Servière, and Jean-Louis Lacoume. A proposition for correlation power analysis enhancement. In *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, pages 174–186, 2006. doi : 10.1007/11894063_14. URL http://dx.doi.org/10.1007/11894063_14.

[29] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks : Revealing the Secrets of Smart Cards*, volume 31. Springer Publishing Company, Incorporated, 1st edition, December 2006.

[30] Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Tarik Graba, and Yves Mathieu. Evaluation of power-constant dual-rail logic as a protection of cryptographic applications in fpgas. In *Second International Conference on Secure System Integration and Reliability Improvement, SSIRI 2008, July 14-17, 2008, Yokohama, Japan*, pages 16–23, 2008. doi : 10.1109/SSIRI.2008.31. URL http://dx.doi.org/10.1109/SSIRI.2008.31.

[31] Victor Lomné, Philippe Maurine, Lionel Torres, Michel Robert, Rafael Soares, and Ney Calazans. Evaluation on FPGA of triple rail logic robustness against DPA and DEMA. In *Design, Automation and Test in Europe, DATE 2009, Nice, France, April 20-24, 2009*, pages 634–639, 2009. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?isnumber=5090609&arnumber=5090744&count=326&index=130.

[32] Shengqi Yang, Wayne Wolf, Narayanan Vijaykrishnan, Dimitrios N. Serpanos, and Yuan Xie. Power Attack Resistant Cryptosystem Design : A Dynamic Voltage and Frequency Switching Approach. In *DATE*, 2005.

[33] Matthieu Rivain, Emmanuel Prouff, and Julien Doget. Higher-order Masking and Shuffling for Software Implementations of Block Ciphers. *IACR Cryptology ePrint Archive*, 2009 :420, 2009.

[34] Richard DeMillo Dan Boneh and Richard Lipton. New Threat Model Breaks Crypto Codes. In *Bellcore Press Release*, 1996.

[35] Richard DeMillo Dan Boneh and Richard Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In *EUROCRYPT*, pages 37–51, 1997.

[36] Eli Biham and Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In *CRYPTO*, pages 513–525, 1997.

[37] Christophe Giraud. DFA on AES. In *Advanced Encryption Standard - AES, 4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers*, pages 27–41, 2004. doi : 10.1007/11506447_4. URL http://dx.doi.org/10.1007/11506447_4.

[38] Gilles Piret and Jean-Jacques Quisquater. A differential fault attack technique against SPN structures, with application to the AES and KHAZAD. In *Cryptographic Hardware and Embedded Systems - CHES 2003, 5th International Workshop, Cologne, Germany, September 8-10, 2003, Proceedings*, pages 77–88, 2003. doi : 10.1007/978-3-540-45238-6_7. URL http://dx.doi.org/10.1007/978-3-540-45238-6_7.

[39] Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall, and Claire Whelan. The sorcerer's apprentice guide to fault attacks. *IACR Cryptology ePrint Archive*, 2004 :100, 2004. URL http://eprint.iacr.org/2004/100.

[40] Mathilde Soucarros, Cécile Canovas-Dumas, Jessy Clédière, Philippe Elbaz-Vincent, and Denis Réal. Influence of the temperature on true random number generators. In *HOST 2011, Proceedings of the 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 5-6 June 2011, San Diego, California, USA*, pages 24–27, 2011. doi : 10.1109/HST.2011.5954990. URL http://dx.doi.org/10.1109/HST.2011.5954990.

[41] P. Maurine and D. Auvergne. Output transition time modeling of cmos structures. In *IEEE International Symposium on Circuits and Systems*, pages 363–366, 2001.

[42] Alessandro Barenghi, Guido Marco Bertoni, Luca Breveglieri, and Gerardo Pelosi. A fault induction technique based on voltage underfeeding with application to attacks against AES and RSA. *Journal of Systems and Software*, 86(7) :1864–1878, 2013. doi : 10.1016/j.jss.2013.02.021. URL http://dx.doi.org/10.1016/j.jss.2013.02.021.

[43] Alessandro Barenghi, Guido Bertoni, Emanuele Parrinello, and Gerardo Pelosi. Low voltage fault attacks on the RSA cryptosystem. In *Sixth International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2009, Lausanne, Switzerland, 6 September 2009*, pages 23–31, 2009. doi : 10.1109/FDTC.2009.30. URL http://dx.doi.org/10.1109/FDTC.2009.30.

[44] Alessandro Barenghi, Guido Bertoni, Luca Breveglieri, Mauro Pellicioli, and Gerardo Pelosi. Low voltage fault attacks to AES. In *HOST 2010, Proceedings of the 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 13-14 June 2010, Anaheim Convention Center, California, USA*, pages 7–12, 2010. doi : 10.1109/HST.2010.5513121. URL http://dx.doi.org/10.1109/HST.2010.5513121.

[45] Jörn-Marc Schmidt and Christoph Herbst. A practical fault attack on square and multiply. In *Fifth International Workshop on Fault Diagnosis and Tolerance in Cryptography, 2008, FDTC 2008, Washington, DC, USA, 10 August 2008*, pages 53–58, 2008. doi : 10.1109/FDTC.2008.10. URL http://dx.doi.org/10.1109/FDTC.2008.10.

[46] Karim Tobich, Philippe Maurine, Pierre-Yvan Liardet, Mathieu Lisart, and Thomas Ordas. Voltage spikes on the substrate to obtain timing faults. In *2013 Euromicro Conference on Digital System Design, DSD 2013, Los Alamitos, CA, USA, September 4-6, 2013*, pages 483–486, 2013. doi : 10.1109/DSD.2013.146. URL http://dx.doi.org/10.1109/DSD.2013.146.

[47] Markus Kuhn and Oliver Kömmerling. Physical security of smartcards. *Inf. Sec. Techn. Report*, 4(2) :28–41, 1999. doi : 10.1016/S0167-4048(99)80012-0. URL http://dx.doi.org/10.1016/S0167-4048(99)80012-0.

[48] Toshinori Fukunaga and Junko Takahashi. Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers. In *Sixth International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2009, Lausanne, Switzerland, 6 September 2009*, pages 84–92, 2009. doi : 10.1109/FDTC.2009.34. URL http://dx.doi.org/10.1109/FDTC.2009.34.

[49] Sergei P. Skorobogatov and Ross J. Anderson. Optical fault induction attacks. In *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, pages 2–12, 2002. doi : 10.1007/3-540-36400-5_2. URL http://dx.doi.org/10.1007/3-540-36400-5_2.

[50] Sergei P. Skorobogatov. Using optical emission analysis for estimating contribution to power analysis. In *Sixth International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2009, Lausanne, Switzerland, 6 September 2009*, pages 111–119, 2009. doi : 10.1109/FDTC.2009.39. URL http://dx.doi.org/10.1109/FDTC.2009.39.

[51] D.H Habing. Use of laser to simulate radiation induced transients in semiconductors and circuits. In *IEEE Trans. Nucl. Sci.*, pages 91–100, 1965.

[52] Jörn marc Schmidt and Michael Hutter. Optical and em fault-attacks on crt-based rsa : Concrete results, 2007.

[53] Ingrid Verbauwhede, Dusko Karaklajic, and Jörn-Marc Schmidt. The fault attack jungle - A classification model to guide you. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011, Tokyo, Japan, September 29, 2011*, pages 3–8, 2011. doi : 10.1109/FDTC.2011.13. URL http://dx.doi.org/10.1109/FDTC.2011.13.

[54] Alessandro Barenghi, Luca Breveglieri, Israel Koren, and David Naccache. Fault injection attacks on cryptographic devices : Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11) :3056–3076, 2012. doi : 10.1109/JPROC.2012.2188769. URL http://dx.doi.org/10.1109/JPROC.2012.2188769.

[55] Elena Trichina and Roman Korkikyan. Multi Fault Laser Attacks on Protected CRT-RSA. In Luca Breveglieri, Marc Joye, Israel Koren, David Naccache, and Ingrid Verbauwhede, editors, *2010 Workshop on Fault Diagnosis and Tolerance*

in Cryptography, FDTC 2010, Santa Barbara, California, USA, 21 August 2010, pages 75–86. IEEE Computer Society, 2010.

[56] Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede. An In-depth and Black-box Characterization of the Effects of Clock Glitches on 8-bit MCUs. In Luca Breveglieri, Sylvain Guilley, Israel Koren, David Naccache, and Junko Takahashi, editors, *Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011, Tokyo, Japan, September 29, 2011*, pages 105–114. IEEE, 2011.

[57] Tim Hummel. Exploring effects of electromagnetic fault injection on a 32-bit high speed embedded device microprocessor, July 2014. URL http://essay.utwente.nl/65596/.

[58] Guillaume Barbu, Guillaume Duc, and Philippe Hoogvorst. Java card operand stack : Fault attacks, combined attacks and countermeasures. In *Smart Card Research and Advanced Applications - 10th IFIP WG 8.8/11.2 International Conference, CARDIS 2011, Leuven, Belgium, September 14-16, 2011, Revised Selected Papers*, pages 297–313, 2011. doi : 10.1007/978-3-642-27257-8_19. URL http://dx.doi.org/10.1007/978-3-642-27257-8_19.

[59] Sung-Ming Yen and Marc Joye. Checking before output may not be enough against fault-based cryptanalysis. *IEEE Trans. Computers*, 49(9) :967–970, 2000. doi : 10.1109/12.869328. URL http://doi.ieeecomputersociety.org/10.1109/12.869328.

[60] Christophe Clavier. Secret external encodings do not prevent transient fault analysis. In *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, pages 181–194, 2007. doi : 10.1007/978-3-540-74735-2_13. URL http://dx.doi.org/10.1007/978-3-540-74735-2_13.

[61] Bruno Robisson and Pascal Manet. Differential behavioral analysis. In *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, pages 413–426, 2007. doi : 10.1007/978-3-540-74735-2_28. URL http://dx.doi.org/10.1007/978-3-540-74735-2_28.

[62] Jasper G. J. van Woudenberg, Marc F. Witteman, and Federico Menarini. Practical optical fault injection on secure microcontrollers. In *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011, Tokyo, Japan, September 29, 2011*, pages 91–99, 2011. doi : 10.1109/FDTC.2011.12. URL http://dx.doi.org/10.1109/FDTC.2011.12.

[63] Johannes Blömer, Ricardo Gomes da Silva, Peter Günther, Juliane Krämer, and Jean-Pierre Seifert. A practical second-order fault attack against a real-world pairing implementation. In *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2014, Busan, South Korea, September 23, 2014*, pages 123–136, 2014. doi : 10.1109/FDTC.2014.22. URL http://dx.doi.org/10.1109/FDTC.2014.22.

[64] Pierre-Alain Fouque, Delphine Leresteux, and Frédéric Valette. Using faults for buffer overflow effects. In *Proceedings of the ACM Symposium on Applied Computing, SAC 2012, Riva, Trento, Italy, March 26-30, 2012*, pages 1638–1639, 2012. doi : 10.1145/2245276.2232038. URL http://doi.acm.org/10.1145/2245276.2232038.

[65] Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache, Anne-Lise Ribotta, Assia Tria, and Thierry Vaschalde. Fault round modification analysis of the advanced encryption standard. In *2012 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2012, San Francisco, CA, USA, June 3-4, 2012*, pages 140–145, 2012. doi : 10.1109/HST.2012.6224334. URL http://dx.doi.org/10.1109/HST.2012.6224334.

[66] Amine Dehbaoui, Amir-Pasha Mirbaha, Nicolas Moro, Jean-Max Dutertre, and Assia Tria. Electromagnetic glitch on the AES round counter. In *Constructive Side-Channel Analysis and Secure Design - 4th International Workshop, COSADE 2013, Paris, France, March 6-8, 2013, Revised Selected Papers*, pages 17–31, 2013. doi : 10.1007/978-3-642-40026-1_2. URL http://dx.doi.org/10.1007/978-3-642-40026-1_2.

[67] Manuel San Pedro, Mate Soos, and Sylvain Guilley. FIRE : fault injection for reverse engineering. In *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication - 5th IFIP WG 11.2 International Workshop, WISTP 2011, Heraklion, Crete, Greece, June 1-3, 2011.*

Proceedings, pages 280–293, 2011. doi : 10.1007/978-3-642-21040-2_20. URL http://dx.doi.org/10.1007/978-3-642-21040-2_20.

[68] Hélène Le Bouder, Sylvain Guilley, Bruno Robisson, and Assia Tria. Fault injection to reverse engineer des-like cryptosystems. In *Foundations and Practice of Security - 6th International Symposium, FPS 2013, La Rochelle, France, October 21-22, 2013, Revised Selected Papers*, pages 105–121, 2013. doi : 10.1007/978-3-319-05302-8_7. URL http://dx.doi.org/10.1007/978-3-319-05302-8_7.

[69] Christophe Clavier and Antoine Wurcker. Reverse engineering of a secret aes-like cipher by ineffective fault analysis. In *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography, Los Alamitos, CA, USA, August 20, 2013*, pages 119–128, 2013. doi : 10.1109/FDTC.2013.16. URL http://dx.doi.org/10.1109/FDTC.2013.16.

[70] Alexandre Sarafianos, Mathieu Lisart, Olivier Gagliano, Valerie Serradeil, Cyril Roscian, Jean-Max Dutertre, and Assia Tria. Robustness improvement of an SRAM cell against laser-induced fault injection. In *2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, DFT 2013, New York City, NY, USA, October 2-4, 2013*, pages 149–154, 2013. doi : 10.1109/DFT.2013.6653598. URL http://dx.doi.org/10.1109/DFT.2013.6653598.

[71] Jean-Max Dutertre, Jacques Fournier, Amir Pasha Mirbaha, David Naccache, Jean-Baptiste Rigaud, Bruno Robisson, and Assia Tria. Review of fault injection mechanisms and consequences on countermeasures design. In *Design & Technology of Integrated Systems in Nanoscale Era (DTIS), 2011 6th International Conference on*, pages 1 – 6, athens, Greece, April 2011. doi : 10.1109/DTIS.2011.5941421. URL http://hal-emse.ccsd.cnrs.fr/emse-00623133.

[72] Loïc Zussa, Amine Dehbaoui, Karim Tobich, Jean-Max Dutertre, Philippe Maurine, Ludovic Guillaume-Sage, Jessy Clédière, and Assia Tria. Efficiency of a glitch detector against electromagnetic fault injection. In *Design, Automation & Test in Europe Conference & Exhibition, DATE 2014, Dresden, Germany, March 24-28, 2014*, pages 1–6, 2014. doi : 10.7873/DATE.2014.216. URL http://dx.doi.org/10.7873/DATE.2014.216.

[73] Alessandro Barenghi, Luca Breveglieri, Israel Koren, Gerardo Pelosi, and Francesco Regazzoni. Countermeasures against fault attacks on software implemented AES : effectiveness and cost. In *Proceedings of the 5th Workshop on Embedded Systems Security, WESS 2010, Scottsdale, AZ, USA, October 24, 2010*, page 7, 2010. doi : 10.1145/1873548.1873555. URL http://doi.acm.org/10.1145/1873548.1873555.

[74] Christian Aumüller, Peter Bier, Wieland Fischer, Peter Hofreiter, and Jean-Pierre Seifert. Fault attacks on RSA with CRT : concrete results and practical countermeasures. In *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers*, pages 260–275, 2002. doi : 10.1007/3-540-36400-5_20. URL http://dx.doi.org/10.1007/3-540-36400-5_20.

[75] David Vigilant. RSA with CRT : A new cost-effective solution to thwart fault attacks. In *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings*, pages 130–145, 2008. doi : 10.1007/978-3-540-85053-3_9. URL http://dx.doi.org/10.1007/978-3-540-85053-3_9.

[76] Jean-Sébastien Coron, Christophe Giraud, Nicolas Morin, Gilles Piret, and David Vigilant. Fault attacks and countermeasures on vigilant's RSA-CRT algorithm. In *2010 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2010, Santa Barbara, California, USA, 21 August 2010*, pages 89–96, 2010. doi : 10.1109/FDTC.2010.9. URL http://doi.ieeecomputersociety.org/10.1109/FDTC.2010.9.

[77] Marc Joye. A method for preventing "skipping" attacks. In *2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, USA, May 24-25, 2012*, pages 12–15, 2012. doi : 10.1109/SPW.2012.14. URL http://dx.doi.org/10.1109/SPW.2012.14.

[78] Sébastien Tiran, Sébastien Ordas, Yannick Teglia, Michel Agoyan, and Philippe Maurine. A frequency leakage model for SCA. In *HOST*, pages 97–100, 2014.

[79] Nicolas Debande, Youssef Souissi, Maxime Nassar, Sylvain Guilley, Thanh-Ha Le, and Jean-Luc Danger. "re-synchronization by moments" : An efficient solution to

align side-channel traces. In *2011 IEEE International Workshop on Information Forensics and Security, WIFS 2011, Iguacu Falls, Brazil, November 29 - December 2, 2011*, pages 1–6, 2011. doi : 10.1109/WIFS.2011.6123143. URL http://dx.doi.org/10.1109/WIFS.2011.6123143.

[80] Jörn marc Schmidt and Michael Hutter. Optical and em fault-attacks on crt-based rsa : Concrete results, 2007.

[81] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis : Concrete Results. In *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '01, pages 251–261, London, UK, UK, 2001. Springer-Verlag.

[82] François Poucheret, Karim Tobich, Mathieu Lisart, Laurent Chusseau, Bruno Robisson, and Philippe Maurine. Local and Direct EM Injection of Power Into CMOS Integrated Circuits. In Luca Breveglieri, Sylvain Guilley, Israel Koren, David Naccache, and Junko Takahashi, editors, *Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011, Tokyo, Japan, September 29, 2011*, pages 100–104. IEEE, 2011.

[83] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, P. Orsatelli, Philippe Maurine, and Assia Tria. Injection of transient faults using electromagnetic pulses -practical results on a cryptographic system-. *IACR Cryptology ePrint Archive*, 2012 :123, 2012. URL http://eprint.iacr.org/2012/123.

[84] K. Baddam and M. Zwolinski. Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure. In *VLSI Design*, pages 854–862, 2007.

[85] Behzad Razavi. *Design of Analog CMOS Integrated Circuits*. McGraw-Hill, Inc., New York, NY, USA, 1 edition, 2001. ISBN 0072380322, 9780072380323.

[86] Denis Réal, Cécile Canovas, Jessy Clédière, M'hamed Drissi, and Frédéric Valette. Defeating classical hardware countermeasures : a new processing for side channel analysis. In *Design, Automation and Test in Europe, DATE 2008, Munich, Germany, March 10-14, 2008*, pages 1274–1279, 2008. doi : 10.1109/DATE.2008.4484854. URL http://dx.doi.org/10.1109/DATE.2008.4484854.

[87] Stefan Mangard. Hardware Countermeasures against DPA - A Statistical Analysis of Their Effectiveness. In Tatsuaki Okamoto, editor, *CT-RSA*, Lecture Notes in Computer Science, pages 222–235. Springer, 2004.

[88] Stan Salvador and Philip Chan. Toward accurate dynamic time warping in linear time and space. *Intell. Data Anal.*, 11(5) :561–580, 2007. URL http://content.iospress.com/articles/intelligent-data-analysis/ida00303.

[89] Ruben A. Muijrers, Jasper G. J. van Woudenberg, and Lejla Batina. RAM : rapid alignment method. In *Smart Card Research and Advanced Applications - 10th IFIP WG 8.8/11.2 International Conference, CARDIS 2011, Leuven, Belgium, September 14-16, 2011, Revised Selected Papers*, pages 266–282, 2011. doi : 10.1007/978-3-642-27257-8_17. URL http://dx.doi.org/10.1007/978-3-642-27257-8_17.

[90] Rodrigo Possamai Bastos, Frank Sill Torres, Jean-Max Dutertre, Marie-Lise Flottes, Giorgio Di Natale, and Bruno Rouzeyre. A bulk built-in sensor for detection of fault attacks. In *2013 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2013, Austin, TX, USA, June 2-3, 2013*, pages 51–54, 2013. doi : 10.1109/HST.2013.6581565. URL http://dx.doi.org/10.1109/HST.2013.6581565.

[91] Jean-Jacques Quisquater and David Samyde. Eddy current for magnetic analysis with active sensor. In *E-Smart 2002,NOVAMEDIA*, pages 185–194, 2002.

[92] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In *Constructive Side-Channel Analysis and Secure Design - Third International Workshop, COSADE 2012, Darmstadt, Germany, May 3-4, 2012. Proceedings*, pages 151–166, 2012. doi : 10.1007/978-3-642-29912-4_12. URL http://dx.doi.org/10.1007/978-3-642-29912-4_12.

[93] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, and Assia Tria. Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES. In Guido Bertoni and Benedikt Gierlichs, editors, *2012 Workshop on*

Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012, pages 7–15. IEEE, 2012.

[94] Philippe Maurine. Techniques for EM fault injection : Equipments and experimental results. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012*, pages 3–4, 2012. doi : 10.1109/FDTC.2012.21. URL http://dx.doi.org/10.1109/FDTC.2012.21.

[95] R.Omarouayache, J.Raoult, S.Jarrix, L.Chusseau, and P.Maurine. Magnetic microprobe design for em fault attack. In *EMC Europe 2013*, 2013.

[96] Gaetan Canivet, Jessy Clédière, Jean Baptiste Ferron, Frédéric Valette, Marc Renaudin, and Régis Leveugle. Detailed analyses of single laser shot effects in the configuration of a virtex-ii FPGA. In *14th IEEE International On-Line Testing Symposium (IOLTS 2008), 7-9 July 2008, Rhodes, Greece*, pages 289–294, 2008. doi : 10.1109/IOLTS.2008.41. URL http://doi.ieeecomputersociety.org/10.1109/IOLTS.2008.41.

[97] Takaaki Okumura and Masanori Hashimoto. Setup time, hold time and clock-to-q delay computation under dynamic supply noise. *IEICE Transactions*, 94-A (10) :1948–1953, 2011. URL http://search.ieice.org/bin/summary.php?id=e94-a_10_1948.

[98] Sébastien Tiran, Sébastien Ordas, Yannick Teglia, Michel Agoyan, and Philippe Maurine. A model of the leakage in the frequency domain and its application to CPA and DPA. *J. Cryptographic Engineering*, 4(3) :197–212, 2014.

[99] Sébastien Tiran, Sébastien Ordas, Yannick Teglia, Michel Agoyan, and Philippe Maurine. A frequency leakage model and its application to CPA and DPA. *IACR Cryptology ePrint Archive*, 2013 :278, 2013. URL http://eprint.iacr.org/2013/278.

[100] Sébastien Tiran. *Side Channels in the Frequency Domain.* PhD thesis, I2S, 2013.

[101] F. van der Meer and S.M. de Jong. Imaging spectrometry : Basic principles and prospective applications. In *Remote sensing and digital image processing. Kluwer Academic Publishers*, 2006.

[102] Julien Doget, Emmanuel Prouff, Matthieu Rivain, and François-Xavier Standaert. Univariate side channel attacks and leakage modeling. *IACR Cryptology ePrint Archive*, 2011 :302, 2011. URL http://eprint.iacr.org/2011/302.

[103] François-Xavier Standaert, Tal Malkin, and Moti Yung. A unified framework for the analysis of side-channel key recovery attacks. In *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, pages 443–461, 2009. doi : 10.1007/978-3-642-01001-9_26. URL http://dx.doi.org/10.1007/978-3-642-01001-9_26.

[104] TELECOM ParisTech SEN research group : DPA Contest. 2008-2014.