Modélisation de l'injection de faute électromagnétique sur circuits intégrés sécurisés et contre-mesures

Mathieu Dumont

THÈSE POUR OBTENIR LE GRADE DE DOCTEUR
DE L'UNIVERSITÉ DE MONTPELLIER

En Systèmes Automatiques et Micro-Électroniques

École doctorale : Information, Structure et Systèmes (I2S)

Unité de recherche : LIRMM, UMR 5506

Modélisation de l'injection de faute électromagnétique sur circuits intégrés sécurisés et contre-mesures

Présentée par **Mathieu DUMONT**

Le 9 Octobre 2020

Sous la direction de Philippe MAURINE
et Mathieu LISART

Devant le jury composé de

Jean-Luc DANGER, Professeur à l'Université Télécom Paristech	Rapporteur
Vincent BEROULLE, Professeur à l'Université Grenoble Alpes, LCIS	Rapporteur
Pascal NOUET, Professeur à l'Université Montpellier, LIRMM	Président du jury
Bruno ROUZEYRE, Professeur à l'Université Montpellier, LIRMM	Examinateur
Christophe LAURENCIN, Ingénieur à STMicroelectronics Rousset	Examinateur
Philippe MAURINE, Maître de conférences à l'Université Montpellier, LIRMM	Directeur de thèse
Mathieu LISART, Ingénieur à STMicroelectronics Rousset	Co-encadrant

UNIVERSITÉ DE MONTPELLIER

À ma mamie ...

Remerciements

Se lancer dans une thèse peut paraître facile, mais la mener au bout l'est beaucoup moins. Cette expérience enrichissante et passionnante représente une tranche de ma vie, qui n'aurait pas été réalisable sans le soutien de nombreuses personnes que je souhaite remercier chaleureusement.

Cette thèse a été effectuée au sein de la division SMD (Secure Microcontroler Division) de la société STMicroelectronics de Rousset en collaboration avec le LIRMM (Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier) de l'Université de Montpellier II.

Je tiens tout d'abord à remercier très sincèrement mes deux encadrants, qui m'ont soutenu durant ces trois années. Philippe Maurine, mon directeur de thèse, pour son investissement, ses conseils et le temps consacré aux relectures. Et Mathieu Lisart, mon tuteur industriel, dans un premier temps pour m'avoir permis de réaliser cette thèse, puis pour tous ses enseignements, ses idées et pour la confiance qu'il m'a accordé. Merci à vous, les réunions ensemble ont toujours été riches en expériences et nos débats sur l'EM vont me manquer.

J'adresse aussi toute ma gratitude à Christophe Laurencin, manager de notre équipe Architecture Sécurité, qui a toujours su me donner des conseils très pertinents. Merci d'avoir pris le temps de m'écouter et de m'avoir reboosté quand il le fallait. Travailler dans ton équipe a été une vraie chance pour moi.

Je n'aurais certainement pas pu achever cette thèse sans le soutien, autant moral que professionnel, de trois personnes : Alexandre, Clément et Nicolas. Ils m'ont épaulé sans cesse, et m'ont consacré de leur temps sans hésitations en transmettant leur expérience et leur connaissance en tant qu'ancien thésard. Je vous remercie infiniment pour avoir su me remotiver dans les moments difficiles mais également pour tous les bons moments passés ensemble.

Je souhaite remercier Fabrice et Stéphane, mes voisins de box. Travailler à leurs côtés a été un vrai plaisir et nos discussions ont toujours été très enrichissantes. Les échanges et « chambrages » de ce box (avec Mathieu et Alexandre) vont me manquer ! Sans oublier mes premiers voisins Olivier Giaume, Marc Benveniste et Alexandre Tramoni, que je remercie également.

De même, j'adresse toute ma reconnaissance à l'ensemble de l'équipe Architecture Sécurité, notamment à Pierre-Yvan, David, Yanis, Daniele, Bruno, Thomas et Ibrahima. Leur disponibilité, et leur aide ont conditionné la réussite de ma thèse. Merci également aux thésards de l'équipe, Raphaël, Davide et Simon, pour leur bonne humeur et le soutien qu'on a pu s'apporter les uns aux autres.

Je tiens également à remercier toutes les personnes de mon étage pour leur accueil chaleureux et leur convivialité, et tout particulièrement les équipes de Design Analog et Digital qui m'ont aidé à de maintes reprises. Je garderai que de bons souvenirs, surtout des petits-déjeuners en leur compagnies.

Durant ces 3 années passées à STMicroelectronics, j'ai eu l'occasion de côtoyer de nombreuses personnes qui m'ont apporté leurs aides et ayant partagé leur expérience avec moi. J'aimerais ainsi remercier Bruno-Gerard Perrin et François Bonnard qui se sont toujours montrés disponibles pour m'aider à résoudre des problèmes techniques. Merci à Anthony Tornambe pour ses cours sur l'EM et à toute l'équipe Appli en général. En outre je remercie, Marc Lacruche, Michel Agoyan, Sandrine Clément, Jérôme Collière, Kiki, Camille Botella, Joseph Rimlinger, Johann Meleard, Karim Benhissou (le Capo), Alban Formisano, et toutes les personnes ayant contribué à la réalisation de cette thèse.

J'aimerais remercier les collègues, chercheurs, professeurs et thésards du laboratoire LIRMM de Montpellier pour leur suivi. De même, j'adresse ma reconnaissance aux personnes du laboratoire des MINES de Gardanne avec qui j'ai eu l'occasion de travailler. Je remercie également les membres du projet CSAFE+, les réunions portant sur le sujet de ma thèse ont été très enrichissantes et les études réalisées par les autres membres ont largement contribué à l'avancement de ma thèse.

Cette thèse n'aurait pas été possible sans un groupe d'amis formidables que j'ai eu la chance de côtoyer à ST, à savoir Geoffrey, Florian, Matthias, Kerry, Laure, Marjo, Eugenia, Thibault K., Thibault B., Abde, Romeric, Franck, Leo, Sophia (et Romain), Lisa, Claire, Anna, JJ, David, Audrey, Geoffrey H., Arnaud, Cloe, Malek, Ivhan, Stéphane et tous les autres. Merci à la BAP (Brasserie Artisanale de Provence), notre repère, pour toutes ces bonnes soirées. Je remercie également Sébastien Vidal qui m'a toujours aidé pour mes problèmes informatiques et avec qui parler basket est toujours un plaisir. Par ailleurs, je tiens à remercier toute l'équipe de basket de ST (PiF, Sylvain, Gilles, Antonio, Julien, Dim …) pour ces entrainements façon NBA du Mardi midi.

Mes plus profonds remerciements vont évidemment à ma famille, ma mère qui a tout donné pour me donner toutes les chances de réussir, mon père, mon frère, ma sœur et ma tante France qui m'ont toujours encouragé tout au long de mes études, ainsi que

toute ma famille. Merci également à tout mon groupe d'amis de Marseille, ma deuxième famille, qui m'ont soutenu indirectement grâce à tous les moments passés ensemble depuis bientôt plus de 7 ans.

Il reste une personne sans qui je ne serai jamais arrivé jusque-là, ma fiancée Mélanie, qui m'a donné la motivation pour mener à bien cette thèse, malgré les sacrifices et qui a trouvé le courage de relire et corriger parfaitement l'ensemble de ce manuscrit.

Enfin, je remercie le jury et les rapporteurs de me faire l'honneur d'évaluer mes trois années de thèse. Et plus généralement, à toutes les personnes qui liront ce manuscrit, je vous souhaite une bonne lecture.

Table des matières

Introduction générale

De nos jours, la volonté de sécurisation des informations dites « confidentielles » est omniprésente. Avec le développement des nouvelles technologies, les circuits intégrés sont devenus les principaux supports de toutes ces informations. L'exemple le plus probant est la carte à puce. Celle-ci est maintenant un élément, à part entière, de notre vie quotidienne, dans de nombreux domaines tels que la téléphonie, l'identification, le médical, le divertissement ou encore la collecte et la protection des données bancaires. Aujourd'hui, on estime le nombre de cartes à puces en circulation dans le monde autour de 30 à 50 milliards. Celles-ci contiennent de nombreuses informations personnelles, dont le piratage peut avoir des conséquences désastreuses pour son propriétaire. C'est pourquoi la sécurité et la fiabilité des circuits intégrés sont devenus un enjeu majeur pour les industries de semi-conducteur.

De plus, avec l'avènement de l'internet des objets (IoT), les risques sont d'autant plus importants. Les objets connectés se retrouvent partout dans nos domiciles, nos voitures, nos villes, où ils manipulent des données critiques et leur nombre ne cesse d'augmenter. Il est estimé qu'il y aurait actuellement plus de 25 milliards d'objets connectés dans le monde, et ce nombre pourrait être amené à doubler dans les prochaines années. Ces produits, issus de divers fabricants parfois « peu regardant » sur l'aspect sécuritaire, échangent des quantités massives de données entre eux et par des moyens non-contrôlés. Les attaques visant ces systèmes sont nombreuses : un aspirateur autonome connecté Xiaomi dont on peut prendre le contrôle[1], un lapin connecté pour enfant permettant d'espionner son propriétaire[2] ou encore de pouvoir déverrouiller à distance une porte d'entrée de maison connectée [3].

En marge de ces piratages ayant pour but de compromettre les données de leur propriétaire, les entreprises doivent également faire face à une menace grandissante : la contrefaçon. En effet, des entités spécialisées dans ces manœuvres illicites vont utiliser différentes techniques d'attaques sur une puce afin de connaître l'intégralité de son plan de routage. Ces pratiques permettent de copier la puce mais également de réaliser des gains de temps de fabrication considérables. En effet, grâce aux informations collectées illégalement, ces entreprises pourront être à mêmes de reproduire un modèle de puce équivalent en quelques mois contre un an en moyenne de développement pour les fabricants de circuits intégrés « traditionnels ». De plus, le peu de moyen requis pour ce modèle contrefait permet de casser le prix du circuit intégré, contrairement à un fabricant, tels

que STMicroelectronics, qui va investir des moyens humains et financiers conséquents dans le développement d'un nouveau circuit.

Toutes ces raisons poussent les entreprises à développer sans cesse de nouvelles contre-mesures contre ces attaques. Ainsi, une course effrénée s'est engagée entre les attaquants et les concepteurs, entre les attaques et les contre-mesures. Depuis plus de trois décennies, les algorithmes cryptographiques se sont renforcés, menant à la définition d'algorithmes de chiffrement standards, devenus particulièrement robustes face à des attaques logiques. Mais les plateformes matérielles exécutant ces algorithmes sont également des cibles potentielles pour pirater un circuit, et leur sécurité est primordiale. Ainsi, deux types de sécurités peuvent être distingués :

- La sécurité logicielle, consistant à étudier les failles pouvant exister dans le logiciel embarqué sur le circuit dans le but de corrompre des données.

- La sécurité matérielle, consistant à étudier physiquement le circuit, support de l'information. Les attaques vont utiliser les phénomènes physiques du circuit afin d'en déterminer des informations confidentielles et les contre-mesures seront développées pour renforcer les circuits.

La sécurité matérielle est souvent plus coûteuse et complexe à mettre en œuvre que des protections logicielles, d'autant plus que celle-ci est implémentée dans un circuit lors de sa conception, rendant impossible les mises à jour face à de nouvelles attaques. Ainsi, le recours à ces attaques par les pirates est de plus en plus fréquent et notamment les attaques par injections de fautes. Ces attaques emploient différents moyens pour induire des perturbations dans un circuit altérant son fonctionnement et permettant d'obtenir des informations sensibles. Parmi ces moyens, on retrouve le champ électromagnétique.

L'attaque par injection de faute électromagnétique constitue une attaque de choix car elle nécessite peu de moyens et de travaux de préparations de la puce ciblée. Pourtant, cette technique d'injection reste encore peu comprise et encore peu de méthodes de conception permettent d'accroître la robustesse des circuits face à ce type d'attaque.

C'est dans ce contexte que ces travaux de thèse ont été menés, en collaboration avec la division SMD (Secure Microcontroller Division) de STMicroelectronics et le laboratoire LIRMM (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier), l'objectif premier étant d'approfondir la compréhension de cette attaque afin d'en déduire des moyens de protection efficaces.

Le premier chapitre présente un état de l'art des recherches scientifiques du domaine de la sécurité des circuits intégrés. Avant de se concentrer sur l'attaque utilisée dans ces travaux, à savoir l'injection de fautes électromagnétiques, les attaques matérielles par injection de fautes sont préalablement définies et un rappel des principes fondamentaux de l'électromagnétisme est donné. Enfin, cette partie permet d'affiner le contexte et de délimiter les objectifs de la thèse.

Le deuxième chapitre est consacré à l'étude du couplage entre le champ électromagnétique et le circuit intégré. Quelques notions sur la structure d'un circuit sont d'abord rappelées, afin de permettre l'analyse des phénomènes physiques liés à l'induction du champ EM sur le circuit. Puis, une modélisation de ces effets est présentée permettant de simuler le couplage entre le champ EM et les grilles d'alimentation d'un circuit.

Le troisième chapitre a pour objectif d'étudier le phénomène d'induction de faute dans un circuit synchrone soumis à une attaque par injection de faute électromagnétique. Pour cela, la modélisation précédente est réutilisée pour être appliquée à une simulation électrique d'un circuit. Les différentes fautes obtenues et leur mécanisme de formation peuvent être ainsi analysés. Les résultats de ces simulations sont corrélés avec des mesures expérimentales effectuées sur une puce de test embarquant un algorithme de chiffrement de type AES, permettant de confirmer la modélisation de l'EMFI élaborée tout au long de cette thèse.

Le quatrième chapitre est dédié à la sécurisation des circuits intégrés. Il présente des idées de contre-mesures face à l'attaque par injection de fautes électromagnétique. Il peut s'agir de règles de conception pour augmenter la robustesse des circuits, ou de détecteurs dédiés à l'injection de fautes EM.

À la suite de ces chapitres une synthèse, sous forme de questions/réponses, permet de répondre aux principales interrogations qu'un lecteur pourrait se poser tout au long de cette thèse. Pour finir, une conclusion vient résumer la totalité des résultats obtenues tout en abordant les perspectives envisageables à la suite des travaux réalisés dans cette thèse.

Chapitre 1 . État de l'Art

Ce chapitre est consacré à un état de l'Art de la sécurité des circuits intégrés et plus précisément de l'attaque par injection par médium électromagnétique.

Il débute par quelques rappels relatifs aux circuits intégrés sécurisés afin de rappeler le fonctionnement de ce qui a constitué la cible de nos attaques et expérimentations lors du déroulement de ma thèse. S'en suit une description des différentes attaques matérielles applicables sur ces circuits.

Ce chapitre se focalise ensuite sur le cœur de thèse : la modélisation de l'EMFI (Electromagnetic Fault Injection) en commençant par rappeler les notions d'électromagnétisme qui m'ont été utiles pour mener mes travaux. Il retrace l'historique de ces attaques ainsi que les contre-mesures proposées face à cette menace.

Le chapitre se termine par une présentation du contexte et des objectifs de la thèse.

1.1 Les cartes à puces et la sécurité

Le 25 Mars 1974, le français Roland Moreno dépose un brevet décrivant un circuit microélectronique embarquant une mémoire, intégrée dans une fine carte plastique. Ces circuits sont appelés cartes à puce, ou smartcard en anglais. Deux ans plus tard, dans le but de sécuriser les informations contenues dans cette mémoire, un autre français, Michel Ugon, parviendra à intégrer un microprocesseur dans ces cartes plastiques. Le microcontrôleur sécurisé est né. Depuis, la carte à puce s'est très largement répandue dans de nombreux domaines tels que la communication (carte SIM), le secteur bancaire (carte bancaire), le médical (carte vitale) ou comme moyen d'identification (passeport biométrique, badge d'entreprise…).

1.1.1 Composition et fonctionnement des cartes à puces

La communication entre une carte à puce et le lecteur est réalisée par un micromodule doré très mince, représenté à gauche dans la Figure 1.1, mettant en contant les broches du lecteur avec les différents contacts de la puce embarquée dans la carte plastique. Une alternative pour communiquer avec la puce a été récemment mise en œuvre et déployée auprès des consommateurs. Il s'agit d'un protocole radio-fréquence : le protocole NFC pour Near Field Communication, qui ne nécessite donc aucun contact physique avec la carte.

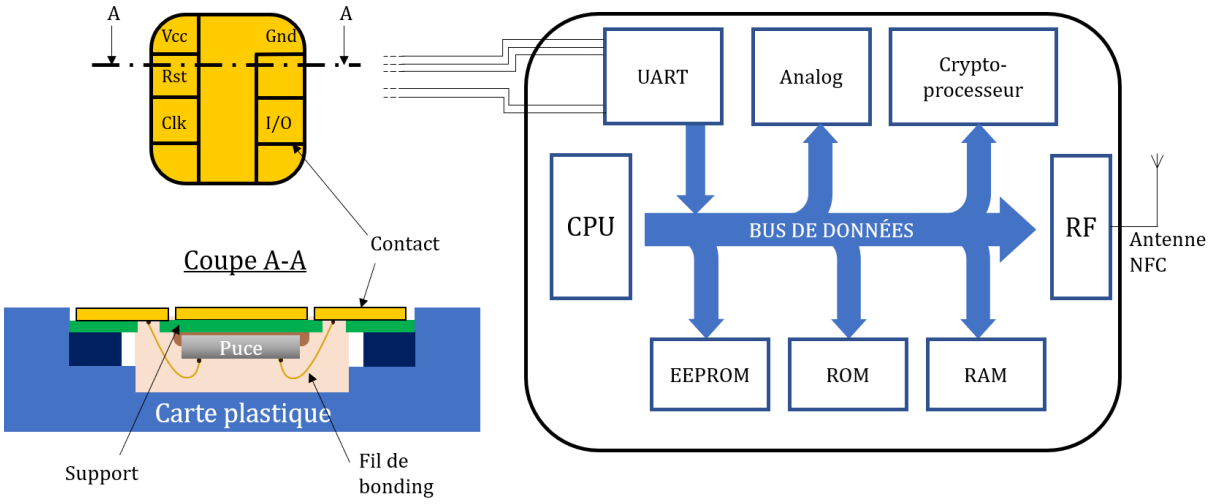


Figure 1.1 – À gauche, contact du micromodule et plan de coupe A-A, à droite, composition d'une carte à puce.

Le micromodule comporte 5 points de contact (les trois autres ne sont pas ou plus utilisés). Le plot Vcc fournit l'alimentation générale du circuit intégré (CI), tandis que le plot Gnd est utilisé comme potentiel de masse (ou Ground, Gnd). Le CI étant un circuit

synchrone, un signal d'horloge (CLK) est fourni par le plot de contact Clk, bien que maintenant la majorité des circuits aient un générateur de signaux d'horloge interne pour des raisons de sécurité. Le transfert des données entre le lecteur et la carte à puce est assuré par le contact d'entrée/sortie, I/O (Input/Output). Enfin, le contact Rst (Reset) permet d'envoyer un signal de réinitialisation à la puce lors de son fonctionnement.

Le bloc de droite de la Figure 1.1 présente un schéma de la composition et du fonctionnement du CI contenu dans une carte à puce. Sa communication avec le lecteur extérieur se fait via l'émetteur récepteur asynchrone universel appelé l'UART (Universal Asynchronous Receiver Transmitter), au moyen des plots de contacts. Elle est également constituée des éléments classiques d'un microcontrôleur, à savoir un microprocesseur (CPU), des mémoires (RAM, ROM et EEPROM) et d'un bloc analogique. Les signaux de données sont transportés dans l'ensemble des éléments du circuit via le bus de données. Un module d'interface radiofréquence (RF) permet la communication avec l'extérieur par la technologie NFC et une antenne. Enfin, les puces conçues pour des applications sécuritaires, intègrent généralement un ou plusieurs processeurs cryptographiques (ou crypto-processeurs), permettant de chiffrer plus efficacement et de manière plus sûre des données. Ces éléments primordiaux et les concepts de la cryptographie sont détaillés dans la section suivante.

1.1.2 Le crypto-processeur

Une carte à puce peut contenir des données personnelles et sensibles dont il est primordial d'assurer la sécurité. La sécurisation de ce type de données est devenue un enjeu d'autant plus important que les objets connectés (Internet Of Things), constituant des cibles de choix pour les pirates, se sont multipliés ces dernières années.

L'intégration d'algorithmes cryptographiques au sein des puces est donc devenue incontournable ces dernières années : même les microcontrôleurs dédiés à des applications standards (non sécuritaires) intègrent désormais de tels algorithmes.

L'objectif d'un système sécurisé est d'assurer :

- La confidentialité des données : seules les personnes autorisées peuvent lire les informations chiffrées.

- L'intégrité des données : le message chiffré ne peut pas être modifié ou altéré sans que cela soit perçu par les personnes autorisées.

- L'authenticité des données : les données lues par le destinataire ont bien été envoyées par l'émetteur signant ces données.

- La non-répudiation : l'auteur d'un message codé ne peut pas renier en être la source.

Les algorithmes de chiffrement se basent sur les principes de Kerckhoff [4]. Ces derniers partent du postulat selon lequel toutes les méthodes de chiffrement sont connues de l'ennemi, et affirment donc que la sécurité d'un système cryptographique ne doit reposer que sur la confidentialité des clés de chiffrement et en aucun cas sur la méthode de chiffrement.

La méthode de chiffrement la plus utilisée est le chiffrement symétrique (utilisant la même clé secrète pour le cryptage et décryptage) par bloc. De tels algorithmes se déroulent en général en plusieurs rondes durant lesquelles une sous-clé (dérivée de la clé secrète) est utilisée pour chiffrer le message. Le nombre de rondes dépend du nombre de bits de la clé secrète. Par exemple, les algorithmes AES (Advanced Encryption Standard) à 128bits, 192 bits et 256bits se déroulent en 10, 12 et 14 rondes respectivement. Au terme de la dernière ronde, le message est entièrement crypté.

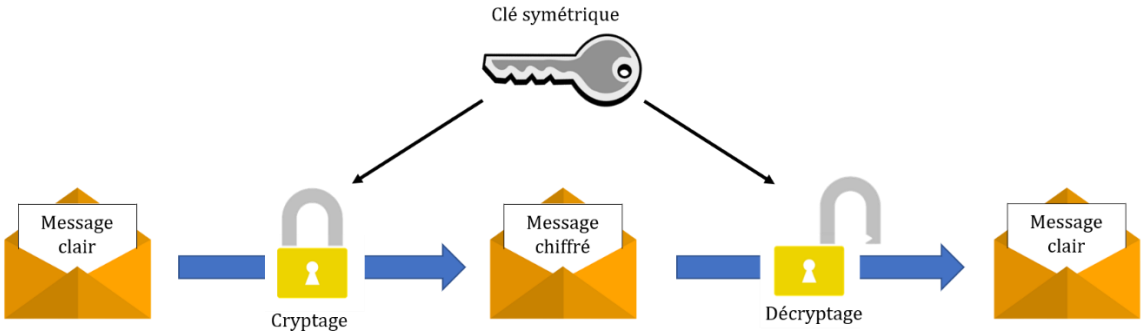


Figure 1.2 - Principe de la cryptographie symétrique.

La Figure 1.2 présente le principe de fonctionnement de la cryptographie symétrique. Le message (ou cyphertext) que l'on souhaite transmettre est d'abord chiffré par un algorithme de cryptage, en utilisant une clé symétrique. Ce message est ainsi chiffré pour être transmis à un tiers, via un canal non sécurisé. Le destinataire du message le décrypte alors en utilisant la même clé.

Des crypto-processeurs matériels sont souvent utilisés pour effectuer les algorithmes cryptographies, pour gérer les clefs et messages cryptographiques et pour implanter les protocoles cryptographiques décrits dans le paragraphe précédent. Ils sont utilisés pour leur flexibilité et leur haute performance et sont donc également les cibles d'attaques logicielles et matérielles dont le but est souvent de révéler les clés secrètes de chiffrement.

1.2 Les attaques matérielles sur le circuit

Il est difficile de fournir un catalogue exhaustif des attaques actuellement déployées pour extraire des secrets contenus dans un circuit du fait de leur nombre. Toutefois, ces attaques font l'objet de classifications. L'attaquant peut avoir un rôle actif en perturbant le fonctionnement du circuit cible ou passif en observant simplement certaines variables physiques liées au système. On parle alors d'attaques actives ou passives.

1.2.1 Classification des attaques matérielles

Une classification, très largement répandue, de ces attaques est réalisée en fonction du travail de préparation de la puce nécessaire à l'application de l'attaque :

- Attaques invasives : ces attaques sont menées directement sur la structure physique de la puce. Elle a pour résultat final de rendre le circuit inutilisable, voire de détruire la puce. En général, ces attaques sont menées par des experts car elles requièrent un matériel lourd et coûteux. L'une des attaques les plus connues [5] permet de reconstituer l'ensemble d'un layout en utilisant des techniques d'analyse du circuit couche par couche.
- Attaques non-invasives : ces attaques sont très répandues car elles n'impliquent aucune préparation de la puce, ni de contact avec celle-ci. Deux types d'approches peuvent être menées pour ces attaques. La première est d'observer certains paramètres physiques fuitant du circuit lors de son exécution (attaque par canaux cachés). La seconde consiste à corrompre son fonctionnement en perturbant des paramètres externes tels que sa température, sa tension d'alimentation ou son horloge.
- Attaques semi-invasives : ces attaques ont été introduites par Sergei Skorobogatov et Ross Anderson [6], [7]. Ce type d'attaques requiert l'ouverture de la puce, c'est-à-dire le retrait de son boîtier, pour être au plus proche du circuit. Toutefois, contrairement aux attaques invasives, la structure de la puce n'est en rien altérée lors de l'application d'une attaque semi-invasive.

Ces attaques, de plus en plus variées, peuvent également être classées en trois catégories : les attaques physiques, les attaques par canaux cachés et les attaques par injection de fautes.

1.2.1.a Les attaques physiques

Les attaques physiques rentrent dans la catégorie des attaques invasives au cours desquelles la structure physique du circuit est modifiée ce qui peut conduire à la destruction de la puce. La plus connue est la rétro-conception (reverse engineering) [8], où chaque couche du circuit successivement est photographiée à l'aide d'un microscope pour en déduire le schéma fonctionnel du circuit. Une autre attaque consiste à mesurer directement les échanges de signaux sur les niveaux de métallisation par micro-sondages (micro-probing) [9]. La modification du circuit est également possible en utilisant un FIB (Focus Ion Beam) [10]. L'attaquant peut dans ce cas découper ou déposer des métaux pour, par exemple, désactiver une fonction sécuritaire.

1.2.1.b Les attaques par canaux cachés

Les attaques par canaux cachés (side channel) sont probablement les attaques les plus redoutables, du fait qu'elles sont faciles à mettre œuvre car non-invasives. Elles ont pour but d'extraire les clés secrètes utilisées lors d'opérations de chiffrement. Lors d'une opération dans un circuit, de nombreuses grandeurs peuvent être exploitées comme montré dans la Figure 1.3.

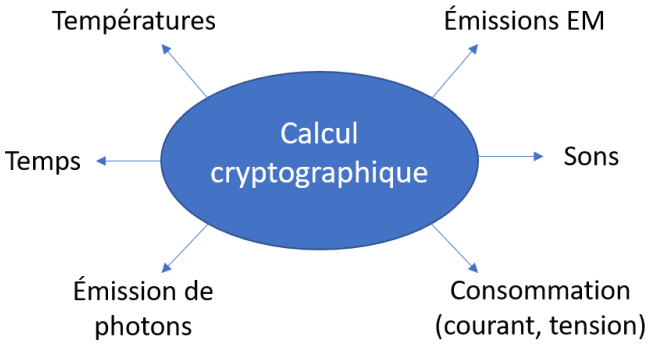


Figure 1.3 – Grandeurs physiques exploitées lors d'attaques par canaux cachés.

Les attaques par analyses temporelles consistent à étudier la durée des opérations de chiffrement. La plus connue est celle proposée par P.Kocher [11] basée sur la corrélation entre les données manipulées et les temps d'exécution d'une instruction.

Les attaques par analyse de consommation utilisent la différence de consommation des portes lorsqu'elles commutent de '0' vers '1' ou de '1' vers '0'. Deux types d'attaques sont concernés par l'analyse de consommation : la SPA (Simple Power Analysis) et la DPA (Differential Power Analysis). La première consiste à analyser directement (lecture directe) des profils en courant durant les opérations cryptographiques. La DPA [12]

utilise des outils statistiques pour identifier l'hypothèse de clef la plus probable selon un modèle de consommation .

L'émission de rayonnements électromagnétique (EM) d'un circuit apparaît lors de la commutation des portes logiques qui induit un flot de courant dans les réseaux de distribution d'alimentation. Il peut être mesuré à l'aide d'une antenne (Figure 1.4). L'analyse de ces émissions EM permet de récupérer des informations confidentielles [13][14] de la même façon qu'avec une SPA ou une DPA mais de manière plus locale et donc plus efficace.

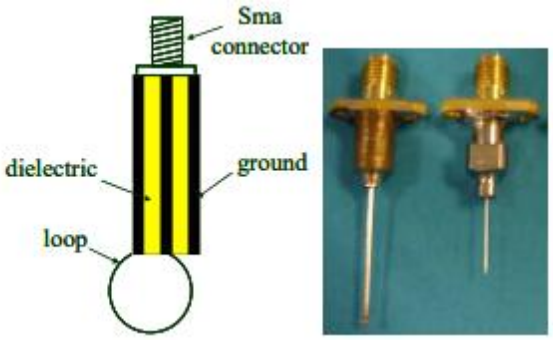


Figure 1.4 – Sonde utilisée pour l'analyse des rayonnements EM d'un circuit [13].

L'émission des rayonnements thermiques peut également être utilisée. En effet, la consommation d'un circuit étant directement proportionnelle à sa température, les émissions thermiques peuvent être visualisées à l'aide d'une caméra infrarouge et interprétées [15] [16], tout comme tout autre canal caché.

1.2.2 Attaques par injection de fautes

Les attaques par injection de fautes [7], également appelées attaques par perturbation, consistent à perturber le fonctionnement d'un circuit dans le but d'induire un comportement fautif dont l'observation permettra d'extraire des données confidentielles comme la clé secrète par exemple.

Les premières injections de fautes ont été constatées [17] par hasard, dans les années 1970, lorsque des circuits électroniques composant des satellites ont montré que des erreurs pouvaient être causées par des rayons cosmiques (particules radioactives). Des recherches ont donc été lancées par l'industrie aérospatiale dans le but de modéliser les effets physiques provoqués par l'interaction de ces particules avec le silicium.

Depuis, de nombreuses propositions ont été soumises pour expliquer la création et la propagation de ces fautes au sein des circuits intégrés et ce sans faire de lien avec la

conception de circuits pour la sécurité. Puis, en 1997, Bonneh, Demillo et Lipton démontrèrent dans [18] qu'en exploitant des résultats de calculs erronés, il est possible d'attaquer l'algorithme de signature RSA (Rivest Shamir Adleman, cryptographie asymétrique). Cette attaque, particulièrement efficace, est communément appelée, attaque de Bellcore.

Parallèlement, Biham [19] démontrait que les algorithmes symétriques étaient tout autant vulnérables face à ce type d'attaques et qu'une analyse différentielle de fautes (DFA) comparant deux ensembles de résultats de chiffrement (des chiffrés corrects et des chiffrés fautés) permettait de dévoiler la clef secrète manipulée par un algorithme DES. Enfin, G.Piret et JJ.Quisquater proposèrent [20] des DFA spécifiques à l'algorithme AES.

Néanmoins, la cryptanalyse matérielle des algorithmes de chiffrement n'est pas l'unique menace que constituent les attaques par injection de fautes. En effet, les programmes embarqués dans les circuits intégrés sont également la cible de ce type d'attaques, afin de contourner des dispositifs de sécurité comme par exemple la vérification d'un code PIN.

1.2.2.a Types de fautes

Les fautes générées dans un circuit synchrone peuvent être de différentes natures [21]. Dans un premier temps, lors d'une attaque par perturbation, une faute simple (Single Event Upsets : SEU) ou plusieurs fautes peuvent être induites (Multiple Cell Upsets : MCU) pendant le fonctionnement du circuit.

On distingue trois types de fautes :

- Les fautes destructives : ces fautes se produisent quand un transistor ou une interconnexion est détruit(e) et génère un collage ou un circuit ouvert ayant pour conséquence de figer le signal du transistor. Cette faute rend le circuit irrémédiablement inutilisable.
- Les fautes permanentes : ces fautes induites persistent jusqu'à un redémarrage du circuit.
- Les fautes transitoires : à l'inverse des fautes permanentes, celles-ci sont induites pendant une durée limitée dans le temps. En général, c'est ce type de fautes qu'un attaquant cherche à générer car elles lui permettent de reproduire la même attaque un grand nombre de fois (pour différentes données manipulées) sur un même circuit, sans risquer de l'endommager.

Un attaquant pourra déterminer quel type de fautes induire, suivant la technique d'attaque choisie. Connaître la valeur booléenne lors de l'induction d'une faute est déterminant pour un attaquant. On retrouve quatre types de fautes :

- Le bit set : force la valeur du signal à '1',
- Le bit reset : force la valeur du signal à '0',
- Le bit flip : inverse la valeur du signal ('0' devient '1' et inversement),
- Le bit stick : colle une valeur à son état ('0' reste '0' et inversement).

Les techniques d'attaques se sont largement diversifiées au fil des années. Celles-ci sont présentées dans les sections suivantes.

1.2.2.b Attaques par perturbation globale

Lors de la conception des circuits intégrés, les concepteurs prennent en considération des marges de conception (marges PVT pour Process, Voltage,Temperature), afin de s'assurer que le circuit opèrera correctement sur une large plage de conditions de fonctionnement. Ces plages de fonctionnement sont définies par la fréquence maximale de fonctionnement et par les valeurs maximales ou minimales de la tension d'alimentation et de la température.

Les attaques par perturbation globale, aussi appelées attaques en limite de fonctionnement, consistent à faire fonctionner le circuit hors de sa plage de fonctionnement normale afin d'induire des fautes. La plupart des fautes induites sont dues à une variation des temps de propagation des signaux dans le circuit, ceci pouvant conduire à un mauvais échantillonnage d'une valeur par une bascule ou un registre. On parle alors de fautes de timing . Pour les induire, on peut appliquer au circuit :

- Une variation de température : cela consiste à amener le circuit sur une plage de fonctionnement non prévue en faisant variant sa température. Pour cela, on peut utiliser soit des résistances chauffantes, des liquides refroidissants ou encore des modules Peltier. La mobilité des porteurs (électrons et trous) est alors altérée et des fautes se produisent. Par exemple, dans [22] un générateur de nombres aléatoires (TRNG) est perturbé en faisant varier sa température de fonctionnement.
- Une variation de la tension d'alimentation du circuit : cela consiste à sur ou sous alimenter le circuit. Les délais de propagation des portes logiques étant directement proportionnels à la tension d'alimentation du circuit [23], modifier celle-ci permet

de produire des fautes de timing. Par exemple, dans [24] et [25], une baisse de la tension d'alimentation a été appliquée pour fauter des algorithmes de chiffrement RSA ou AES.

- Variation de la fréquence d'horloge : cela consiste à augmenter la fréquence de l'horloge d'un circuit au-delà de ses limites de fonctionnement et ainsi causer des fautes [26]. Pour appliquer cette technique d'overclocking, le signal d'horloge utilisé par le circuit doit être fourni par son environnement. C'est une des raisons pour lesquelles les circuits sécurisés embarquent tous des générateurs internes de signaux d'horloge.

1.2.2.c Attaques par perturbation locale

Contrairement aux attaques par perturbation globale, les attaques par perturbation locale s'effectuent dans les plages de fonctionnement normales du circuit. L'attaquant induit une très courte perturbation locale, appelé glitch. Plusieurs types de glitches peuvent être utilisés :

- Glitch de tension : il s'agit d'une très brève variation d'amplitude de la tension d'alimentation du circuit. Cette variation peut être appliquée sur le plot d'alimentation (Vdd) ou le plot de masse (Gnd pour « ground »). Elle induit une brève variation de la polarisation des portes logiques et ainsi un bref changement de leur temps de propagation et donc des fautes de timing [18] [27].
- Glitch d'horloge : ce moyen d'injection consiste à l'induction d'un front parasite sur le signal d'horloge et donc à générer un échantillonnage anticipé des données. Par exemple, dans [28] la génération d'un glitch d'horloge très précis a permis d'induire des fautes sur plusieurs algorithmes cryptographiques afin de retrouver la clé de chiffrement avec la DFA décrite dans [20].

Les techniques d'injection présentées dans ces deux dernières sections sont les premières à avoir été utilisées comme médium d'attaque par injection de fautes. De nombreuses contre-mesures ont depuis été développées pour protéger les circuits. Les techniques présentées dans les sections suivantes sont plus récentes et ont la particularité d'utiliser des techniques d'injection de fautes ayant de meilleures résolutions spatiales et temporelles. Elles sont donc plus prisées par les attaquants de nos jours.

1.2.2.d Perturbation de la polarisation du substrat

Dans certains cas, après une ouverture de la puce, il n'est possible d'accéder qu'à sa face arrière et donc à son substrat. Avec une simple pointe métallique et un générateur

d'impulsion de tension, il est dès lors possible de modifier localement la polarisation du substrat et donc d'induire des fautes. Cette technique d'injection de fautes est appelée BBI pour Body Bias Injection. L'effet de ce type de glitch est mal connu. Toutefois, on peut penser qu'il modifie également les temps de propagation des portes logiques et induit donc des fautes de timing, comme on peut le retrouver dans [29] [30].

Cette attaque ressemble aux attaques par glitch de tension. Toutefois, dans ce cas, la modification de tension peut être appliquée localement à la surface du substrat ce qui permet de contourner certaines contre-mesures.

1.2.2.e Attaques par particules ionisantes

Comme cela a été mentionné précédemment, les premières observations de fautes induites dans des circuits, ont été faites sur des circuits embarqués dans des satellites et donc soumis à des rayons cosmiques [17]. Ainsi, il est également possible d'induire des fautes dans un circuit en utilisant des ions lourds, ou d'autres particules. Dans [31] et [32] les grilles flottantes, d'une mémoire non volatile de type flash (NOR ou NAND), sont soumises à une source de rayonnement de protons d'énergie 2 MeV (Méga électronVolt) ou 100 MeV. L'effet de ces radiations est à l'origine du changement des tensions de seuil des grilles et entraîne ainsi une dégradation de l'information stockée.

Récemment, des attaques par injection de fautes utilisant des rayons ionisants très énergétiques ont permis de corrompre des systèmes cryptographiques. Dans [33] des irradiations ioniques d'une énergie de 1GeV, réalisées avec des ions carbones, sont appliquées sur un système de chiffrement RSA implémenté dans un FPGA. Des défaillances ont été constatées et ont permis de retrouver la clé secrète. Un des avantages de cette technique est que, contrairement aux attaques invasives par FIB [10], celles réalisées par microfaisceaux d'ions lourds permettent de fauter des registres sans pour autant les endommager.

Ce type d'attaques reste toutefois très coûteux puisqu'elles sont réalisées avec des équipements lourds comme des sondes ioniques focalisées à haute énergie ou encore des accélérateurs de particules (tels que les accélérateurs de TRIUMF du centre national d'accélération des particules au Canada utilisés dans [31]).

1.2.2.f Attaques par illumination

Les attaques par illumination sont basées sur le dysfonctionnement des transistors MOS lorsque ceux-ci sont soumis à des flux lumineux intense. L'énergie lumineuse, absorbée par les recombinaisons électrons-trous se produisant dans le silicium, permet aux

porteurs de passer de la bande de valence interdite à la bande de conduction, ce qui a pour conséquence de générer un courant parasite appelé photocourant.

Les portes logiques soumises à l'illumination sont alors susceptibles de changer d'état et donc d'induire des fautes transitoires dans le circuit. C'est le cas Figure 1.5, où un inverseur CMOS voit son drain illuminé par un laser. Le photocourant généré entre le drain et la masse décharge temporairement la capacité de sortie de l'inverseur et change l'état de sa sortie de '1' à '0'. À l'inverse, l'illumination du drain d'un transistor PMOS, générant un photocourant entre le drain et l'alimentation Vdd, change l'état de sortie de '0' à '1'.

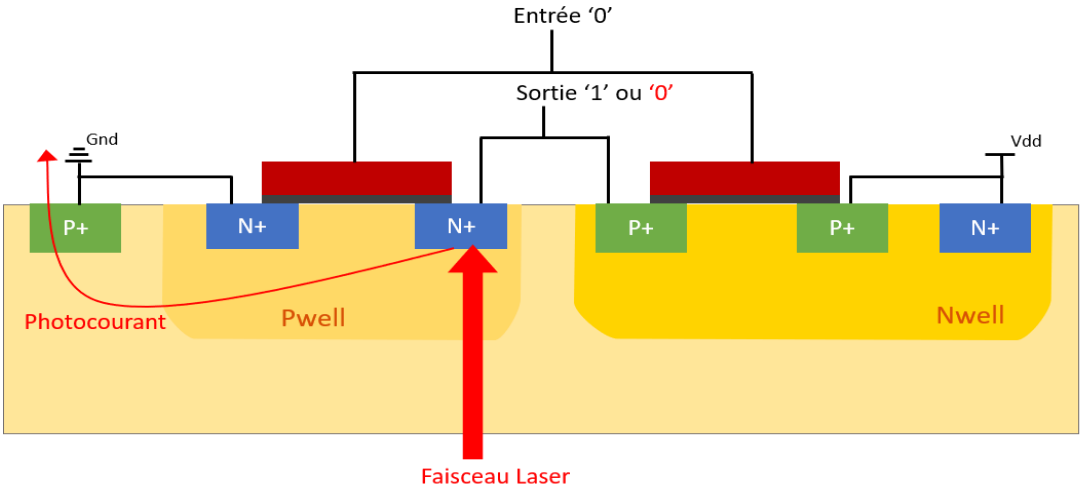


Figure 1.5 - Photocourant généré par une illumination laser sur le drain du transistor NMOS d'un inverseur.

Les premières fautes induites par l'utilisation de cette technique d'attaque ont été réalisées dans [6] avec un simple flash d'appareil photo dont la lumière a été concentrée à l'aide d'un microscope. Ce système a été utilisé pour induire des fautes dans des mémoires SRAM. Une amélioration est apportée dans [34] avec l'utilisation d'une fibre optique pour diriger spatialement le faisceau lumineux sur la puce.

De nos jours, l'utilisation du laser comme médium d'injection de perturbations dans les circuits a fortement évolué et est devenue la principale technique d'injection de fautes. Elle offre l'avantage de générer un grand nombre de fautes et ce de façon très précise, dans le temps (quelques picosecondes) et dans l'espace (quelques micromètres carrés).

De nombreux modèles de fautes par injection laser permettent de prédire les zones sensibles, de différents éléments du circuit tels que les SRAM [35], les transistors NMOS

[36] ou PMOS [37] ou des bascules D [38]. Le laser constitue une technique d'injection idéale pour fauter précisément un AES [39].

Dans [40], deux sources laser ont été utilisées pour attaquer un AES implémenté sur un FPGA protégé par une contre-mesure (de type redondance matérielle). La double illumination a permis d'induire les mêmes erreurs dans les deux chiffrements AES et donc de contourner la contre-mesure.

La face avant d'un circuit étant réfléchissante (forte densité de métallisation), cette attaque est réalisée généralement par la face arrière après amincissement du substrat, ce qui implique une étape de préparation de la puce. De récentes études ont montré qu'il était toutefois possible de réaliser des attaques laser latérales, par le côté de la puce [41].

1.2.2.g Attaque par injection électromagnétiques

Les attaques par injection de fautes électromagnétiques, appelées EMFI (Electromagnetic Fault Injection), sont basées sur la génération d'un champ EM (Électromagnétique) au voisinage de la surface avant ou arrière d'un circuit. Ce champ est généré par une sonde d'injection, un solénoïde, couplant avec le circuit. L'avantage considérable de cette technique d'attaque est de ne pas nécessiter une ouverture du circuit. En effet, elle peut être conduite à travers le boitier, même si une sonde d'injection au plus proche du circuit permet d'augmenter l'effet de couplage et la résolution. Cette technique d'injection est présentée dans le détail dans les paragraphes suivants.

Il paraît important d'ajouter une dernière technique d'attaque, récemment apparue, utilisant un autre type de champ électromagnétique, les rayons X. Dans [42] un faisceau intense de rayons X est utilisé pour cibler l'EEPROM et la RAM d'un circuit. Les résultats montrent qu'il est possible de corrompre un seul transistor dans un état semi-permanent. Un simple traitement thermique permet de supprimer l'effet induit, rendant ainsi la faute réversible. Cependant ce type d'attaque requiert un équipement très spécifique et coûteux.

1.3 Rappel de fondements de l'électromagnétisme

Un champ électromagnétique apparaît dès lors que des charges électriques sont en mouvement. Ce champ résulte en la combinaison des ondes électriques et magnétiques, modélisées mathématiquement par les équations de Maxwell. Comme représenté dans la

Figure 1.6, le champs magnétique $\vec{B}$ et électrique $\vec{E}$, composant le champ EM, sont perpendiculaires l'un à l'autre et se propagent, en espace libre, dans le même sens de propagation à la vitesse de la lumière.

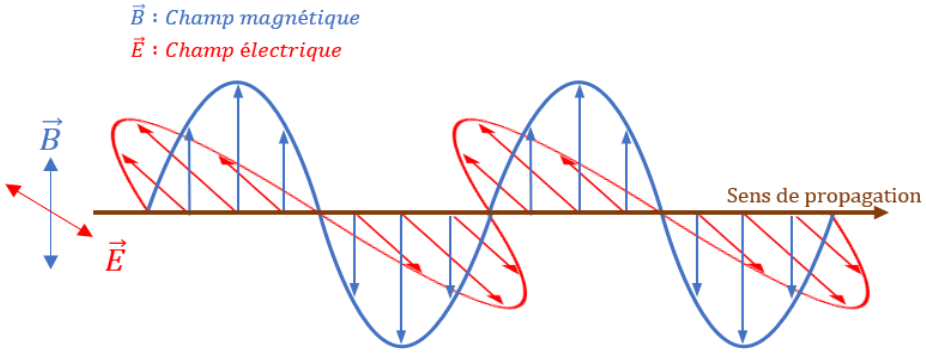


Figure 1.6 - Champ électromagnétique composé d'un champ magnétique $\vec{B}$ et un champ électrique $\vec{E}$ perpendiculaires.

1.3.1 Création d'un champ électromagnétique

Selon la loi de Biot-Savart, un conducteur filiforme traversé par un courant I constant créé un champ magnétique autour de celui-ci. Cette loi énonce [43] que le champ magnétique créé en un point r, à une position de l'espace par ce conducteur de courbe C a pour expression :

$$\vec{B}(\vec{r}) = \frac{\mu_0}{4\pi} \oint_C \frac{I\, d\vec{l} \wedge (\vec{r} - \vec{r'})}{\left|\vec{r} - \vec{r'}\right|^3} \qquad (1.1)$$

r' étant un point de ce conducteur, $d\vec{l}$ le vecteur élémentaire tangent à C en r'.

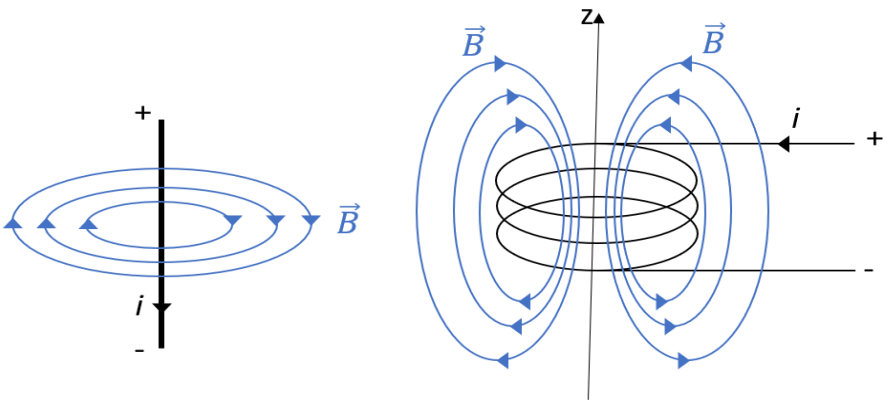


Figure 1.7 - Exemples de champs magnétiques H créés par différents types de conducteurs traversés par un courant I.

La Figure 1.7 représente le champ magnétique créé par deux différents types de conducteurs parcourus par un courant I. Le fil rectiligne (à gauche) génère des lignes de champ H formant des cercles centrés par rapport au fil conducteur. Le fil bobiné ou solénoïde (à droite), génère des lignes de champ ellipsoïdales traversant la surface de la bobine et concentrées le long de l'axe z. À l'intérieur de celle-ci les lignes de champ sont très concentrées tandis qu'à l'extérieur elles se dispersent rapidement. C'est ce type de structure géométrique qui est utilisé lors des attaques par injection de fautes électromagnétique.

Lorsque que le courant qui circule dans cette bobine varie ($\frac{dI}{dt} > 0$), le champ magnétique devient variable et crée, selon l'équation de Maxwell-Faraday (1.2), un champ électrique tournant autour du champ magnétique, constituant un champ électromagnétique.

$$\overrightarrow{rot}\vec{E} = \frac{\partial \vec{B}}{\partial t} \qquad (1.2)$$

1.3.2 Le couplage électromagnétique

Le flux magnétique, noté ϕ, caractérise l'intensité et la répartition spatiale d'un champ magnétique. Cette grandeur est égale au flux de l'induction magnétique $\vec{B}$ à travers une surface S. Lorsque qu'un fil conducteur, formant une boucle fermée de surface S, est placé dans un champ électromagnétique, il y a création d'une force électromotrice (fem), s'opposant au sens du flux magnétique. Cette fem est donnée par la loi de Lenz-Faraday (1.3).

$$fem = -\frac{d\phi}{dt} = -\frac{d}{dt}\iint_S \vec{B}.\overrightarrow{dS} = \oint_C \vec{E}\,.\overrightarrow{dl} \qquad (1.3)$$

Ainsi, la variation de courant dans une antenne (solénoïde) placée à proximité d'un circuit génère des forces électromotrices à l'intérieur de ce dernier, ce qui provoque des perturbations de sa tension, localement.

Le couplage entre une antenne d'injection et une portion d'un circuit est représenté Figure 1.8. Le flux magnétique à travers le circuit peut s'exprimer par :

$$\phi = L_{cir}.i_{cir} + M.i_{antenne} \qquad (1.4)$$

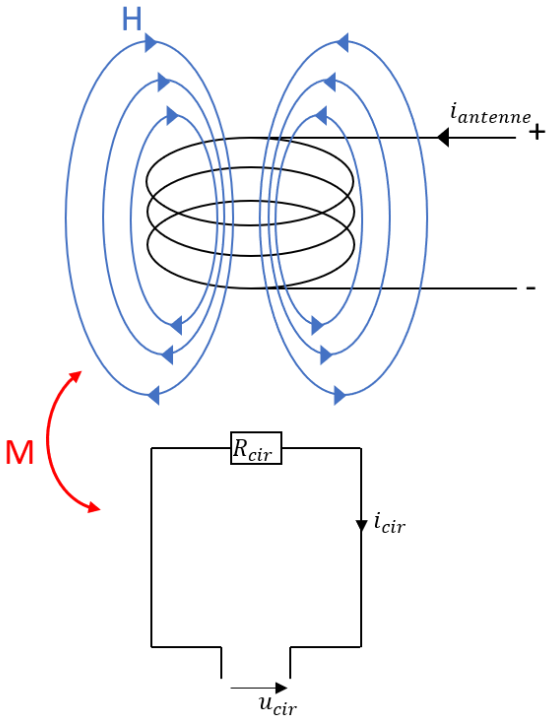


Figure 1.8 - Couplage entre un solénoïde et un circuit électrique.

Avec L_{cir} l'inductance propre de la portion du circuit et M l'inductance mutuelle entre l'antenne et le circuit. Donc, la tension u_{cir} aux bornes du circuit traversé par un champ EM est la somme :

$$u_{cir}(t) = r_{cir}.i_{cir} + L_{cir}\frac{di_{cir}(t)}{dt} + M\frac{di_{antenne}(t)}{dt} \qquad (1.5)$$

L'inductance mutuelle M est donné par :

$$M = k.\sqrt{L_{cir}.L_{antenne}} \qquad (1.6)$$

Avec, L_{cir} et $L_{antenne}$ les inductances du circuit et de l'antenne et k, le coefficient de couplage, compris entre 0 et 1, représentant le pourcentage de flux magnétique traversant la portion du circuit.

1.4 L'apparition de l'injection de fautes électromagnétique

Les attaques par injection de fautes laser restent la technique la plus utilisée en raison de leur précision spatiale et temporelle. Cependant, cette attaque est connue depuis plus de 20 ans, ce qui a permis le développement de nombreuses contre-mesures comme le détecteur de tir laser [44]. De plus, le nombre de couches métalliques ne cesse d'augmenter et peut atteindre maintenant 15 niveaux. Cela a pour effet de rendre de plus en plus difficile les attaques laser en face avant. Et la face arrière est souvent protégée par des contre-mesures contre cette attaque.

L'injection de fautes par médium électromagnétique est une technique relativement récente. Elle n'a donc pas le même niveau de maturité que les injections laser et donc pas les mêmes performances. Toutefois, ses effets sont méconnus et il n'existe pas ou peu de contremesures spécifiques. Pour ces raisons couplées avec la facilité de mise en œuvre et sa capacité à être efficace en face avant et face arrière des circuits, après ou sans retrait du boitier, font de cette technique une technique de plus en plus utilisée.

1.4.1 Première injection de faute

Le champ EM a été utilisé pour la première fois comme medium d'injection de fautes au sein des circuits en 2002, par JJ. Quisquater et D. Samyde. Lors de leurs expérimentations [45], le fort courant d'un flash d'appareil photo est injecté dans un solénoïde pour produire un champ EM puissant. Des fautes sont alors induites dans des mémoires (RAM et EPROM). F. Vargas confirme cette technique d'attaque en 2005 [46], en injectant des fautes dans un microcontrôleur grâce à un champ EM, induit par un générateur de signaux délivrant un signal continu de 1GHz.

Les premières EMFIs sur une implémentation d'un algorithme cryptographique (RSA) ont été réalisées en 2007 [34]. Un allume-gaz détourné est utilisé pour produire un arc électrique, donc une impulsion EM intense, de courte durée, afin de démontrer l'efficacité de cette technique d'injection EM à faible coût.

L'effet de ces EMFIs sur la consommation du circuit lors d'un calcul du système RSA est représenté Figure 1.9 (a). On distingue clairement un pic de consommation lors de l'induction du champ EM. La Figure 1.9 (b) montre la tension induite aux bornes du circuit en fonction de sa hauteur Les courbes démontrent que même si l'EMFI est réalisable sur une puce non décapsulée, elle demeure plus efficace au plus près du circuit. On

peut aussi noter qu'une injection sur la face avant de la puce semble induire une variation de tension plus importante que sur la face arrière.

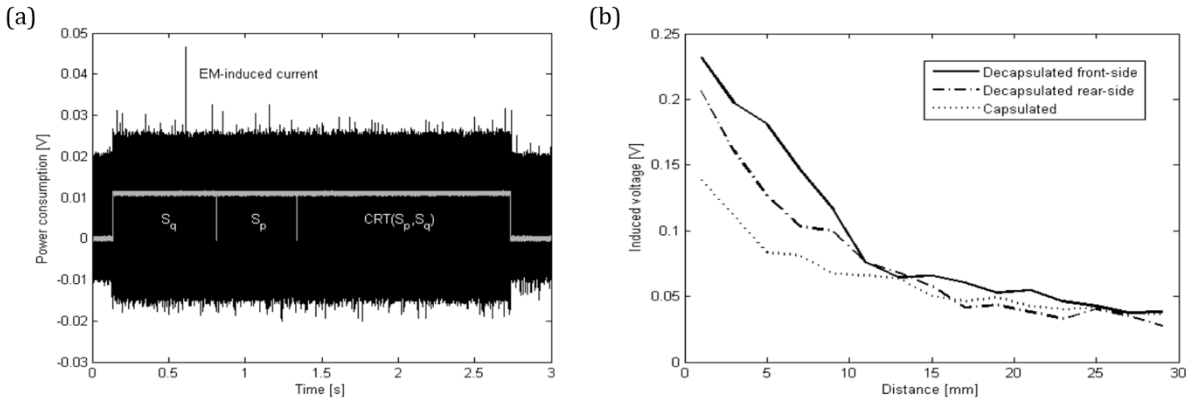


Figure 1.9 – (a) Trace de la consommation du circuit pendant le calcul d'un système de chiffrement RSA et lors d'une EMFI. (b) Courbes de la tension mesurée aux bornes du circuit lors d'une EMFI en fonction de la hauteur de la sonde par rapport au circuit. Ces EMFIs sont effectuées sur une puce décapsulée en face avant (front-side), face arrière (rear-side) et sur une puce non ouverte (capsulated)[34].

1.4.2 Les injections EM harmoniques

Les EMFIs réalisées suite à ces premiers articles sont majoritairement des injections EM harmoniques. Cela signifie que le champ EM est produit par une sonde d'injection alimentée par une variation de courant sinusoïdale, dont la fréquence et l'amplitude peuvent être changées.

Ce type d'injection EM a été démontré efficace pour perturber la fréquence d'oscillateurs en anneaux (ou RO : Ring Oscillator) permettant la génération d'un signal d'horloge dans un circuit [47]. Une augmentation de la fréquence des ROs de 46,6% a été constatée. Suite à ces travaux, des injections EM harmoniques [48] ont été utilisées pour perturber un élément clé des circuits cryptographiques: un générateur de nombres aléatoires (TRNG). Celui-ci est basé sur le fonctionnement de ROs, et permet la génération des clés cryptographiques. Il a été démontré [48] que ce type d'injection EM permettait de contrôler la séquence (l'entropie) de nombres aléatoires générée par le TRNG. Un TRNG plus résistant face à ces injections EM a d'ailleurs été développé [49].

Plus récemment, [50] a introduit un modèle de fautes par EMFI harmonique sur le cache d'instructions d'un microcontrôleur. La grande reproductibilité (96%) des défauts induits, permet d'être utilisée pour déchiffrer des algorithmes cryptographiques.

Enfin, une attaque présentée dans [51], utilise l'émission EM émanant de l'opération de chiffrement d'un AES pour identifier les rondes, et l'EMFI pour fauter celui-ci. L'association des deux méthodes lors d'une expérimentation offre une grande résolution temporelle aux EMFIs.

Enfin, [52] présente comment mettre en place une plateforme d'injection de fautes EM harmonique, mais également une plateforme d'injection d'un champ EM pulsé. C'est cette dernière qui a été utilisée lors de ma thèse.

1.4.3 Les injections par impulsion EM

Une plateforme EM pulsée produit une variation courte et intense du champ EM en injectant une forte impulsion de tension/courant dans une sonde d'injection. C'est ce type de plateforme qui a été utilisé lors des premières EMFIs [34][45]. La variation du champ EM produite par ce type de plateforme a pour effet de créer une variation soudaine de la tension dans les réseaux d'alimentation des circuits tout comme le font des attaques par glitch de tension sur les plots d'alimentation. Toutefois, ces variations sont appliquées localement à la surface du circuit et n'ont pas nécessairement les mêmes caractéristiques que celles produites par un glitch de tension appliquée sur un plot.

Les auteurs de [53] suggèrent d'ailleurs l'existence d'une corrélation entre les cartographies des fautes induites par les EMFIs et les cartographies des chutes de tension (IR drop) induites par les injections EM. L'impact des caractéristiques de la sonde utilisée pour conduire ces injections EM sur ces chutes de tension a d'ailleurs été analysé dans [54]. Cette étude a montré que les caractéristiques de la sonde (taille de la boucle, forme du noyau de ferrite) ont une grande influence sur cette tension induite. En outre, dans cet article, différents types de dysfonctionnement (redémarrage, crash complet, écran noir) d'un OS android embarqué dans un processeur ARM soumis à des EMFI sont reportés.

D'autres types de circuits intégrés ou éléments fonctionnels de circuits intégrés ont été soumis à des EMFI, tels qu'un microcontrôleur 32bits (ARM) [55] ou un DC-TRNG [56]. Dans [57], cette technique d'attaque est utilisée sur un microcontrôleur largement utilisé dans les objets connectés, sans système de sécurité. L'EMFI permet d'y modifier la valeur et l'adresse d'une mémoire.

Enfin, A. Dehbaoui démontre dans [58] et [59] que des fautes peuvent être injectées dans le calcul d'un algorithme AES par des impulsions EM. Dans ces articles il émet d'ailleurs l'hypothèse selon laquelle ces fautes sont des fautes de timing.

1.5 Les différents modèles de fautes de l'injection de fautes électromagnétique

Identifier la nature des fautes induites dans les circuits intégrés par un système d'injection donné est d'une importance capitale tant pour l'attaquant que pour le défenseur afin, pour l'un de les exploiter au mieux, et pour l'autre d'en limiter les effets. On parle d'identifier le modèle de faute.

L'état de l'art relatif aux EMFIs suggère que les fautes logiques induites sont de type bistet, bireset ou bitflip. Les modèles présentés permettent de déterminer comment ces fautes sont induites dans le circuit [60].

1.5.1 Fautes de timing

Les perturbations émises par les EMFIs induisent des variations de tension dans les circuits. Celles-ci altèrent donc les temps de propagation des signaux au travers des portes logiques. Lors de l'étape d'échantillonnage d'une bascule, si les contraintes temporelles, ne sont pas respectées, il y a apparition de fautes temporelles ou fautes de timing. Le fonctionnement d'une bascule D et le phénomène sous-jacent à l'apparition de ce type de fautes sont détaillés section 3.1.3.

L'hypothèse selon laquelle l'EMFI induit des fautes de timing est évoquée dès 2005 par F. Vargas dans [46]. Elle fut reprise dans [58] et [59], supposant que les perturbations induites dans le calcul de l'AES sont des fautes de timing. Lors des expérimentations réalisées par les auteurs de cet article, les fautes ont été injectées dans les différentes rondes de l'AES et ont permis d'obtenir des fautes mono-bit, multi-bits ou encore d'induire des sauts d'instruction. De plus, il a été observé que la nature et les caractéristiques des défauts injectés changent avec la sonde d'injection EM ce qui démontre, l'effet local de l'EMFI. Dans [61], des fautes sur un bit de l'AES sont désignées comme constantes, c'est-à-dire indépendantes du message (ciphertext) de base. Ce type de fautes, reproductible à 100%, permet de réduire le nombre de fautes requis à 5 (au lieu de plusieurs dizaines voire centaines) pour exécuter une attaque DFA et déchiffrer l'algorithme de chiffrement.

1.5.2 Fautes d'échantillonnage

En 2014, S. Ordas fait la constatation dans [62], que l'impulsion de tension appliquée à la sonde d'injection dans le but d'obtenir une faute, doit être plus forte sur un AES opérant à 50MHz, qu'à 100MHz. . S'interrogeant sur le lien entre les caractéristiques des EMFIs devant être appliquées pour obtenir des fautes et la fréquence d'horloge de la cible,

il effectue des tirs sur un circuit dont l'horloge est arrêtée. Il constate alors l'apparition de bitsets et bitresets. Ces résultats démontrent que les fautes de timing ne sont pas les seules fautes que peuvent induire les EMFIs. En effet, si l'horloge est arrêtée, le circuit ne fonctionne pas et ne doit donc satisfaire aucune contrainte temporelle.

Suite à ces travaux, dans [63][64], ce même auteur propose un nouveau modèle de faute appelé modèle de faute d'échantillonnage (ou sampling fault model). Celui-ci est décrit dans la Figure 1.10.

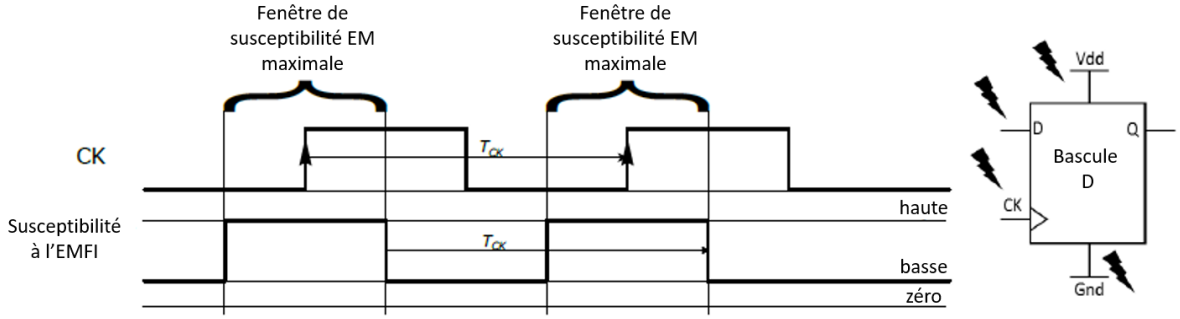


Figure 1.10 –Modèle de faute d'échantillonnage [64].

Ce modèle montre que la susceptibilité aux EMFIs dans le circuit est maximale autour des fronts montants d'horloge. Ces « fenêtres de susceptibilité », pendant lesquelles l'injection EM est capable de produire des défauts, sont périodiques avec une période égale à celle de l'horloge, et une largeur indépendante de la fréquence d'horloge. Le modèle de faute d'échantillonnage repose également sur l'hypothèse que l'injection EM est capable de modifier suffisamment l'amplitude d'un ou plusieurs signaux d'entrée d'une bascule D (D, CLK, Set, Reset), ainsi que son alimentation et sa masse, de sorte que l'échantillonnage de la bascule soit perturbé, entraînant une valeur erronée en sortie.

De récents articles appuient ce modèle de fautes. En effet, dans [65], [66], les variations des temps de propagation Δt_p induites par des EMFIs sur une cascade de portes logiques (5000 buffers) ont été mesurées. De premières mesures ont constaté que suivant la position de la sonde d'injection au-dessus du circuit, Δt_p pouvait être soit positif soit négatif, correspondant à un ralentissement ou une accélération du temps de propagation du signal dans le chemin logique. Il a également été constaté que l'injection d'une seule impulsion ne révèle pas de variation majeure de Δt_p. Par conséquent, une salve (burst) de pulses EM (séparés par un intervalle de temps de 3ns) a été appliquée au FPGA. La Figure 1.11 donne les variations du temps de propagation en fonction du nombre d'impulsions, pour un ralentissement (a) et une accélération (b) des portes logiques. Ces évolutions, linéaires, montrent qu'il faut au moins 600 impulsions EM successives pour ralentir la propagation du signal de 9ns, ou l'accélérer de -23ns. Ceci correspond respectivement à

18ps et -46ps par buffer ou encore 15ps et 38ps par impulsion. Ces résultats suggèrent qu'il est peu probable d'induire des fautes de timing lors de l'injection d'un unique pulse EM. Ceci est d'autant plus vrai si le circuit travaille avec une fréquence d'horloge faible.

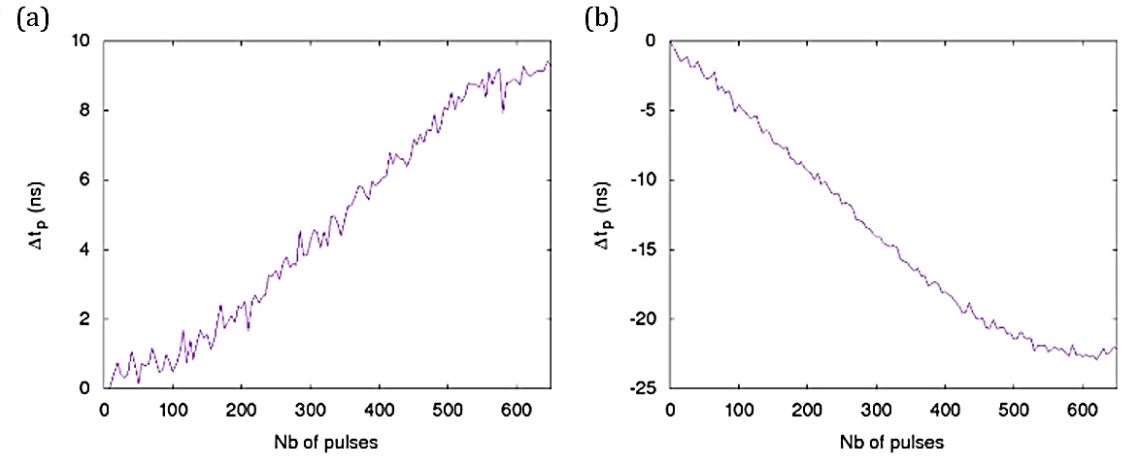


Figure 1.11 – Variation des temps de propagation Δt_p en fonction du nombre de pulse à deux positions de sondes d'injection différentes [65].

Enfin, dans [67] les auteurs ont retrouvé, lors de leurs expérimentations conduites sur un microcontrôleur, des fenêtres de fautes, montrant que les fenêtres correspondant à des bitsets ou des bitresets sont décalées dans le temps.

1.5.3 Autres modèles de fautes

D'autres types de fautes ont été observés lors d'EMFIs. Par exemple, [68] reporte que l'EMFI fait apparaître des fronts parasites sur le signal, ces fronts étant visualisés à l'oscilloscope. De même, [69] démontre l'importance de prendre en compte le temps de montée des fronts d'horloge, car des fronts parasites peuvent apparaître lorsque ceux-ci sont trop longs.

Des EMFIs en face arrière ont été réalisées dans [70]. L'auteur établit un nouveau modèle de faute basé sur la charge d'un nœud du circuit. L'hypothèse se base sur la charge et la décharge des capacités liées à un nœud du circuit. À basse fréquence, une charge maximale est accumulée sur le nœud et l'impulsion EM ne peut pas modifier cette charge. À haute fréquence, les capacités sont chargées tout aussi rapidement mais pour une durée d'horloge plus courte, ce qui fait que la charge accumulée sur le nœud est moindre. La capacité n'étant pas complètement chargée, une EMFI appliquée à ce nœud est capable de perturber une quantité suffisante de charge pour modifier la valeur du bit (par exemple, au moment de l'échantillonnage d'une bascule de '0' vers '1', le seuil de '1' n'est pas atteint et le bit devient donc un '0').

1.5.4 Modélisation de l'EMFI

De nombreuses modélisations du champ électromagnétique existent. Elles permettent de mieux appréhender les effets de ce champ sur un élément (fil, rails métalliques, circuit…). Dans un premier temps, [71]–[73] fournissent des analyses du couplage entre différentes sondes d'injection et des lignes de métaux. Des modélisations électriques de sondes d'injection sont données ou encore des modèles de la distribution du champ magnétique comme représentés sur la Figure 1.12. Ces derniers montrent qu'avec une sonde proche du circuit (a), la valeur du champ magnétique est plutôt constante au centre de la sonde et très variable sur les bords, tandis que lorsque celle-ci est éloignée du circuit, la distribution du champ magnétique suit une loi normale.

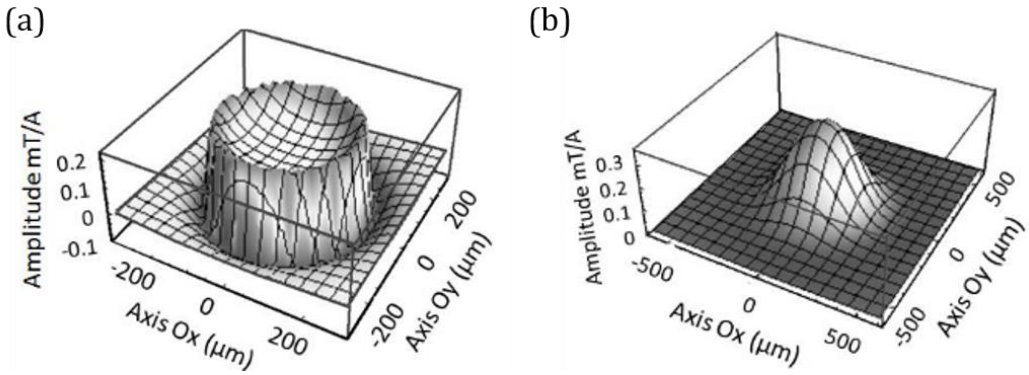


Figure 1.12 – Modèle de la distribution du champ magnétique pour une sonde d'injection (a) proche du circuit (ou en contact), (b) éloignée du circuit [71].

D'autres modélisations ont été proposées dans [74]–[76], dans le domaine de la CEM (Compatibilité Électromagnétique) pour évaluer la susceptibilité des circuits au champ électromagnétique. Ces articles présentent des modélisations et des mesures expérimentales, d'un champ EM avec des lignes de métaux de circuit intégré, analysant les tensions induites et l'effet de différentes caractéristiques de la sonde d'injection mais également de la cible (caractéristiques des fils, résistance du substrat…).

Un modèle général de couplage avec un circuit multicouche est proposé dans [77], et permet de déterminer la puissance couplée par l'EM couche par couche. Ce modèle met en évidence l'effet des différentes couches de métaux et d'isolants sur la propagation, en profondeur, de l'onde EM dans le circuit.

1.6 Contre-mesures face aux attaques par injection de fautes et EMFI

Les concepteurs de circuits intégrés doivent assurer la robustesse des puces face à différentes attaques par faute(s). Pour cela, plusieurs approches peuvent être considérées telles que la conception de protections physiques (boucliers par exemple), la conception de briques durcies, l'intégration de capteurs internes permettant la détection directe d'attaque ou l'induction d'une faute, tant au niveau matériel que logiciel. Dans cette section, nous nous intéresserons aux dispositifs matériels de défense contre les attaques par injection de fautes.

1.6.1 Conception du circuit

L'ajout d'un bouclier sur un circuit permet de limiter l'efficacité (ou détecter) les attaques par injection de fautes mais également des attaques par modifications du circuit, par micro-sondages et des attaques invasives en général. Il existe des boucliers passifs [78] constitués d'un maillage de pistes métalliques implantés dans les plus haut niveaux de métaux du circuit, où le courant et les capacités (constantes) sont surveillés par des composants analogiques. Des boucliers actifs sont également réalisable [79], dans lesquels les signaux traversant le bouclier ne sont plus constants afin de compliquer un éventuel contournement du bouclier par l'attaquant.

La protection contre les attaques par injection de fautes peut se faire dès la conception du circuit, en rendant plus robustes certains éléments du circuit. Ainsi, dans [80] il est proposé des méthodes dans le but de renforcer des cellules mémoires SRAM.

La redondance matérielle est un moyen de protection bien connu capable d'empêcher une faute. Elle utilise plusieurs circuits identiques et un bloc permettant un vote majoritaire définissant le résultat correct.

Ces moyens de défense restent coûteux en argent ou en surface rendant difficile leur intégration dans un circuit. Certains d'entre eux ont même une consommation de courant relativement élevée.

1.6.2 Capteur de variation physique

Les capteurs physiques implémentés sur un circuit permettent la détection de perturbations physiques engendrées par l'attaque, tels que des variations d'alimentation [81], de l'horloge, de la température, de l'éclairement ou d'un champ EM. Une alarme est

connectée à ces détecteurs. Un seuil de détection doit être mis en place pour permettre au capteur de détecter l'attaque, avant que celle-ci n'induise une faute. Ce seuil ne doit pas être trop bas pour ne pas créer de fausses erreurs (alarme intempestive), mais également en dessous du seuil pour lequel une faute est créée. La plupart du temps, ces détecteurs sont positionnés en réseau sur la surface d'un circuit pour couvrir une zone du circuit à sécuriser.

Pour les attaques par injection laser, des phototransistors [82] ou des photodiodes [83] peuvent être utilisés pour détecter ces attaques.

Pour les attaques par EMFI, l'utilisation d'une antenne permet de détecter un couplage. Dans [84], une bobine est intégrée dans le circuit pour détecter la présence d'une sonde EM au voisinage du circuit. Pour ce faire, la valeur de l'inductance mutuelle de la bobine est calculée en permanence, afin de détecter la présence éventuelle d'une sonde EM au-dessus de celle-ci ; présence qui altère la valeur de l'inductance mutuelle. Toutefois, ce capteur ne détecte pas les courants induits, donc une sonde EM placée suffisamment loin et parcourue par un fort courant peut induire une faute sans déclencher d'alarme. De plus, le placement du circuit dans un environnement électromagnétique naturellement agressif peut engendrer de fausses erreurs, cette solution paraît difficile à mettre en œuvre. Un brevet [85] utilise également une antenne (déjà présente dans le circuit) pour capter une injection de champ EM. La détection se fait lorsqu'une variation de courant est induite par le champ EM, déclenchant une alarme.

Les fautes de timing peuvent être détectées en utilisant des jauges de délai. Par exemple, L. Zussa présente dans [86] un détecteur de violation de contraintes de temps, et montre son efficacité partielle à détecter les EMFIs. Il se base sur la mise en place d'un « délai de garde ». Ce délai représente la période de l'horloge moins les temps de propagation du signal logique entre deux fronts d'horloge (pour voir les différents temps de propagation se référer aux explications partie 3.1.3).

Le principe du détecteur est représenté Figure 1.13. Un même signal d'horloge CK alimente les entrées D et CLK d'une bascule D. Un bloc (delay) est implémenté sur l'entrée de la CLK pour induire le « délai de garde ». En fonctionnement normal, la sortie Q qui constitue l'alarme, reste toujours à l'état '0'.

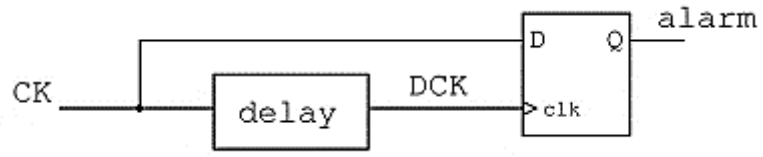


Figure 1.13 – Schéma du principe de fonctionnement du détecteur de faute de timing [86].

Lors d'une injection de fautes par champ EM, le temps de propagation du bloc delay change et un retard est induit sur DCK. Ce décalage entre les signaux provoque une faute de timing sur la bascule D et ainsi déclenche l'alarme. Cependant ce détecteur présente un taux de détection faible en fonction des caractéristiques de la sonde d'injection. Il est également très sensible aux variations de process PVT.

Un détecteur utilisant un principe équivalent est présenté dans [87]. Cependant, celui-ci permet de détecter un ralentissement des temps de propagation mais également les accélérations de ceux-ci.

Toujours basé sur le principe de détection de faute de timing par perturbation des temps de propagation, une contre-mesure a été présentée dans [88], [89]. Elle utilise une PLL (boucle à phase asservie) et un oscillateur en anneaux (RO). Le RO, qui génère un signal oscillant est connecté à l'entrée de la PLL. En fonctionnement normal, le signal en sortie du RO est stable, la PLL se synchronise avec ce signal. S'il est en phase il n'y a pas d'alarme. Lors d'une EMFI, la fréquence du signal en sortie du RO change, ce qui est détecté par la PLL qui déclenche l'alarme. Cependant, la consommation de ce détecteur est significative dûe à l'utilisation d'une PLL.

Enfin, [90] utilise un détecteur toujours basé sur des perturbations de fréquence de RO, mais avec une comparaison effectuée par un détecteur de phase Hogge [91]. Cette contre-mesure présente un fort taux de détection mais également un taux élevé de fausses alarmes, ce qui limite son exploitation dans de vrais produits.

1.6.3 Détecteur numérique

Pour s'affranchir des inconvénients relatifs aux contre-mesures précédentes, des détecteurs numériques ont été proposés. Le fait qu'ils soient entièrement digitaux permet une intégration facile dans n'importe quel circuit numérique, et leur consommation est relativement faible.

Le premier capteur, entièrement digital permettant de détecter des EMFIs a été donné par D. El-Baze dans [92], [93]. Cette contre-mesure est expliquée en détail dans la section 4.4 et son schéma de fonctionnement donné Figure 4.9 de cette même partie. Ce

détecteur se base sur le modèle de faute d'échantillonnage. Ainsi, 4 bascules D servent de capteur de faute d'échantillonnage. Ces 4 bascules sont configurées de façon à couvrir toutes les configurations possibles (synchronisées sur fronts montants et descendants de l'horloge, transition de '0' vers '1' et inversement). Les sorties des bascules sont ensuite comparées les unes aux autres dans un bloc comparateur (éloigné des 4 bascules), ainsi si l'une (ou plusieurs) est fautée(s), une alarme sera déclenchée. Mais ce détecteur doit être implémenté de sorte à couvrir une grande surface du circuit pour avoir un bon taux de détection.

Sur le même principe, [94] propose un détecteur de faute d'échantillonnage entre utilisant deux bascules D. L'une des bascules dite « fantôme » n'est pas affectée par l'EMFI tandis que l'autre représente la « cible ». Une simple comparaison des sorties est ensuite effectuée pour déterminer si une faute a été induite.

1.7 Contexte et objectifs de la thèse

De nos jours, la sécurité des circuits intégrés est devenue un enjeu primordial pour les industries. Les attaques par injection de fautes font partie des techniques qu'un attaquant peut utiliser pour corrompre un circuit et récupérer des informations confidentielles contenues dans celui-ci. Parmi les attaques envisageables, on retrouve l'attaque par injection de faute électromagnétique.

Des études montrent que l'EMFI induit des fautes dans un circuit, pouvant même déchiffrer une clé cryptographique. Cependant, les effets du champ EM à l'intérieur du circuit sont encore peu compris. Pourtant, la connaissance totale des effets d'une attaque sur un circuit est capitale pour les concepteurs, afin de pouvoir déterminer des contre-mesures. C'est pourquoi, à ce jour, peu de moyens de défenses sont intégrés dans les circuits du commerce pour contrer cette technique d'attaque.

Cette difficulté de compréhension peut se justifier par l'effet du champ EM en lui-même, qui rayonne très largement. En comparaison, un laser va permettre de cibler très précisément une partie du circuit, permettant de savoir exactement ce qui se produit expérimentalement. L'attaque EM implique de très nombreux éléments, chacun couplant plus ou moins avec le champ EM et réagissant différemment, complexifiant largement sa compréhension.

De même, le modèle de faute associé à l'EMFI est encore incertain. Il a été montré que le champ EM induit une variation de tension dans le circuit menant à des fautes de contraintes temporelles. Mais, à ce jour, peu de mesures permettent de connaître précisé-

ment l'amplitude de ces variations de tension induites au cœur du circuit. De plus, de nouvelles analyses ont montré que les variations des temps de propagation induites par l'EMFI étaient très faibles. Ainsi, pour un circuit cadencé avec une horloge basse fréquence, donc des grandes marges de temps, il paraît compliqué d'induire des fautes avec une impulsion EM. Le modèle de faute d'échantillonnage constate des fautes induites autour des fronts montant d'horloge, et ce quelle que soit la fréquence d'horloge et les marges de temps. Ce modèle pourrait expliquer les fautes induites à basse fréquence, mais le phénomène amenant à l'induction de cette faute est encore peu renseigné.

Dans ce contexte, il est donc vital de bien comprendre les phénomènes physiques mis en jeu lorsqu'une puce de silicium est soumise à un champ électromagnétique. Cette compréhension fine des effets physiques peut alors permettre une modélisation et la simulation de l'attaque par injection de fautes électromagnétique. Ces simulations pourront ensuite servir à tester la robustesse d'un circuit face à cette attaque, mais également de concevoir des contre-mesures afin d'accroître la sécurité des circuits.

Le premier objectif de ma thèse a donc été de comprendre les interactions physiques entre un champ EM et un circuit intégré, dans un premier temps, en déterminant les différents éléments, analogique ou digitaux, du circuit pouvant être vecteur d'une injection de faute lorsqu'il est soumis à un champ EM et dans un second temps, en analysant les effets physiques du couplage entre le champ EM et les éléments identifiés dans le circuit.

Le second objectif est de pouvoir modéliser et simuler les effets de l'EMFI. Les analyses serviront ainsi à mettre en place une modélisation électrique complète du phénomène amenant à l'induction d'une faute dans un circuit soumis à une impulsion électromagnétique.

Enfin, les analyses et la modélisation permettront l'élaboration de dispositifs permettant de détecter les attaques par injection de fautes EM ou d'améliorer la robustesse d'un circuit face à celles-ci.

Ces objectifs peuvent être résumés en trois questions auxquelles nous tâcherons d'apporter une réponse au cours de cette thèse :

- Quels sont les effets d'une attaque par injection de faute électromagnétique sur un circuit ?
- Comment définir une modélisation de l'effet d'une EMFI sur un circuit ?
- Comment protéger un circuit intégré face à une EMFI ?

Chapitre 2 . Modélisation de l'impact de l'EMFI sur l'alimentation d'un circuit intégré

Il existe plusieurs modèles justifiant l'apparition de faute(s) lorsqu'une impulsion EM est produite dans le voisinage d'un CI. Toutefois, ces modèles sont largement basés sur l'intuition et manquent de fondements. Dans ce contexte, ce chapitre, et plus largement cette thèse, a pour objectif de modéliser et définir une méthodologie de simulation des EMFIs. Une telle méthodologie facilitera la compréhension des effets du champ EM sur un circuit et devrait permettre de définir des règles de conception permettant de faire face à la menace que constituent les EMFIs et de développer des contremesures efficaces au juste coût.

Ce chapitre décrit une partie de la modélisation et de la méthodologie de simulation : la modélisation et la simulation de l'impact d'une impulsion EM sur les réseaux d'alimentation des CIs. Les travaux détaillés dans ce chapitre ont fait l'objet de la soumission d'un article en vue d'une publication dans la revue IEEE Transaction on Computer Aided Design.

2.1 Structure d'un circuit intégré

De manière générale, les techniques d'injection de faute(s) s'appuient sur des phénomènes physiques pouvant être mis en œuvre dans les CIs à l'aide de dispositifs extérieurs à ces derniers. Par exemple, les injections laser exploitent l'apparition de photocourants dans les jonctions PN polarisées en inverse. Contrairement aux injections laser, la compréhension des phénomènes conduisant à l'apparition de faute(s) au sein des CIs soumis à des EMFIs est plus obscure. Toutefois, la physique nous indique que ces effets sont probablement liés à l'induction électromagnétique. Ce phénomène génère des forces électromotrices (fem) et des courants qui, si induits au sein de CIs, pourraient expliquer l'apparition de faute(s), comme expliqué dans la section 1.3.2.

Afin de pouvoir appréhender comment le phénomène de l'induction EM pourrait perturber le fonctionnement des circuits, il est nécessaire d'avoir de bonnes connaissances de la structure des CIs et de leur topologie. Les prochains paragraphes décrivent quelques caractéristiques clés de la structure des CIs.

2.1.1 Les différents niveaux de métallisation

Les circuits intégrés modernes peuvent être perçus, dans leur grande majorité, comme un dépôt d'un très grand nombre de transistors MOS, interconnectés entre eux, sur un substrat silicium. On parle en général de technologie CMOS. Comme le montre la Figure 2.1, cette technologie permet de déposer des couches très fines de matériaux semi-conducteurs, conducteurs et isolants sur un substrat semi-conducteur.

Le terme FEOL (Front-End-of-Line) désigne les premières étapes de fabrication des CIs permettant le dépôt des transistors MOS sur le substrat silicium. Par abus de langage, il désigne également la partie active des CIs. Celle-ci inclut les puits N et P pour la fabrication des transistors, l'oxyde mince et le polysilicium permettant de réaliser les capacités MOS des transistors ou des capacités de découplage.

Par complément, le terme BEOL désigne le reste des étapes de fabrication des CIs. Celles-ci consistent en des dépôts successifs de matériaux conducteurs et isolants permettant d'interconnecter les transistors entre eux mais également de les alimenter. Les isolants séparent les interconnexions et les vias qui sont généralement en aluminium (Al), cuivre (Cu) ou encore tungstène (W). Le nombre de couches métalliques ne cesse d'augmenter, et peuvent atteindre jusqu'à 15 couches avec l'évolution de la technologie CMOS.

Les couches les plus basses sont essentiellement dédiées au routage des signaux logiques entre les portes logiques et au signal d'horloge. D'autres couches, généralement

les plus hautes (Métal 4, Métal 5 ou plus) et la plus basse (Métal1), sont essentiellement utilisées pour alimenter les transistors.

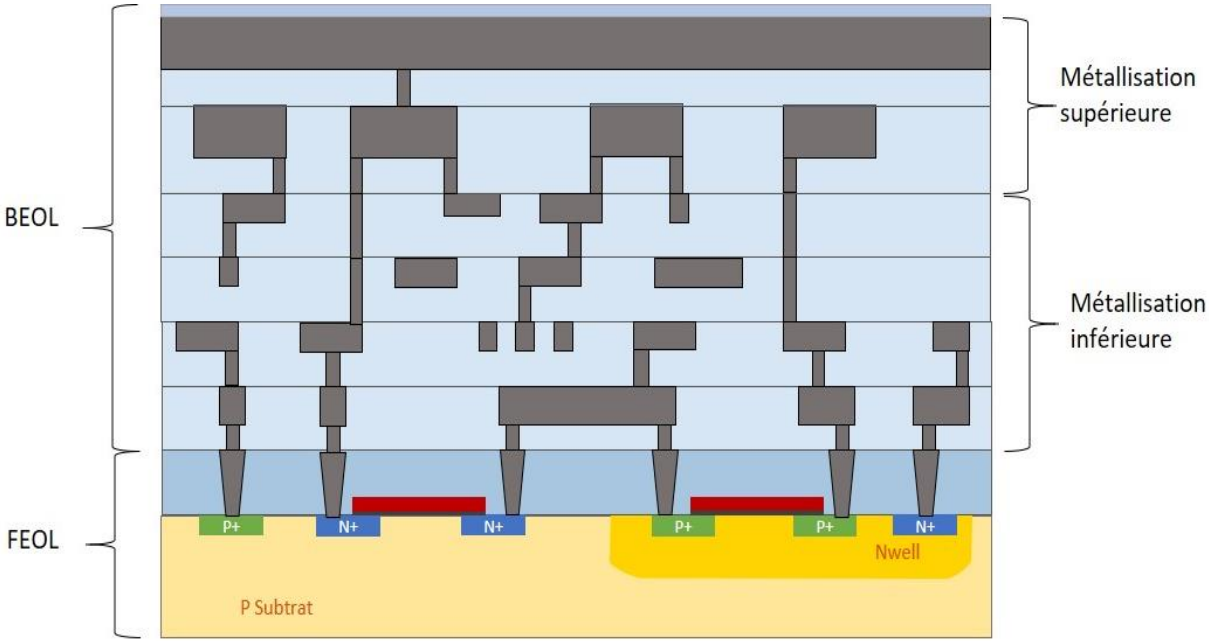


Figure 2.1 – Vue en coupe de la structure interne d'un circuit intégré.

L'observation des lignes d'interconnexions (Figure 2.2) montre que les rails connectant les portes logiques entre elles sont rectilignes et que leur placement peut sembler « désordonnés ». Au contraire, l'observation des lignes dédiées à l'alimentation (Figure 2.3) des transistors met en évidence une organisation très rigoureuse. En effet, les portes logiques standards sont alimentées par des pistes en Métal1 (de largeur ~0,15µm en technologie 40nm) parallèles uniformément séparées les unes des autres. Toutes ces pistes sont elles-mêmes connectées aux rails en métal supérieur également parallèles entre eux et uniformément espacés. Ces pistes ont une largeur nettement plus importante (~1µm en technologie 40nm).

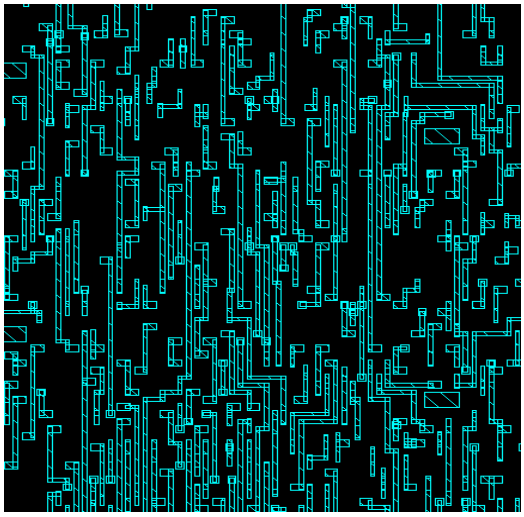


Figure 2.2 – Morceau de layout montrant les interconnexions, d'un niveau de Métal bas, entre les cellules.

2.1.2 Layout d'un circuit

Le layout d'un circuit constitue son plan de fabrication. Il est obtenu après le placement et le routage de ses différents éléments constitutifs. Les portes logiques sont dites standards car elles sont conçues selon certaines règles qui stipulent qu'elles ont toutes la même hauteur ou encore que leur longueur soit un multiple. Ces règles facilitent les étapes de placement routage et permettent de réduire les temps de mise sur le marché. C'est ce qui explique la régularité du réseau d'alimentation mais également de la Figure 2.3 montrant un morceau de layout. On y distingue, comme évoqué précédemment, la distribution de l'alimentation et les rangées de cellules logiques délimitées par les pistes de Métal1 (en bleu). Ces dernières alimentent les portes logiques et donnent un aspect matriciel à la figure.

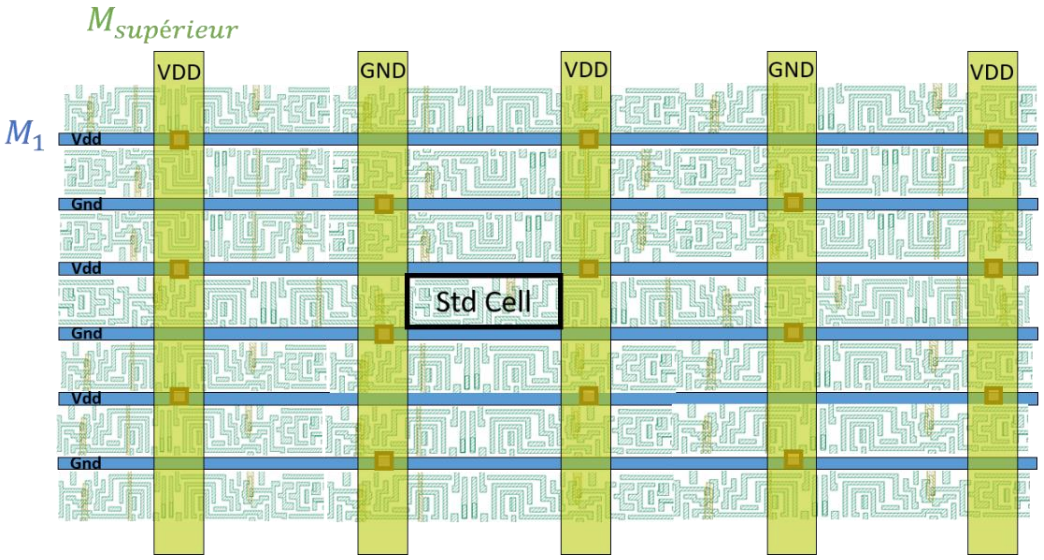


Figure 2.3 – Morceau de layout d'un circuit montrant l'aspect matriciel du placement des cellules logiques et la régularité du réseau d'alimentation.

Une porte logique standard réalise une fonction logique simple. Elle est constituée d'un réseau de transistors N lithographiés dans des puits P (Pwells) et d'un réseau de transistors P implantés dans des puits N (Nwells). Comme illustré sur la Figure 2.4, ces puits forment des bandes parallèles de substrat, dopées N ou P selon le cas, qui s'entrelacent parallèlement aux pistes de Métal1 fournissant de manière alternée l'alimentation Vdd ou la masse Gnd. Les substrats des transistors N et P devant être polarisés respectivement à Vdd ou Gnd, ces puits sont connectés aux pistes de Métal1 par des prises substrat communément appelées 'Tap'.

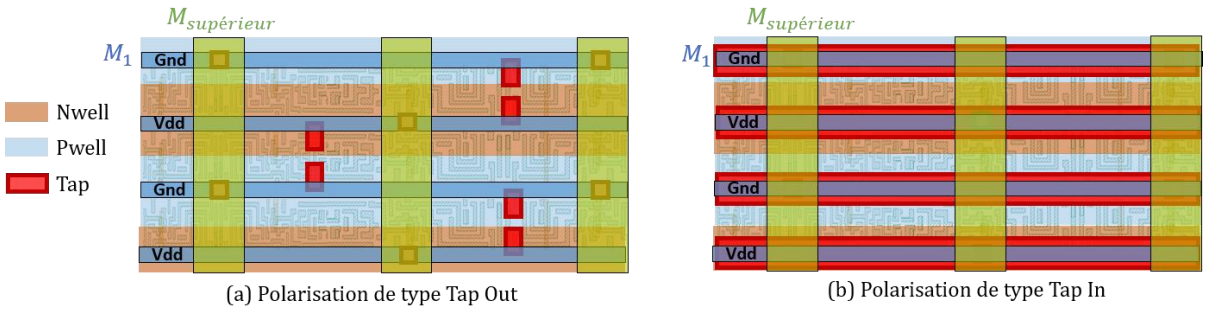


Figure 2.4 - Disposition des puits Nwells et Pwells ainsi que des prises de polarisation selon l'approche standard cell choisie : (a) Tap Out et (b) Tap In.

Il existe deux manières de polariser les puits N et P. La méthode classique est appelée 'Tap In'. Elle est illustrée sur la Figure 2.4.b et consiste à prévoir dans le layout de chaque cellule des prises de polarisation N et P pour polariser les substrats.

La seconde méthode, appelée 'Tap Out' consiste à insérer des cellules de polarisation de manière régulière, à l'extérieur des cellules logiques, afin de minimiser les phénomènes de latch-up [95] lors du placement de cellules. Ces cellules de polarisation contiennent des prises de polarisation. Cette méthode de conception permet de réduire la surface de silicium nécessaire à la fabrication d'un circuit.

L'approche 'Tap Out' est largement utilisée dans la division dans laquelle j'ai effectué ma thèse. Ainsi tous les circuits avec lesquels j'ai travaillé sont de type 'Tap Out'.

Les paragraphes ci-avant rappelaient certaines notions quant à la structure des circuits intégrés. Ce rappel était nécessaire car ces observations ont été largement exploitées lors de nos travaux de modélisation.

2.2 Problématiques expérimentales de l'EMFI

La pratique de l'injection EM requiert de prendre en compte de nombreux éléments. En effet, les impulsions EM nécessaires pour induire des fautes au sein des CIs ont une grande amplitude et sont mesurables à une dizaine de mètres avec une simple bobine, et ce sans système d'amplification. Ces impulsions polluent donc toutes les mesures analogiques, synchrones avec l'impulsion, que l'on pourrait effectuer au voisinage du circuit sous test. Seules les mesures de grandeurs logiques sont donc possibles pour analyser les effets des EMFI. L'objectif de cette section est, à la base, de caractériser expérimentalement le couplage entre le champ EM et différentes architectures de grilles d'alimentations. Cependant, nous allons voir que de telles mesures sont relativement complexes.

2.2.1.a Plateforme d'injection de pulses électromagnétiques

Plusieurs plateformes EMFI ont été introduites dans la littérature [34], [52], [59], [64], [67]. Le prix de ces plateformes, qui requiert la fabrication ou l'achat de peu d'équipements [34], reste modéré et varie entre quelques centaines d'euros à quelques milliers d'euros. Toutefois, ces plateformes ont des caractéristiques très variables.

La plateforme EMFI que j'ai mise en place à STMicroelectronics et avec laquelle j'ai effectué mes travaux est visible sur la Figure 2.5. Celle-ci dispose d'une cage de Faraday permettant d'isoler le dispositif sous test de l'environnement extérieur. Elle protège également les appareils de mesures présents dans le laboratoire, du rayonnement EM généré lors de nos mesures. Toutefois, aucune protection n'est mise en place pour limiter le bruit conduit. Un ordinateur permet de contrôler les différents éléments de la plateforme.

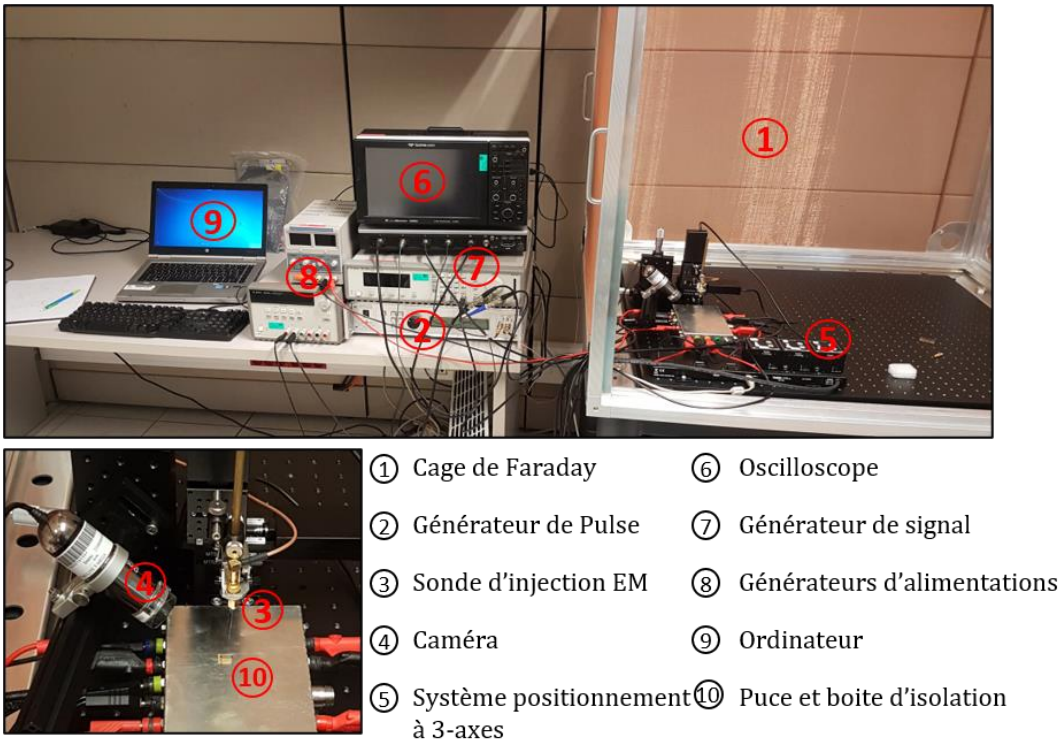


Figure 2.5 - Plateforme EMFI développée et utilisée lors de mes travaux de thèse.

La chaîne de puissance de la plateforme EMFI est constituée d'une des sondes d'injection fabriquées par le LIRMM. Celles-ci sont visibles sur la Figure 2.6. Ces sondes sont constituées d'un noyau de ferrite autour duquel est enroulé un fil de cuivre (de diamètre 100µm) de sorte à former une bobine de 3 à 7 spires selon les modèles. La ferrite qui permet de guider les lignes de champs magnétiques (et de les concentrer quand elle est appointée) a un diamètre qui varie de 300µm à 2mm selon le modèle de sonde. De plus amples informations sont disponibles dans [72] quant à l'influence des divers paramètres géométriques et structurels des sondes sur les caractéristiques du champ rayonné.

Afin de générer une impulsion EM brève mais puissante, une impulsion de tension est appliquée à l'entrée des sondes. Celle-ci est fournie par un générateur développé par la société américaine Avtech. Ce modèle est capable de fournir des impulsions d'amplitude comprise entre ±50 et ±400V. La largeur des impulsions délivrées par ce générateur peut être ajustée, par pas de 10ps, entre 6ns et 100ns. Les temps de montée et descente de l'impulsion sont constants et égaux à 160V/ns et 80V/ns respectivement pour le premier et second front de l'impulsion respectivement. Cela correspond à des durées de front, mesurées entre 10% et 90%, égales à 2ns et 4ns pour une amplitude de 400V.

La sonde d'injection peut être déplacée au-dessus du circuit grâce à une table XYZ, dont la précision des déplacements est de 1µm. Ces déplacements au-dessus de la surface des puces peuvent être observés et contrôlés à l'aide d'une caméra.

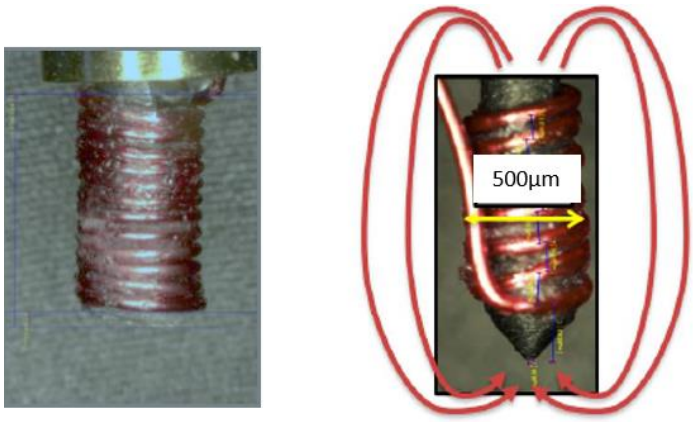


Figure 2.6 - Sondes d'EMFI à extrémité plate (à gauche) et conique (à droite).

Pour faire fonctionner nos puces de tests, deux alimentations externes délivrant 1,2V et 3,3V ont été nécessaires ainsi qu'un générateur de signal fournissant le signal d'horloge au circuit. Afin d'optimiser les expérimentations, les supports de puces de test ont été soudées sur un PCB, lui-même intégré dans une boite en aluminium reliée à la terre. Celle-ci est dotée d'une lucarne afin d'approcher les sondes au voisinage de la surface des circuits. Ce dispositif a été conçu afin de protéger les éléments du PCB du rayonnement de la sonde (notamment le signal d'horloge et les alimentations) et limiter le bruit conduit depuis le PCB dans le circuit.

2.2.1.b Développement de circuits de tests

Deux jeux de puces de test ont été réalisés afin d'analyser l'impact d'une impulsion EM sur des pistes métalliques ou sur le fonctionnement des CIs. Pour limiter les coûts et les temps de développement, ces deux premières puces sont des Test Element Groups (TEG). Les TEG sont des structures de test de 2mm x 100µm lithographiés en bordure de vrais circuits, et plus précisément sur les lignes de découpe de circuit multi-projets. Ces circuits multi-projets embarquent des éléments de test, de diverses divisions, en cours de conception. J'ai pu réaliser les étapes de sciage, mise en boîtier, et micro-câblage des fils de bonding au sein du Centre Microélectronique de Provence (CMP) Gardanne.

Le premier circuit sur TEG que nous avons réalisé n'embarque pas de fonction logique mais des pistes métalliques dessinées sur différents niveaux et avec diverses géométries. Chaque piste, d'une longueur de 1,5mm, étant connectée à deux plots lui étant propres, le courant la traversant et la tension à ses bornes sont mesurables.

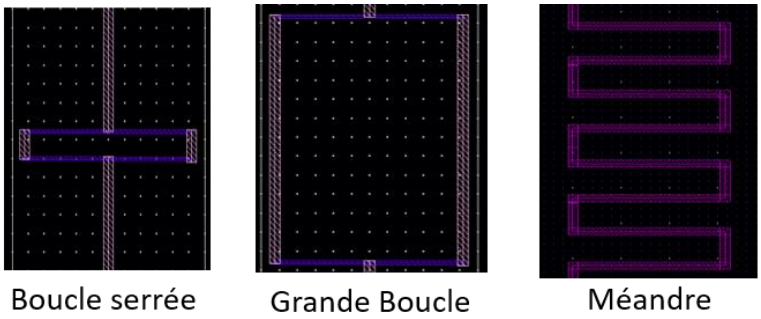


Figure 2.7 - Motifs implantés sur TEG. À gauche : petite boucle de (80µmx12µm). Au centre : grande boucle (80µmx110µm). À droite : méandre.

La géométrie de ces lignes, comme l'illustre la Figure 2.7, varie de la simple piste rectiligne (de largeur égale à 0,07µm ou 1µm) à des boucles (petites ou grandes) en passant par des méandres. Ces motifs sont des motifs que l'on retrouve fréquemment dans de vrais produits et notamment dans le dessin des grilles d'alimentation.

Le deuxième circuit sur TEG embarque différents oscillateurs en anneau (RO) alimentés par une grille alimentation dont la géométrie a été déclinée en trois versions différentes. La conception et la fabrication de cette TEG ont pour objectif d'analyser l'impact d'une EMFI sur la tension d'alimentation des CIs et sur les délais de propagation de ses éléments constitutifs. En effet, d'après l'équation (2.1) [96], la fréquence d'oscillation d'un RO constitué d'inverseurs dépend du délai de propagation t_d d'un inverseur (inversement proportionnel au premier ordre à la tension d'alimentation Vdd [97]) et du nombre d'inverseurs N. Par conséquent, si les EMFIs perturbent la tension d'alimentation d'un CI, cela pourra être observé en monitorant les variations de fréquence des ROs. Ces différents ROs sont sélectionnés via un registre à décalage (Shift Register) composé d'une succession de 30 DFFs.

$$f_{osc} = \frac{1}{2.N.t_d} \qquad (2.1)$$

2.2.2 Problématique des fils de bonding

2.2.2.a Injection EM sur des pistes métalliques

Après le développement de la plateforme, les premières expérimentations que j'ai menées ont été sur le circuit embarquant des pistes métalliques. L'objectif était d'identifier le motif de grille d'alimentation le moins susceptible à l'injection EM.

Dans un premier temps, des tirs EM ont été effectués au-dessus du circuit embarquant de simples lignes de métal. Pour cela, le circuit est alimenté par une tension de 1,2V puis soumis à des impulsions EM. Pour ce faire, la sonde d'injection a été placée dans un premier temps à 100µm au-dessus du centre des lignes. Des impulsions, de largeur PW=20ns et d'amplitude V_{pulse} égale à + 50V, + 70V et +100V ont été appliquées à cette dernière. Lors de ces EMFI, la tension aux bornes de la piste de Métal1 de largeur 1µm a été mesurée. Les évolutions de celle-ci sont reportées sur la Figure 2.8.

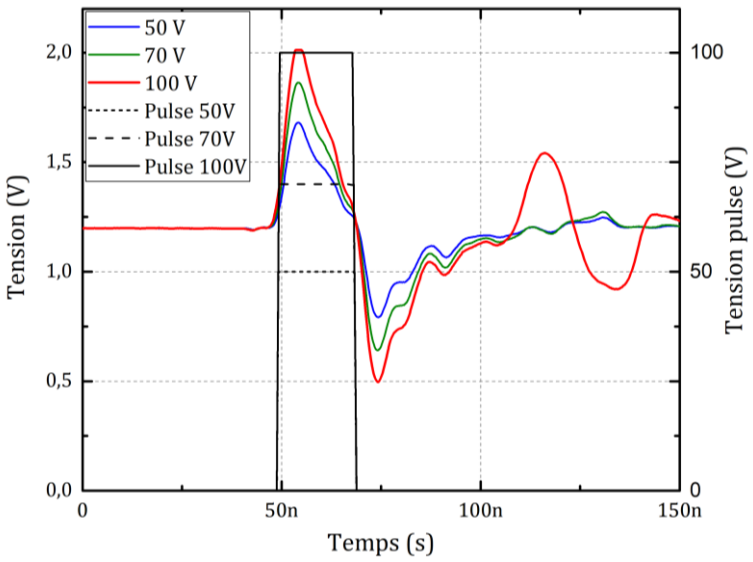


Figure 2.8 - Tension aux bornes d'une piste de Métal1 de 1µm de large soumise à EMFI. La sonde reçoit des impulsions de tension de largeur 20ns et d'amplitude +50V, +70V et + 100V.

La figure montre que les EMFIs semblent provoquer de soudaines variations de la tension aux bornes de la piste. L'amplitude de ces variations est égale à 0,8V, 0,6V et 0,45V respectivement. En outre, les deux extrema de ces variations sont séparés de 20ns, la durée de l'impulsion appliquée à la sonde. Le premier lobe est donc à priori généré par le front montant de l'impulsion et le second par le front descendant. On notera que la réponse en tension de la piste métallique ressemble à une réponse de type RC de l'impulsion en tension appliquée à la sonde EM. Cette expérience a été répétée sur les différentes structures de rails présentées Figure 2.7. Mais aucun écart significatif dans les réponses obtenues, pour les différents motifs, n'a été observée.

Suite à ces premiers tests, des cartographies de l'amplitude ΔV de la perturbation induite dans la piste ont été réalisées afin d'identifier les positions de la sonde conduisant à un meilleur couplage avec la piste. Ces cartographies ont été menées sur une surface de 6mm x 6mm avec un pas de 10µm.

La première cartographie, représentée Figure 2.10 (a), a mis en évidence une distribution uniforme bruitée de ΔV sur l'ensemble de la surface scannée. Ce résultat a été

interprété comme étant dû à un couplage plus important de la sonde avec les équipements de mesure ou les fils de bonding de la TEG.

Afin de soustraire l'effet de ce couplage prépondérant et relativement indépendant de la position de la sonde, deux cartographies successives ont été lancées avec la sonde positionnée à deux hauteurs différentes de la surface du circuit : Z1 et Z1+100µm. Si l'on suppose qu'à une hauteur Z, les couplages sonde-circuit et sonde-fils de bonding peuvent être modélisés par les inductances mutuelles $M_{circuit}$ et $M_{bonding}$, il vient que la différence entre les deux cartographies est essentiellement due à la variation de $M_{circuit}$ avec Z. En effet, ΔZ =100µm est petit devant la distance séparant la sonde des fils de bonding.

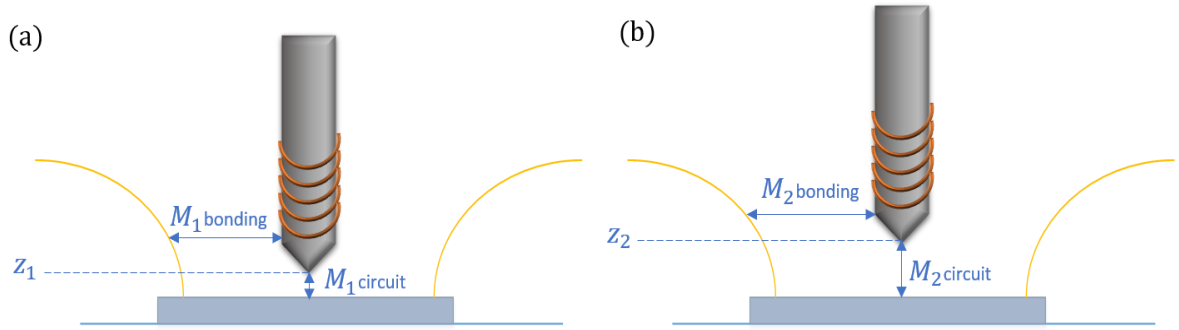


Figure 2.9 – Couplage sonde-circuit et sonde-bonding à deux hauteurs Z de la surface du circuit.

La Figure 2.10 donne la cartographie de ΔV_{Z1} - ΔV_{Z2} qui fait apparaître une structure liée au circuit sur TEG et aux fils de bonding et n'est donc plus uniforme. Comme attendu, la perturbation ΔV est maximale lorsque la sonde est positionnée de part et d'autre de la piste et minimale quand elle est placée au-dessus de la TEG ou des fils de bonding. Il est à noter que malgré les précautions prises, les fils de bonding sont encore parfaitement visibles.

Enfin, le fait de devoir effectuer la différence de deux cartographies pour voir apparaître un motif de ligne d'alimentation met clairement en évidence que $M_{bonding} \gg M_{circuit}$. Ce résultat montre combien il est difficile d'effectuer des mesures analogiques lors d'EMFIs.

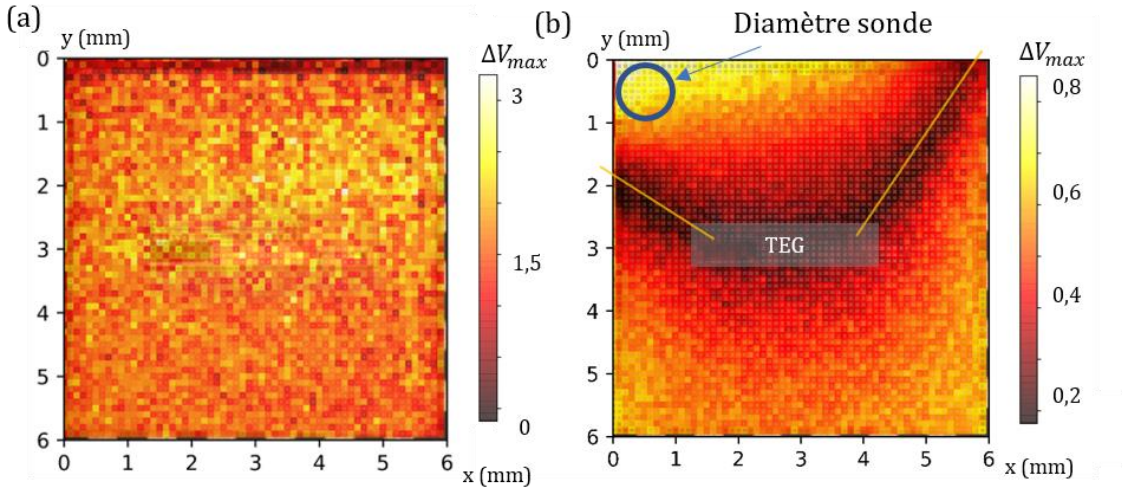


Figure 2.10 – Cartographie du (a) $\Delta V_{max}(Z)$ et (b) du $\Delta V_{max}(Z_1) - \Delta V_{max}(Z_2)$, pour une injection EM effectuée avec V_{pulse} = 50V.

2.2.2.b Effet d'une EMFI sur un registre à décalage

La seconde série d'expériences a ciblé le circuit sur TEG embarquant trente ROs, chacun alimenté par une grille d'alimentation avec des géométries différentes. L'objectif étant toujours d'identifier des géométries de grille moins susceptibles à l'EMFI.

Pour sélectionner le RO qui sera actif et devant être monitoré, un registre à décalage constitué de 30 bascules D est disponible. Ainsi, pour en mesurer la fréquence, on doit en premier lieu le sélectionner via le registre à décalage. Ceci est réalisé en positionnant une impulsion sur l'entrée IN du circuit et N fronts d'horloge sur l'entrée CLK, avec N le numéro du RO dont on veut mesurer la fréquence. La mise à '1' de la bascule numéro N permet d'activer le RO correspondant.

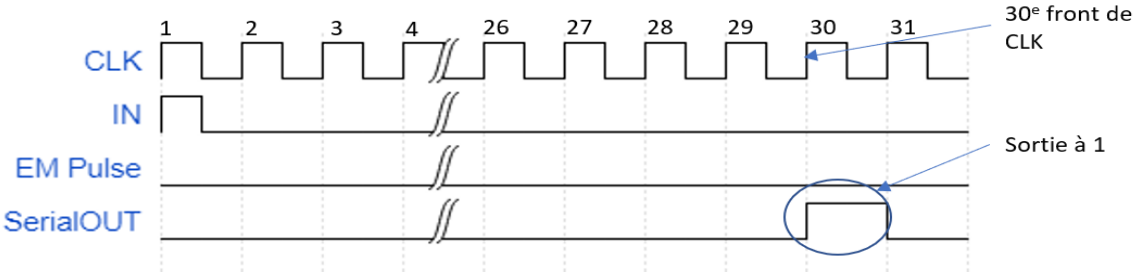


Figure 2.11 - Fonctionnement du registre à décalage pour sélectionner un RO.

Par exemple, dans le cas de la Figure 2.11, on souhaite sélectionner le 30e RO. Pour ce faire, une impulsion est appliquée sur le signal IN et 30 fronts d'horloge. On peut alors vérifier que l'opération de sélection a été correctement effectuée en vérifiant l'apparition

d'une impulsion sur la sortie SerialOUT, après la 30e impulsions. Le comportement du RO peut alors être observé sur une sortie dédiée.

Avec ce mode opératoire, les variations de fréquence Δf des ROs induites par une injection EM (V_{pulse}=+50V et PW=20ns) ont été mesurées. Les variations qui ont été observées ne dépassent pas 1% de la fréquence nominale des oscillateurs. En outre, aucun comportement singulier n'a été observé. Par contre, il a été observé que dans certaines conditions, le tir EM induisait une modification du RO sélectionné. En effet, comme le montre le chronogramme de la Figure 2.12, lors de tirs EM, la sortie SerialOUT passait à l'état logique '1', un front d'horloge plus tôt. Une faute survenait donc dans certaines conditions. Ainsi, lors des mesures de Δf, le RO sélectionné changeait à chaque tir, expliquant les résultats incohérents obtenus.

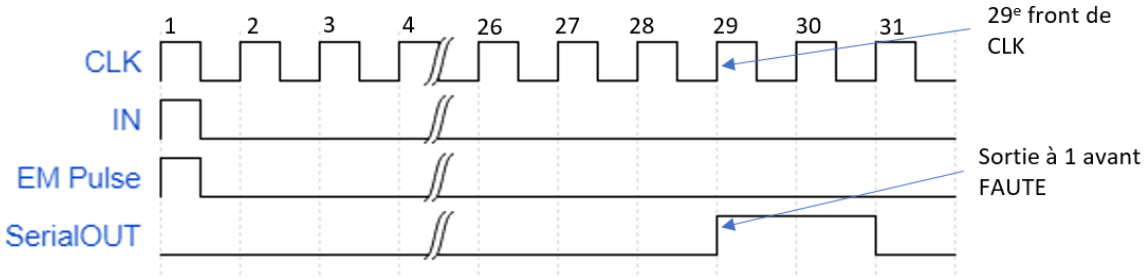


Figure 2.12 – Fonctionnement erroné du registre à décalage lors d'une injection EM.

L'occurrence de cette faute a été analysée. L'explication la plus probable étant la création d'un front d'horloge parasite dû à l'injection EM. Ce signal d'horloge a été désactivé avant le tir EM puis réactivé après celui-ci et ce, sans réduire le nombre total de fronts d'horloge. Conformément à l'hypothèse émise, la montée anticipée de SerialOUT a pu être observée. Cette même constatation a été faite dans [11].

Suite à ce résultat, la cause expliquant l'apparition de ce front d'horloge parasite a été recherchée. Ceci a conduit à retirer le fil de bonding amenant le signal d'horloge du boitier au plot dédié du circuit, laissant son entrée flottante. Cela fait, les mêmes injections EM ont été effectuées. Aucune d'entre elles n'a permis de reproduire la faute. L'apparition du front d'horloge était donc due à la création d'un front parasite directement sur le fil de bonding et non pas dans le circuit. Il convient de noter que le cas de ce circuit de test n'est pas représentatif d'un produit. En effet, les produits intègrent généralement des éléments permettant de filtrer des bruits parasites externes.

En conclusion, bien que ces expérimentations n'aient pas permis d'identifier des structures de grille d'alimentation moins susceptibles à l'injection EM, elles ont été riches

d'enseignements. En effet, elles m'ont permis de gagner de l'expérience quant à la pratique des EMFIs, mais elles ont surtout mis en évidence le soin qu'il faut accorder aux fils de bonding lors des spécifications de puces de test. Cette leçon aura été profitable pour le développement de nouvelles puces de test, qui ont été utilisées durant le reste de ma thèse.

Concernant, la caractérisation du couplage entre la sonde d'injection EM et le circuit, suite à ces résultats, notre stratégie a été d'approfondir notre compréhension de l'injection EM par la simulation, le temps que les nouvelles puces de test soient conçues, fabriquées et encapsulées. Nous avons donc dans un premier temps cherché à modéliser le couplage sonde-circuit.

2.3 Couplage entre la sonde d'injection EM et le circuit

La modélisation du couplage EM entre une sonde et des lignes métalliques simples (appelées aussi striplines) a fait l'objet de nombreux travaux relatifs à l'étude de la susceptibilité EM des dispositifs électroniques [8], [12] – [14]. Toutefois, aucun travail n'a été dédié à la modélisation du couplage entre une sonde et un circuit c'est à dire à un réseau complexe de lignes de métallisation. C'est ce que nous allons essayer de réaliser dans les prochaines sections. Avant de rentrer dans le détail de la modélisation du couplage sonde-circuit, il est nécessaire de rappeler quelques fondamentaux sur le couplage électromagnétique. Il est également temps d'exploiter les analyses de la structure générale des circuits intégrés qui ont été conduites en première partie de ce chapitre.

2.3.1 Hypothèses de couplage

Notre objectif étant de comprendre comment les EMFIs induisent des fautes au sein des CIs, nos travaux se sont portés sur la modélisation du couplage et de l'interaction sonde-circuit uniquement. Ils excluent donc la prise en compte du boitier et des fils de bonding. Ce choix est justifié, par le fait que :

- les premières expérimentations conduites sur les TEG nous ont permis d'appréhender la problématique des fils de bonding longs (cas de nos TEG),

- ces mêmes fils de bonding sont nettement plus courts et moins encombrants dans le cas de produits.

Les nouvelles puces de test que nous avons utilisées par la suite, ont d'ailleurs été conçues de sorte à être plus représentatives de véritables produits. Les surfaces des circuits sont plus grandes (2mmx2mm), ainsi les fils de bonding sont nettement plus courts. Elles intègrent également un régulateur LDO (Low DropOut) pour filtrer les bruits parasites à l'entrée de l'alimentation DC du circuit.

Comme cela a été rappelé dans la section 1.3.2, M. Faraday a montré qu'une fem (force électromotrice), ε, est induite dans une boucle de fil lorsque le champ magnétique qui traverse sa surface change au cours du temps. Il a également démontré que la fem est proportionnelle à la dérivée du flux magnétique traversant la surface de cette boucle. La direction de la fem est donnée par la loi de Lenz-Faraday (équation 2.2). Elle stipule que le courant induit circulant dans la boucle est de sens opposé au changement qui la produit, avec $d\phi$ la variation du flux magnétique dans le temps, traversant la surface de la boucle.

$$\varepsilon = -\frac{d\phi}{dt} \qquad (2.2)$$

La première leçon des observations de M. Faraday est que l'EMFI dépose une fem dans toutes les boucles du circuit intégré cible. L'amplitude de chacun de ces courant est proportionnelle au taux de variation du flux magnétique. La question importante est donc de savoir quelles sont les boucles que le champ magnétique peut traverser dans un circuit.

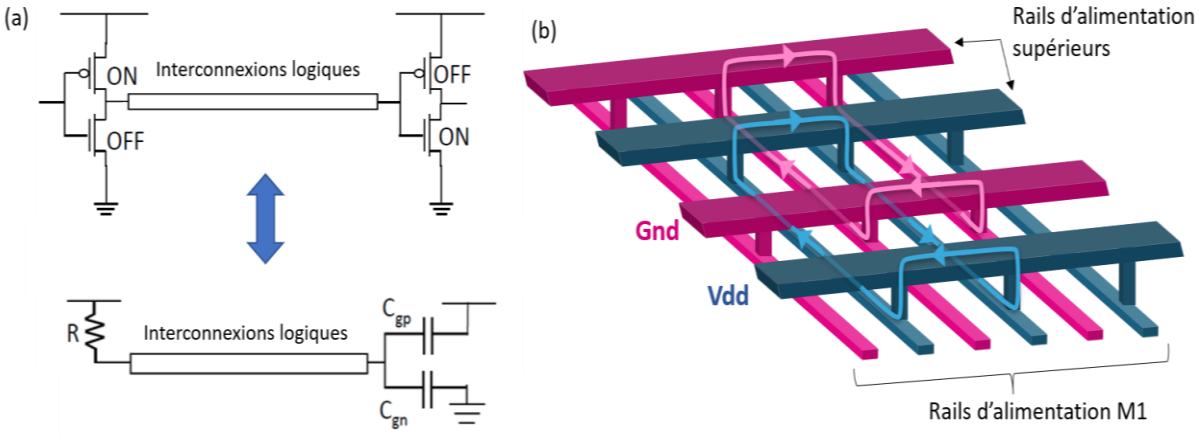


Figure 2.13 - Différentes lignes de métaux dans un CI. (a) Rails d'interconnexions logiques, (b) rails d'alimentations Vdd et Gnd, sur deux niveaux de métaux.

Comme nous l'avons montré dans la section 2.1 et illustré Figure 2.13, il existe deux types d'interconnexions dans les circuits intégrés : les interconnexions logiques et les rails d'alimentation Vdd et Gnd.

Un fil d'interconnexion transporte le signal électrique (signal de d'horloge inclue) de la sortie d'une porte CMOS à l'entrée (aux entrées) d'une (ou plusieurs) porte(s) CMOS.

Par conséquent, à l'une de ses extrémités, le fil d'interconnexion est connecté à un rail d'alimentation (Vdd ou Gnd) par l'intermédiaire d'un transistor en conduction, étant équivalent à une résistance R [98]. À l'autre extrémité il est connecté à une ou plusieurs portes(s) CMOS, c'est-à-dire à des capacités MOS qui ont une résistance extrêmement élevée (voir infinie en théorie). Par conséquent, les fils d'interconnexions ne forment pas de boucles conductrices dans lequel un courant peut être induit ou si c'est le cas celles-ci sont extrêmement résistives. Ils ne sont donc pas sujets (ou faiblement) à l'induction EM.

Contrairement aux fils d'interconnexions, les rails Vdd et Gnd forment deux grilles 3D qui délivrent l'alimentation aux portes CMOS. Ces deux grilles, Figure 2.13 (b), comprennent plusieurs boucles verticales et horizontales. En effet, la matrice formée par les rails d'alimentation et leurs connexions sur plusieurs niveaux, forment un réseau de boucles couvrant l'ensemble de la surface du circuit. Lors d'une EMFI, ces boucles verticales et horizontales vont être traversées par des lignes de champ magnétique longitudinales ou transversales, contrairement aux fils d'interconnexions. De plus, leur faible résistivité linéique augmente également leur susceptibilité face à un champ EM (voir équation 2.3). En effet, le courant induit peut y prendre des valeurs importantes. Les rails d'alimentations sont donc extrêmement susceptibles à l'EM.

À partir de ces simples considérations, on peut affirmer que les perturbations électromagnétiques altèrent principalement le comportement des réseaux d'alimentation Vdd et Gnd. Nous allons maintenant modéliser le couplage entre ces réseaux d'alimentation et une sonde EM.

2.3.2 Profils de distribution du champ EM et principe de superposition

De nos jours, les sondes EM sont conçues sur la base d'un noyau de ferrite autour duquel est enroulé un fil pour former une bobine. Le diamètre, d_{probe}, de la tige de ferrite varie généralement de 300µm à 2mm, valeurs qui sont beaucoup plus grandes que le pas de routage du réseau d'alimentation.

Selon que le boîtier du CI ciblé ait été retiré ou non, les EMFIs peuvent être effectuées avec la sonde assez loin (à une distance $D > d_{probe}$) ou à proximité, voire en contact ($D \ll d_{probe}$) de la surface du circuit comme décrit dans la Figure 2.14.

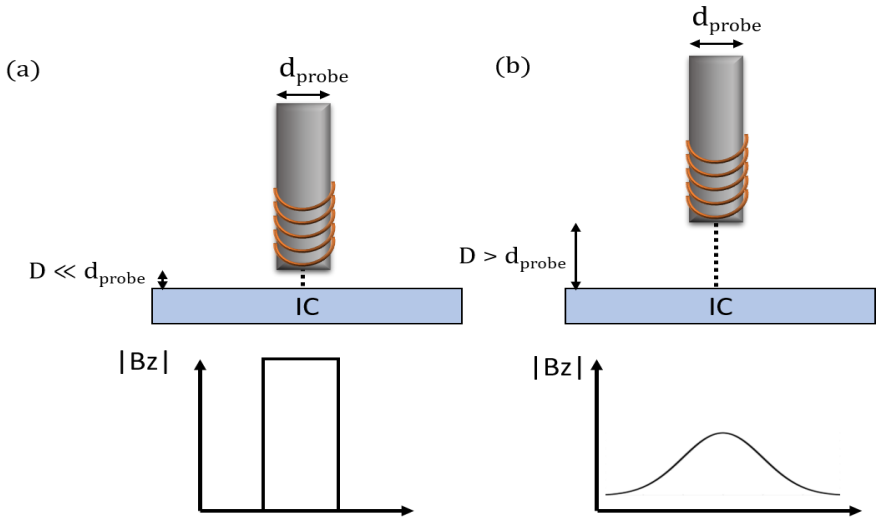


Figure 2.14 - Modèle de la distribution verticale du champ magnétique le long d'un axe à 2 différentes hauteurs. (a) Cas où la sonde EM est proche de la surface. (b) Cas ou la sonde est éloignée de la surface.

Selon [71] ou [99], dans le cas (a) où $D \ll d_{probe}$ l'amplitude du champ magnétique $|B_z|$ vertical induit est supposée constante sous la surface sonde. Dans le cas où la sonde est plus éloignée du circuit (b), $D > d_{probe}$, la sonde produit un champ $|B_z|$ ayant une distribution de la forme d'une loi normale.

Dans les deux cas, la sonde génère un flux magnétique traversant la surface de plusieurs boucles et induit donc à l'intérieur de celles-ci, plusieurs fems. En faisant la supposition que chaque branche d'une boucle a la même résistance R, chaque fem génère en retour un courant i(t) proportionnel à 1/R dans chaque boucle du CI conformément à l'équation 2.3. L'orientation de i(t) suit la loi de Lenz.

$$i(t) = -\frac{1}{R}\frac{\partial \varphi}{\partial t} \qquad (2.3)$$

La distribution de ces fems sur une partie d'une grille d'alimentation, ou de masse, est représentée sur la Figure 2.15. Par souci de simplicité ainsi que pour faciliter la lecture de ce document, une sonde carrée a été considérée. Le rectangle rouge représente la projection verticale des bords de la sonde EM sur la surface du CI. Bien entendu, le nombre de boucles incluses dans l'empreinte de la sonde est réduit à une faible valeur pour des questions de lisibilité. En réalité, ce nombre est compris entre 600 et 4000 pour un diamètre de sonde compris entre 300µm et 800µm et un pas de routage entre les lignes d'alimentation égal à 30µm pour le métal de niveau supérieur et de 5µm pour le Métal 1. Comme indiqué, chaque boucle subit une force électromotrice induisant le même courant dans chaque branche de la boucle du fait de la rotation du champ électrique en son sein (équation 1.3).

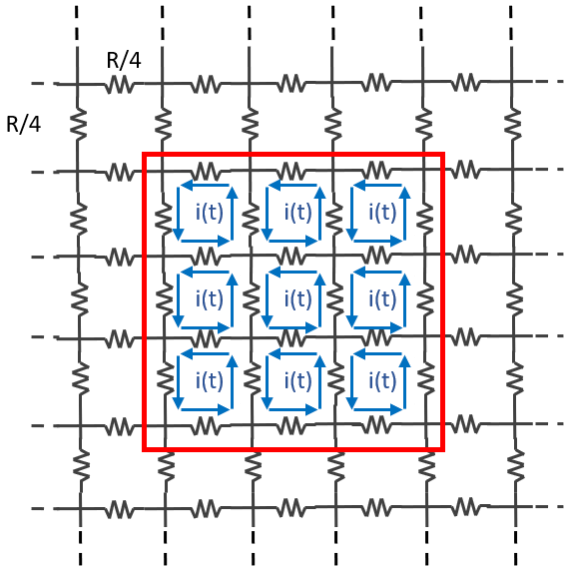


Figure 2.15 – Fems déposées par une EMFI sur une grille d'alimentation. Le carré rouge représente la projection verticale sur la surface des bords de la sonde d'injection.

Le point clé à observer dans la Figure 2.15 est qu'au milieu de la surface de la sonde, chaque fem contrebalance les effets de ses fems voisines selon le principe de superposition. L'importance de cet effet de compensation dépend du taux de variation du flux magnétique dans chaque boucle, c'est-à-dire de la distribution de $|B_z|$ sur la surface.

Dans le cas d'une injection EM effectuée avec la sonde à proximité de la surface (par exemple avec le noyau de ferrite au contact de la surface du circuit), on peut supposer, selon [72], que le flux magnétique est uniforme sous toute la surface de la sonde. Dans ce cas, tous les courants induits par toutes les fems ont la même amplitude mais différentes orientations suivant les axes x et y. L'application du principe de superposition indique, comme le montre la Figure 2.16 (a), que, dans ce cas idéal, l'EMFI produit un seul courant d'induction circulant le long des bords de la sonde EM. La concentration de l'effet d'un champ électrique sous les bords de la sonde est également présentée dans [47].

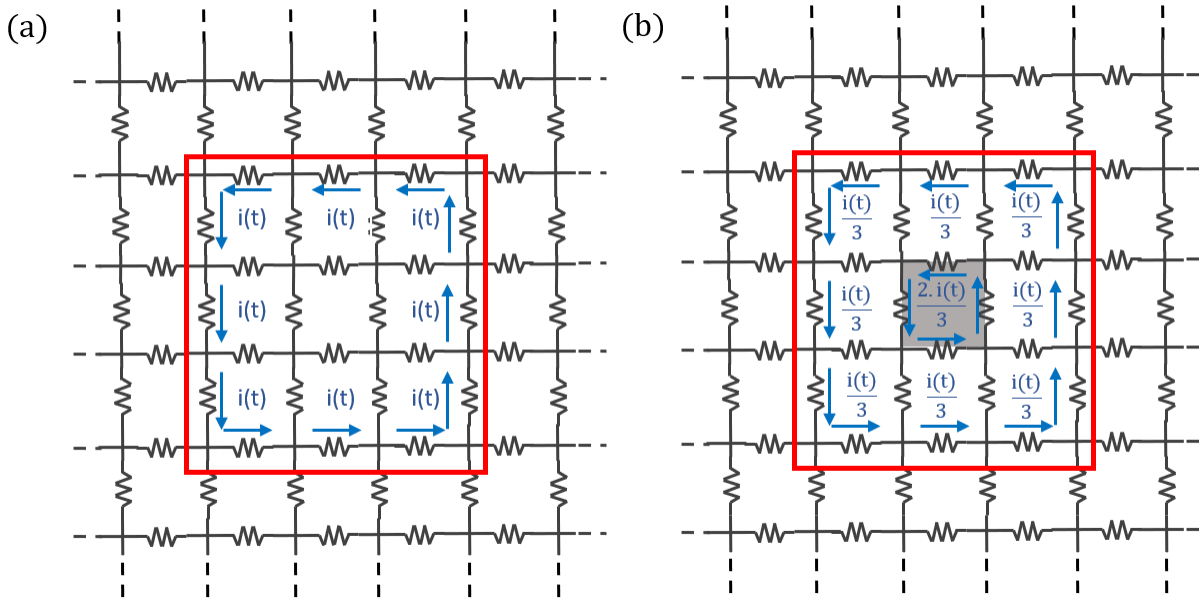


Figure 2.16 - Application du principe de superposition sur une grille d'alimentation dans le cas d'une EMFI effectuée avec la sonde (a) à proximité (b) éloignée de la surface du circuit.

Le cas d'une EMFI produit avec la sonde éloignée de la surface de l'IC est plus complexe. Pour donner un aperçu de ce qui peut se produire, supposons qu'en raison de la distribution normale du champ, le flux magnétique moyen traversant la boucle centrale (représentée en gris foncé sur la Figure 2.16 (b)) est trois fois plus important que celui traversant les boucles périphériques. Dans ce cas, l'EMFI induit un courant i(t) dans la boucle centrale et un courant $\frac{i(t)}{3}$ dans toutes les boucles périphériques. L'application du principe de superposition montre alors que la boucle centrale est parcourue par un courant $\frac{2.i(t)}{3}$ et que les branches externes des boucles périphériques sont quant à elles parcoures par un courant $\frac{i(t)}{3}$. L'EMFI conduit donc à deux courants concentriques, ce qui ressemble à des courants de Foucault contraints de suivre la grille. On note que, plus le nombre de boucles sous la sonde est important, alors plus le nombre de courants concentriques est également important. Toutefois, l'amplitude de ces courants suit la loi de distribution normale.

Hormis les deux types d'injection EM, et donc les deux formes de distribution du champ $|B_z|$, aucune atténuation du champ EM en fonction de la distance entre la sonde et le circuit cible n'est prise en compte. En effet, notre objectif étant de mettre en évidence les différences entre les effets spatiaux de ces deux types d'EMFI. Ce choix n'a que peu d'influence sur le résultat général car la prise en compte de la distance entre la sonde et le circuit se fait en réduisant les coefficients de la mutuelle inductance. Une telle réduction peut être simplement contrebalancée avec une augmentation du V_{pulse}.

À ce stade, la plupart des éléments ont été décrits, indiquant qu'une EMFI induit des courants parasites dans certaines branches de certaines boucles d'un circuit. La prochaine section vise à définir comment simuler cette interaction avec des simulateurs largement utilisés lors de la conception des circuits intégrés, afin de prévoir comment l'EMFI influe sur les polarisations.

2.4 Modélisation de l'effet du couplage EM avec les grilles d'alimentation

Une modélisation complète entre une sonde d'injection EM et les grilles d'alimentation d'un circuit intégré est présentée dans cette partie. Mise en œuvre pour simuler l'effet d'une EMFI sur les réseaux d'alimentation et de masses, elle permettra d'appréhender comment les fautes sont induites dans les circuits synchrones.

Pour mettre en place cette modélisation, différents logiciels ont été utilisés. Les schémas électriques sont réalisés sur Virtuoso du groupe Cadence et les simulations électriques effectuées avec Eldo de Mentor Graphics.

On notera que les modélisations se veulent être les plus précises possible, en prenant en compte un maximum d'éléments afin de représenter au mieux la réalité. Certains logiciels permettent de modéliser des couplages EM avec une très grande précision sur des éléments simples. Ils s'appuient sur la résolution des équations de Maxwell. Toutefois, la résolution de ces équations sur des grilles d'alimentation aussi complexe est hors de portée calculatoire. D'où le modèle introduit dans ce chapitre.

Ce modèle global des EMFIs, inclut un modèle électrique du réseau d'alimentation d'un CI, un modèle électrique du couplage EM ainsi que les éléments principaux des circuits susceptibles d'agir sur le comportement du réseau d'alimentation. Toutefois, ces modèles reposent sur des approximations et hypothèses. Les sections suivantes reprennent unes à unes les éléments de cette modélisation.

2.4.1 Modélisation du couplage entre une sonde d'injection EM et le réseau d'alimentation et de masse

Nos travaux ont, dans un premier temps, porté sur la modélisation électrique d'une sonde d'injection EM ainsi que son couplage avec les grilles Vdd et Gnd. La sonde et le réseau d'alimentation d'un CI (les boucles le constituant) peuvent être comparés à deux antennes, donc deux inductances, couplées l'une avec l'autre.

Toutefois, d'après les considérations des sections précédentes, l'interaction entre une sonde EMFI et un CI ne se réduit non pas à un seul couplage EM mais à deux : un entre la sonde et le réseau Vdd et l'autre entre la sonde et le réseau Gnd comme illustré Figure 2.17 à droite. En outre, chaque couplage EM génère plusieurs fems : une pour chaque boucle du réseau considéré (Vdd ou Gnd). L'effet d'une fem étant généralement modélisé par une inductance mutuelle [100], il est proposé de modéliser la situation par le transformateur, représenté Figure 2.17. Ce transformateur possède un enroulement primaire représentant la sonde EM et de nombreux enroulements secondaires.

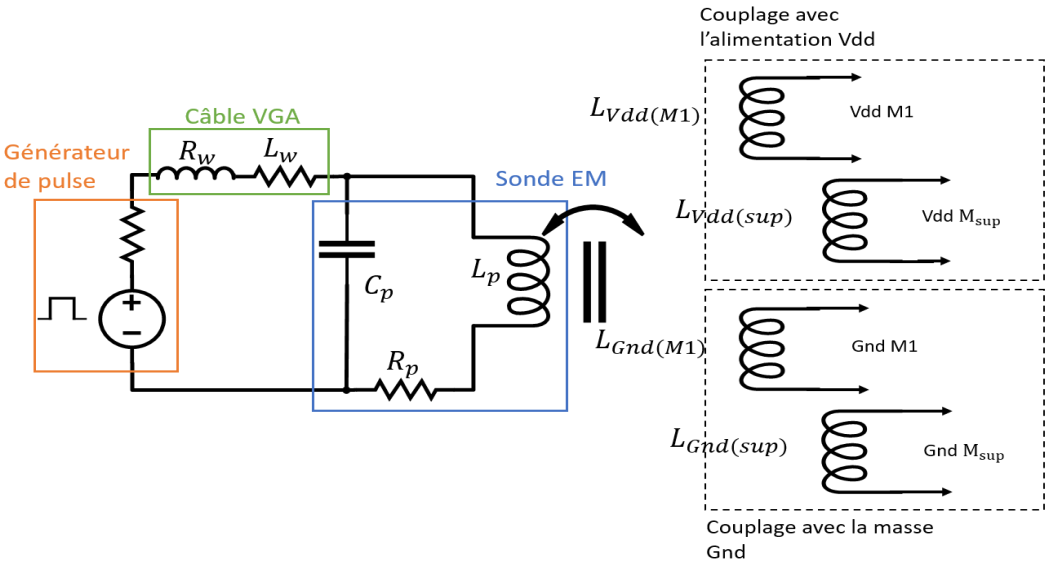


Figure 2.17 - Modélisation électrique d'une sonde EMFI, et de son couplage EM avec les boucles du circuit par des inductances mutuelles $L_{VDD(Mx)}$ et $L_{GND(Mx)}$ (avec 'x' correspondant au niveau de Métal) pour les réseaux Vdd et Gnd respectivement.

La modélisation de la sonde d'injection d'EMFI complète [72] est représentée sur la partie gauche de la Figure 2.17. Elle est constituée d'un générateur d'impulsion et de son impédance de sortie de 50Ω, qui délivre à la sonde une impulsion de tension d'amplitude V_{pulse} et de largeur PW avec des fronts montants et descendants de durée T_R et T_F, respectivement. Le générateur est connecté au câble SMA (SubMiniature version A) de résistance R_w et d'inductance L_w.

La sonde EM, considérée de forme carrée, est constituée d'un barreau de ferrite entouré par N spires de cuivre, et modélisée par sa capacité C_p (entre les spires de la bobine), sa résistance R_p et son inductance L_p qui constitue l'enroulement primaire du transformateur du modèle. Une estimation de L_p est donnée par l'équation 2.4 [111].

$$L_p = 2.N^2 \frac{\mu_0.\mu_R.L^2}{\pi}.ln\left(\frac{L}{D_w} - 0{,}774\right) \quad (2.4)$$

Avec μ_0 la perméabilité magnétique du vide ($4\pi.10^{-7}$), μ_R la perméabilité magnétique de la ferrite, N le nombre de spires, L la longueur du carré et D_W la section du fil.

Outre l'étude du layout conduite en début de chapitre, des informations sur la modélisation des réseaux d'alimentation ont été tirées de [101]–[103]. La représentation d'une boucle constituant le réseau d'alimentation Vdd ou Gnd et son schéma électrique sont représentés Figure 2.18 (a) et (b). Elle est constituée de deux rails de Métal supérieurs de résistance R_{Msup} connectés, par des vias de résistance R_{VIA} aux deux rails de Métal1 de résistance R_{M1}.

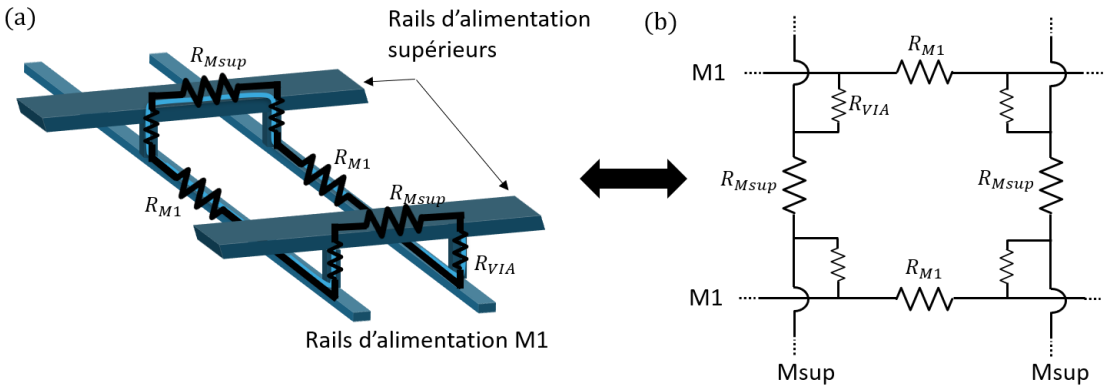


Figure 2.18 - Modélisations d'une boucle d'une grille d'alimentation Vdd ou Gnd.

Lorsque le champ magnétique émis par la sonde et traversant une boucle varie, une fem est déposée le long des fils de cette boucle. Cette fem provoque la circulation d'un courant dont la valeur est proportionnelle à l'inductance de la boucle L_{loop} et inversement proportionnel à la résistance de la boucle. Son expression est en fait :

$$i_{Loop}(t) = -\frac{L_{Loop}}{2 \cdot (R_{M1} + R_{Msup})} \frac{di_{secondaire}(t)}{dt} \quad (2.5)$$

Avec $i_{Secondaire}(t)$ le courant (flèche rose sur la Figure 2.19) circulant dans les quatre bobines du secondaire nécessaires pour modéliser le dépôt de la fem le long de la boucle considérée. Ces quatre bobines sont représentées sur la Figure 2.19. Les deux rattachées aux pistes de métal supérieur ont pour valeur $L_{Vdd/Gnd(Msup)}$. Les deux rattachées aux pistes de Métal1 ont pour valeur $L_{Vdd/Gnd(M1)}$.

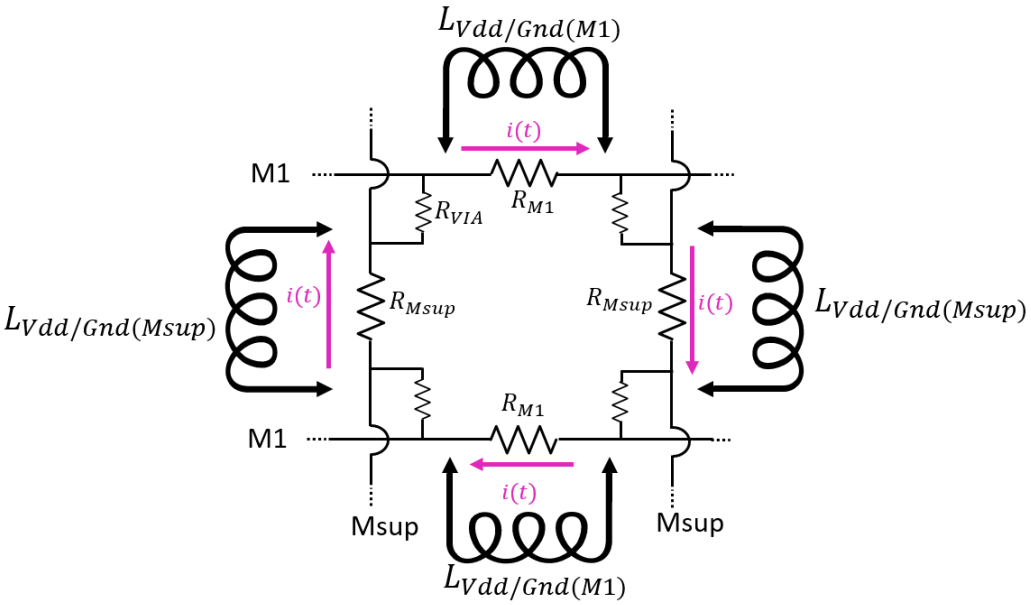


Figure 2.19 - Modèle d'une boucle de grille d'alimentation avec les couplages représentés par les bobines secondaires des inductances mutuelles.

La valeur de L_{loop} peut être estimée à partir de l'équation suivante qui est spécifique aux bobines de section rectangulaire :

$$L_{Loop}=\frac{\mu_0 \cdot \mu_R}{\pi}\left\{\begin{array}{c} -2(L+l)+2\sqrt{L^2+l^2}-ln\left(\frac{l+\sqrt{L^2+l^2}}{L}\right) \\ -ln\left(\frac{L+\sqrt{L^2+l^2}}{l}\right)+l\cdot ln\left(\frac{4\cdot l}{D_W}\right)+L\cdot ln\left(\frac{4\cdot L}{D_W}\right) \end{array}\right\} \qquad (2.6)$$

Avec L la longueur de la boucle (30µm dans notre cas), l sa largeur (5µm dans notre cas) et enfin w la section du fil (0,15µm dans notre cas).

Les valeurs de $L_{Vdd/Gnd(Msup)}$ et $L_{Vdd/Gnd(M1)}$ sont calculées en considérant que le courant induit dans la boucle circule dans toutes les branches. Il vient alors que :

$$L_{Vdd/Gnd(Msup)} = L_{Loop}\cdot\frac{R_{Mup}}{2\cdot\left(R_{M1}+\cdot R_{Msup}\right)} \qquad (2.7.a)$$

$$L_{Vdd/Gnd(M1)} = L_{Loop}\cdot\frac{R_{M1}}{2\cdot\left(R_{M1}+\cdot R_{Msup}\right)} \qquad (2.7.b)$$

Une difficulté inhérente à la modélisation de l'EMFI est de disposer d'une estimation de la perméabilité μ_R du matériau constituant le noyau des boucles. En effet, ce matériau n'est pas uniforme. Il ne s'agit en aucun cas de dioxyde de silicium seul, dont la

perméabilité relative est comprise entre 3.4 et 3.9. Il ne s'agit pas non plus de silicium pur dont la perméabilité est de l'ordre de 11 à 12. Il s'agit, en fait, d'un empilement de couches de dioxyde de silicium, d'isolant SOD (Spin-On Dielectric), le tout traversé par des interconnexions en aluminium et/ou cuivre ou tungstène. La densité de celles-ci est telle que l'on pourrait même les modéliser comme un film mince de métal. La perméabilité relative de couches métalliques fines est de l'ordre de 1000. Ce point reste non élucidé dans mes travaux de thèse dans lesquels nous considérons des fourchettes de valeurs pour μ_R.

Toutefois, quelles que soient les valeurs considérées, on peut s'attendre à ce que $L_{Vdd(Mx)}$ et $L_{Gnd(Mx)}$ aient des valeurs très proches en raison de la géométrie de routage commune entre les grilles d'alimentation et de masse dans les CIs modernes.

Le composant utilisé pour modéliser le couplage est un transformateur. Il prend en compte la valeur de couplage entre les 2 antennes, c'est-à-dire l'efficacité du transfert d'énergie de l'enroulement primaire (sonde) à un enroulement secondaire (branche de la boucle de fil). L'efficacité du couplage entre la sonde et le réseau Vdd et la sonde et le réseau Gnd est modélisée par les coefficients d'inductance mutuelle M_{Vdd} et M_{Gnd}.

$$M_{Gnd} = k_{Gnd}.\sqrt{L_{probe}.L_{Gnd(Mx)}} \qquad (2.8.a)$$

$$M_{Vdd} = k_{Vdd}.\sqrt{L_{probe}.L_{Vdd(Mx)}} \qquad (2.8.b)$$

Ces coefficients permettent de considérer, en contrôlant les valeurs k_{Gnd} et k_{Vdd}, le rapport des surfaces en regard entre la sonde et chaque boucle de fil (ainsi que l'effet de la distance séparant la boucle d'alimentation et la sonde EM). Bien sûr, dans le cas d'une EMFI effectuée avec la sonde proche du circuit, les valeurs k_{Gnd} et k_{Vdd} sont identiques (distribution uniforme du champ magnétique). Par contre, dans le cas où la sonde est éloignée du circuit, k_{Gnd} et k_{Vdd} suivent une loi normale, modélisant le profil du champ magnétique traversant la surface du circuit.

Pour la ferrite, les trois valeurs correspondent à des valeurs fournies par le fabricant de tiges de ferrite américain Fairite [104] qui tient compte d'un facteur correcteur K relatif à la longueur de l'enroulement autour de la ferrite. Les trois valeurs de perméabilité pour le circuit correspondent à celle du SiO_2, du Si et enfin d'une estimation consistant à considérer que 10% du volume se comporte comme une feuille fine de métal et 90% comme du SiO_2.

Le Tableau 1 reporte les valeurs des différents paramètres intervenant dans la modélisation du couplage sonde-circuit et ce pour différentes valeurs des perméabilités relatives de la ferrite et des boucles dans le circuit. En outre, pour dresser ce tableau, il a été considéré que la sonde est un carré de section 300µm dont les fils ont une largeur de D_W=10µm, que les boucles ont une longueur L=30µm, une largeur l=5µm et que les pistes de métal sont de largeur 0,15µm. Les calculs de R_{Mx} et du facteur de couplage k sont développés dans l'annexe 1.

Tableau 1 - Valeurs des paramètres de simulation du couplage entre une sonde-circuit.

	Paramètres	Valeurs		
Sonde EMFI carrée	$\boldsymbol{R_w}$	0,25 Ω		
	$\boldsymbol{L_w}$	40 nH		
	$\boldsymbol{C_p}$	1 pF		
	L(sonde)	300 µm		
	$\boldsymbol{D_W}$	10 µm		
	$\boldsymbol{R_p}$	2 Ω		
	N(sonde)	5		
	$\boldsymbol{\mu_R}$(ferrite)	48(K=1)	96(K=2)	192(K=4)
	$\boldsymbol{L_p}$(éq2.9)	0,76 µH	1,51 µH	3,03 µH
Boucle de grille d'alimentation	**L**(boucle)	30 µm		
	l(boucle)	5 µm		
	$\boldsymbol{\mu_R}$(circuit)	3,9	12	103
	$\boldsymbol{L_{Vdd/Gnd(M1)}}$(éq2.8.a)	92 pH	282 pH	2423 pH
	$\boldsymbol{L_{Vdd/Gnd(Msup)}}$(éq2.8.b)	17 pH	54 pH	466 pH
	$\mathbf{R_{M1}}$	26 Ω		
	$\mathbf{R_{Msup}}$	5 Ω		
	$\mathbf{R_{VIA}}$	5 Ω		
	$\boldsymbol{k_{Gnd} = k_{Vdd}}$	0,0017 (cas d'une sonde proche)		

2.4.2 Modélisation des portes logiques standards

Après avoir modélisé la sonde EM, les boucles des rails d'alimentation Vdd et Gnd, nous nous intéresserons dans cette partie à ce qui alimente les boucles, c'est-à-dire à la charge que constituent les portes logiques, les cellules de couplage etc. Pour cela, le layout de la puce de test (qui sera utilisée lors des mesures de la section 3.4) a été analysé afin d'en déduire un modèle électrique de la charge des boucles.

La puce de test a une structure de polarisation des cellules de type Tap Out. Les boucles d'alimentation des rails Vdd et Gnd ont une longueur L de 30µm représentant la distance entre deux cellules de polarisation et une hauteur l = 5µm correspondant à la hauteur de deux rangées de cellules logiques.

Le modèle électrique qui a été élaboré pour ces segments de circuit, appelés segments logiques ou Std Cell (Standard Cell) par la suite, est représenté sur la Figure 2.20. Chacun des éléments spécifiques, marqués de (1) à (5), de ce modèle sont décrits dans les prochains paragraphes.

Un segment Std Cell est alimenté par les rails en Métal 1 (1) fournissant les tensions Vdd et Gnd aux portes logiques. Ces rails sont eux-mêmes connectés aux rails d'alimentation Vdd et Gnd des Métaux supérieurs (les vias ne sont pas représentés dans la figure par souci de clarté). Les résistances de ces rails sont R_{M1} et R_{Msup}. Celles-ci ont été distribuées sur plusieurs résistances dans le modèle afin de pouvoir facilement représenter une grande surface de circuit en interconnectant le sous-circuit de la figure 2.19.

L'encadré (2) modélise les capacités de découplage entre Vdd et Gnd dont l'ensemble à une capacité totale, C_{DECAP} [105]. Les résistances R_{DECAP} modélisent les résistances d'accès moyennes entre une cellule et les prises de polarisation. Ces dernières (3) offrent une résistance d'accès R_{NW} aux puits N (Nwell) et une résistance d'accès R_{Psub} aux puits P(Pwell).

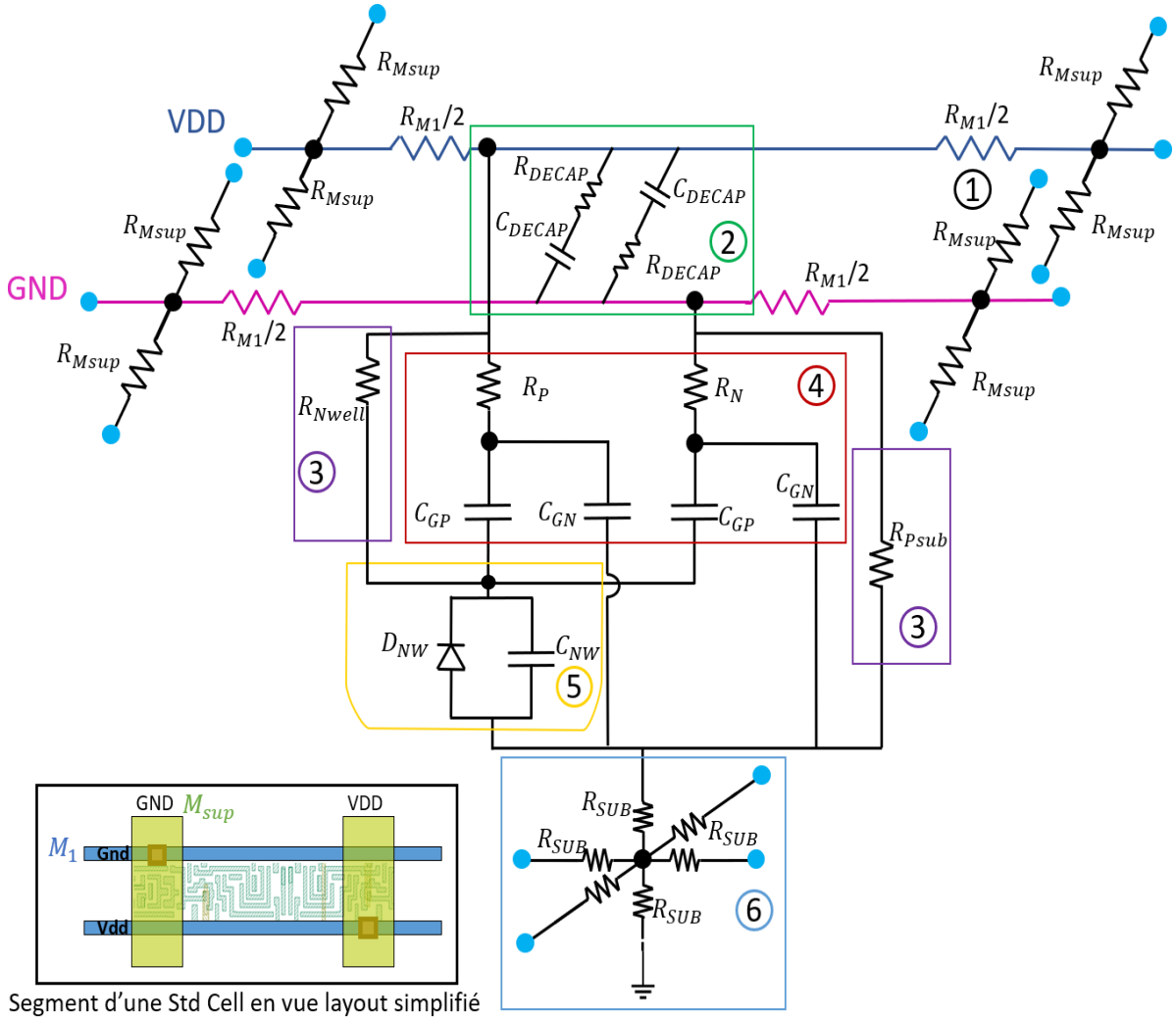


Figure 2.20 - Modèle d'un segment de Std Cell comprenant (1) les rails d'alimentations, (2) capacités de découplage, (3) plots de polarisation, (4) CMOS, (5) Nwell, (6) Substrat profond.

Le modèle de l'ensemble des cellules CMOS d'un segment Std Cell est donné dans l'encadré (4). Une première représentation du modèle des portes logiques CMOS a été donnée Figure 2.13 lors de l'étude des différents types d'interconnexions. On estime que dans un circuit 50% des transistors P et 50% des transistors N sont passants. L'ensemble de ces transistors N (P) passants, dont la source est connectée à Gnd (Vdd), est équivalent à une résistance de valeur R_P (R_N) dont la valeur dépend de la technologie considérée. Les drains de ces transistors N et P passants sont connectés à des grilles de transistors N et P, c'est-à-dire à des capacités MOS dont les valeurs C_{GN} et C_{GP} dépendent de la technologie. Les capacités de grille de ces transistors N (P), donc C_{GN} (C_{GP}) sont elles-mêmes connectées aux puits N (P).

L'encadré (5) modélise le Nwell avec la diode D_{NW} de la jonction PN entre le well et le substrat P et C_{NW} la capacité de cette interface. Enfin, (6) modélise le substrat profond avec une matrice de résistance R_{SUB}. Cette modélisation de substrat et ses valeurs

sont issues de [106]–[108]. Les points bleus aux extrémités (pour les rails d'alimentation et la matrice du substrat) représentent les points d'entrée/sortie du sous-circuit. Ils sont utilisés pour connecter aisément les segments de Std Cells entre eux.

Un point clé à retenir dans ce modèle électrique est l'asymétrie du routage des transistors P et N reliés aux grilles Vdd et Gnd. Elle est due à l'utilisation de puits N pour fabriquer les transistors P qui créent un diviseur de tension (C_{GP}, R_{NW}, C_{NW}) qui n'existe pas côté Gnd. Cela donne une grille Vdd plus sensible aux perturbations EM parasites que la grille Gnd.

Les valeurs des éléments énoncés dans cette partie, issues de la puces de test, sont données dans le Tableau 2. Les différents calculs de la modélisation sont détaillés dans l'Annexe 1.

Tableau 2 - Résumé des valeurs des paramètres de simulation d'un segment de Std Cell.

Paramètres	Valeurs
C_{DECAP}	2,25 fF
R_{DECAP}	2 Ω
R_{NW}	3,2 kΩ
R_{Psub}	3,1 kΩ
R_P	6,4 Ω
R_N	3,6 Ω
C_{GN}	25,2fF
C_{GP}	35,25 fF
C_{NW}	20,7 fF
R_{SUB}	10 kΩ

2.4.3 Simulation de l'effet d'une induction EM sur la grille d'alimentation d'un circuit intégré

L'ensemble des éléments d'un circuit intégré ayant été étudié et modélisé dans les sections précédentes, des simulations ont été exécutées afin d'analyser l'impact d'une EMFI sur les réseaux d'alimentation Vdd et Gnd. Cette partie décrit comment ces simulations ont été conduites et les résultats qu'elles ont fournis.

Dans un premier temps, des simulations d'EMFI avec la sonde proche du CI (cas illustré de la Figure 2.14 (a)) ont été effectuées. Ce cas correspond à la majorité des EMFIs

expérimentales qui ont été faites durant mes travaux de thèse et ce notamment pour confronter résultats de simulation et résultat expérimentaux. Dans un deuxième temps, le cas d'EMFIs avec la sonde éloignée du circuit a été simulé (cas illustré dans la Figure 2.14 (b)).

2.4.3.a Modélisation de l'ensemble d'un circuit intégré

Pour modéliser une surface d'un CI égale à 1mm x 1mm, une matrice de segments Standard Cells connectés les uns aux autres a été mise en place. La surface d'un segment étant de 30µm x 5µm, la matrice du circuit complète fait 34 x 200 segments, soit 6800 segments. Pour cette simulation, la sonde EMFI a été considérée de forme carrée avec des côtés de longueur 300µm.

2.4.3.b Modèle de l'impulsion de tension appliquée à la sonde EMFI

La Figure 2.21 donne la forme des impulsions de tension appliquées à la sonde EM pour différents V_{pulse}. La pente des fronts montants et descendants de ces impulsions est constante et égale à 120V/ns. Il s'agit là d'une des caractéristiques du générateur d'impulsion de tension de notre plateforme EMFI. L'amplitude V_{pulse} de l'impulsion EM modifie donc la largeur de l'impulsion mais également la durée des fronts. C'est la raison pour laquelle la largeur PW de l'impulsion est mesurée à la base de l'impulsion. C'est également pour cela que la valeur minimale de PW est de 6ns à la tension maximale 400V. Durant les simulations qui ont été effectuées, V_{pulse} a été fixée à +400V et PW à 8ns.

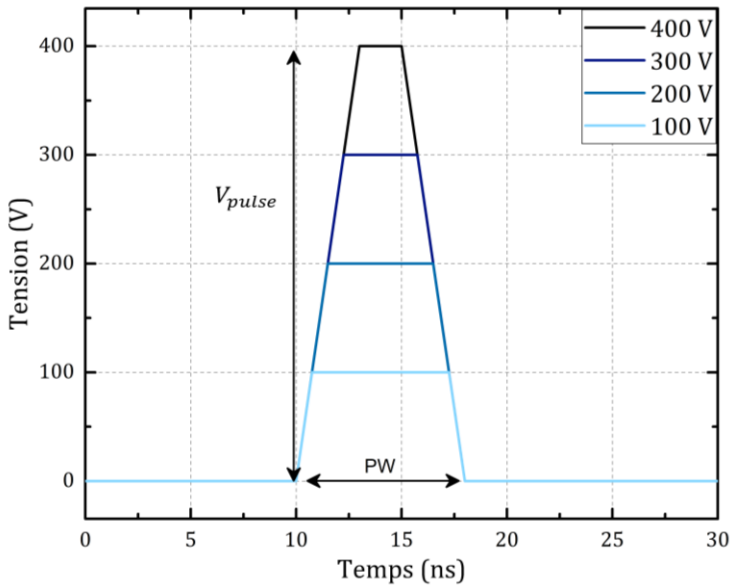


Figure 2.21 - Représentation de l'impulsion de tension appliquée à la sonde EMFI pour différentes valeurs de V_{pulse}.

2.4.3.c Simulation d'une EMFI : sonde proche du circuit

La Figure 2.22 donne une vue de la matrice de segments avec, en rouge, la projection des bords de la sonde carrée sur la celle-ci. Pour des questions de lisibilité, seul un plus petit nombre de segments y est dessiné. L'application du principe de superposition à ces grilles conduit, à la Figure 2.22, pour une EMFI effectuée avec la sonde à proximité du circuit. Comme indiqué, deux boucles de courant concentriques (marquées par des flèches roses) sont induites par l'EMFI sous les bords de la sonde : une sur le rail Vdd et l'autre sur le rail Gnd.

Les rails d'alimentation des segments Seg au centre de l'empreinte de la sonde ne sont pas affectés de manière directe par l'EMFI. Ce n'est pas le cas pour les segments sous le bord de la sonde. En effet, les rails d'alimentation Vdd et Gnd des segments labellisés SegE endurent une même fem, tandis que ceux désignés par SegO ou SegI (premiers segments à l'extérieur (Outside) ou à l'intérieur (Inside) de l'empreinte de la sonde) endurent quant à eux une unique fem affectante soit le rail Vdd, soit Gnd.

La modélisation du couplage se traduit donc par la connexion des bobines secondaires de l'inductance mutuelle sur les rails Vdd et Gnd des segments, SegE. En outre, le principe de superposition indique que le swing S(t)=Vdd(t)-Gnd(t) des segments SegO, SegI et SegE doit être altéré par l'EMFI. La valeur nominale de S(t) est de 1,2V pour la puce de test.

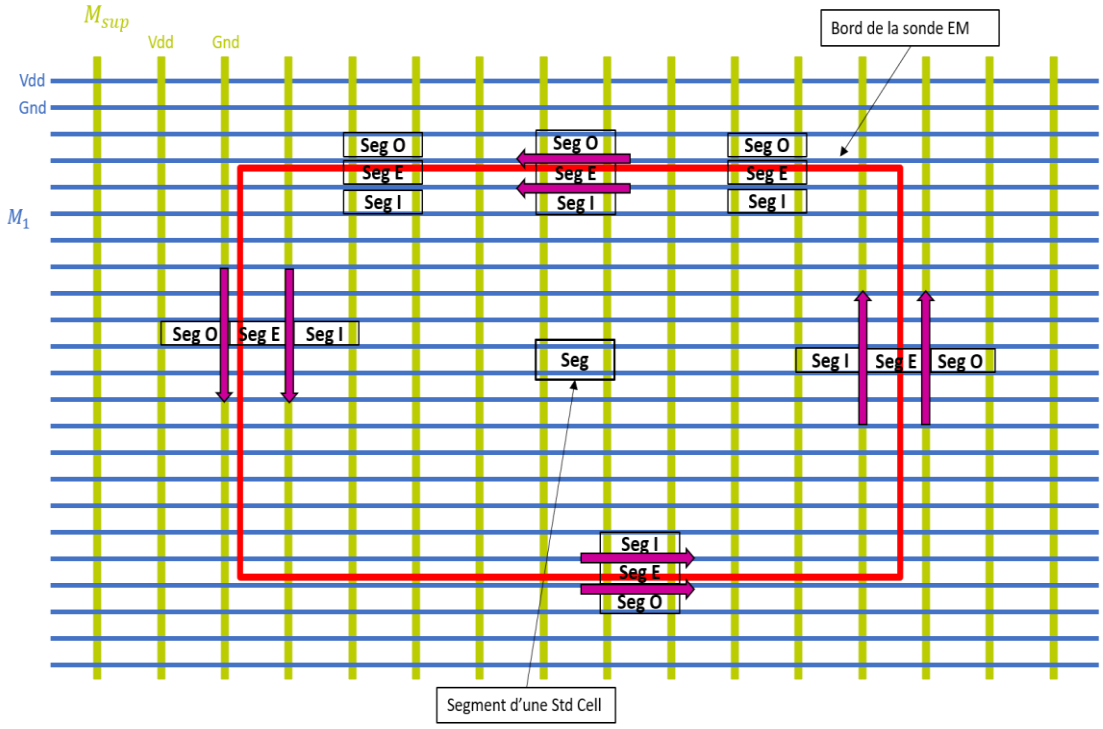


Figure 2.22 - Vue de la surface du CI. Application du principe de superposition dans le cas d'une EMFI effectuée avec la sonde à proximité du circuit.

La Figure 2.23 donne les évolutions de Vdd(t), Gnd(t) et de S(t) pour ces trois types de segments. Comme attendu, une EMFI induit des chutes et des rebonds de Vdd et Gnd. L'allure de ces variations ressemblent fortement à des réponses RC à une impulsion de très courte durée.

Pour les segments SegE, dont les rails Vdd et Gnd sont tous deux parcourus par un même courant induit, les chutes des tensions Vdd et Gnd qui en résultent sont toutes deux de -2,5V. La variation de swing (Figure 2.23) est donc nulle pour ces segments. Par contre, les variations de swing observées dans les segments SegO et SegI sont d'amplitude 2,7V et 4,4V respectivement. L'alimentation de ces segments peut donc être temporairement inversée (S(t)<0) ou bien fortement surélevée (S(t)>1,2V). On notera également que pour ces segments, les variations de la tension des rails (Vdd ou Gnd selon le cas) n'endurant pas de fem sont nettement plus faibles. Elles sont dues à la propagation des courants induits par l'EMFI dans les segments SegE dans le réseau d'alimentation. Compte tenu de cette observation, on peut conclure que les courants induits dans les segments SegE sont en grande partie absorbés par les réseaux RC qui les modélisent.

Dans l'état de l'art, des mesures expérimentales montraient des variations de tension d'alimentation (Figure 1.9) de l'ordre de quelques centaines de millivolts, dues à une EMFI, contrairement aux résultats précédents où ces variations sont de l'ordre du volt. Cette différence s'explique par le fait que les mesures étaient effectuées aux bornes du circuit, où une grande partie des perturbations étaient filtrées. Mais l'effet local de l'impulsion EM suppose que les variations, brèves, induites au cœur du circuit sont beaucoup plus importantes.

La polarité de V_{pulse} n'a que peu d'impact sur la forme des résultats. Le changement de celle-ci va simplement inverser la polarité de toutes les perturbations engendrées. Les chutes et montées de swing dans les segments seront donc interverties entre les segments SegI et les segments SegO.

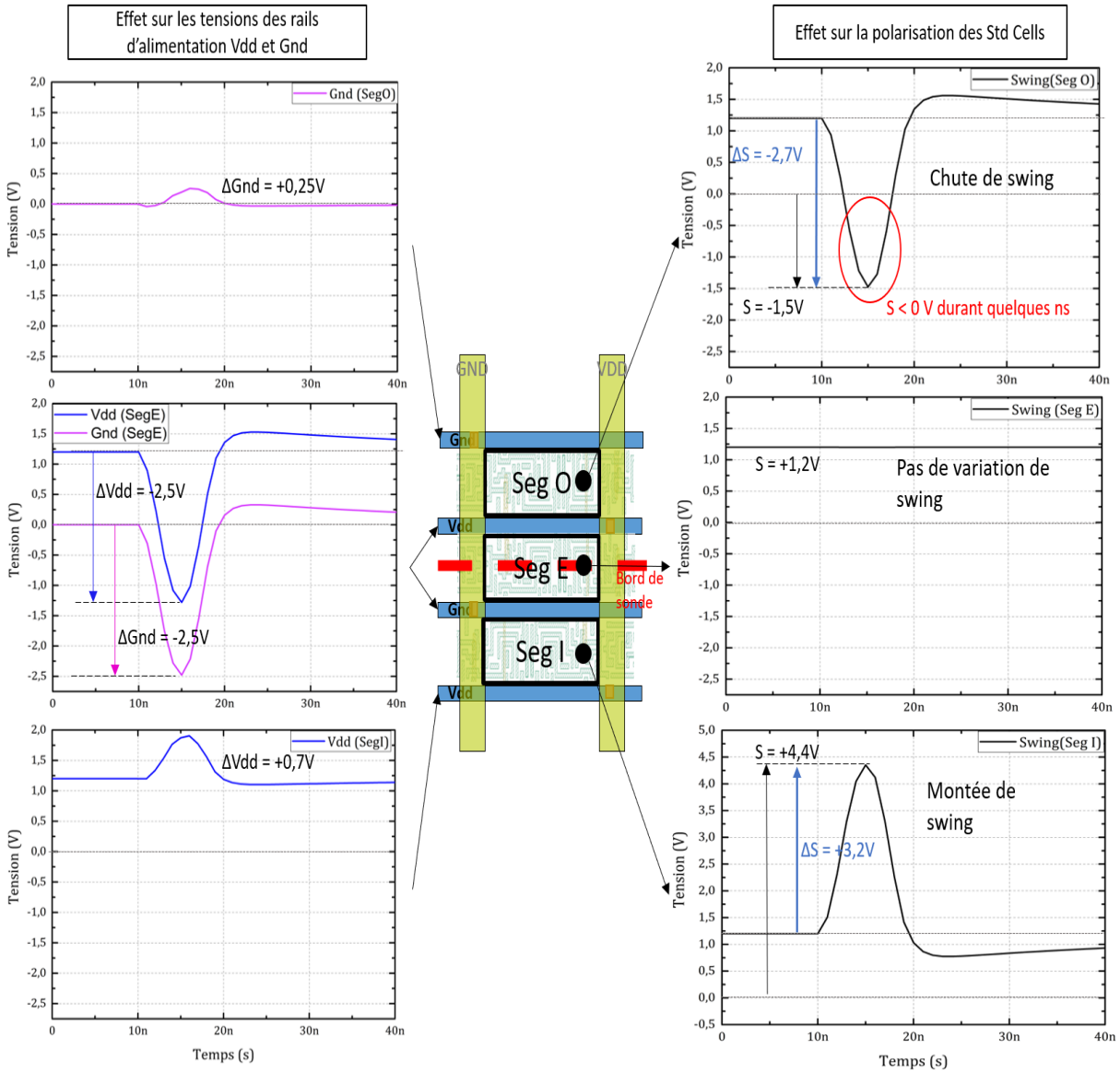


Figure 2.23 - Variations des tensions Vdd et Gnd (à gauche) et du swing (à droite) induites par une EMFI dans les segments SegE, SegI et SegO.

Deux cas de chutes de swing peuvent être distingués comme montré dans la Figure 2.24. La courbe (a) de la figure représente le cas, vu précédemment, où la perturbation de tension sur Vdd descend en dessous de Gnd, ce qui a pour effet d'induire une chute de swing de ΔS=-2,7V. Tandis que la courbe (b) représente le cas où la chute de swing (ΔS=2,2V) est induite via la perturbation Gnd montant au-dessus de Vdd. Nous verrons que ces deux différents cas auront des effets différents sur les fautes induites dans le CI.

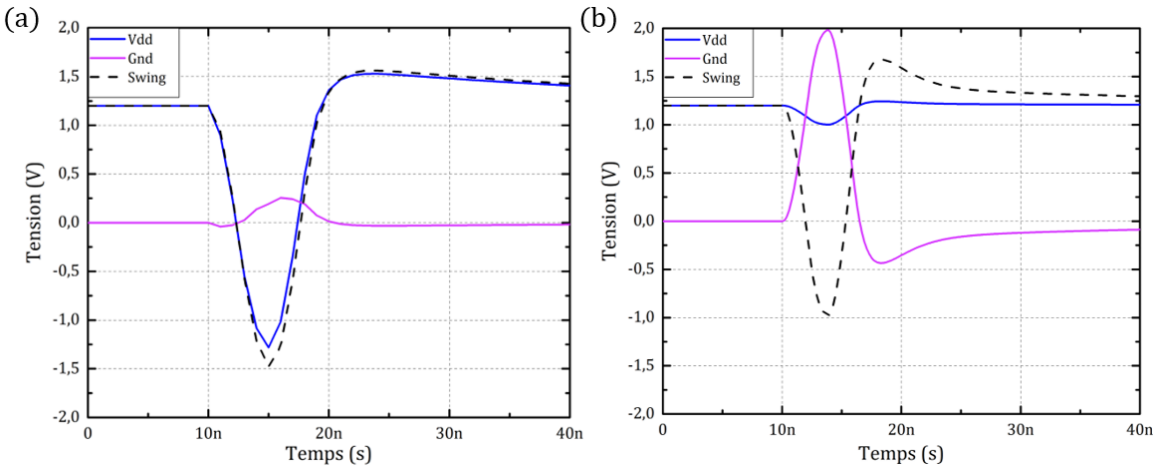


Figure 2.24 – Variations du swing. (a) Vdd descend en dessous de Gnd, (b) Gnd monte au-dessus de Vdd.

Afin d'observer l'effet d'une EMFI sur l'ensemble du réseau d'alimentation d'un CI, des cartographies du swing normalisé, $S(t)_{Normalisé}$, ont été dressées. Le swing normalisé est défini comme :

$$S(t)_{Norm} = \frac{S(t)_{inj} - S(t)_{réf}}{S(t)_{réf}} \qquad (2.9)$$

Avec $S(t)_{réf}$ le swing en condition normale de fonctionnement (1,2V) et $S(t)_{inj}$ le swing lors d'une perturbation. Les cartographies obtenues pour des instants caractéristiques de l'impulsion de tension appliquée à la sonde sont visibles Figure 2.25. Afin de mettre en évidence la distribution spatiale de l'effet d'une EMFI, l'échelle des couleurs de ces cartographies a été limitée à l'intervalle [-1, +1]. Une valeur de +1 correspond à un doublement du swing. Une valeur de -1 à un swing négatif. Par conséquent, les positions en rouge correspondent à des positions pour lesquelles la valeur du swing est au moins doublée et les positions en bleu sont des positions pour lesquelles le swing est négatif.

Sur la Figure 2.25, on peut observer que les chutes ou rebonds du swing les plus importants sont concentrés sous les bords horizontaux (parallèles aux rangées de cellules de la sonde). En outre, les amplitudes maximales de ces variations de swing sont atteintes à t=16ns (Figure 2.25 (d)) avec des valeurs extrémales égales à -1,95V et +4,35V. Partout ailleurs, et en particulier sous le noyau de ferrite, la situation est différente. L'amplitude des chutes et rebonds de Vdd et Gnd y est en effet limitée à -0,2V et +0,2V. Ces variations sont principalement dues à la propagation des perturbations induites dans les segments SegE. La propagation sur l'ensemble du circuit de la perturbation et sa dissipation sont visibles Figure 2.25(e) et (f) qui correspondent à des instants postérieurs à la fin de l'impulsion de tension appliquée à la sonde EMFI.

Un zoom sur la Figure 2.25(d) est visible Figure 2.26. Il montre le coin supérieur gauche de cette cartographie et met en évidence la variation brutale du swing sur de très courtes distances. Ceci est dû, comme nous l'avons montré Figure 2.23, au fait que les fortes variations du swing endurés par les segments SegI et SegO, distants les uns des autres, de 10µm sont de polarité inverse.

Compte tenu des résultats obtenus, on peut conclure que les EMFIs effectuées près de la surface du CI sont finalement assez locales par rapport à la taille de la sonde EM. En effet, elles n'induisent des impacts significatifs que sous les bords de la sonde et ces effets ne se dispersent que faiblement dans le reste du circuit et plus précisément dans les autres segments. Deux raisons peuvent expliquer pourquoi ces chutes et rebonds importants ne se propagent pas très loin du bord de la sonde.

La première raison est liée à la forme de la perturbation EM : l'impact principal est généré par le premier front de l'impulsion (par exemple, un front montant). Toutefois, il est, quelques nanosecondes plus tard, compensé par le second front (par exemple, un front descendant). La Figure 2.25 (a) illustre ce phénomène. Elle montre que la perturbation atteint sa valeur maximale légèrement après la fin du front montant (temps de réponse RC du circuit) et remonte soudainement sous l'impulsion du second front du pulse. Ainsi, si on augmente lentement la valeur de V_{pulse}, pendant une EMFI, on atteint le V_{pulse} minimal requis pour induire une faute tout en limitant au mieux l'amplitude de la dispersion et la zone affectée par le tir.

La seconde raison est en lien avec la structure du réseau d'alimentation. En effet, la perturbation générée dans les segments SegI et SegO se propage nécessairement en suivant le chemin de plus faible résistance. Ce chemin consiste en une remontée sur la partie supérieure du réseau d'alimentation en direction des plots d'alimentation. Une propagation directe le long des rails ou une redescente vers d'autres segments étant plus résistives.

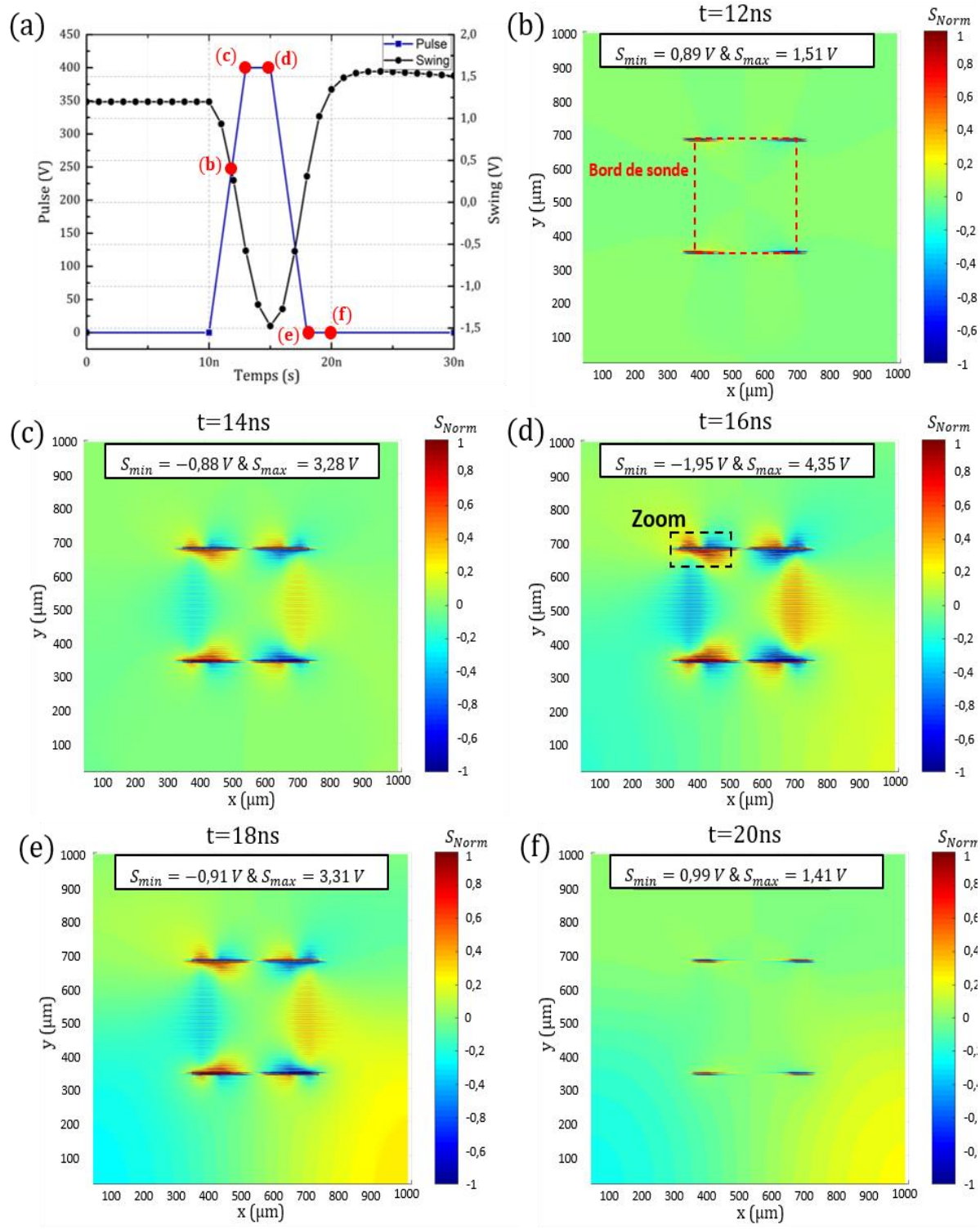


Figure 2.25 - Cartographie de $S(t)_{Norm}$ durant la simulation d'une injection EMFI effectuée avec une sonde proche du circuit et V_{pulse}= 400V, PW = 8ns à différents moments t de l'injection.

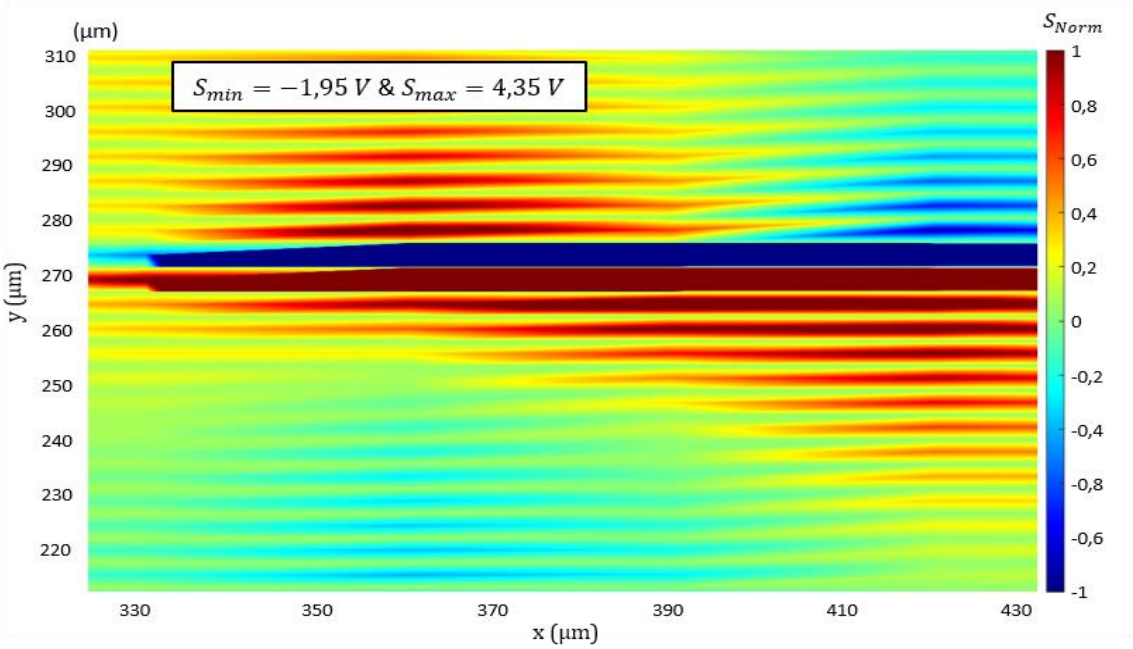


Figure 2.26 - Zoom de la cartographie à t=16ns, sur les perturbations présentes dans un coin du bord de la sonde.

2.4.3.d Simulation d'une EMFI : sonde éloignée du circuit

Pour simuler les EMFIs effectuées à distance de la surface, tous les segments de Std Cell doivent être considérés comme des segments SegE, c'est-à-dire des segments pour lesquels les rails Vdd et Gnd subissent tous deux une fem. Comme représenté dans la Figure 2.27, le secondaire du transformateur utilisé pour modéliser le couplage EM (flèche rose) comporte beaucoup plus d'enroulements que dans le cas précédent. En outre, les coefficients d'inductance mutuelle entre l'enroulement primaire et chaque enroulement secondaire doivent être modifiés pour tenir compte de la distribution normale. Cela peut être fait en ajustant les valeurs de k_{Gi} et k_{Vi} (voir Tableau 1). À cette fin, on note L la longueur d'un segment, l sa largeur et sa position est déterminée par le couple d'indice (i, j) dans la matrice modélisant la surface du CI. De ce fait, les valeurs de k_{Gi} et k_{Vi} sont données par la formule 2.10. Avec (i_c, j_c) qui sont les coordonnées du segment de Std Cell sous le centre de la sonde. σ_i et σ_j sont des rapports de longueur, déterminés avec L_P, la longueur d'un côté de la sonde EM.

$$k_{V/D}(i,j) = \frac{k_{V/D}}{2\ .\ \sigma_i\ .\sigma_j} \exp\left(\frac{(i-i_c)^2}{\sigma_i^2} + \frac{(j-j_c)^2}{{\sigma_j}^2}\right) \qquad (2.10)$$

$$\text{Avec :} \quad \sigma_i = \frac{L_p}{2\ .L_{SC}} \quad \text{et} \quad \sigma_j = \frac{L_p}{2\ .l_{SC}}$$

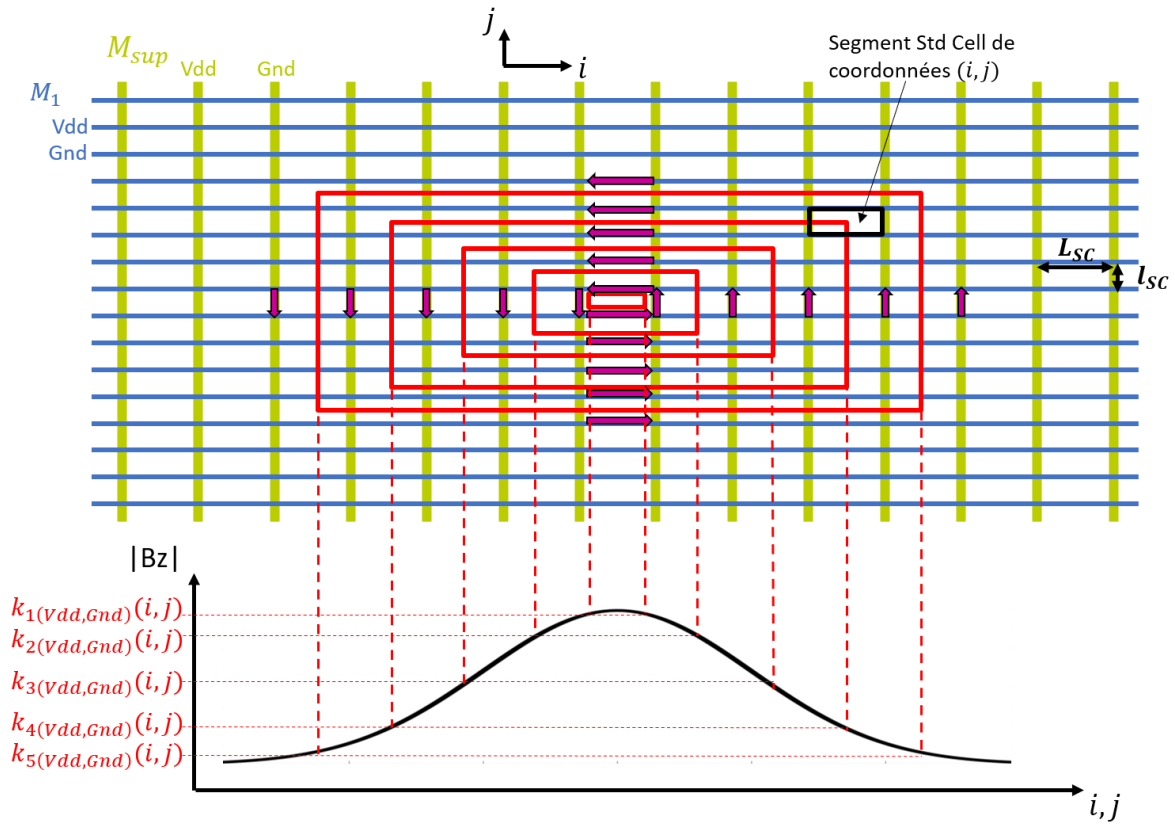


Figure 2.27 - Vue de la surface de l'IC. Application de la loi normale sur Vdd et Gnd, dans le cas d'une sonde éloignée du circuit.

Après ces changements, les simulations sont lancées avec les mêmes paramètres que précédemment. Les résultats sont donnés dans la Figure 2.28 pour différents instants t de l'injection. De même que dans le cas où la sonde est proche du circuit, les variations maximales du swing se situent sur les bords supérieurs et inférieurs de la sonde. Cependant, les perturbations sont moins importantes sous les bords gauche et droite de la sonde, et au contraire, des variations apparaissent sous le noyau de la ferrite. Cela s'explique par le fait que les dérivés de la loi normale prennent de fortes valeurs au voisinage de σ. C'est pourquoi les variations de tension induites par les EMFIs sur les rails Vdd et Gnd compris dans cette zone, sont très différentes d'un segment à un autre et résultent à des fluctuations importantes du swing.

À t=18ns, on observe les valeurs de minimales et maximales du swing : S_{min}= -0,05V et S_{max}=2,35V. Les variations de swing sont donc moins importantes dans ce cas que dans celui d'une EMFI effectuée avec la sonde à proximité de la surface. Néanmoins, un swing proche de 0V reste suffisant pour induire des fautes dans un circuit. Ces simulations montrent ainsi que, même en champ éloigné, l'effet de l'EMFI reste assez local.

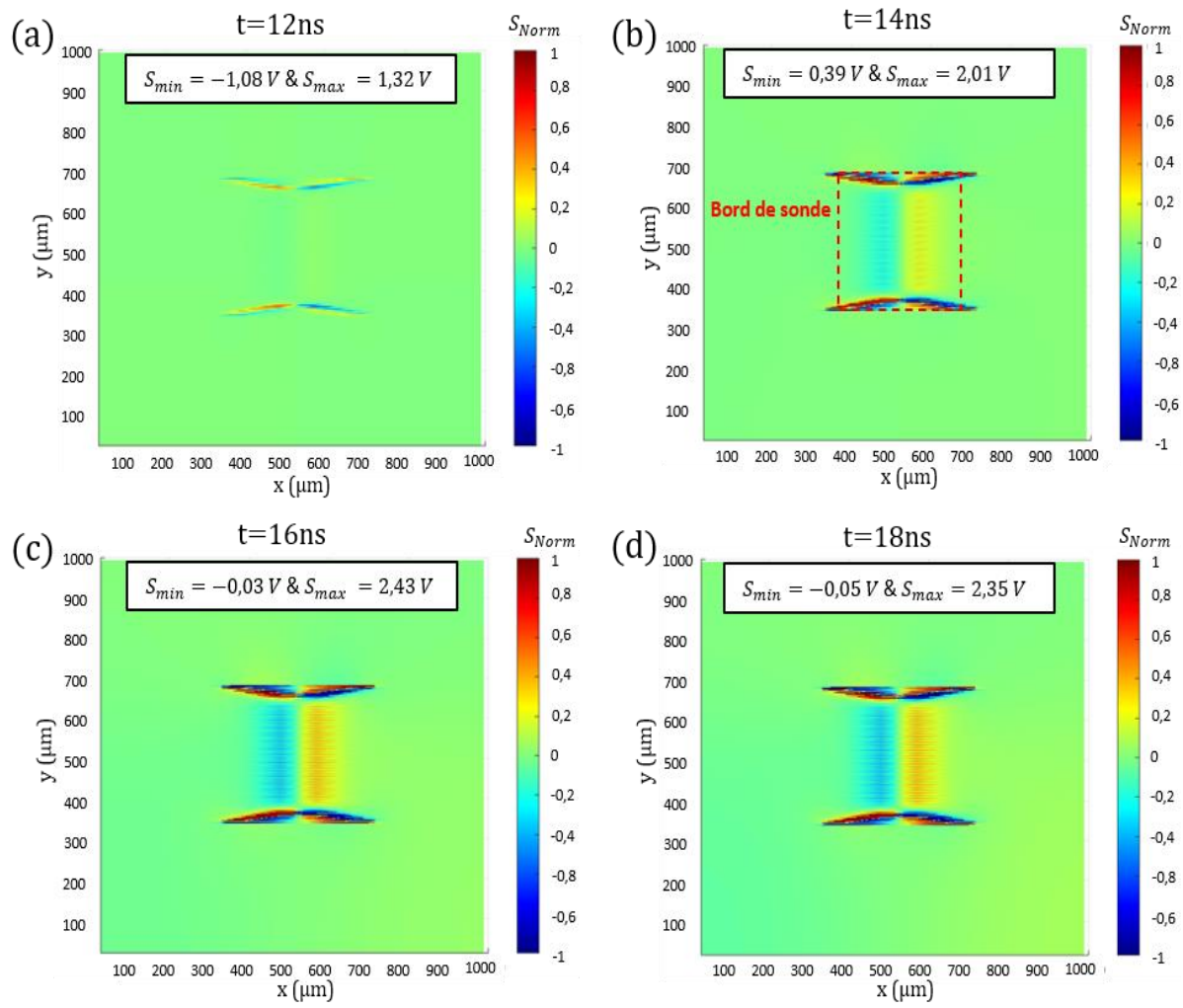


Figure 2.28 - Cartographie de $S(t)_{Norm}$ durant la simulation d'une injection EMFI effectuée avec une sonde éloignée du circuit et V_{pulse}= 400V, PW = 8ns, à différents moments t de l'injection.

2.4.3.e Analyse des variations de swing

Après avoir analysé la distribution spatiale des effets d'une EMFI sur le réseau d'alimentation des CI, des analyses paramétriques ont été menées afin d'étudier les liens entre V_{pulse} et PW sur les caractéristiques des variations de swing induites sous les bords de la sonde.

Les évolutions temporelles de S(t) pour différentes valeurs de l'amplitude V_{pulse} de l'impulsion de tension (pour PW=8ns) sont données Figure 2.29. Les valeurs considérées pour V_{pulse} sont comprises entre -400V à +400V avec un pas de 100V. Selon la polarité de l'impulsion S(t) endure une chute ou un rebond. Cependant, les variations sont totalement symétriques. En effet, à V_{pulse}= ±400V, on peut mesurer S = +5,1V et S = -2,7V,

mais ΔS = ±3,9V, dans les 2 cas (voir Tableau 3). De même, les pentes des swings sont toujours égales, ceci étant lié aux pentes constantes du pulse quel que soit le V_{pulse}.

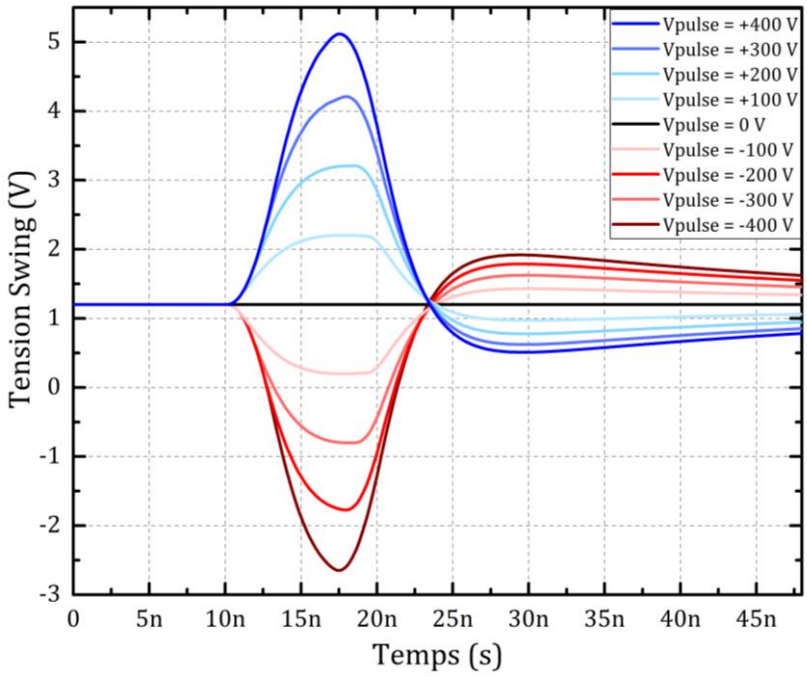


Figure 2.29 – Courbes des variations du swing en fonction du V_{pulse}.

Tableau 3 - Résultats des variations du swing ΔS en fonction de la tension du pulse V_{pulse}.

$\pm V_{pulse}$ (V)	$\pm \Delta S$ (V)
400	3,9
300	3
200	2
100	1

La Figure 2.30 présente l'évolution du swing avec la largeur de pulse PW (V_{pulse}= -300V). Les valeurs considérées pour PW s'étalent entre 6 et 50ns. Ces courbes nous permettent de mettre en évidence le rôle des fronts de l'impulsion de tension. Le premier front provoque une chute du swing alors que le second provoque sa remontée (ou l'inverse si V_{pulse} est positif). Nous verrons dans le chapitre suivant que cette remontée rapide sera cruciale à l'induction d'une faute dans le circuit. Pour PW<10ns, on voit cet effet, mais on peut également remarquer que le second front provoque la remontée du swing avant même qu'il ait pu atteindre sa valeur ΔS maximale atteinte pour PW=10ns. En outre, pour PW >10ns, le swing entame une remontée naturelle vers sa valeur d'origine avant

l'arrivée du second front. Cette lente remontée a une pente qui dépend des caractéristiques RC du circuit. Le Tableau 4 montre comment la largeur S_{width} influe sur la chute de swing mesurée à S=1,2V. Comme on peut le constater l'évolution est linéaire.

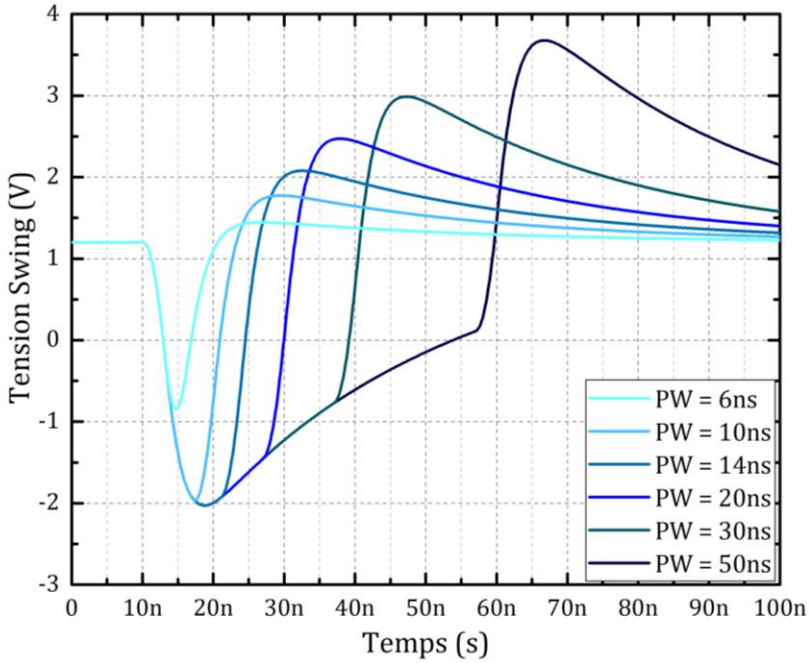


Figure 2.30 – Évolutions de S(t) pour différentes largeurs PW de l'impulsion de tension appliquée à la sonde EMFI.

Compte tenu de ces résultats, on peut conclure qu'il existe une valeur optimale de PW, ayant une chute et une remontée rapide tout en atteignant sa valeur maximale. Celle-ci vaut 10ns dans notre cas. Elle correspond à la création de la chute de swing ayant la durée minimale mais atteignant toutefois l'amplitude maximale.

Tableau 4 - Résultats des variations de la largeur du swing S_{width} en fonction de la largeur pulse PW.

$\boldsymbol{PW}$ **(ns)**	$\boldsymbol{S_{width}}$ **(ns)**
6	10,63
10	13,27
14	16,4
20	21,53
30	30,7
50	59,6

2.5 Conclusion

Les travaux de simulation et de modélisation de l'effet d'une EMFI sur l'alimentation d'un circuit, ont apporté de nombreux éléments de compréhension sur l'EMFI.

Les premières expérimentations, bien que peu concluantes, ont permis d'identifier le problème relatif à la propagation sur une large distance des impulsions EM. Celui-ci se traduit par la perturbation des équipements de mesure utilisés mais également des fils de bonding. Une attention particulière doit être portée sur ces derniers, dès la conception de la puce de test, pour garantir des résultats expérimentaux fiables, lors d'EMFI.

Ces précautions prises pour fabriquer de nouvelles puces de test, une étude approfondie de leur layout et de la structuration des différents rails de métallisation a permis de déterminer les éléments clés intervenant dans le couplage d'une sonde avec un circuit. Il a été ainsi démontré que les alimentations Vdd et Gnd sont les plus susceptibles aux EMFI et de manière générale aux variations du champ magnétique environnant.

Ces éléments clés identifiés, des travaux de modélisations ont pu être menés. Ils ont porté, dans un premier temps, sur le couplage entre une sonde EM et le réseau d'alimentation des circuits. Les travaux se sont ensuite concentrés sur la modélisation de la charge de ce réseau d'alimentation constituée par les portes logiques et les cellules de découplage. Ceci a permis d'aboutir à une modélisation complète du processus d'EMFI.

L'exploitation de ce modèle a prouvé qu'une impulsion EM induit des variations de tension sur les rails d'alimentation, conduisant à des rebonds et des chutes du swing (Vdd(t)-Gnd(t)) qui sont maximaux sous les bords des sondes EMFI et ce, que cette dernière soit proche ou éloignée du circuit. Ce résultat a montré que l'EMFI est finalement, beaucoup plus locale que nous le pensions et les caractéristiques de l'impulsion de tension appliquée à la sonde EM peuvent être réglées pour améliorer la localité d'une EMFI sans en réduire l'effet. Sachant ceci, une bonne connaissance du layout ainsi qu'une configuration correcte de la sonde et du pulse permettent d'induire des fautes avec une meilleure précision spatiale lors d'une EMFI.

Bien que l'ensemble de notre modèle soit étayé par des mesures expérimentales dans le chapitre suivant, une confirmation corroborant ces premières analyses seraient idéales. Les mesures analogiques directes étant impossibles ou, en tout état de cause, peu fiables, les mesures de tension des grilles d'alimentation réalisées grâce à des oscillateurs en anneaux semblent un bon compromis.

Chapitre 3 . Modélisation de l'impact d'une EMFI sur le fonctionnement d'un CI synchrone

Lors d'une attaque par injection de faute, quelle que soit la technique d'injection utilisée, les fautes générées lors de l'opération d'un circuit synchrone sont souvent considérées comme des fautes de timing. Or, des expérimentations EMFI ont montré qu'un autre type de fautes peut être induit, les fautes d'échantillonnage.

Dans ce contexte, l'un des objectifs de cette thèse est de comprendre le phénomène d'apparition de fautes lors d'une EMFI et plus largement de le modéliser. En s'appuyant sur les résultats précédents, ce chapitre a pour but d'étendre la modélisation de l'EMFI lorsque celle-ci est effectuée pendant l'opération synchrone d'un CI et plus particulièrement lors de l'opération d'échantillonnage d'une bascule D. C'est pourquoi, un rappel sur le fonctionnement des bascules est d'abord donné, pour ensuite être appliqué lors de simulation d'EMFI sur un circuit logique. Enfin, les résultats obtenus lors de cette étude seront confrontés à des mesures expérimentales afin de confirmer la validité de la modélisation proposée.

Les travaux présentés dans ce chapitre ont fait l'objet de deux publications : une dans la conférence FDTC (Fault Diagnosis and Tolerance in Cryptography) et l'autre dans la conférence EMC COMPO (Electromagnetic Compatibility of Integrated Circuits).

3.1 La bascule, base de la logique séquentielle

Dans la majorité des circuits intégrés, les échanges de données entre les différents blocs sont synchronisés par un signal d'horloge (H ou CLK). On parle alors de circuits synchrones (ou circuits séquentiels). Ce signal d'horloge est généralement distribué dans l'ensemble du circuit via l'arbre d'horloge comme décrit dans la partie 2.1.2. C'est ce signal qui fixe la fréquence de fonctionnement et donc le nombre d'opérations qu'il peut exécuter par unité de temps. Les calculs d'un circuit synchrone sont effectués par des portes logiques intercalées entre les registres. En règle générale, ces registres sont composés de bascules.

3.1.1 Les bascules dans un circuit synchrone

La Figure 3.1 montre la composition classique d'une partie de circuit synchrone, comprenant deux bascules ou registres (plusieurs bascules en parallèle). Entre les bascules se trouve un chemin logique (ou bloc logique) constitué de portes logiques combinatoires. Le bloc nommé 'chemin d'horloge' représente le morceau d'arbre d'horloge acheminant le signal d'horloge à ces deux bascules ou registres. Ces derniers assurent et cadencent les échanges de données entre les divers blocs logiques des circuits et permettent donc la conception de circuits séquentiels.

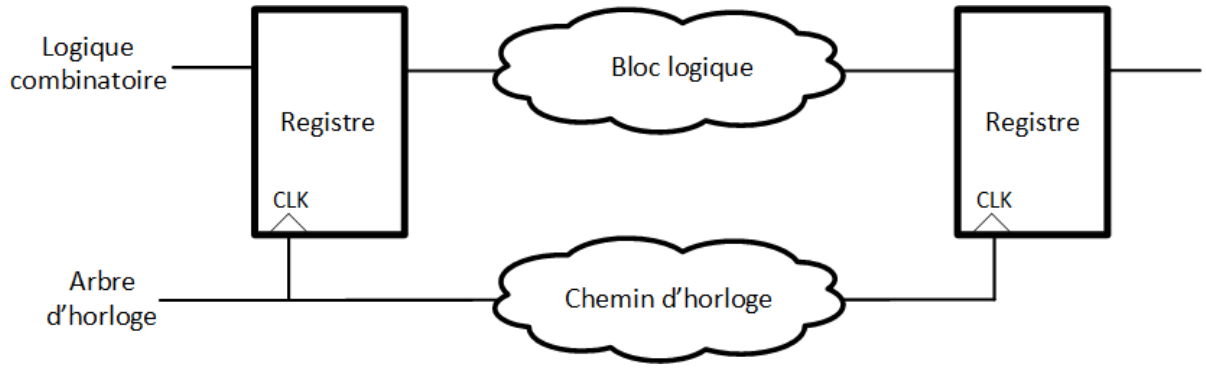


Figure 3.1 – Morceau d'un circuit synchrone.

Les bascules synchrones que l'on trouve dans les circuits synchrones ont une triple fonction : la mémorisation, la synchronisation et la stabilisation. Suivant la fonctionnalité de la bascule, il peut exister différents types de synchronisations (Figure 3.2) :

- Synchronisation sur un niveau : il suffit d'appliquer le niveau convenable sur l'horloge (niveau haut ou bas), appelé niveau actif, pour que l'état de sortie de la bascule puisse changer d'état à tout moment, tant que le niveau actif est appliqué. On parle alors de « latch » ou verrou et non pas de bascule.

- Synchronisation sur les fronts : le changement d'état de la bascule ne se fait que lors de l'occurrence de fronts. La sortie de la bascule ne change pas d'état pendant un niveau (haut ou bas) de l'horloge, et ce, même si l'entrée de la bascule varie. On parle alors de bascules D-Flip-Flop. Elles peuvent être actives sur front montant (cas usuel), ou sur font descendant ou bien les deux.

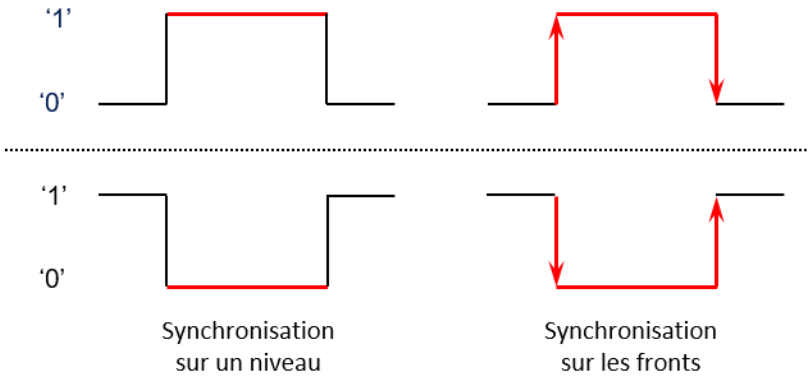
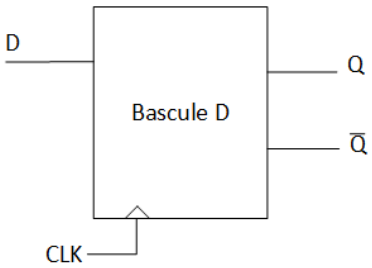


Figure 3.2 - Différents types de synchronisation.

3.1.2 Bascule D : fonctionnement et contraintes de temps

La bascule D, ou bien DFF pour D-Flip-Flop, représentée Figure 3.3, est l'élément fondamental de la logique synchrone d'un circuit intégré, c'est également celle que l'on retrouve en plus grand nombre dans ces circuits. Sa table de vérité est simple, à chaque front montant d'horloge, son entrée D est recopiée sur sa sortie Q. Sur les états stables de signal d'horloge, elle maintient sa valeur de sortie malgré d'éventuels changements sur son entrée.

(a)



(b)

CLK	D	Q
0	X	Q (inchangé = mémorisation)
↑	0	0 (reset)
↑	1	1 (set)

Figure 3.3 - (a) Symbole logique (b) et table de vérité, d'une bascule D.

Lors de sa mise sous tension, la sortie de la bascule DFF prend une valeur inconnue (soit '0', soit '1'). C'est pourquoi il est nécessaire d'initialiser les bascules DFF. Les bascules DFF possèdent donc en général une entrée supplémentaire (entrée Set ou Reset), asynchrone ou synchrone, pour initialiser la sortie Q à '1' ou à '0'. Toutefois, pour faciliter la

compréhension du fonctionnement des bascules DFF, nous nous limitons dans ce document à étudier une DFF simple (sans Set ou Reset).

La Figure 3.4 donne le chronogramme du fonctionnement normal d'une DFF dans le cas d'une transition de '0' vers '1' de la sortie. Les entrées D et CLK y sont représentées ainsi que sa sortie Q. Comme on peut le constater, au front montant du signal d'horloge, la bascule copie la valeur présente sur D sur Q. La durée de cette opération qui commence à l'arrivée du front montant de l'horloge est appelée temps de propagation de D vers Q. Ce temps de propagation est en général noté CK2Q. Il est matérialisé par la flèche (3) Figure 3.4. Les flèches (1) et (2) matérialisent quant à elles les temps d'établissement (ou de setup) et de maintien (ou hold) de la bascule. Ces trois grandeurs sont définies ci-après.

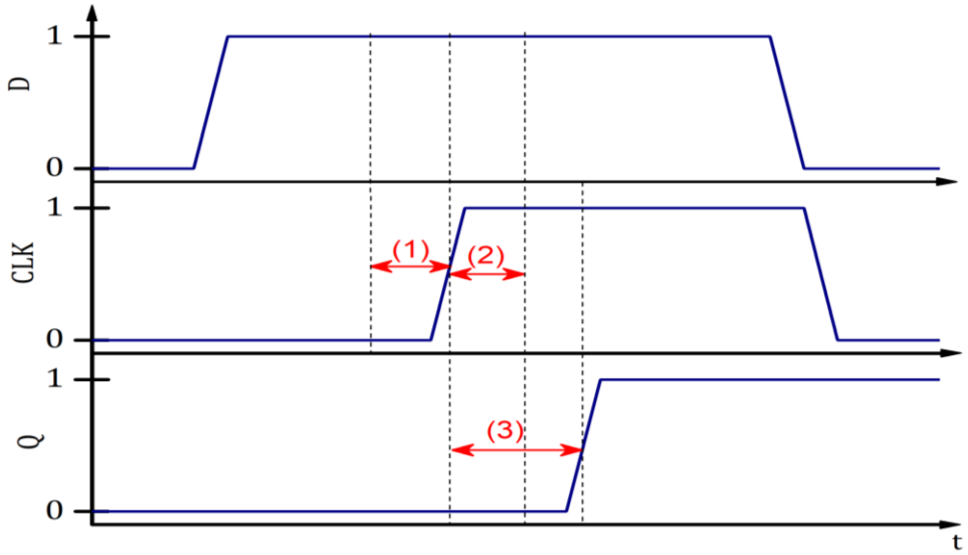


Figure 3.4 - Fonctionnement normal de la bascule DFF.

- Temps de propagation (CK2Q) : c'est le temps mis par la bascule pour recopier D sur Q. Il est mesuré comme le temps s'écoulant entre le passage du signal d'horloge à 0.05V et le passage de Q à Vdd/2.
- Temps d'établissement (ou de setup : t_{setup}) : c'est l'intervalle de temps minimum qui doit séparer l'arrivée du front montant de l'horloge, de l'arrivée d'une donnée D pour que la bascule copie effectivement D sur Q. Pendant cette durée, l'entrée D doit être stable.
- Temps de maintien (ou de hold : t_{hold}) : c'est l'intervalle de temps minimum durant lequel la donnée D doit rester stable après le front montant de l'horloge pour que la bascule copie effectivement D sur Q.

Un schéma fonctionnel d'une DFF est donné par la Figure 3.5. Elle est constituée de deux verrous Maîtres et Esclaves, l'un permettant l'échantillonnage de la donnée D et

l'autre le maintien de Q. Le signal externe CLK est divisé par deux inverseurs en deux signaux de commande internes et complémentaires : CPI et CPN. CPI est une recopie de CLK retardée d'un délai égal au délai de propagation des deux inverseurs. CPN est le complément de CLK retardé d'un délai égal à celui du premier inverseur. Ces retards entre CPI et CPN, comme expliqués ultérieurement dans ce chapitre, ont une grande importance dans l'occurrence de fautes EM. Ces deux signaux internes d'horloge commandent quatre portes dites portes tri-state ou pass-gate (notées PG). Une pass-gate se comporte comme un interrupteur inverseur ouvert ou comme un interrupteur inverseur fermé selon la valeur de ses deux signaux de commande devant être complémentaires pour un fonctionnement correct.

Lorsque CLK est à l'état bas (Figure 3.5 (a)), les portes tri-state PG_1 et PG_4 sont passantes, tandis que PG_2 et PG_3 sont bloquées. La boucle (verrou) esclave est donc fermée et assure le maintien de la valeur Q (flèche bleue). Pendant ce temps, la donnée D peut pénétrer dans l'étage maître (flèche verte) qui est isolé de l'esclave par le tri-state, PG3 se comportant comme un interrupteur ouvert.

Lorsque le front montant de l'horloge arrive (Figure 3.5 (b)), celui se propage à travers les deux inverseurs et vient ouvrir l'interrupteur PG1 et fermer l'interrupteur PG3 (Ce délai T1 d'ouverture et de fermeture de ces interrupteurs fixe en partie la valeur de t_{setup} qui est au premier ordre égal au délai de propagation de D jusqu'à PG3 moins T1). La donnée, qui est alors mémorisée par le verrou maître se propage alors jusqu'à Q (flèche verte) en temps CK2Q égal au la somme des délais de propagation de PG1 et PG3. On notera que PG_1 étant bloquée, un changement d'état de D n'influe pas sur la valeur mémorisée (flèche bleue) par le verrou maître.

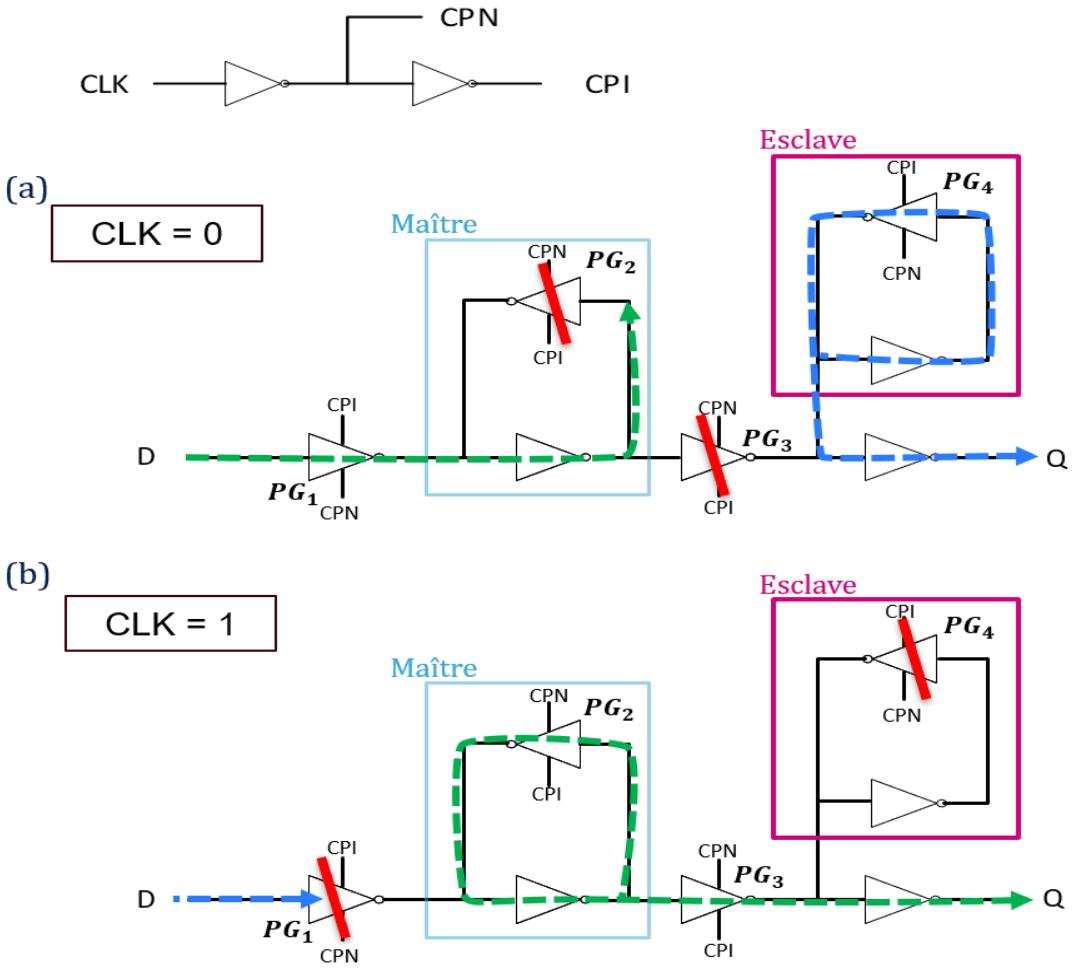


Figure 3.5 - Structure interne et fonctionnement d'une DFF à (a) CLK = 0 et (b) CLK = 1.

3.1.3 Principe de fonctionnement des CIs synchrones

Le schéma classique utilisé pour expliquer le fonctionnement d'un circuit synchrone est donné Figure 3.6. Il comprend deux bascules (ou registres), séparées par un chemin logique (ou un bloc logique).

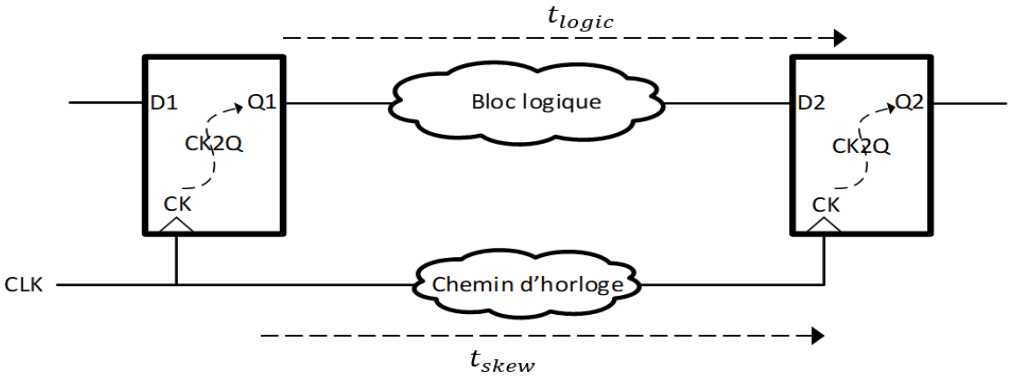


Figure 3.6 - Représentation d'un bloc logique entre deux bascules.

Comme représenté dans la Figure 3.7, un signal d'horloge, de période T_{CLK}, cadence le fonctionnement du chemin logique en commandant les deux bascules (registres). Compte tenu que les données en entrée des deux bascules doivent être établies et stables t_{setup} picosecondes avant le front d'horloge et maintenues stables t_{hold} picosecondes après celui-ci, le temps de propagation du chemin doit respecter deux contraintes dites contraintes de setup et de hold. Ces contraintes s'expriment sous la forme des deux inéquations suivantes :

$$CK2Q_1 + t_{logic} \leq T_{CLK} - t_{setup2} + t_{skew} \quad (3.1)$$

$$CK2Q_1 + t_{logic} \geq t_{hold2} + t_{skew} \quad (3.2)$$

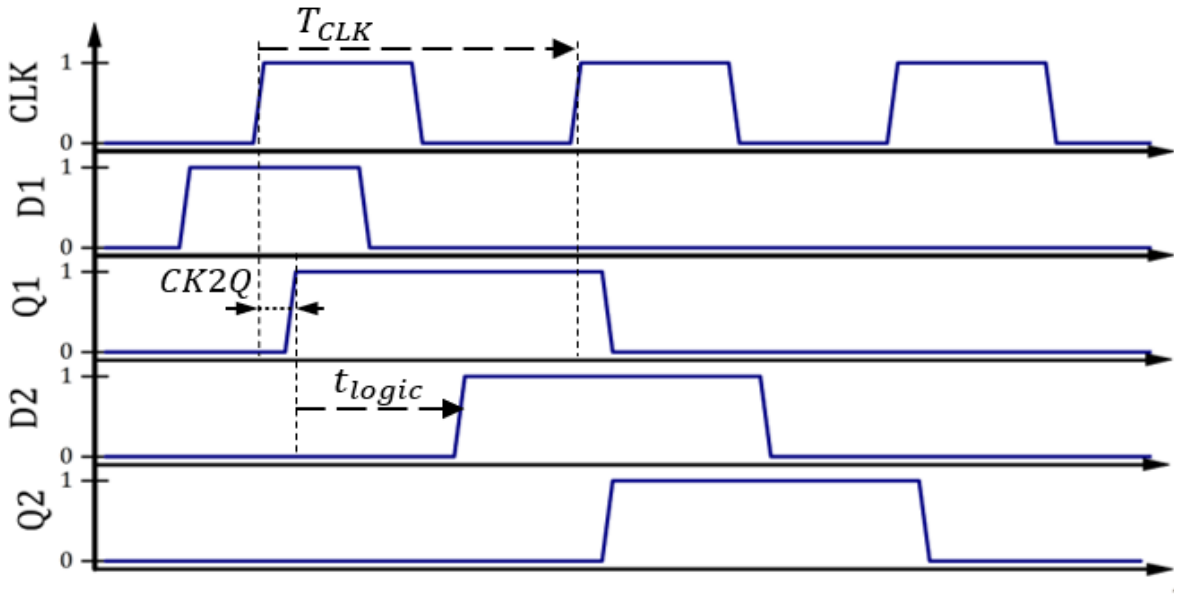


Figure 3.7 - Chronogramme du fonctionnement logique entre deux DFFs.

La première inéquation, appelée contrainte de setup, stipule que le temps de propagation de la donnée D, en entrée de la première bascule, jusqu'à la sortie du chemin logique doit être inférieur à la période d'horloge moins le temps de setup, au décalage t_{skew} près des temps d'arrivée de l'horloge à l'entrée des deux bascules, de sorte à être correctement échantillonnée par la seconde bascule au prochain front d'horloge.

La seconde inéquation, appelée contrainte de hold, stipule que le temps de propagation de la donnée D, en entrée de la première bascule, jusqu'à la sortie du chemin logique doit être supérieur au temps t_{hold} plus la différence des temps d'arrivée des deux bascules, de sorte à ne pas écraser la donnée présente à l'entrée de la seconde bascule et donc permettre son échantillonnage correct par celle-ci.

Pour éviter l'occurrence de fautes de timing, les concepteurs font en sorte que ces contraintes soient vérifiées pour tous les chemins logiques du circuit dans les pires et meilleures conditions PVT (Process, Voltage, Temperature) pour les temps de propagation. Ces pires et meilleures conditions PVT coïncident à des délais de propagation statistiquement peu probables. Cette approche pire et meilleur cas introduit des marges de timing extrêmement importantes dépassant souvent 50% de la valeur moyenne en technologie CMOS avancée.

3.2 Simulation d'EMFI sur CI synchrone

En s'appuyant sur les résultats obtenus dans le chapitre précédent, une modélisation de l'effet d'une EMFI sur le fonctionnement des CIs synchrones est proposée dans les sections qui suivent. Cette modélisation et la méthodologie de simulation associée permettent de mieux comprendre comment une faute est induite dans un CI lors d'une EMFI.

3.2.1 Présentation des conditions de simulation

Compte tenu du modèle de faute EM établi dans [63], l'étude de l'effet d'une EMFI sur le fonctionnement des CIs synchrones a été conduite par simulation sur le circuit représenté sur la Figure 3.8. Il s'agit d'une structure commune que l'on trouve des milliers de fois dans un CI synchrone. Il représente la fin d'un chemin logique, ou cône logique amont, arrivant à l'entrée d'une DFF et un chemin logique, ou cône logique aval, alimenté par cette bascule. La bascule est commandée par un morceau d'arbre d'horloge.

Les cônes logiques amont et aval sont modélisés par une chaîne de vingt inverseurs. Le morceau d'arbre d'horloge est lui modélisé par quatre inverseurs. En général, les portes logiques des cônes logiques ont un « drive » plus faible que les inverseurs et buffer de l'arbre d'horloge. Le drive d'une porte représente sa capacité à fournir du courant et donc à piloter une charge capacitive plus ou moins importante. Le drive d'une porte est en général quantifié grâce aux termes x0.5, x1, x2, x4, …, x16. Ainsi, une porte inverseuse INVx8 réalise exactement la même fonction logique que la porte INVx4 mais délivre 2 fois plus de courant. On constate donc que la porte INVx1 est donc prise comme référence de courant et l'on obtient une porte INVx8 à partir de celle-ci en multipliant la taille de ses transistors N et P par 8 (ou en parallélisant 8 transistors de même taille). Ainsi, dans les simulations, les inverseurs de l'arbre d'horloge ont un drive x24 et les inverseurs des cônes logiques un drive x3. La capacité C_D représente la charge présente à la

sortie du cône logique amont (portes logiques connectées à ce nœud et routage). La capacité C_{CLK} est la charge à la sortie du morceau d'arbre d'horloge (autres bascules et routage).

Le circuit considéré étant petit, on peut supposer que ses éléments (en particulier la DFF et quelques inverseurs en amont et en aval ainsi que le dernier étage de l'arbre d'horloge) sont placés et routés dans une zone réduite du CI et sont donc polarisés de la même manière. Par conséquent, si une EMFI induit une perturbation dans cette zone, celle-ci affecte tous les éléments du circuit.

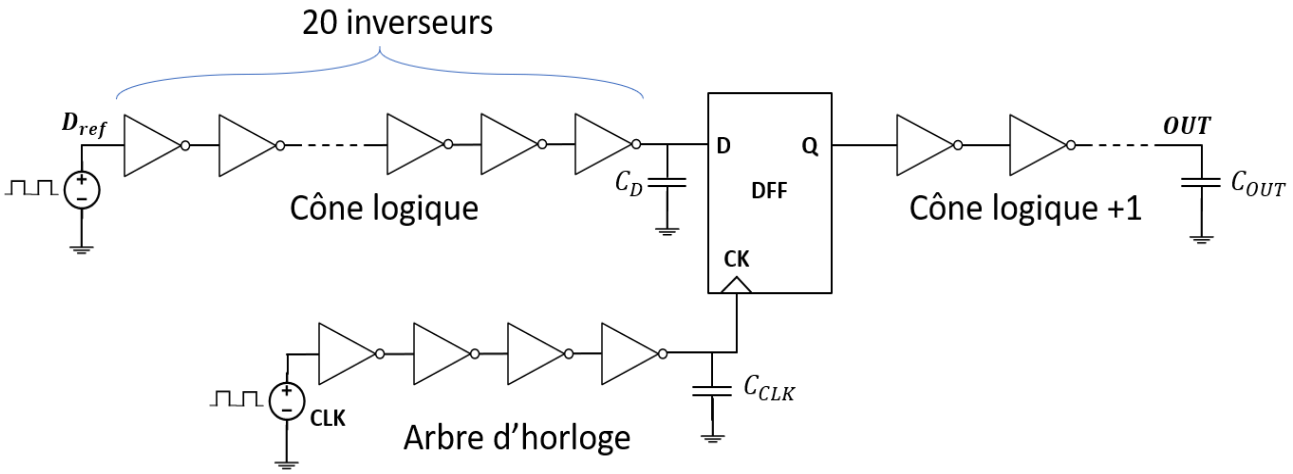


Figure 3.8 - Circuit considéré pour analyser l'impact d'une EMFI sur le fonctionnement de CIs synchrones en simulation.

Le chronogramme de la Figure 3.9 donne le comportement du circuit dans des conditions normales de fonctionnement. Conformément au modèle de faute d'échantillonnage stipulant que les fautes EM induites ne sont pas seulement des fautes de timing, nous avons considéré le signal D_{ref} stable à la valeur logique '1' (ou '0') (depuis plus d'une période d'horloge) de sorte que les fautes apparaissant lors de la simulation ne puissent être des fautes de timing mais soient bien des fautes d'échantillonnage. Ces précautions prises, le comportement du circuit avant et après le front montant du signal d'horloge a été observé. Les simulations ont été réalisées pour une transition du signal Q de '0' vers '1' (bitset) mais également de '1' vers '0' (bitreset) avec initialisation de Q à '0' ou '1' selon le cas considéré. Les délais de propagation de CK2Q, Q2OUT et CK2OUT ont été mesurés dans les conditions normales de fonctionnement. Leur valeur sont respectivement de 100ps, 190ps et 290ps respectivement.

Le temps de propagation du signal dans la bascule est mesuré entre CP (signal d'horloge interne de la DFF) et Q à V=0,6V, définis par CK2Q. On définit également le

temps de propagation du signal Q à OUT par CK2OUT. En conditions normales, ces temps sont CK2Q = 100ps et CK2OUT = 290ps.

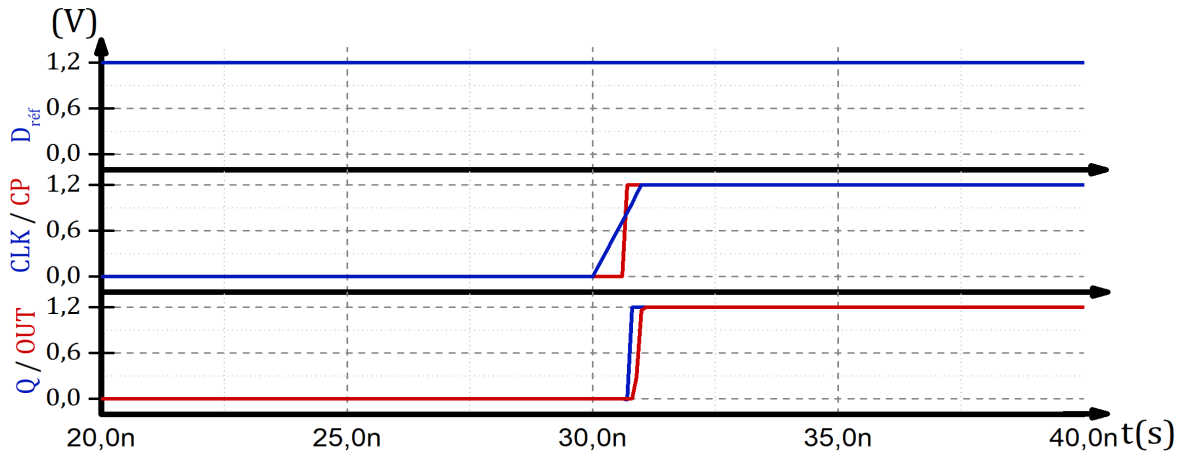


Figure 3.9 - Chronogramme des signaux de base du circuit simulé.

Dans le but de simuler l'effet d'EMFIs sur le fonctionnement de ce circuit, les chutes de swing observées en section 2.4.3 ont été introduites dans la simulation en utilisant un générateur de tension adéquat (V_{PWL}). Au cours des simulations réalisées, nous avons fait varier l'instant auquel la variation de swing s'achève (retour à Vdd=1,2Vde S(t)) de sorte à balayer un large intervalle de temps autour du front montant. L'instant auquel s'achève la perte de swing a été nommé E. En prenant le début du front d'horloge comme référence temporelle, cela nous a conduit à définir le paramètre CK2E, qui est le temps séparant la fin de la chute de swing de la montée du front d'horloge.

Ce paramètre peut bien sûr prendre des valeurs négatives et des valeurs positives comme illustré Figure 3.10. Figure 3.10(a) la chute de swing s'achève avant la montée du front d'horloge et CK2E vaut -5,4ns tandis que Figure 3.10(b), elle s'achève après et CK2E vaut +4,3ns. Lors de nos simulations, nous avons fait varier CK2E dans l'intervalle [-5ns,+5ns]. En outre, les simulations effectuées l'ont été pour diverses valeurs de ΔS, l'amplitude de la chute de swing et de S_{width} sa largeur. Enfin, les simulations ont également été effectuées pour différentes valeurs de la tension nominale Vdd du circuit.

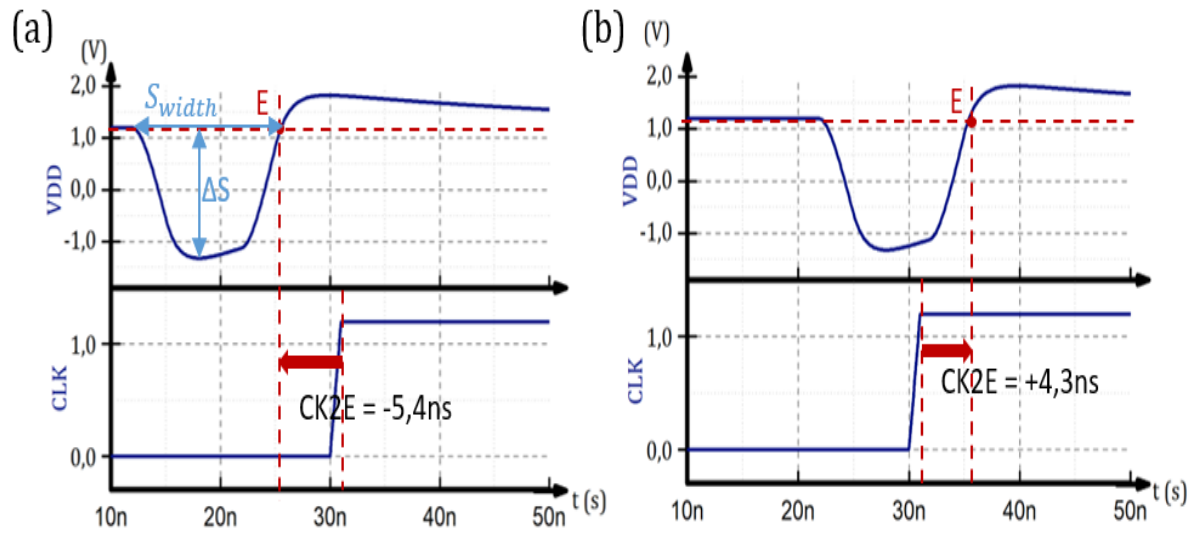


Figure 3.10 - Balayage de la chute de swing autour du front d'horloge et définition de CK2E.

3.2.2 Critère de faute F

Parce que nous avons prévu d'explorer l'effet de nombreux paramètres liés soit au paramétrage de l'EMFI, soit à celui du circuit, deux figures de mérite, FQ et FOUT, ont été établies pour estimer rapidement l'effet d'une EMFI sur le fonctionnement du circuit. Elles sont définies comme suit :

$$F_Q = \frac{CK2Q|_{réf}}{CK2Q|_{EMFI}} \tag{3.3}$$

$$F_{OUT} = \frac{CK2OUT|_{réf}}{CK2OUT|_{EMFI}} \tag{3.4}$$

avec $CK2Q|_{réf}$ et $CK2OUT|_{réf}$ les délais de propagation dans les conditions normales de fonctionnement, et $CK2Q|_{EMFI}$ et $CK2OUT|_{EMFI}$ les délais de propagation en présence d'une perturbation. Ces définitions permettent de différencier plusieurs effets de l'EMFI :

- $F > 1$: l'EMFI accélère la propagation de D à Q (OUT),
- $F = 1$: l'EMFI n'a pas d'effet sur le fonctionnement du CI.
- $0 < F < 1$: l'EMFI ralentit la propagation de D à Q (OUT), ce qui peut induire des fautes de timing au prochain front d'horloge au niveau des bascules en aval du chemin,
- $F = 0$: $CK2Q(OUT)|_{EMFI} \rightarrow \infty$. D n'est pas échantillonné par la bascule. Q reste à '0' (ou '1'). Cela correspond à l'apparition d'une faute d'échantillonnage.

Ainsi, lors des simulations et ce pour chaque valeur de CK2E, les délais de propagation et les critères F_Q et F_{OUT} sont calculés. De la sorte, on peut mettre en valeur l'effet des EMFIs sur le fonctionnement du circuit.

3.3 Effet d'une EMFI sur un CI synchrone

Cette partie décrit les résultats des simulations qui ont été effectuées et analyse les effets possibles d'une EMFI sur le fonctionnement d'un CI synchrone.

3.3.1 Apparition des fautes d'échantillonnage

Au cours des simulations qui ont été réalisées pour estimer l'effet d'une EMFI sur les réseaux Vdd et Gnd, il a été observé que l'amplitude des chutes et montées de swing était proportionnelle à V_{pulse}, un paramètre clé lors de la réalisation de véritables EMFIs. Cela explique pourquoi, en simulation, l'effet de ΔS, l'amplitude de la chute de swing, sur l'occurrence des fautes a été analysée en premier lieu.

3.3.1.a Cas d'une transition de l'état '0' vers '1'

Dans un premier temps, le cas d'une transition de '0' vers '1' en sortie de la bascule a été étudié. Il correspond à un bitset de la DFF. La variation de swing considérée lors de cette étude est celle d'une chute de la tension Vdd à une valeur inférieure à celle de Gnd, comme illustrée Figure 2.24 (a).

La Figure 3.11 donne les évolutions avec CK2E des critères F_Q et F_{OUT} dans le cas d'une chute de swing d'amplitude ΔS et de durée S_{width}=10,9ns. Deux cas peuvent être observés. Pour ΔS ≤ 0,96V (courbes bleues), l'amplitude de la chute de swing n'est pas assez importante pour que le swing prenne une valeur négative. Par conséquent F_Q et F_{OUT} n'atteignent jamais 0 et l'EMFI ne fait qu'altérer les délais de propagation. Plus précisément, il force une copie anticipée (pour F>1) ou retardée (pour F<1) de D sur Q, selon la valeur de CK2E. Au pire, quand ΔS=0,6V, F_Q atteint une valeur de 0,1. Une telle valeur signifie que le délai CK2Q est multiplié par 10. Quant à F_{OUT} il atteint 0,4 pour ΔS=0,95V, ce qui correspond à une multiplication par 2,5 de CK2OUT.

Ces valeurs impliquent qu'une faute de timing peut se produire (en fonction de la période d'horloge et des marges de temps considérées pour tenir compte des variations PVT) au prochain front d'horloge dans une bascule en aval du chemin logique.

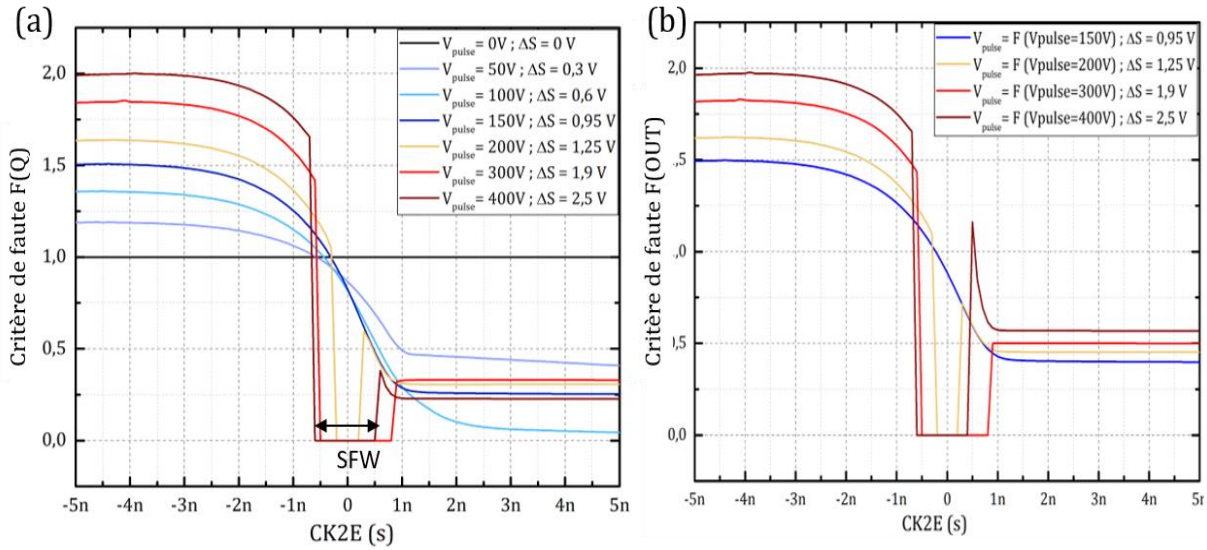


Figure 3.11 - (a) F(Q) et (b) F(OUT) à différentes valeurs de ΔS, dans le cas d'une transition de '0' vers '1'.

Toutefois, de telles valeurs doivent être considérées avec prudence. En effet, dans nos simulations, nous supposons que l'ensemble des éléments du circuit subissent exactement la même perturbation. Il s'agit là d'une situation pire cas, car il est extrêmement peu probable que l'ensemble des éléments (ici, la bascule et les 40 inverseurs des cônes amont et aval) soient placés et routés dans un seul segment Std Cell, c'est-à-dire, dans notre cas, une zone de 30µm x 5µm. En effet, pour une densité d'intégration typique de 60% on peut trouver entre 50 et 150 portes logiques dans un segment. Ces portes logiques sont généralement impliquées dans différents chemins logiques. Il est donc plus probable que certaines portes de notre chemin subissent une chute de swing tandis que d'autres subissent une chute de swing plus modérée, voire une montée de swing, en fonction de leur placement.

Pour ΔS = 1,25V, 1,9V et 2,5V (courbes rouges et oranges), l'amplitude de l'impulsion EM est suffisante pour que le swing devienne temporairement négatif. Par conséquent, l'EMFI perturbe (gèle) le fonctionnement de la DFF et F_Q et F_{OUT} sont égaux à 0 pour un ensemble de valeurs de CK2E. Ceci signifie que des fautes d'échantillonnage sont induites. Ces valeurs de CK2E forment une fenêtre temporelle, appelée fenêtre de fautes d'échantillonnage (SFW pour Sampling Faults Window) par la suite, dans laquelle une EMFI doit être effectuée pour induire une faute d'échantillonnage. On peut observer que la durée des SFW augmente avec V_{pulse}. En effet pour V_{pulse}=200V on obtient une fenêtre de largeur égale à 0,4ns alors que pour V_{pulse}=400V la largeur est de 1,12ns. Pour ce type de transition, les fautes d'échantillonnage induites sont des bitresets. Ces fautes sont induites pour un V_{pulse} minimum de 200V. L'existence d'un tel seuil a été observé en pratique.

3.3.1.b Cas d'une transition de '1' vers '0'

On s'intéresse maintenant au cas où la sortie Q de la DFF effectue une transition de l'état '1' vers '0'. Pour cela, nous changeons quelques conditions de simulation : D_{ref} est, dans ce cas, stable à '0' (au lieu de '1') et Q est initialisé à l'état '1' (au lieu de '0'). De plus, pour simuler l'EMFI, la chute de swing utilisée est définie comme le cas où la variation de tension sur Gnd passe au-dessus de Vdd, comme illustré précédemment dans la Figure 2.24 (b).

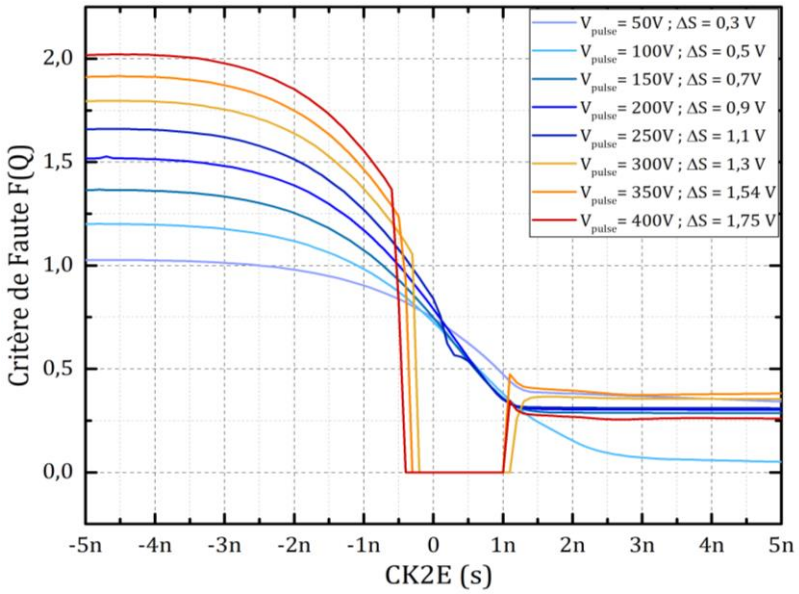


Figure 3.12 - F(Q) pour différentes valeurs de ΔS, dans le cas d'une transition de '1' vers '0'.

Les évolutions de F_Q avec CK2E obtenues lors de ces simulations pour différentes valeurs de ΔS sont visibles Figure 3.12. Comme pour la transition de '0' vers '1', on constate que l'EMFI induit :

- une réduction ou une augmentation des temps de propagation, pour de faibles valeurs de ΔS (≤250V) l'EMFI,

- et pour de fortes valeurs de ΔS (>250V) des fautes d'échantillonnage et plus spécifiquement des bitsets ; la valeur de Q restant bloquée à l'état initial '1'.

En comparant, pour les deux types de transition possibles, les valeurs seuils de V_{pulse} et ΔS au-delà desquelles des fautes d'échantillonnage sont induites, on remarque que l'induction d'un swing négatif (donc ΔS>1,2V) demande une tension de pulse beaucoup plus forte. En effet, ΔS>1,2V à V_{pulse} ≥300V, or, précédemment cette valeur était V_{pulse} ≥200V. Ainsi la première SFW apparaît à V_{pulse} =300V. Cela peut être expliqué par

le fait qu'il est plus difficile de perturber Gnd que Vdd comme nous l'avions expliqué section 2.4.2. Ce comportement asymétrique de l'EMFI avec sa polarité a également été observé dans la pratique [109], tout comme le fait qu'une polarité induise des bitsets et l'autre des bitresets.

3.3.2 Impact des réglages de l'EMFI sur la fenêtre de faute d'échantillonnage

Après l'étude de l'impact de V_{pulse}, et donc de ΔS, sur l'effet d'une EMFI, l'impact de la durée PW de l'impulsion de tension, et donc de celle de la perturbation du swing, S_{width}, a été étudié ainsi que celui de la tension d'alimentation Vdd du circuit. Les résultats des simulations conduites à cette fin sont reportés, sans perte de généralité, uniquement pour le cas d'une transition '0' vers '1' et pour V_{pulse}=400V.

3.3.2.a Impact du S_{width}

Un paramètre qui peut être ajusté facilement lors d'une EMFI est la largeur PW de l'impulsion de tension appliquée à la sonde EM. Ayant observé dans la partie 2.4.3.e que la largeur de la chute de perturbation, S_{width}, est proportionnelle au PW, l'impact de S_{width} sur la largeur des SFW a donc été analysé.

La Figure 3.13 donne les évolutions du critère F_Q par rapport à CK2E pour différentes valeurs du couple (PW, S_{width}). Les tendances obtenues sont similaires à celles observées lors de l'analyse paramétrique menée sur le couple (V_{pulse}, ΔS).

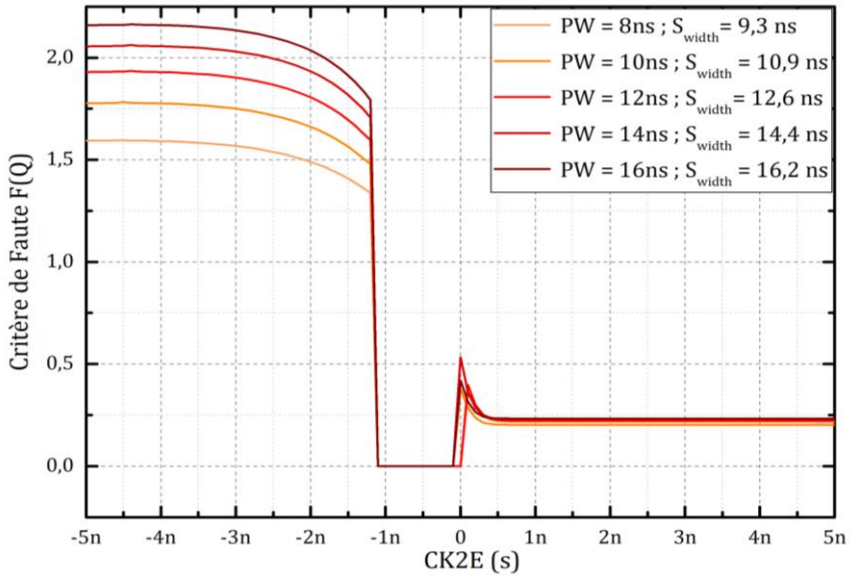


Figure 3.13 - F_Q pour différentes valeurs de S_{width}(PW) avec V_{pulse}=400V et Vdd=1,2V.

Cependant, contrairement à ce qui a été obtenu en faisant varier ΔS, la durée de la SFW est quasi-indépendante des changements appliqués à S_{width}. En effet, la durée des SFW reste constante à 1ns, excepté pour S_{width}=12,6ns où elle est de 1,1ns. Cette constance peut s'expliquer par le fait que la faute est induite lors du front montant (comme nous l'expliquerons dans la partie 3.3.3 suivante) et que les caractéristiques de ce front ne sont pas, ou très peu altérées, par un changement de la valeur de PW. Donc le paramètre de l'impulsion de tension PW n'a que peu d'influence sur la largeur de la SFW.

3.3.2.b Impact de Vdd la tension nominale d'alimentation du CI

Parmi les paramètres qui peuvent être facilement réglés lors d'une EMFI réelle, on peut trouver des paramètres liés à l'EMFI elle-même comme PW et V_{pulse}. Mais on peut également identifier les paramètres de fonctionnement du CI sous test, tels que sa tension d'alimentation Vdd. Des simulations d'une EMFI avec V_{pulse}=400V et PW=12ns ont donc été relancées pour différentes valeurs de tension d'alimentation Vdd (considérée égale à 1,2V jusqu'à présent).

Les résultats des simulations sont donnés dans la Figure 3.14. Les mêmes tendances que précédemment peuvent y être observées. Néanmoins, en ce qui concerne la largeur des SFW, on remarque que celle-ci diminue légèrement avec l'augmentation de Vdd. En effet, sa largeur passe de 1,35ns pour Vdd=0,9V à 1,05ns pour Vdd=1,5V.

Cette diminution peut être expliquée par le fait que l'amplitude ΔS=2,5V de la chute de swing est constante. Compte tenu que Vdd n'est pas constant, la valeur minimale S_{min}

atteinte par le swing est d'autant plus faible que Vdd est faible. Par exemple, pour Vdd=0,9V et ΔS=2,5V, S_{min}=-1,6V, tandis que pour Vdd=1,5V, S_{min}=-1V. Ainsi, un expérimentateur n'obtenant pas de fautes avec le V_{pulse} maximal de son générateur peut envisager de baisser la valeur de la tension d'alimentation du circuit pour espérer en obtenir.

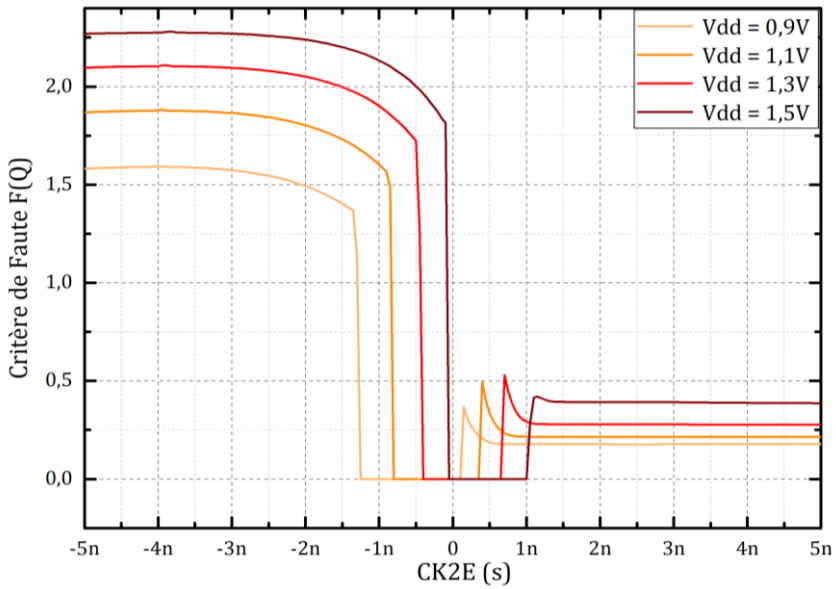


Figure 3.14 - F_Q pour différentes valeurs de tension d'alimentation Vdd avec S_{width}=12,6ns et ΔS=2,5V.

3.3.3 Mécanisme de la formation de faute d'échantillonnage

Si toutes les observations paramétriques qui ont été effectuées dans les paragraphes précédents sont confrontées à des observations expérimentales section 3.4, afin d'étayer la pertinence du modèle établi, intéressons-nous auparavant au mécanisme d'occurrence des fautes.

Afin de comprendre comment ces fautes apparaissent, la Figure 3.15 reporte les chronogrammes relatifs au fonctionnement de la DFF de notre circuit sous EMFI pour différentes valeurs de CK2E. Elle donne également un zoom sur ce même chronogramme (à gauche). Les signaux composant ce chronogramme sont le swing S, l'entrée D de la DFF, le signal D+1 représentant le signal dans la bascule après la porte pass-gate PG_1 (voir Figure 3.5), l'horloge de référence CLK, l'entrée CP de la bascule, et enfin sa sortie Q. La faute se produit pour une transition de la DFF de '0' vers '1'. De plus, la chute de swing induite est provoquée par la perturbation de la tension Vdd passant en-dessous de la tension Gnd (Figure 2.24 (a)).

Les courbes rouges correspondent à des valeurs de CK2E=-0,5ns et 0ns pour lesquelles des fautes d'échantillonnage se produisent. Les courbes en bleu clair (foncé) ont

été obtenues pour CK2E =-1,1ns et -0,6ns (0,7ns). Elles ne conduisent pas à l'occurrence d'une faute.

Comme illustré, la Figure 3.15 peut être divisée en cinq régions, dont les positions relatives dépendent de CK2E. Ces cinq régions sont délimitées par des lignes verticales en pointillés uniquement pour la valeur CK2E=-1,1ns pour des questions de visibilité.

La région (1) correspond au premier front de la chute de swing provoqué par le premier front de l'impulsion de tension appliquée à la sonde EM. Dans cette région, la tension d'alimentation est brutalement inversée par les courants induits. Par conséquent, tous les signaux, ainsi que le swing S deviennent négatifs. Le fonctionnement du circuit est donc gelé par l'EMFI. On constate, par ailleurs, que tous les signaux logiques se stabilisent à -0,6V, valeur minimale qu'ils peuvent atteindre à cause de la jonction (Diode) Well/substrat, bloquant les tensions négatives.

À la fin du premier front de la chute de swing, le circuit rentre dans la région (2). Son fonctionnement reste gelé, même si l'on peut remarquer une remontée très lente du swing sous l'effet des courants sous le seuil.

La région (3) correspond au début du deuxième front de l'impulsion de tension appliquée à la sonde. Ce front étant de polarité inverse, il provoque une remontée rapide du swing et ainsi le début du rétablissement de l'alimentation du circuit. Cette région s'arrête lorsque le swing atteint une valeur suffisante (environ Vdd-$|V_T|$) pour permettre aux transistors de fonctionner à nouveau en forte inversion. Les transistors étant toujours bloqués (fonctionnement sous le seuil) dans cette région, tous les signaux restent quasiment stables (faible récupération des tensions sous l'effet des courants sous le seuil) et le circuit (partie affectée par l'EMFI) reste gelé.

La région (4) commence quand la tension du swing croise Vdd-$|V_T|$. La zone du circuit affectée par l'EMFI, qui était qu'alors gelée, recommence à fonctionner. En effet, les transistors reviennent progressivement en régime de forte inversion. C'est dans cette région que le circuit converge vers un état final qui se traduit par l'apparition ou non d'une faute d'échantillonnage dans la région (5).

Afin de mieux appréhender ce qui se passe dans la région (4), un zoom sur l'évolution des signaux dans cet intervalle de temps est donné sur la partie droite de la figure. Comme illustré, le signal D (première courbe bleue) remonte lentement pour atteindre sa valeur initiale. Or, pendant sa remontée, quand D<0,6V ($\frac{Vdd}{2}$), D+1 (qui est l'inverse de D) monte vers l'état '1', jusqu'à ce que D>0,6V, à ce moment-là D+1 descend et se stabilise

correctement à l'état '0' avant que le front d'horloge CP n'apparaisse. Ainsi, la valeur logique correcte entre dans le maître et au moment du front d'horloge, cette valeur est mémorisée dans la DFF. Les règles de contraintes de temps sont respectées, et Q passe bien à l'état '1'. Aucune faute n'est induite.

Dans le cas de la courbe rouge, la remontée de D est plus proche du front d'horloge. Une course de signaux entre D et l'horloge a lieu. Les portes du chemin logique, étant moins puissantes que celles de l'arbre de l'horloge, le signal CP est restauré plus rapidement que D et la DFF échantillonne un '0' au lieu d'un '1'. Plus précisément, quand D passe à $\frac{Vdd}{2}$, le signal D+1 commence à descendre vers '0' mais le front d'horloge apparaît à ce moment et une valeur erronée de D+1 est échantillonnée par l'étage maître. Cela revient à violer la contrainte de setup de la bascule et non du chemin. Une faute d'échantillonnage est ainsi induite.

Enfin, si le swing remonte encore plus tard (courbe bleu foncé), D passe $\frac{Vdd}{2}$ bien après le front montant. La période où D<0,6V se situe donc après le front montant d'horloge. Par conséquent, le signal D+1 n'a pas le temps de remonter vers l'état '1', et se stabilise directement à l'état '0'. Ainsi, la bonne valeur est mémorisée dans la boucle esclave et la DFF délivre une valeur correcte mais de manière retardée.

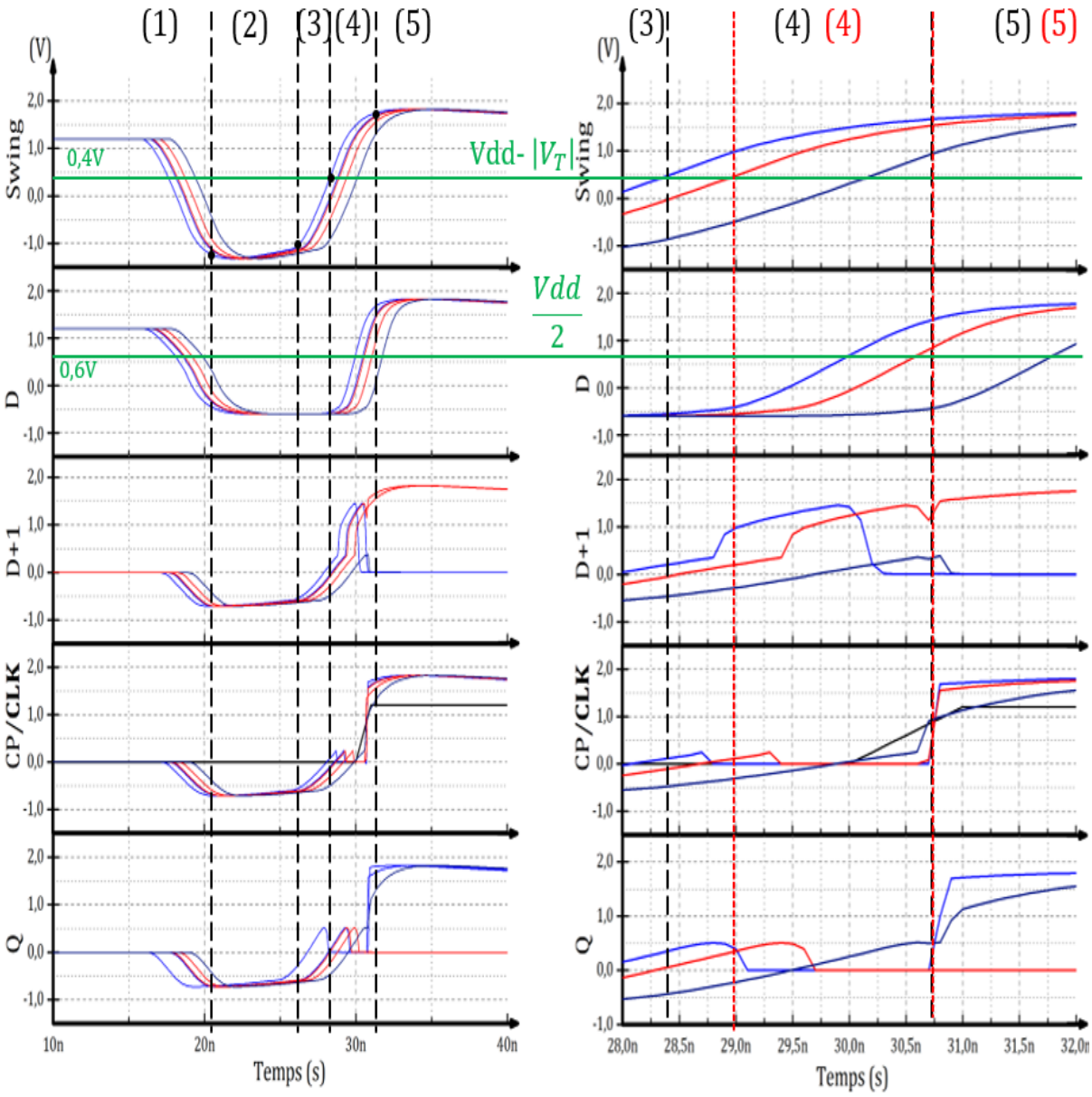


Figure 3.15 - Chronogramme des signaux S, D, D+1, CP/CLK, CPI/CPN et Q à différentes valeurs de CK2E. Les courbes de droite sont une version zoomée du chronogramme de gauche.

Pour une transition de la DFF de '1' vers '0', le mécanisme de formation d'une faute est relativement similaire. La chute de swing appliquée doit être induite via une perturbation de Gnd passant au-dessus de la tension Vdd (Figure 2.24 (b)). Dans ce cas, en condition normale le signal d'entrée D sera égal à '0'. Lors de l'application de l'EMFI le signal D va suivre la variation de Gnd et ainsi monté vers '1'. Comme précédemment, si la récupération du front montant d'horloge arrive au moment où D est toujours à '1', la DFF va échantillonner un '1' au lieu d'un '0' est induire une faute d'échantillonnage dans la bascule.

3.3.4 Variations de swing hétérogènes sur les différentes parties du circuit

Le phénomène à l'origine des fautes d'échantillonnage étant expliqué dans le cas où tous les éléments du circuit subiraient la même perturbation, nous nous intéresserons maintenant à l'hypothèse où les différents éléments du circuit (bloc logique, DFF et arbre d'horloge) sont placés et routés dans différents segments Std Cells et ne subissent donc pas la même perturbation de swing.

Dans un premier temps, le cas où seul un élément parmi les trois est perturbé est analysé. Une EMFI affectant uniquement l'arbre d'horloge a en premier lieu été simulée et ce, pour différentes valeurs de ΔS. La Figure 3.16 donne les évolutions de F_Q qui ont été obtenues. Comme on peut le constater, aucune faute d'échantillonnage n'a été observée (F_Q>0). Toutefois, ces courbes montrent qu'une accélération ou qu'un ralentissement de la propagation des signaux est induit. Ces variations sont équivalentes à des réductions (respectivement des augmentations) et des augmentations (respectivement des réductions) temporaires de la période d'horloge en cours (respectivement suivante). Cela peut donc engendrer une violation des contraintes de setup ou de hold.

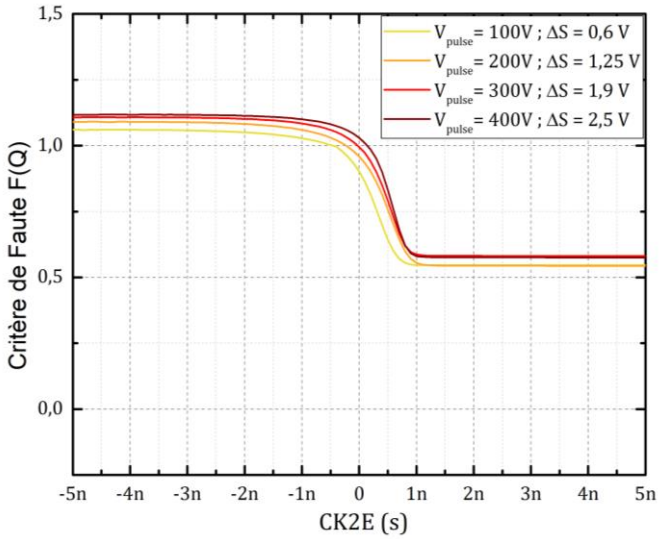


Figure 3.16 - Critère F_Q pour différents ΔS lors d'une EMFI effectuée seulement sur le bloc d'horloge.

De manière similaire à la Figure 3.16**,** la Figure 3.17 donne l'évolution de F_Q en fonction de CK2E pour des EMFIs affectant uniquement le bloc logique (à gauche), et la bascule DFF (à droite) et ce pour ΔS= 0,6V, 1,25V, 1,9V et 2,5V.

Lorsqu'une EMFI perturbe uniquement le bloc logique, cette figure montre que le critère F_Q est soit égal à 1 soit à 0. En effet, les perturbations n'affectant ni l'arbre d'hor-

loge, ni l'horloge interne de la DFF, le cadencement du circuit n'est pas affecté. Par conséquent aucun retard n'est induit et seules des fautes apparaissent. La durée pendant laquelle des fautes d'échantillonnage se produisent augmente avec ΔS, mais celle-ci est plus longue que précédemment observé. Dans ce cas de figure, l'occurrence de fautes s'explique aisément. Elles sont dues au fait que la tension du signal D à l'entrée de la bascule (dans cet intervalle de temps et pour ΔS>0,6V) est inférieure à 0,6V au moment où se produit le front montant de l'horloge.

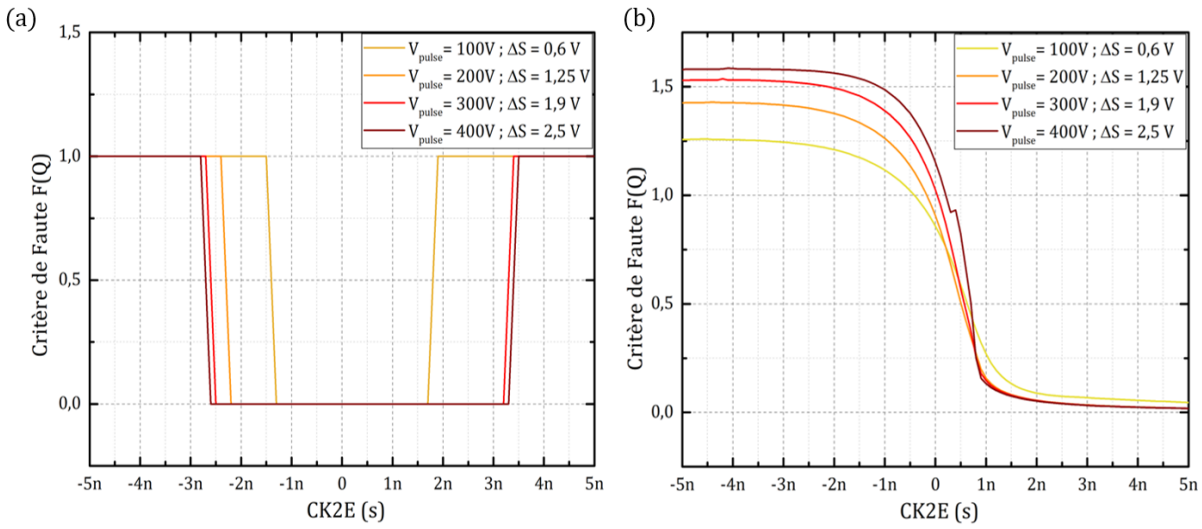


Figure 3.17 - Critère F_Q pour différentes valeurs de ΔS lorsqu'une EMFI affecte uniquement (a) le bloc logique ou (b) la DFF.

Sur la Figure 3.17(b) on peut observer que F_Q n'atteint jamais zéro. Ceci signifie qu'aucune faute n'est induite par une EMFI affectant uniquement la DFF. Néanmoins le délai de propagation de la DFF est soit réduit soit accru. Cela s'explique par le fait que seule une chute de tension significative du signal D peut induire une perturbation suffisamment importante du signal D+1 pour induire une faute d'échantillonnage.

Cette hypothèse est confirmée par la Figure 3.18 qui donne l'évolution de F_Q dans le cas d'EMFI affectant simultanément le bloc logique et la DFF. Dans ce cas, F_Q atteint 0 pour certaines valeurs ΔS. On remarque en outre que les variations de F_Q sont quasiment identiques à celles obtenues pour des EMFIs perturbant l'ensemble du circuit (Figure 3.11 (a)). Néanmoins la durée des SFW est plus grande car le signal CP n'est pas retardé.

Ces analyses ont mis en évidence le rôle respectif de chaque bloc du circuit lors de l'occurrence de fautes d'échantillonnage. Il apparaît que c'est l'association des perturbations du swing du chemin logique et de la DFF qui est à l'origine des fautes. Quant à la perturbation de l'arbre d'horloge, elle n'a que peu ou pas d'effet hormis le cas où des

fautes de timing sont induites au prochain front de l'horloge (cas des circuits avec des fréquences de cadencement élevées.)

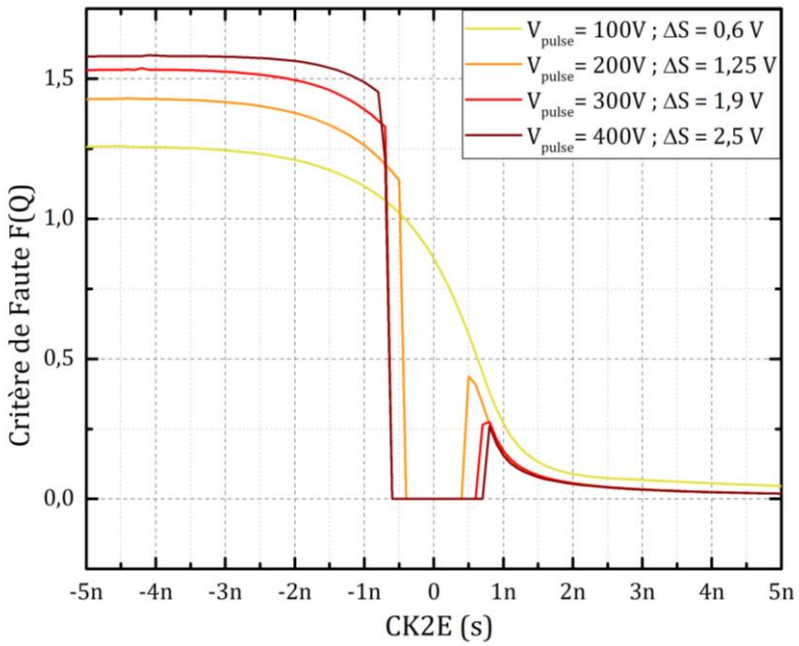


Figure 3.18 - Critère F_Q pour différentes valeurs de ΔS lors d'une EMFI affectant simultanément le bloc logique et la DFF.

Les analyses conduites par simulation et décrites dans ces dernières pages sont riches d'enseignement. Elles permettent en effet d'appréhender quand et comment les fautes d'échantillonnage se produisent. Elles permettent également d'appréhender comment les réglages d'une EMFI favorisent ou non l'apparition de fautes.

À ce stade, il est toutefois nécessaire de confronter les résultats obtenus par simulation à des résultats expérimentaux afin d'étayer leur validité et de manière générale de confirmer la justesse des raisonnements conduits jusqu'à ce stade.

3.4 Parallèle simulations vs expérimentations du modèle de faute d'échantillonnage

Obtenir des preuves expérimentales relatives à la justesse de la modélisation des EMFIs est difficile. En effet, comme l'a montré la section 2.2, le champ EM pollue toutes les mesures analogiques et ce jusqu'à plusieurs mètres de distance. Une alternative possible pour contourner cet écueil serait d'intégrer des capteurs embarqués (voire des oscilloscopes intégrés [109]) dans le CI. Toutefois, même cette approche apparaît insuffisante car la tension d'alimentation de ces capteurs intégrés serait alors fortement perturbée par les EMFIs lors des mesures.

Des mesures indirectes ont donc été choisies comme vecteur de démonstration de la validité du modèle. Plus précisément, la solution adoptée a consisté à mesurer la probabilité P_f d'induire une faute dans le CI, ce qui peut être réalisé sans mesure analogique ou intégration de capteurs.

3.4.1 Plateforme et conditions expérimentales

La plateforme EMFI utilisée lors de ces campagnes de validation est celle décrite section 2.2. Elles ont été effectuées sur la puce de test, étudiée dans le chapitre précédent, que l'on nommera TC1 (pour TestChip 1). Ce circuit est monté sur une carte qui est visible Figure 3.19.

La puce TC1 est un circuit conçu en technologie CMOS 40nm faible consommation. Sa surface est de 2150µm x 2150µm et sa tension nominale d'alimentation Vdd est de 1,2V. La fréquence d'horloge peut être fixée, à l'aide d'un générateur de signal externe, entre 5MHz et 100MHz. Cette puce embarque différents blocs dont un AES 128bits matériel (Advanced Encryption Standard) qui a constitué une des principales cibles des EMFIs avec un registre 32bits.

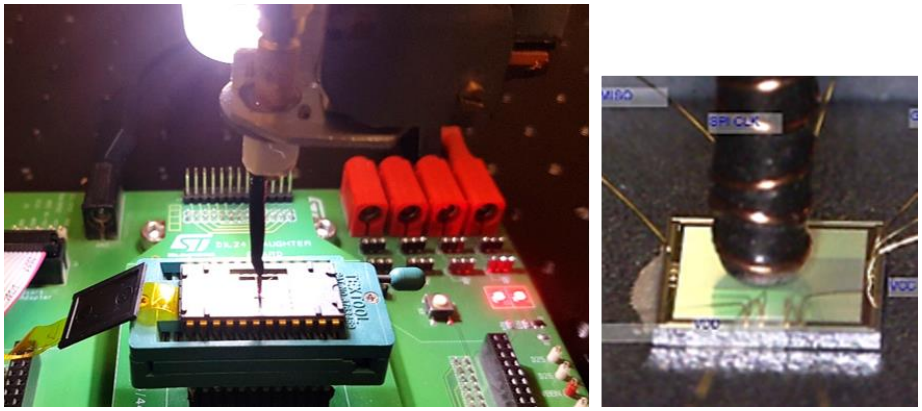


Figure 3.19 – Vue d'une puce, sur sa carte d'émulation, ciblée par les EMFIs.

Le banc est piloté par un programme Python développé pour ces expérimentations. Il permet l'écriture du message d'entrée (plaintext) et la clé (key) de l'AES, mais également la lecture de son message de sortie (ciphertext). Un AES effectué par ce code python permet de vérifier à la volée si les messages chiffrés fournis par la puce sont corrects ou erronés. Les paramètres du générateur d'impulsion de tension sont également pilotés par ce programme. La sonde EM utilisée lors de ces campagnes d'injection est une sonde fabriquée au LIRMM caractérisée par un diamètre de 500µm. Lors des campagnes d'injection, elle a été systématiquement placée au contact de la puce, en face avant.

Les messages (ou clés) hexadécimaux fournis à l'AES ainsi qu'au registre 32bits (opérations d'écriture puis de lecture), sont de la forme : 55AA, 1111 ou 0000. En ce qui concerne les EMFIs ciblant l'AES, elles ont été réalisées de sorte à fauter sa 10ème ronde, tandis que les EMFIs ciblant le registre ont été effectuées pendant les opérations de lecture de son contenu.

Afin de valider la modélisation des EMFIs établie dans ce document, des EMFIs ont été effectuées avec différentes valeurs de V_{pulse} et PW, à différents instants t_{pulse} (différentes valeurs de CK2E) du fonctionnement des cibles, et ce pour différentes valeurs de la tension d'alimentation et de la fréquence de fonctionnement de la puce. Dans chaque configuration et pour chaque instant de tir, la probabilité P_f d'induire une faute (fauter 1 bit ou plusieurs) a été mesurée en effectuant 100 tirs pour chaque valeur de t_{pulse}. Une faute est considérée lorsque le message de sortie de l'AES physique est différent de celui donné par l'AES logiciel. Les valeurs de t_{pulse} ont été choisies de sorte à balayer plusieurs périodes d'horloge avec un pas de 100ps.

3.4.2 Fautes et fréquence d'horloge

Selon [3] et [23] et les simulations que nous avons effectué, les fautes d'échantillonnage apparaissent lorsque les EMFIs précèdent ou chevauchent les fronts montants d'horloge. Si tel est le cas en pratique, les chronogrammes de P_f obtenus en faisant varier t_{pulse} de sorte à couvrir plusieurs périodes d'horloge doivent être caractérisés par l'apparition périodique de fenêtres où $P_f = 1$ séparant des fenêtres où $P_f = 0$.

C'est pourquoi des EMFIs ont effectuées pour trois fréquences de fonctionnement différentes de la puce de test : 30MHz (T_{CLK}=33,3ns), 50MHz (T_{CLK}=20ns) et 70MHz (T_{CLK}=14,3ns). Lors de ces EMFIs, l'amplitude V_{pulse} de l'impulsion appliquée à la sonde a été fixée à une valeur légèrement supérieure à celle permettant d'obtenir de premières fautes soit 250V pour les EMFIs ciblant l'AES et 210V celles ciblant le registre. PW a été fixé à 9ns et la tension d'alimentation du circuit à 1,2V.

La Figure 3.20 donne l'évolution de la Probabilité P_f d'induire une faute dans l'AES (en bleu) et dans le registre (en rouge) en fonction de t_{pulse} et ce pour les trois fréquences de fonctionnement du circuit considéré. Le signal CLK, représenté en pointillés, est donné à titre indicatif, rien ne nous permet de mesurer le signal d'horloge interne du CI.

La Figure 3.20 montre, comme attendu, que des fenêtres de fautes d'échantillonnage apparaissent. Celles-ci sont effectivement espacées les unes des autres d'une période T_{SFW} égale à la période T_{CLK} dans les trois cas. En outre, la largeur des SFW (SFW_{width}),

mesurée à P_f=0,5 est constante et ce pour les trois fréquences de fonctionnement considérées. Cependant une différence significative est observée entre les largeurs des SFW de l'AES ou du registre. Cette différence s'explique par deux raisons. Premièrement, le V_{pulse} a été réglé à 250V et 210V pendant les EMFIs ciblant respectivement l'AES et le registre. Sachant que la réduction du V_{pulse} induit une réduction de la SFW_{width}, c'est la première raison qui explique cette différence. Deuxièmement, l'AES, qui contient au moins 7 fois plus de DFFs que le registre, a été conçu de sorte que le skew entre ses bascules soit important afin de limiter ses émissions EM [110] et sa consommation instantanée de courant. Par conséquent, la SFW observée est probablement une superposition de plusieurs SFW décalées dans le temps ; chacune correspondant à une bascule fautée dont l'horloge est décalée de t_{skew} (Nous ne discriminons pas le fait qu'un ou plusieurs bits soient fautés). Cette hypothèse est étayée par le fait que la largeur des SFW observées pour le registre est d'environ 1ns, valeur qui correspond aux résultats obtenus en simulation.

Tableau 5 - Valeurs des T_{SFW} et des SFW_{width} pour les différentes cibles de l'EMFI (AES et registre) pour différentes fréquences d'horloge.

		$\mathbf{30MHz}$ $(\boldsymbol{T_{CLK} = 33,3ns})$	$\mathbf{50MHz}$ $(\boldsymbol{T_{CLK} = 20ns})$	$\mathbf{70MHz}$ $(\boldsymbol{T_{CLK} = 14,3ns})$
AES	T_{SFW}	32ns	19,5ns	14,5ns
	SFW_{width}	6,5ns	7ns	6,6ns
Registre	T_{SFW}	33,1ns	20ns	14,3ns
	SFW_{width}	1,08ns	1ns	1,01ns

Les mesures des T_{SFW} et des SFW_{width} reportées Tableau 5 confirment que des fautes d'échantillonnage se produisent autour du front montant du signal d'horloge en formant des fenêtres périodiques de période égale à celle du signal d'horloge.

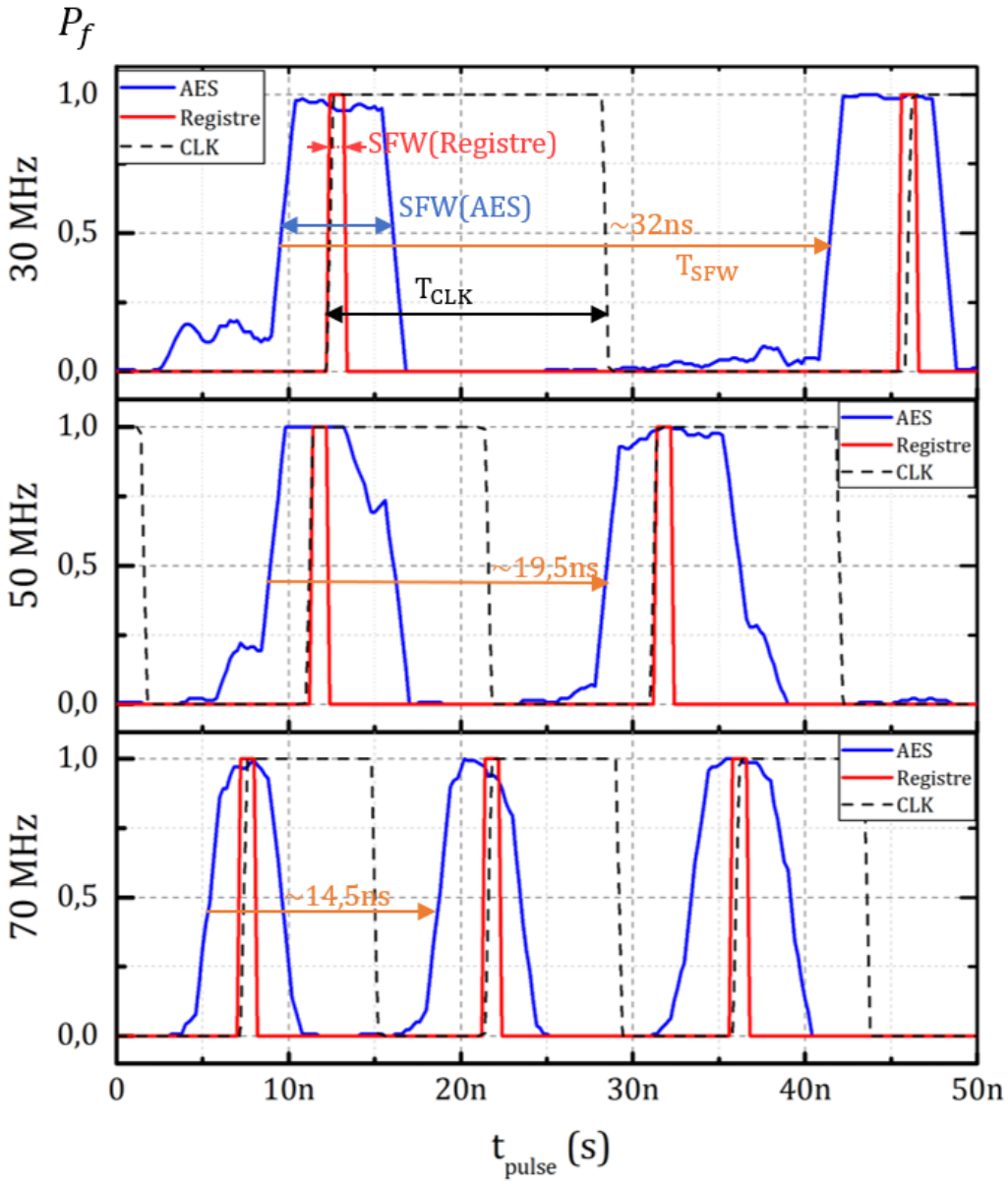


Figure 3.20 – Évolution de la probabilité d'induire une faute dans l'AES (en bleu) et dans le registre (en rouge) en fonction de t_{pulse} et ce pour trois fréquences différentes du circuit : 30MHz (T_{CLK}=33,3ns), 50MHz (T_{CLK}=20ns) et 70MHz (T_{CLK}=14,3ns).

La Figure 3.21 donne l'évolution de la Probabilité P_f d'induire une faute dans l'AES en fonction de t_{pulse} pour une fréquence d'horloge de (a) 10MHz et (b) 100MHz. Pour une fréquence de 10MHz, correspondant à une période d'horloge de 100ns on constate l'apparition de SFW, espacées d'une période quasi-équivalente à celle de l'horloge. Le modèle et [66] ont montré que les retards induits par une ou plusieurs EMFI effectuées sur des blocs logiques étaient de l'ordre de quelques nanosecondes et ce même pour un chemin de plusieurs centaines de portes logiques. Les fautes obtenues à 10MHz, similaires à celles obtenues lors de nos précédentes expérimentations, sont donc bien des fautes d'échantillonnage.

Ces analyses sont aussi confirmées par les mesures de la Figure 3.21 (b). À une fréquence de 100MHz, on constate toujours l'apparition de SFW distantes d'une période quasi-équivalente à celle de l'horloge, d'une valeur T_{CLK}=10ns. Cependant, les fenêtres de fautes ne sont pas aussi distinctes et tranchées que celles obtenues à de plus basses fréquences d'horloge. En effet, la probabilité d'induire une faute P_f ne descend jamais en dessous de 20% qu'importe la valeur de t_{pulse}.

Dans ce cas de figure, d'après nos simulations l'impulsion EM gèle (S<0) le fonctionnement du circuit pour une durée de l'ordre de 2 à 3ns, durée de l'ordre de grandeur de la marge de timing introduite par la prise en compte des pires cas PVT lors de la conception du circuit. Par conséquent, peu importe l'instant auquel débute l'injection EM, les chemins critiques, s'ils doivent commuter, ce qui n'est pas systématiquement le cas, n'ont pas le temps d'effectuer leur calcul et des fautes de timing apparaissent. Ceci explique probablement pourquoi P_f est systématiquement supérieure à 20%. Par contre, si l'injection EM est effectuée de sorte que la fin de l'impulsion EM se produise au voisinage du front montant de l'horloge, le phénomène de fautes d'échantillonnage dominant la probabilité d'induire une faute est proche de 100%.

À partir de ces résultats, on peut émettre des hypothèses relatives à l'effet d'une injection EM sur des circuits fonctionnant à des fréquences encore plus élevées (T_{CLK}<<PW). En effet, compte tenu que l'EMFI devrait geler le fonctionnement du circuit pour une durée supérieure à une période d'horloge, on peut s'attendre à ce que le calcul soit réalisé avec des parties du circuit n'effectuant pas un ou plusieurs cycles d'horloge ce qui peut conduire à des sauts d'instructions.

Ces analyses démontrent la pertinence de mieux comprendre la génération de ce type de faute d'échantillonnage, encore relativement récent dans l'état de l'art des attaques par injections de fautes.

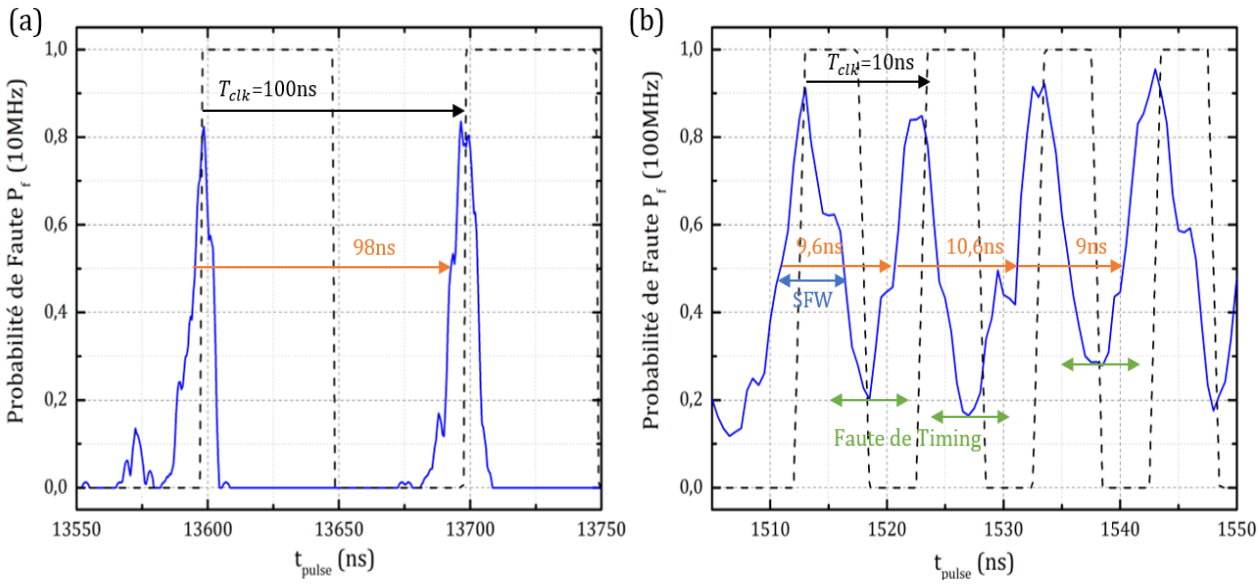


Figure 3.21 - Évolution de la probabilité d'induire une faute dans l'AES en fonction de t_{pulse} pour une fréquence de (a) 10MHz (T_{CLK}=10ns) et (b) 100MHz (T_{CLK}=100ns).

Ces résultats présentés dans cette section constituent une première preuve indirecte de la validité du modèle. Afin de disposer de preuves supplémentaires, une analyse comparée de l'évolution de la largeur des fenêtres d'échantillonnage avec les paramètres de l'EMFI, PW et V_{pulse} et la tension d'alimentation Vdd a été réalisée.

3.4.3 Fautes et paramètres de l'EMFI

3.4.3.a Effet des variations du V_{pulse}

De nouvelles expériences ont été réalisées pour estimer l'évolution, en fonction de V_{pulse}, de la largeur de la fenêtre des fautes d'échantillonnage. Pour mettre en évidence cette évolution, nous avons fait varier l'amplitude V_{pulse} et t_{pulse} lors d'EMFI effectuée sur notre puce de test fonctionnant à 50MHz et alimenté par 1,2V. Ces EMFI ont été opérées PW=8ns.

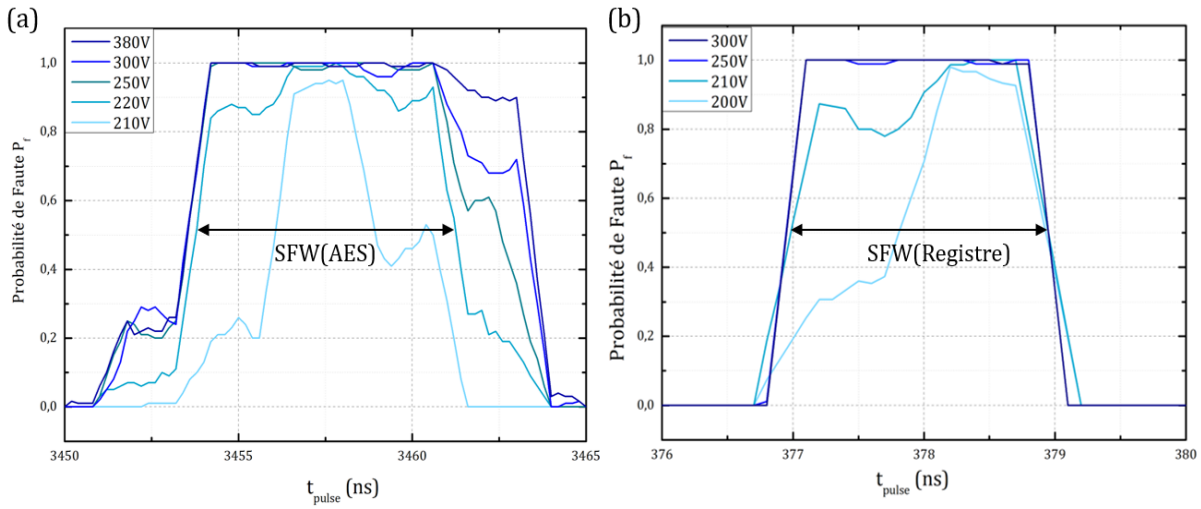


Figure 3.22 - Fenêtres de fautes d'échantillonnage observées lors d'EMFI réalisée sur (a) l'AES, (b) un registre de la puce TC1, pour différentes valeurs de V_{pulse} (PW=8ns).

Les résultats obtenus par simulation, reportés Figure 3.11, prédisent que la largeur des fenêtres de faute d'échantillonnage augmente avec V_{pulse} . Cette prédiction est confirmée par les résultats expérimentaux reportés Figure 3.22. Cette figure montre les SFW observées lors d'EMFI ciblant l'AES (a) et le registre (b). Dans le cas des EMFIs ciblant l'AES, la première SFW apparaît pour V_{pulse}= 210V. Sa largeur augmente rapidement avec l'augmentation de V_{pulse}, passant de 2ns à ~9,5ns pour V_{pulse} ≥340V. Les simulations exécutées avaient montré que les premières fautes apparaissaient à V_{pulse}=200V et que la largeur de la SFW passait de ~1ns, à ~1,8ns pour une augmentation de +100V du V_{pulse}.

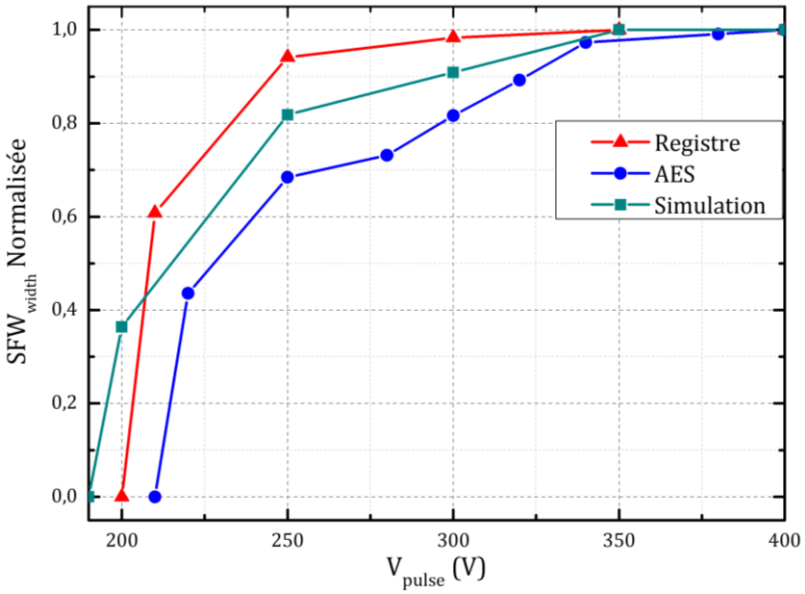


Figure 3.23 - Comparaisons des évolutions simulées et mesurées avec V_{pulse} de la largeur normalisée des fenêtres de faute d'échantillonnage.

La Figure 3.23 compare les évolutions normalisées de la largeur des fenêtres de fautes obtenues expérimentalement et par simulations. La normalisation a été effectuée selon la valeur maximale de SFW_{width}. Comme on peut le constater, tant pour les courbes simulées que pour les courbes expérimentales, l'augmentation de la largeur des fenêtres est rapide pour V_{pulse} compris entre 200V et 250V et est plus modérée au-delà de cette valeur. Ceci confirme la validité de la modélisation des EMFIs proposée.

3.4.3.b Effet des variations du PW

Des expériences similaires à celles décrites dans la section précédente ont été effectuées dans le but d'analyser l'effet de PW sur la largeur des SFW. D'après notre modèle (voir Figure 3.13), la largeur de PW affecte peu la largeur des SFW. Les mesures expérimentales ont confirmé ce résultat comme l'illustre la Figure 3.24. Celle-ci donne les fenêtres de fautes obtenues dans le cas de l'AES (a) et du registre (b), ainsi que les évolutions de leur largeur normalisée obtenues tant en simulations que lors des expérimentations. Là encore, la concordance entre les simulations et les expériences est bonne. En effet, comme l'indiquaient les simulations, la variation de PW n'a quasiment aucun effet sur la largeur des SFW mesurées.

On peut noter, tout de même, une différence dans la probabilité d'induire une faute dans le cas du registre en fonction de PW. Cette probabilité est de 100% pour PW=10ns et 12ns. Elle n'est que de ~60% pour PW=8ns et 14ns. Ceci n'est pas surprenant compte tenu des observations qui ont été faites section 2.4.2, relatives à la Figure 2.30. Ces observations suggéraient qu'il existe des valeurs optimales de PW permettant d'induire la perturbation d'amplitude maximale tout en minimisant sa durée ; l'intérêt de minimiser sa durée étant de limiter le temps durant lequel le circuit est en phase de recouvrement lent de son swing et donc de rapprocher la chute et la remontée du swing imposées par les deux fronts impulsion de tension.

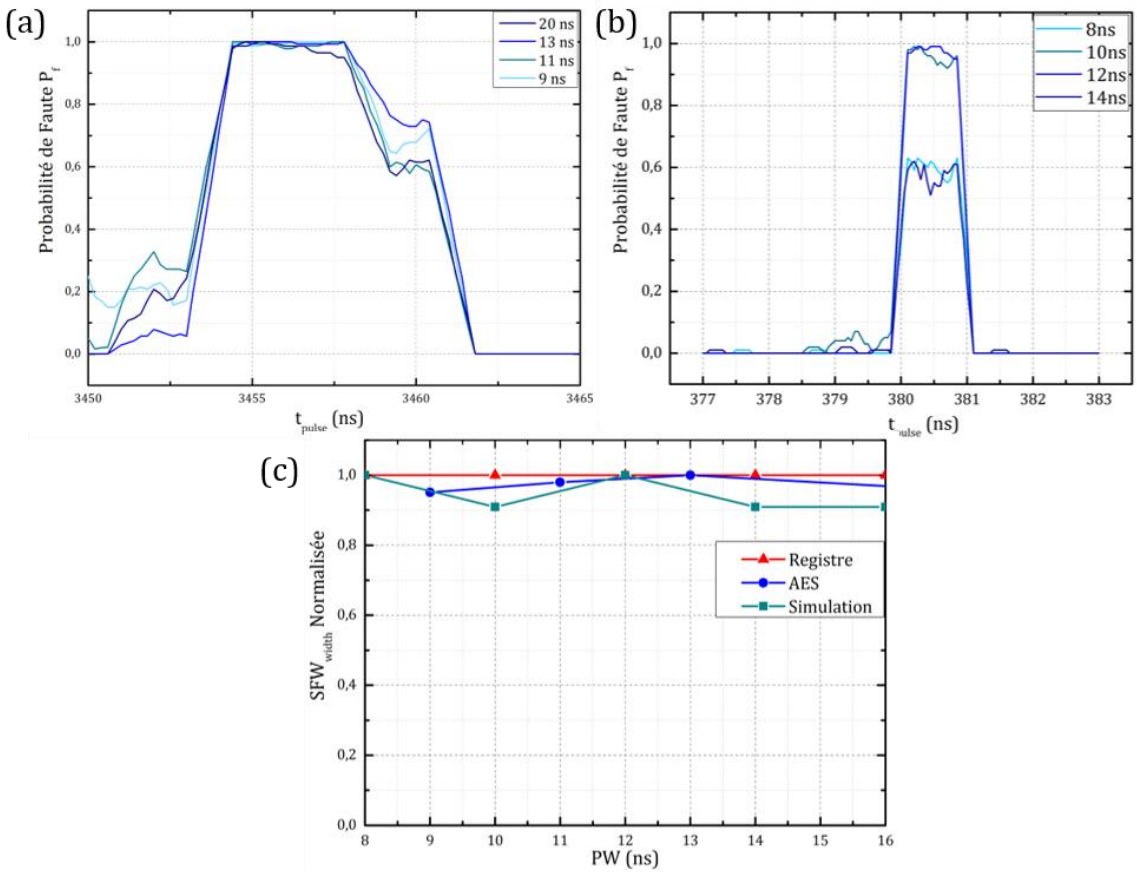


Figure 3.24 - Fenêtres de fautes d'échantillonnage observées lors d'EMFIs réalisées sur (a) l'AES et (b) le registre de la puce TC1, pour différentes valeurs de PW (V_{pulse}=250V pour l'AES et 210V pour le registre, Vdd=1,2V. (c) Comparaisons des évolutions simulées et mesurées avec PW de la largeur normalisée des fenêtres de faute d'échantillonnage.

3.4.3.c Effet des variations de la tension d'alimentation Vdd

La Figure 3.25 reporte les fenêtres de fautes obtenues lors d'EMFIs conduites sur la puce alimentée sous différentes valeurs de Vdd. Ces résultats confirment également la validité de la modélisation proposée dans ce document. En effet, l'augmentation de la tension d'alimentation Vdd entraîne une diminution de la largeur de SFW comme cela a été constaté en simulation (voir Figure 3.14), ou dans [62].

On remarque toutefois que l'impact de la variation de Vdd est plus significatif expérimentalement qu'en simulation. Lors des simulations, l'augmentation de Vdd de 1V à 1,5V entraînait une diminution de seulement 20% de la largeur des SFW. Expérimentalement, cette diminution est de l'ordre de 70% quand l'EMFI cible le registre à Vdd=1,5V. Au-delà de cette valeur plus aucune faute n'est observée. Dans le cas de l'AES, la largeur des SFW diminue de 80%, en passant de 1V à Vdd=1,7V. Cependant, malgré ces différences, les tendances sont globalement en accord avec le modèle.

Ces différences sont probablement dues au fait que notre modélisation de la chute de swing ne fait intervenir que des éléments passifs (R et C). Les transistors ont été modélisés par un réseau RC, ce qui n'est pas vraiment le cas en réalité. Il s'agit d'éléments actifs dont le comportement et notamment la résistance à l'état passant varient fortement (quadratiquement) avec la tension d'alimentation du circuit. Il aurait été souhaitable d'ajuster la valeur de RN et RP dans les simulations pour évaluer plus précisément l'impact de Vdd sur la largeur des fenêtres de fautes. En effet, tout laisse à penser (réponse RC des réseaux Vdd et Gnd) que plus la tension d'alimentation est forte, plus RN et RP sont faibles, plus les fronts de la perturbation de swing sont courts et donc plus la fenêtre de faute est courte. Cette analyse ayant été faites après la fin de mon contrat à STMicroelectronics (lors de l'écriture de ma thèse), je n'ai malheureusement pas pu injecter ce comportement non linéaire dans mes simulations.

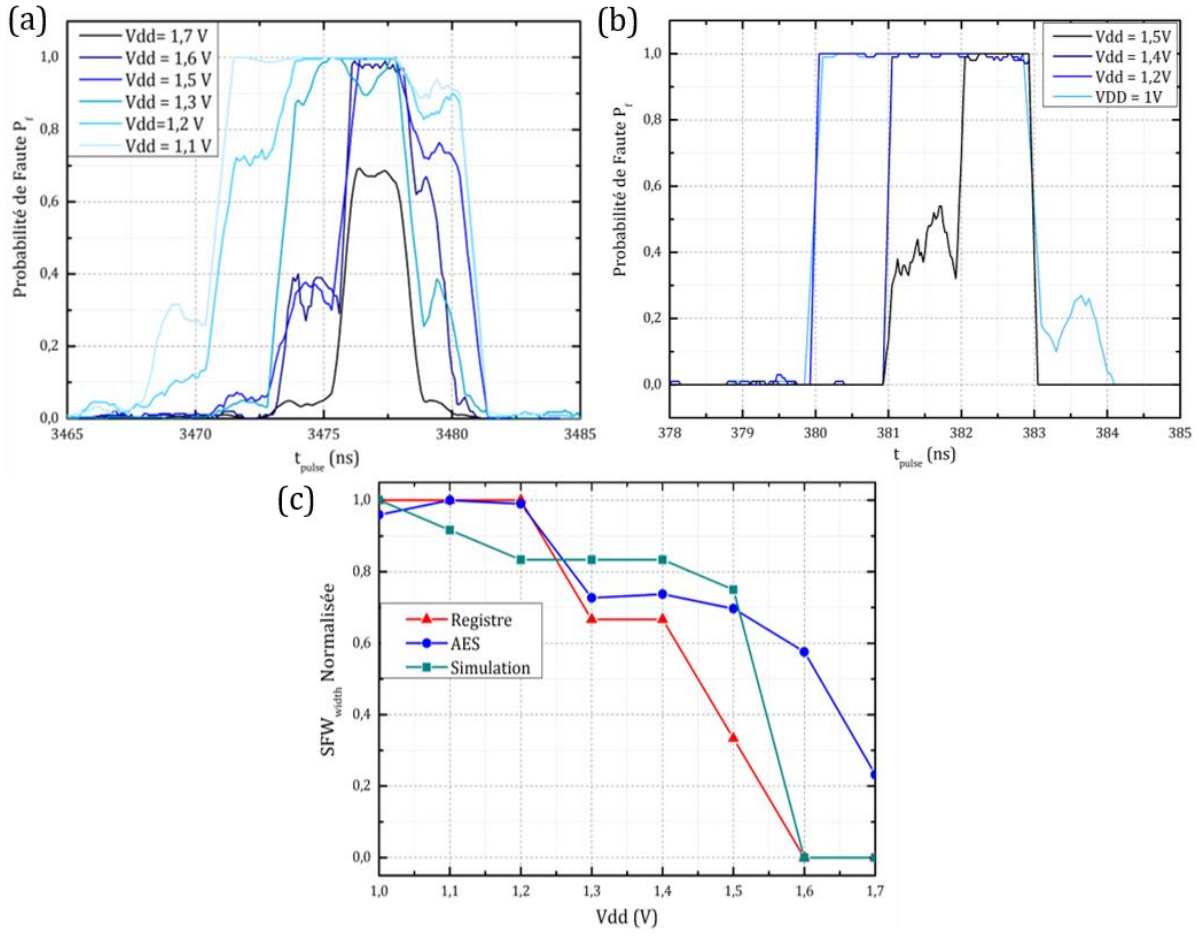


Figure 3.25 - Fenêtres de fautes d'échantillonnage obtenues lors d'EMFIs réalisées sur (a) l'AES et (b) le registre de la puce TC1, pour différentes tensions d'alimentation Vdd, (V_{pulse}=250V pour l'AES et 210V pour le registre). (c) Comparaison des évolutions simulées et mesurées avec Vdd de la largeur normalisée des fenêtres de faute d'échantillonnage.

Ainsi, l'approche de l'analyse des tendances associée aux mesures de la probabilité d'induire une faute, a permis de s'abroger des contraintes expérimentales de l'EMFI. Les tendances des variations des largeurs de SFW, en fonction des modifications effectuées sur certaines paramètres de l'EMFI, ont été comparées avec la modélisation présentée précédemment. Ces tendances semblent en accord avec les simulations, appuyant la véracité du modèle de faute d'échantillonnage proposé.

3.5 Conclusion

Tout comme le chapitre précédent, ces travaux de simulation et de modélisation de l'EMFI, induite pendant l'opération d'un circuit synchrone, ont permis de mieux appréhender l'effet d'une EMFI sur un CI.

L'exploitation des modélisations précédentes met en évidence la création de chutes de swing lors d'EMFI, qui ont été introduites dans une simulation électrique d'un circuit simple. Ces simulations se concentrent sur une infime partie d'un circuit, que l'on retrouve des milliers de fois dans celui-ci : une DFF constituée de son bloc logique et de son arbre d'horloge. De plus, un critère de faute F a été mis en place pour faciliter l'étude des temps de propagations dans les composants du circuit sous EMFI, et ainsi mettre en évidence les différentes fautes induites.

L'analyse de ces simulations a montré que l'EMFI avait différents effets sur un circuit. Dans un premier temps, une accélération ou un retard des temps de propagation peut être induit dans les composants, pouvant conduire à des fautes de timing éventuelles. Néanmoins, les simulations ont montré qu'une EMFI induite à un moment proche du front montant d'horloge menée à l'apparition d'une faute d'échantillonnage. Ces fautes se forment lors de l'opération d'échantillonnages de la DFF. En effet, le circuit est d'abord mis dans un état « gelé » par le premier front de la chute de swing, puis le deuxième front permet le rétablissement rapide de l'alimentation. À ce moment, si le front d'horloge est rétabli avant la stabilisation du signal entrant D, une faute d'échantillonnage apparaît. Ce « défaut » de fonctionnement est induit dès la conception du CI puisque l'horloge est généralement conçue pour être plus rapide que les autres signaux. De plus, contrairement à la faute de timing, les règles de marges de temps établies par les fabricants ne sont aucunement efficaces contre ce type de fautes, celle-ci n'exploitant pas le retard ou l'accélération des signaux, mais plutôt le « gel/dégel » du CI et la rapidité de rétablissement de ces derniers.

Ces fautes d'échantillonnage forment une fenêtre de temps SFW autour du front montant d'horloge durant laquelle une faute d'échantillonnage peut être induite. La largeur de ces fenêtres est variable et dépend de plusieurs paramètres. En effet, la tension du pulse V_{pulse} ou l'alimentation du circuit Vdd entraîne des variations de la largeur de ces fenêtres, tandis que la largeur du pulse PW ne semble pas avoir d'impact sur celles-ci.

Ces résultats et plus généralement l'ensemble de la modélisation, ont été confrontés à des mesures expérimentales ayant le but de confirmer la véracité du modèle. Le balayage de l'impulsion EM sur plusieurs périodes d'horloge ont mis en évidence la création de fenêtres de fautes d'échantillonnage à différentes fréquences, comme observé dans les simulations. Leur période d'apparition est égale à la période d'horloge et leur largeur est indépendante de leur fréquence, contrairement au cas d'une faute de timing,

Ces simulations semblent un bon point de départ pour un concepteur voulant visualiser l'effet d'une EMFI sur un CI avant sa conception. En outre, dans le cadre du projet CSAFE+ auquel nous participons, une autre société a commencé la mise en place du modèle de faute dans un soft d'analyse des temps de propagation des signaux, pour prédire l'apparition de fautes, aussi bien de timing que d'échantillonnage, dans un CI.

Enfin, les variations de la largeur des fenêtres de fautes dues à la modification de certains paramètres ont également été comparées expérimentalement. Celles-ci démontrent que les évolutions simulées et mesurées de la largeur des fenêtres de fautes présentent les mêmes tendances. Cette concordance confirme donc la justesse de la modélisation de l'EMFI développée dans le cadre de ma thèse. Bien que si celle-ci soit perfectible (prise en compte d'effets secondaires comme le comportement des transistors avec la tension d'alimentation et meilleure estimation des paramètres intervenant dans le modèle), nous sommes convaincus qu'elle constitue un pas en avant dans la compréhension de l'EMFI et qu'elle peut d'ores et déjà être utilisée pour définir et valider des contremesures par conception. Le chapitre suivant est dévolu à la proposition de contremesures. Ces propositions ont été imaginées suite aux travaux expérimentaux qui ont été conduits en s'appuyant sur la compréhension de l'EMFI développée lors des travaux de modélisation.

Chapitre 4 . Proposition de contre-mesures

La réalisation d'une EMFI sur un CI demande peu de moyens et peut être efficace pour déchiffrer un algorithme cryptographique, pourtant peu de contre-mesures, propres à cette attaque, sont implémentées dans les circuits intégrés du commerce. La plupart des contre-mesures implémentées sont celles qui ont pour finalité de détecter les fautes de timing. Or, il a été démontré dans le chapitre précédent, que pour des circuits à basse fréquence, il est difficile d'induire des fautes de timing lors d'une EMFI. Les contre-mesures face à l'EMFI, en général, ont été énoncés dans l'état de l'art (1.6), néanmoins la seule contre-mesure face aux fautes d'échantillonnage, est celle proposée par [93].

Le modèle développé dans les chapitres précédents est riche en enseignements. D'une part sur l'effet d'une impulsion EM sur les réseaux d'alimentations du circuit. D'autre part sur l'occurrence des différentes fautes. Ainsi, de nombreuses idées de contre-mesures ont pu en être déduites lors du développement de ce modèle.

Ce chapitre se veut être un descriptif de différents concepts de contre-mesures aux EMFI découlant du modèle de faute décrit précédemment. Celles-ci s'appliquent aussi bien à la détection d'un quelconque champ EM qu'à la détection directe de faute. Ces contre-mesures n'ont pas toute été testées expérimentalement, cependant elles reposent sur des implications du modèle et peuvent aider un lecteur soucieux de vouloir implémenter une nouvelle contre-mesure dans un CI.

4.1 Règle de conception du CI

De nombreux éléments liés à la conception d'un CI ont été analysés dans le but de mettre en place le modèle de faute de l'EMFI. Tout au long de ces analyses, des éléments clés ont été mis en évidence comme vecteurs de perturbations pouvant amener à l'induction de fautes lors d'une EMFI. Ainsi, dès la phase de layout du circuit, des concepts peuvent être mis en place pour augmenter la robustesse d'un CI face à une impulsion EM.

4.1.1 Routages des alimentations

L'un des principaux éléments d'un circuit permettant à l'EMFI d'induire des fautes est le routage de ses alimentations. Celui-ci est fait pour assurer un recouvrement maximal de toute la surface du circuit ainsi qu'une alimentation uniforme à l'ensemble des portes logiques. Cependant, leur routage sur différents niveaux de métaux forme un très grand nombre de boucles et donc d'antennes réceptrices (voir Figure 2.13).

Afin de réduire le couplage d'un circuit avec un champ EM, une idée envisagée peut être de couper les boucles formées par le réseau d'alimentation. La Figure 4.1 est une représentation d'un segment de grille d'alimentation. Les rails du Métal1 ont été coupés en plusieurs segments de même longueur. Ainsi, la surface de recouvrement et l'uniformité du réseau d'alimentation ne change que peu, tout en évitant de former des boucles réceptrices.

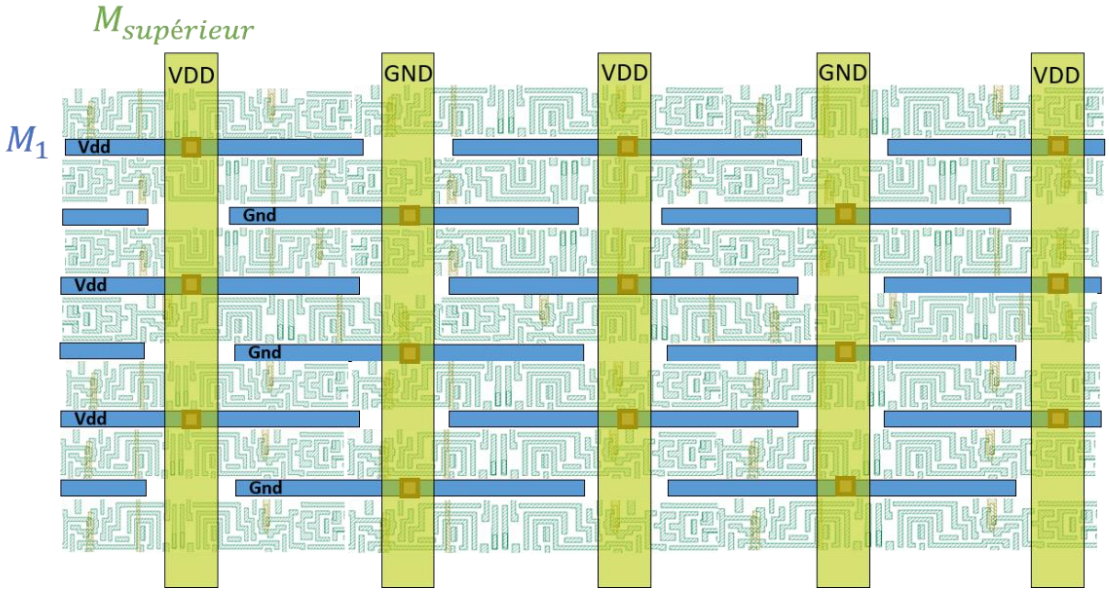


Figure 4.1 - Morceau de layout d'un circuit avec un réseau d'alimentation sans boucle.

Ce concept paraît d'autant plus adapté pour une polarisation de type tap-out. En effet, en se basant sur la Figure 2.4, les plots de polarisation peuvent toujours être placés à la même position que dans le cas d'un routage classique. La polarisation des puits N et P ne change donc pas. Lors d'une conception en tap-in, des problèmes de non-uniformité peuvent apparaître pour les cellules se situant à l'extrémité de deux segments de rails M1. Celles-ci ne seraient pas alimentées directement contrairement aux autres cellules. Une étude RedHawk doit être mise en place pour déterminer la continuité des tensions, dans ce cas de routage d'alimentation.

La modélisation par le calcul ou en simulation est relativement complexe dans le cas de « boucles coupées ». Cependant ce concept peut être expérimenté sur un circuit où une référence contenant un routage classique est disponible et permettrait ainsi de comparer la probabilité d'induire une faute dans les deux circuits.

4.1.2 Routages des blocs logiques

La simulation d'une EMFI sur un circuit synchrone a permis de mettre en évidence l'importance de la rapidité des fronts de certains signaux. En outre, les signaux D d'entrée d'une DFF et de l'horloge ont un rôle majeur dans l'induction d'une faute d'échantillonnage. Lors de nos simulations, C_D et C_{CLK} représentent les capacités de charges respectives en sortie du bloc logique et de l'arbre d'horloge, connectées aux entrées de la DFF. Celles-ci ont été fixées de sorte à avoir $C_D > C_{CLK}$.

Les valeurs des capacités de charge des signaux D et CLK pour lesquelles une faute peut être induite dans une DFF ou non sont données dans la Figure 4.2. Elles ont été déterminées en utilisant les mêmes simulations que dans la partie 3.2. Dans le cas d'une chute de swing produite par une impulsion de tension d'amplitude V_{pulse}=300V et de largeur PW=10ns, les deux valeurs des capacités sont changées et pour chaque couple de valeurs, on détermine si une faute a été induite dans l'opération du circuit ou non.

Dans un premier temps, pour une valeur de C_D à 0,1fF, correspondant à une très faible charge sur la ligne, aucune faute n'est induite. Le front D est suffisamment rapide pour se rétablir correctement avant le rétablissement du front d'horloge. De même, si la charge sur l'entrée CLK de la bascule est forte ($C_{CLK} > 75$fF) l'induction d'une faute est plus difficile car le front d'horloge sera suffisamment retardé pour que D puisse se stabiliser à nouveau avant le front. Cependant pour $C_D > 10$fF, des fautes sont induites indépendamment de la charge sur CLK.

Compte tenu des résultats obtenus, on peut conseiller aux concepteurs de s'assurer que $C_D \leq C_{CLK}$, même si cela reste difficile à mettre en œuvre. En effet, les portes des blocs

logiques sont généralement plus chargées que les portes de l'arbre d'horloge. En outre, les concepteurs cherchent généralement à minimiser la durée des fronts d'horloges de sorte à faciliter la satisfaction des contraintes de temps de propagation.

Une solution alternative équivalente peut consister en l'augmentation du drive (définition du « drive » section 3.2.1) des portes logiques pilotant la DFF pour permettre un rétablissement plus rapide de D.

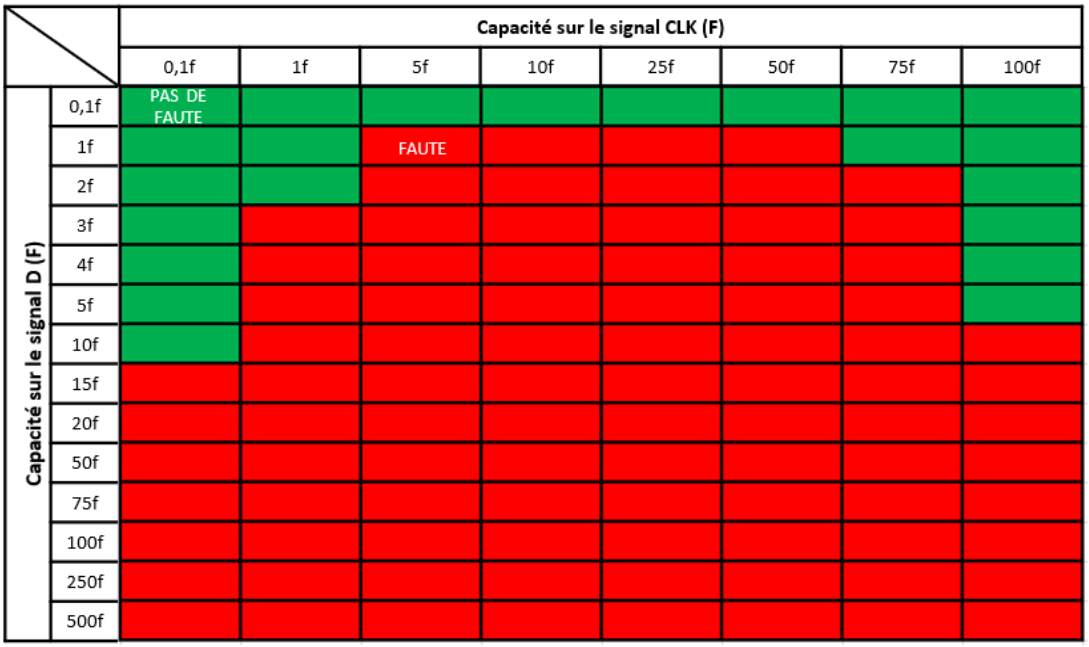


Figure 4.2 - Valeurs des capacités de charge du signal D et CLK pour lesquelles une faute est induite (rouge) ou non(vert), dans la DFF.

4.1.3 Influence des capacités de découplage

La puce de test TC1, possède une version avec un nombre de capacités de découplage accrue. En effet, les 30% de cellules de remplissage présentes dans TC1 (voir Annexe 1) ont été remplacée par des capacités de découplage, portant la surface occupée par les cellules de découplages à 40% (contre 10% pour TC1). Cette version est nommée TC2. L'impact des EMFIs a été évalué sur cette puce dans les mêmes conditions expérimentales que pour la puce de référence. Dans un premier temps, des tirs EM ont été effectués sur l'intervalle de temps correspondant à la durée de fenêtre de faute d'échantillonnage de la puce de référence. La largeur de la fenêtre de fautes obtenue a été mesurée puis comparée à celle de la puce de référence. Aucune différence n'a été constatée entre les 2 puces.

Les mesures ont donc été poussées, dans un second temps, afin de comparer la probabilité d'induire une faute P_f en fonction de la valeur de V_{pulse}. Des EMFIs ont été

réalisées pour un instant de tir fixe correspondant à une probabilité d'induire une faute de 100% pour la puce de référence. L'amplitude V_{pulse} des impulsions de tension a été progressivement changée de -100V à -400V avec un pas de 2V. Le PW a été fixé à 10ns. Les résultats de ces mesures sont donnés dans la Figure 4.3.

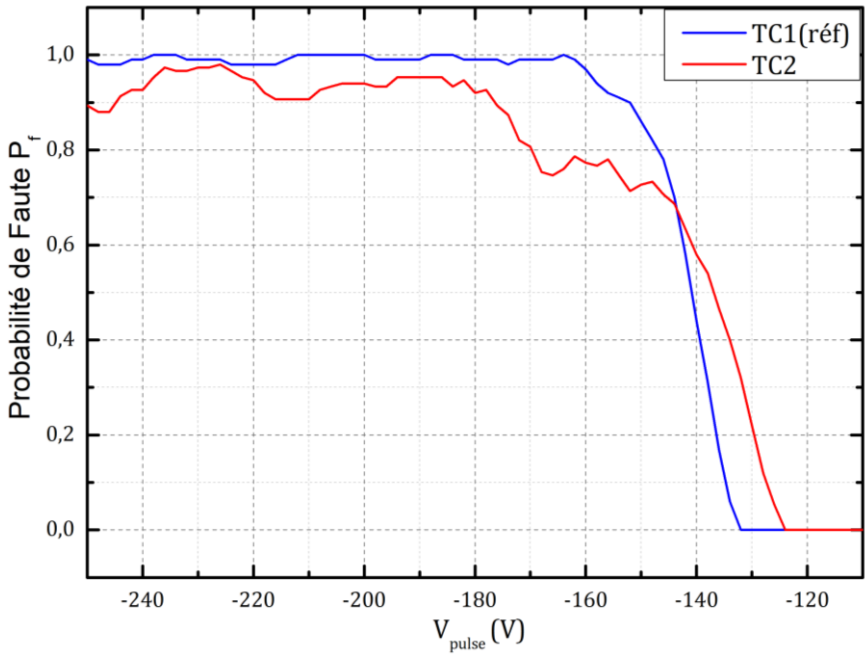


Figure 4.3 - Comparaison de la probabilité d'induction de fautes par EMFI des puces de test TC1 et TC2 en fonction de la tension de pulse V_{pulse}.

Les courbes de cette figure montrent la variation de la probabilité d'induire une faute par EMFI en fonction de V_{pulse}. Ainsi, les premières fautes induites dans la puce de référence TC1 l'ont été pour une valeur V_{pulse}=-132V, tandis qu'elles apparaissent pour une valeur V_{pulse} légèrement plus faible de -124V pour le TC2. Néanmoins on remarque que l'augmentation de P_f en fonction de V_{pulse} est plus rapide pour la puce TC1 que pour la TC2. En effet, P_f passe de 0 à 100% avec une augmentation de V_{pulse} de 32V, tandis que sur la TC2 P_f n'arrive jamais réellement à 100%. Pour que la probabilité de faute atteigne 90% l'augmentation requise du V_{pulse} est de 54V. Malgré cela, on ne constate pas une différence significative entre les deux puces, permettant de définir l'augmentation du nombre de capacités de découplage comme un moyen de rendre un CI plus robuste face aux EMFI, et ceci d'autant plus qu'une incertitude réside quant au placement de la sonde d'injection au-dessus des deux puces.

Pour vérifier ces mesures, des simulations similaires à celles reportées section 2.4 ont été effectuées. De même que pour la puce TC2, les valeurs des capacités de découplage, C_{DECAP}, ont été doublées lors de ces simulations qui ont fourni des cartographies de chute de swing sur la surface du circuit. Ces cartographies sont visuellement identiques à celles

de la Figure 2.25. Les amplitudes de ces chutes de swing sont elles aussi très similaires avec, au maximum, une dizaine de millivolts d'écart. Ces résultats ont permis de valider de manière croisée tant le modèle que les résultats de ces expérimentations délicates.

Les concepts présentés dans cette partie constituent des règles simples pouvant être prises en compte lors de la conception d'un CI. Les parties suivantes abordent quant à elles, des contre-mesures à l'EMFI.

4.2 Exploitation des fils de bonding

Les mesures effectuées dans la partie 2.2 ont mis en évidence le fort couplage pouvant exister entre un champ EM et un fil de bonding. En effet, ces derniers constituent de formidables antennes pouvant être vecteurs de la formation de fronts parasites lors d'une EMFI. En se basant sur ces observations, une contre-mesure a été mise en place avec pour objectif de détecter une impulsion EM effectuée sur un CI.

Le principe de cette contre-mesure est de placer un (ou plusieurs) fils de bonding, traversant le CI ou une partie de celui-ci, comme représenté Figure 4.4. Ces fils de bonding sont connectés à un circuit de détection. Ils peuvent être placés soit sur l'ensemble du circuit soit sur une partie sensible du CI que l'on souhaite protéger.

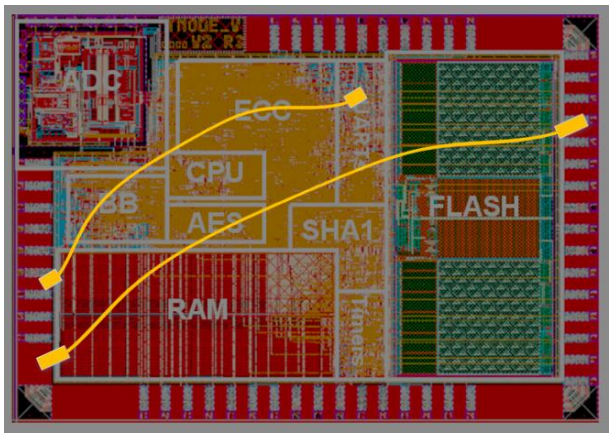


Figure 4.4 - Représentation de la surface d'un CI traversé par de deux fils de bonding pour détecter un champ EM.

Le principe du circuit de détection réside simplement en la comparaison d'un module de référence, connecté au circuit interne classique, et d'un autre module « cible » qui sera connecté aux fils de bonding. Le circuit présenté Figure 4.5 est basé sur les mesures d'EMFI réalisées sur le testchip composé de registre à décalage. Deux registres à décalage sont utilisés. Le registre à décalage de référence a son signal CLK relié à l'horloge interne du circuit et le registre est rebouclé sur lui-même via le réseau d'alimentation interne du

CI. À l'inverse, le registre de détection a son signal CLK relié à un fil de bonding et est rebouclé sur lui-même via un autre fil de bonding. Les deux sorties de registres à décalage sont reliées à une porte NAND et à une alarme.

Lors d'une EMFI sur le circuit, une perturbation est induite sur un ou deux fils de bonding. Celle-ci créée un front parasite sur la CLK et/ou la donnée logique du registre de détection. Dans les deux cas, le bit de sortie à décalage de détection est alors différent de celui de référence et déclenche le signal d'alarme. Un seuil de détection bas doit être mis en place pour éviter de fausses détections dû à des champs EM environnant.

La contre-mesure intègre une détection de suppression des fils de bonding. En effet, si l'un des deux fils de bonding est coupé l'évolution du contenu du registre de détection ne suit pas celle du registre de référence et l'alarme est déclenchée. Elle offre également l'avantage de brouiller les émissions EM du circuit, ce qui complexifie les attaques par observation.

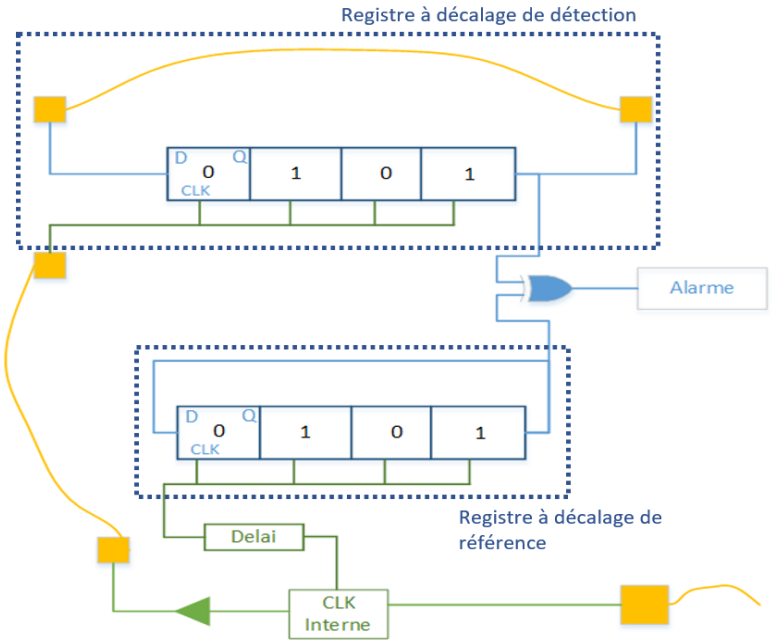


Figure 4.5 - Contre-mesure constituée de deux fils de bonding, connectés au registre à décalage de référence ou de détection.

De plus, cette contre-mesure offre l'avantage de pouvoir utiliser différents circuits de détection. Un premier utilisant les registres à décalages a été décrit. Mais d'autres versions de circuit de détection sont données Figure 4.6.

Le circuit du haut (Figure 4.6 (a)), utilise les entrées reset de deux bascules asynchrones. Les bascules sont initialisées à '1' et les entrées reset des bascules sont connectées à un réseau interne de reset stable à '0'. Lors d'une injection de champ EM, un front

parasite se créé sur le fil de bonding, provoquant un reset dans l'une des bascules et ainsi le déclenchement de l'alarme.

Le second circuit de détection (b) est facilement implémentable dans un circuit puisqu'il ne comprend que 3 portes logiques, deux XOR et une porte OR. Chaque porte XOR est connectée d'une part aux Vdd (ou Gnd) via le circuit interne et d'autre part à Vdd (ou Gnd) via un des fils de bonding de détection. Celles-ci sont ensuite reliées à une porte OR puis à l'alarme. Quand un front parasite, positif ou négatif, est induit sur un fil de bonding l'état de sortie d'une des XOR change, ce qui déclenche l'alarme. L'atout de ce circuit de détection est qu'en fonctionnement normal, il consomme très peu de courant puisqu'il n'est pas relié à une horloge. De même, si un des fils de bonding est retiré (ou cassé) les faibles pull-up ou pull-down, connectés aux portes, permettront de détecter ce retrait.

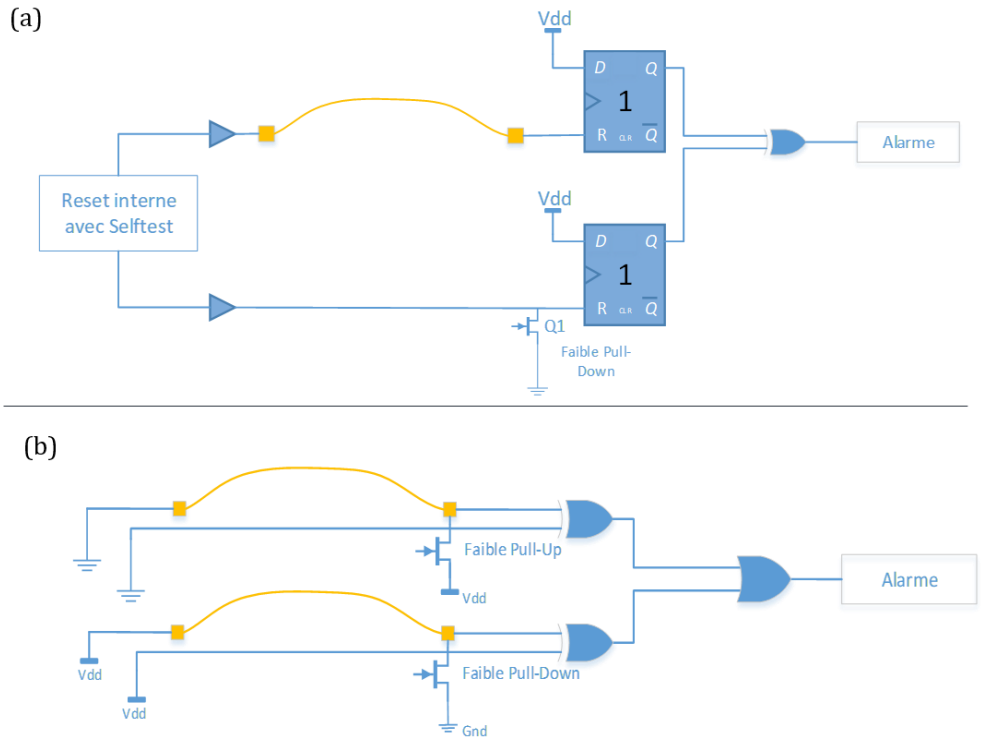


Figure 4.6 - Possibles circuits de détection pour la contre-mesure. (a) Comparaison digitale utilisant le signal reset de bascule asynchrone, (b) détection avec circuit combinatoire.

Ces propositions de circuit de détection permettent aux concepteurs de choisir le circuit convenant le mieux au CI. Son implémentation peut dépendre de la place disponible sur le layout ou de la puissance utilisée par le circuit de détection.

4.3 Détecteurs de dérives temporelles

Le détecteur de dérives temporelles, appelé DTFD (pour Differential Timing Fault Detector) se veut être une contre-mesure contre tout type d'attaque par injection de fautes (Laser, BBI, Glitch). C'est pourquoi dans le cadre de nos mesures, cette contre-mesure implémentée dans un circuit de test en technologie 40nm a été soumise à l'EMFI. C'est une contre-mesure principalement utilisée pour détecter les fautes de violation de contraintes de temps, mais la présence de bascules dans son fonctionnement peut également permettre de détecter des fautes d'échantillonnage. Cette contre-mesure est confidentielle, ce qui limite la description des mesures pouvant être faites dessus, ainsi que les détails d'implémentation donnés dans cette partie.

Contrairement à d'autres détecteurs de fautes de timing comparant le retard induit sur un chemin logique, son fonctionnement se base sur la comparaison de plusieurs chaînes de délai, les unes par rapport aux autres. De plus, cette comparaison de délais s'effectue à un intervalle de temps inférieur à la période de l'horloge. Un schéma d'implantation des chaînes de délai de la contre-mesure est représenté dans la Figure 4.7. Quatre chaînes de délai, constituées d'une cascade de portes logiques, sont routées parallèlement les unes par rapport aux autres. Les temps de propagation des signaux circulant dans ces chemins logiques sont égaux (hors perturbation).

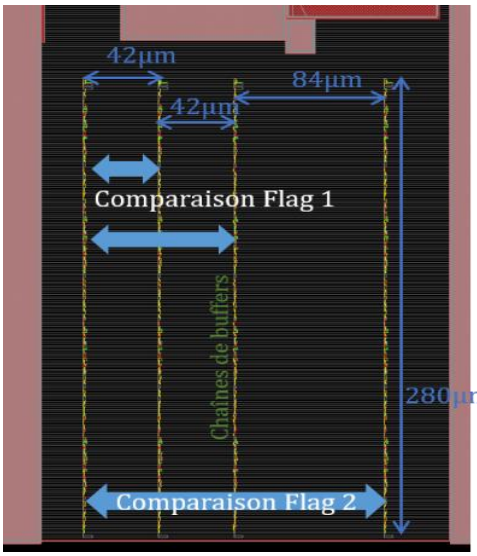


Figure 4.7 - Schéma du principe de fonctionnement de la contre-mesure DTF.

Les chemins logiques de droite sont placés et routés à une distance prédéfinie de celui de gauche à savoir : 42µm, 84µm et 168µm. Les différents espacements entre ces lignes permettent de comparer les délais de transition des portes logiques dans différentes zones du circuit. Des bascules sont disposées uniformément le long des lignes,

entre celles-ci. Elles permettent la comparaison, toutes les 5ns, des temps de propagation des signaux depuis l'entrée jusqu'à différents points répartis le long de ces chemins. Les délais de propagation sont comparés entre la ligne de gauche, servant de référence, et les trois autres lignes. Ainsi, si une différence de temps de propagation entre la ligne 1 et 2 ou 1 et 3 est induite, elle sera détectée et signalée par le Flag 1 passant à '1'. Une différence constatée entre les deux lignes les plus éloignées sera signalée par le Flag 2.

Une campagne de mesure a donc été réalisée dans le but de déterminer l'efficacité de cette contre-mesure face à l'EMFI. Cette contre-mesure étant sensible pour STMicroelectronics, les données reportées ci-après ne sont pas représentatives de tous les essais qui ont été effectués.

Dans le but de déterminer l'efficacité du DTFD, les valeurs contenues dans les deux registres de Flag1 et Flag2 sont scrutées lors des EMFIs ainsi que celle contenue dans un registre quelconque du circuit pris comme témoin du fonctionnement du reste du circuit. Les deux Flag sont d'abord initialisés à '0' et un message hexadécimal de type 55AA est envoyé dans le registre témoin. Une fois l'EMFI effectuée, ces trois registres sont lus. Comme précédemment, l'évolution de la probabilité d'induire une (des) faute(s) dans ces registres en fonction de différents paramètres a été étudiée.

Dans un premier temps, des tirs EM ont été effectués à différents t_{pulse} afin de déterminer quels types de fautes étaient induits dans le circuit. Les paramètres du pulse étaient, lors de ces tests, les suivants : V_{pulse}=-350V et PW=10ns. La sonde utilisée est la même que précédemment, avec un diamètre de 500µm. Les résultats de ces tests sont reportés Figure 4.8 (a). On peut constater qu'aucune faute n'est induite dans le registre témoin (courbe noire), et ce malgré de nombreux essais (changement de certains paramètres tels que Vdd par exemple). Cela peut s'expliquer par plusieurs points. D'abord les règles de contraintes de temps des registres (or détecteur) sont optimisées pour éviter les fautes de timing. De plus, le registre peut être robuste aux fautes d'échantillonnage s'il n'est pas dans les caractéristiques RC requises pour l'obtention d'une faute d'échantillonnage (comme la capacité de charge sur la CLK et D par exemple).

Néanmoins, les registres de détection (Flag) de la perturbation EM ont une probabilité de fautes différente de 0. Donc la contre-mesure a bel et bien détecté une tentative d'attaque EMFI. Aucune fenêtre de faute(s) n'a été observée. Il ne s'agit donc pas de fautes d'échantillonnage et la détection se fait bien par détection d'une différence de temps de propagation des signaux dans les différentes chaînes de délai. Même si, comme nous l'avons dit, l'EMFI induit peu de retard dans les temps de propagation des signaux à travers les portes logiques, la comparaison de ces derniers est suffisamment précise pour détecter même une légère différence.

Le Flag1 (courbe bleue), correspond au résultat de la comparaison des délais des deux chemins logiques les plus proches (les plus à gauche). Sa probabilité de déclenchement, lors de nos EMFIs, a oscillé entre 0,2 et 0,4. Le Flag2 (courbe rouge), compare les délais des deux chemins les plus éloignés. Sa probabilité de déclenchement est restée proche de 1 lors de nos tests. Les distances entre les chemins monitorés par les flag1 et flag2 étant respectivement de 84µm et 168µm, ces observations confirment que l'EMFI a bien un effet plus local qu'escompté.

En effet, les résultats obtenus avec notre modèle nous permettent de penser que les perturbations induites par l'EMFI, sur les trois lignes (très rapprochées) impliquées dans le déclenchement du Flag1, sont similaires. Ainsi, les variations des temps de propagation de ces lignes sont également similaires, ce qui explique le faible taux de déclenchement du Flag1 lors de nos tests. À contrario, les chemins logiques impliqués dans le déclenchement du Flag2 (distants de 164µm) doivent, d'après nos résultats de simulation, subir des perturbations significativement différentes, principalement dans le cas d'un champ proche, ce qui est le cas dans ces mesures. L'un d'eux peut même être soumis à une forte perturbation (en étant situé sous le bord de la sonde), tandis que l'autre n'est pas affecté par l'EMFI (en étant situé sous ou hors de la surface de la sonde). Les variations des temps de propagation entre ces deux lignes sont donc très différentes, ce qui explique le fort taux de déclenchement du Flag2. Dans tous les cas, ces résultats montrent que la perturbation induite à un point dans le circuit n'est pas la même de celle induite à 164µm de là dans le circuit, soit approximativement 33 rangées de standard cells plus loin.

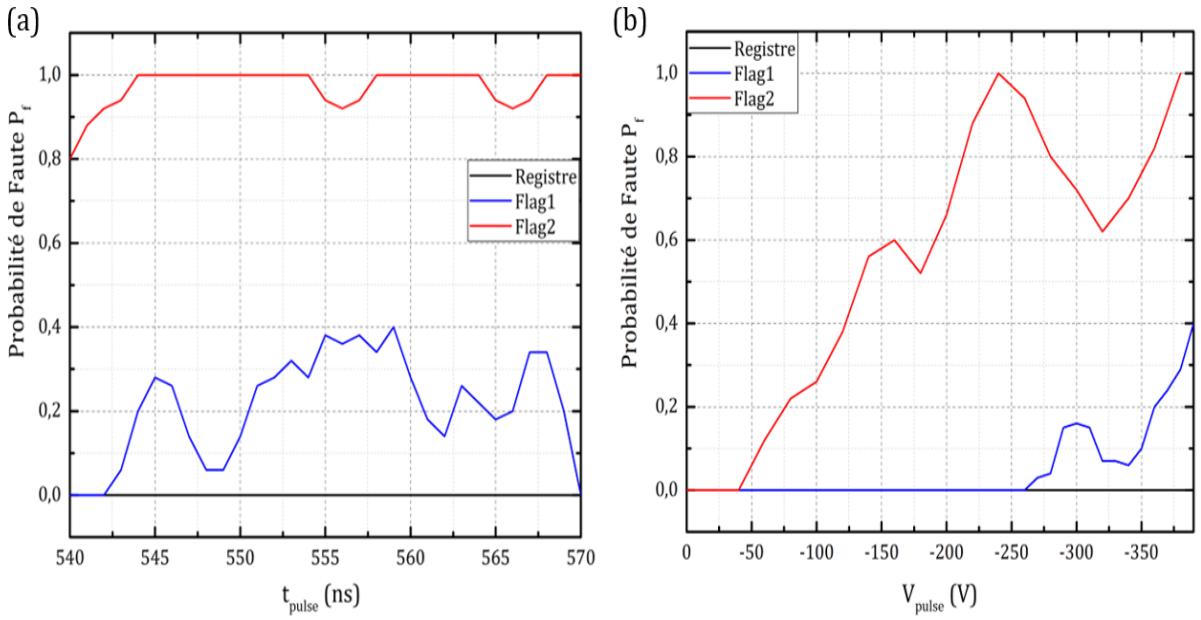


Figure 4.8 - Probabilité d'induire des fautes en fonction du t_{pulse} (à gauche) et V_{pulse} (à droite), lors d'EMFIs effectuées sur la puce DTF.

Dans le but d'évaluer plus finement le DTFD, d'autres mesures ont été réalisées en faisant varier, cette fois, la valeur du V_{pulse} entre 0 et -400V avec un pas de 10V. La Figure 4.8 (a) présente les évolutions de la probabilité d'induire une faute dans le registre témoin ou les Flags de détection, en fonction de la valeur de V_{pulse}. Comme le montre cette figure, aucune faute n'a été induite dans le registre témoin. Le Flag2 permet de détecter les EMFIs avec une fiabilité croissante (quasi-linéairement) de 0% à 100% sur la plage V_{pulse} s'étendant de -40V à -400V. le Flag1 ne détecte rien avant que V_{pulse} ne soit plus grand en valeur absolue à 260V. En outre son taux de détection n'atteint que 40% pour V_{pulse} = -400V.

Les mesures effectuées montrent que le DTFD peut être une contre-mesure efficace face à une attaque par induction EM. La comparaison des délais de propagation entre deux chemins logiques bien espacés semble un bon moyen pour la détection d'une EMFI.

4.4 Simulation et test d'un détecteur d'EMFI

L'une des seules contre-mesures dédiées à la détection de faute d'échantillonnage est celle proposée par [93]et [92]. Cette contre-mesure, entièrement digitale, se base sur le modèle de faute d'échantillonnage et utilise le fait que la bascule D est l'élément le plus sensible dans un circuit soumis à une EMFI. Comme ce détecteur est entièrement numérique, il peut facilement être déployé dans des circuits complexes de smartcards. De plus, sa surface et sa consommation d'énergie sont très faibles par rapport à d'autres contre-mesures analogiques (comme un détecteur de glitch [86], par exemple). Il peut donc être implémenté sous la forme d'un réseau de capteurs sur l'ensemble de la surface d'un CI.

Dans le but de déterminer si notre modèle de faute d'échantillonnage est en adéquation avec les résultats expérimentaux obtenus sur des puces intégrant cette contre-mesure, nous avons simulé son fonctionnement. Le schéma de celle-ci est donné Figure 4.9. Il est constitué de deux blocs distincts. Le premier est la partie « capteur de faute d'échantillonnage », composée de quatre DFFs rebouclées sur elles-mêmes via un inverseur. Ces quatre DFFs représentent toutes les alternatives de configurations de DFF possibles, certaines ayant une entrée Set ou Reset, ou cadencées sur CLK ou $\overline{\text{CLK}}$. Ainsi une détection peut être réalisée autant sur un front montant d'horloge, que sur un front descendant. Leurs sorties Q respectives sont ensuite reliées à la deuxième partie de la contre-mesure : le bloc comparateur. À l'aide de portes XOR, toutes les sorties Q vont être comparées les unes aux autres. Le résultat de la comparaison est ensuite échantillonné par une DFF. Dans le but de mieux identifier les fautes détectées, le schéma a été tronqué. D'autres portes AND sont normalement placées en aval de la sortie OUT pour converger vers un seul signal déclanchant une alarme d'état '0' ou '1'. Les deux blocs, constituant le

détecteur, sont espacés lors de l'implémentation de la CM dans un CI. En effet, il ne faut pas que le bloc comparateur soit perturbé de la même façon que le bloc de détection.

Le chronogramme du détecteur en fonctionnement normal est représenté Figure 4.10 (a). Les signaux de l'horloge ainsi que les six sorties OUT (numérotées de OUT 0 à OUT 5) sont donnés. Chaque sortie est la comparaison XOR de deux sorties Q des DFFs du bloc de détection. Les combinaisons entre les Q comparées et la sortie sont données dans le schéma électrique. Le premier front d'horloge permet d'initialiser correctement le système, ce qui peut être également réalisé avec les entrées Set/Reset des DFFs. Ainsi, en condition normale, les sorties OUT forment le message '110011'. Donc les sorties OUT0, OUT1, OUT4 et OUT5 comparent les signaux Q qui doivent être différents, tandis que ceux sur OUT2 et OUT3 ont la même valeur lors d'un échantillonnage. Si un bit de ce message change, cela veut dire qu'au moins une bascule a été fautées.

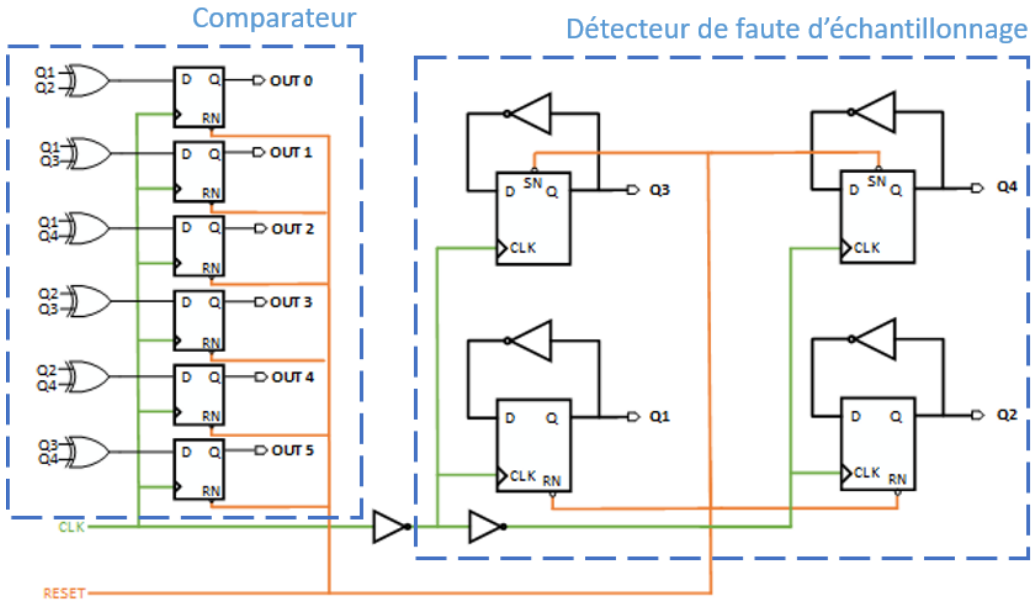


Figure 4.9 - Schéma électrique du capteur d'EMFI.

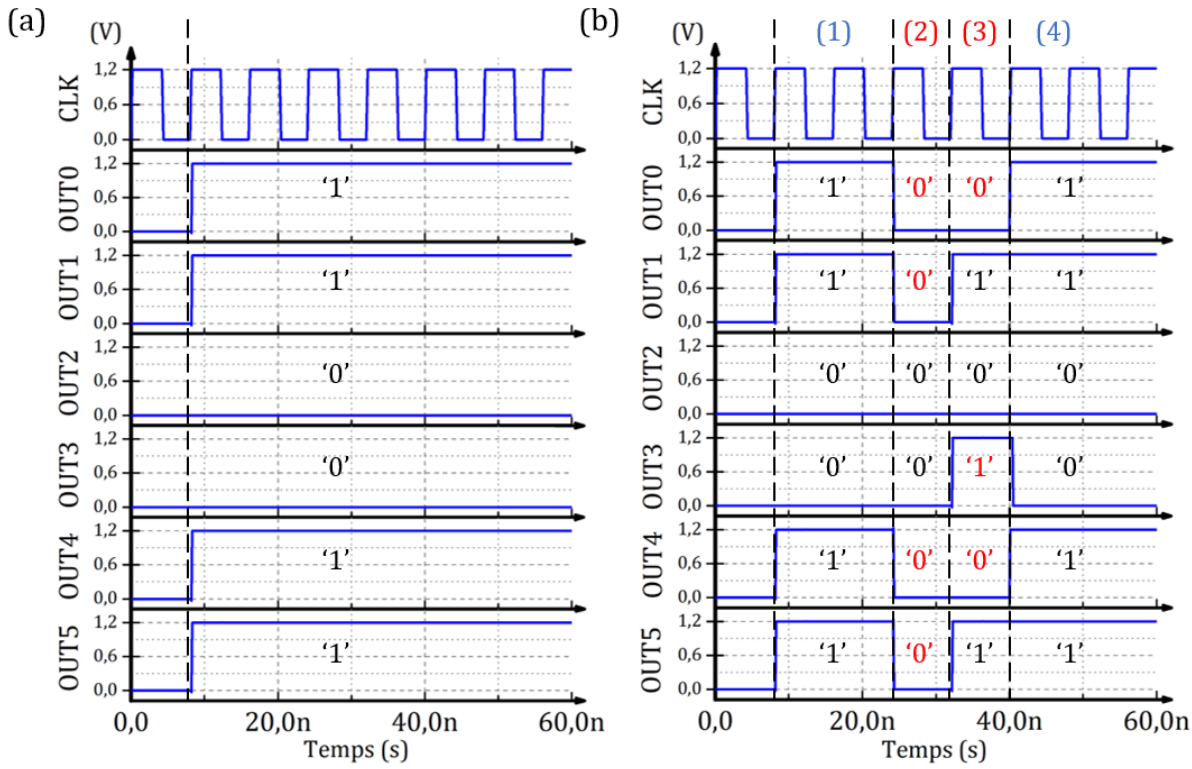


Figure 4.10 – Chronogrammes des signaux du détecteur de fautes d'échantillonnage, (a) en conditions normales ou (b) sous EMFI.

Le circuit a donc été soumis aux simulations d'EMFI comme celle réalisées dans notre modèle. Seulement le bloc de détection (les 4 bascules et leur inverseur) est soumis à une chute de swing. Cette dernière a pour valeurs ΔS=1,9V (V_{pulse}=300V) et S_{width}=10,9ns (PW=10ns). Ces simulations ont été effectuées pour différents instants de

tir autour du front d'horloge se produisant à 32ns. Les résultats de ces simulations sont donnés Figure 4.10 (b) pour CK2E=-3ns. Le chronogramme est découpé en quatre zones distinctes. Dans la zone (1), le CI fonctionne normalement et le message en sortie est correct. Au contraire, les zones (2) et (3) ont des messages différents en sortie, ce qui veut dire que des fautes ont été détectées.

En analysant plus en détail la Figure 4.10, la zone (2) révèle que tous les signaux de sortie sont à '0'. Cela s'explique par le fait que, dans cette zone le circuit est « gelé » (Swing < 0) donc tous ses signaux sont lus comme un état logique '0'. C'est pourquoi les sorties OUT0, OUT1, OUT4 et OUT5 comparent des valeurs égales et sont donc à '0'. Néanmoins, la zone (3) est différente, seules les sorties OUT0, OUT3 et OUT4 sont fautées. Or, la sortie de DFF commune à ces sorties OUT est la sortie Q2. On peut donc en déduire (et le confirmer par des analyses plus poussées des simulations) qu'une faute d'échantillonnage a été induite sur la bascule de sortie Q2. Enfin la zone (4) représente le retour à l'état normal de tous les signaux du détecteur.

Les simulations d'EMFI induites sur le détecteur de fautes ont montré que son fonctionnement pouvait être confirmé par les simulations basées sur notre modélisation. Tout comme les mesures expérimentales effectuées par D. El-Baze [93], des fautes sont induites et détectées par cette contre-mesure. Il semble donc que de telles simulations puissent être utilisées par des concepteurs pour tester la validité et évaluer l'efficacité de contre-mesures avant fabrication. Une contre-mesure a d'ailleurs été définie par simulation dans les derniers mois de ma thèse. Celle-ci fait l'objet d'un dépôt de brevet. Aucun résultat n'est donc donné dans ce document.

4.5 Conclusion

L'état de l'art a mis en évidence le manque de contre-mesures contre l'EMFI. La modélisation présentée tout au long de cette thèse a permis de mettre en avant des éléments clés pouvant permettre la conception de contre-mesures. Certains de ces éléments ont été réutilisés dans ce chapitre pour proposer des règles de conception et des concepts de contre-mesures face aux EMFIs.

Dans un premier temps, une attention particulière peut être portée sur la phase de conception des CIs. En effet, dès le début des règles de conceptions peuvent être mises en place pour rendre les CIs plus robustes face aux EMFI. La première concerne le routage des grilles d'alimentations Vdd et Gnd. Les boucles formées par celles-ci, couplant avec le champ EM, peuvent être coupées au niveau du Métal1. L'alimentation des portes logiques n'en serait que peu altérée et cela permettrait une réduction significative du couplage

entre le CI et le champ EM. Une deuxième règle de conception porte sur le routage des portes logiques du circuit. Le nombre de portes reliées sur un nœud du circuit, traduit par les capacités de charge présentes aux entrée D et CLK de la bascule, ont une grande influence sur l'occurrence d'une faute d'échantillonnage. Celles-ci doivent être pensées soigneusement lors de la conception. Des couples de valeurs de capacités de charge ont été mis en évidence pour réduire les chances d'induire une faute d'échantillonnage. Enfin, des mesures ont été réalisées pour comparer l'effet d'une augmentation du nombre des capacités de découplage des CIs face aux EMFI. Ces dernières n'ont pas révélé de différence notable permettant de définir ce concept comme efficace face à l'EMFI.

Des contre-mesures ont ensuite été proposées. La première s'appuie sur le fort couplage entre le fil de bonding et le champ EM. Le positionnement de fil de bonding sur un CI, relié à un circuit de détection, permettrait de détecter tout champ EM induit au voisinage de la surface du CI. De plus, les analyses et attaques par observation du champ EM rayonné deviendraient également plus complexes car ces fils de bonding brouilleraient les émissions EM du circuit.

Une autre contre-mesure permettant la détection de tous les types d'attaques par injection de fautes, basée sur la détection de dérives temporelles, a été analysée. Elle a été soumise à des mesures EMFI et présente des résultats satisfaisants quant à son efficacité. L'analyse de ces mesures a également confirmé que l'injection EM est plus locale qu'escomptée.

Enfin, la contre-mesure proposée dans [93] a été étudiée par simulation afin d'évaluer son efficacité. Les résultats de ces simulations ont confirmé que ce détecteur numérique était efficace pour la détection des fautes d'échantillonnage.

Synthèse

L'ensemble des analyses et résultats présentés au cours de cette thèse permettent d'apporter de nombreux éclaircissements à des questions concernant l'attaque par injection de faute électromagnétique, que nous allons détailler ci-dessous. Ces réponses permettent de résumer les points importants de cette thèse. Un renvoi vers les parties correspondantes est donné pour le lecteur afin d'avoir plus détails quant à la réponse apportée.

- Quels sont les couplages intervenant dans l'induction d'une faute par EMFI ?

Par analyse et modélisation des effets du champ EM sur le circuit, il a été mis en évidence que les très nombreuses boucles formées par les rails d'alimentations, sur plusieurs niveaux de métaux, constituent des antennes parfaites couplant avec le champ EM. Les rails d'interconnexions, ne formant pas de boucles, sont moins susceptibles de coupler avec le champ EM. Les forces électromotrices, induites par le champ EM, sont donc induites principalement sur les grilles alimentations et de masse des portes logiques (Section 2.3).

- Quelle est la résolution spatiale de l'attaque par EMFI ?

L'EMFI est considérée comme une attaque locale mais ayant un champ d'action très large. Cependant, les simulations ont démontré que les variations maximales de tension pouvaient être induites sur le circuit avec une meilleure localité que ce qui était supposé. En effet, pour une sonde d'injection proche du circuit (ou en contact), l'effet maximal de l'EMFI se concentre principalement sur les bords de la sonde. Les cartographies des variations de tension indiquent que les perturbations pouvaient être concentrées avec une résolution de quelques dizaines de micromètres (Section 2.4.3.c).

- Comment modéliser électriquement l'EMFI ?

Pour réaliser la modélisation de l'EMFI, les rails d'alimentation et de masse sont représentés par une matrice de réseau RC, ceux-ci sont connectés à une modélisation des cellules logiques basées sur les valeurs extraites du circuit. Le couplage entre le circuit et la sonde EM est formé par une inductance mutuelle dont la bobine primaire est connectée à une modélisation d'une sonde d'injection EM, tandis que les bobines secondaires sont connectées aux branches des réseaux d'alimentation et de masse correspondantes. Les alimentations de portes logiques d'une simulation de circuit logique peuvent ensuite être

connectées à la modélisation du réseau d'alimentation pour simuler les effets de l'EMFI sur le fonctionnement du circuit (Section 2.4.1, 2.4.2 et 3.2).

- Quels types de fautes sont induits par l'EMFI ?

L'état de l'art émet l'hypothèse que les fautes induites par l'EMFI sont des fautes de timing. Pourtant, d'autres articles démontrent que les retards induits par une impulsion EM sont très faibles et que des fautes d'échantillonnage peuvent apparaitre. Les résultats présentés dans ce manuscrit de thèse démontrent que les deux modèles de fautes sont valables, en fonction de la fréquence de fonctionnement du circuit. En effet, à haute fréquence, avec des marges de contraintes temporelles faibles, des fautes de timing peuvent se produire, tandis qu'à basse fréquence ce sont des fautes d'échantillonnage, indépendantes des contraintes temporelles qui se produisent autour des fronts d'horloge. À certaines fréquences, les deux modèles de fautes peuvent être distingués : la probabilité d'induire une faute sera maximale sur une fenêtre de temps autour des fronts montants d'horloge (faute d'échantillonnage) tandis qu'entre ces fenêtres, une probabilité plus faible d'induire une faute est présente (faute de timing) (Section 3.4.2).

- Comment se forment les fautes d'échantillonnage dues à une EMFI ?

Le mécanisme de formation d'une faute de timing due à la violation des contraintes temporelles de 'setup' et 'hold' d'une bascule est bien connu. La modélisation nous a permis de mieux comprendre celui d'une faute d'échantillonnage. Celle-ci est due à un phénomène de « gel/dégel » rapide d'une partie du circuit, ainsi qu'à une « course » de rétablissement entre les signaux. En effet, les signaux d'horloge et logique sont « gelés » durant un certain temps puis, au moment du rétablissement de la polarisation des portes logiques, les deux signaux vont converger vers leurs états finaux. Les signaux d'horloge, conçus pour être les plus rapides dans un circuit, vont se rétablir avant le signal D, ainsi la bascule échantillonne une valeur de D erronée engendrant une faute dans la bascule (Section 3.3.3).

- Quels sont les paramètres idéals pour réaliser une faute par EMFI ?

Dans un premier temps, les paramètres de conception de la sonde d'injection EM ont une grande influence sur l'effet de cette attaque, autant pour son efficacité à induire des fautes que pour sa résolution spatiale. Ces paramètres font l'objet de nombreuses études présentées dans l'état de l'art et ne sont pas développés dans cette thèse.

Nous avons étudié les effets des différents paramètres contrôlables durant des mesures expérimentales : l'amplitude et la largeur de l'impulsion, ainsi que la tension d'alimentation du circuit. D'abord, dans le cas d'un circuit à basse fréquence, un balayage du

pulse EM dans le temps permet de mettre en évidence les fenêtres de temps ou la susceptibilité d'induire une faute est maximale, constituant la plage de temps où la variation des autres paramètres permettra une EMFI optimale. L'augmentation de l'amplitude V_{pulse} du générateur d'impulsion de tension se traduit par une augmentation de la largeur de la fenêtre de fautes ainsi que de la probabilité d'induire une faute. Un V_{pulse} minimal pour induire une faute permet également de limiter la dispersion et la zone affectée par le tir EM, augmentant la résolution temporelle de l'attaque (Section 3.4.3.a). La largeur de l'impulsion PW n'a que peu d'effet sur la probabilité d'induire une faute, si ce n'est qu'elle doit être suffisamment large pour que la variation de tension induite puisse atteindre sa valeur maximale, mais assez réduite pour que les fronts de variations soient rapprochés dans le temps (Section 2.4.3.e et 3.4.3.b). Enfin, une diminution de la tension d'alimentation Vdd induit une augmentation de la probabilité d'induire une faute, pouvant être utilisée lorsque l'amplitude maximale d'un générateur ne permet pas d'induire des fautes sur un circuit alimenté par un Vdd normal (Section 3.4.3.c).

- Comment protéger un circuit face à une EMFI ?

On peut définir trois types de techniques permettant de sécuriser un circuit face aux attaques EMFI. D'abord, lors de la conception du circuit, certains paramètres de routage peuvent permettre d'augmenter la robustesse du circuit face aux EMFIs (Section 4.1). On peut également détecter un champ EM, induit au voisinage du circuit, à l'aide de détecteurs (Section 4.2), cependant une attention particulière doit être portée au seuil de détection, pour ne pas déclencher de fausses alarmes dues à un environnement à forte concentration de champ EM. Enfin, des détecteurs de fautes EM sont possibles (Section 4.3 et 4.4). Dans ce cas, des contre-mesures numériques sont préférables, mais le routage et la distance entre les composants du détecteur (bloc de détection et bloc de déclenchement de l'alarme) sont importants pour ne pas que l'EMFI influe sur les composants déclenchant l'alarme.

Conclusion générale et perspectives

Dans cette thèse, nous avons d'abord présenté un état de l'art de la sécurité des circuits intégrés et les différentes attaques pouvant être menées sur ces circuits. Ce premier chapitre se concentre ensuite sur l'étude de l'attaque matérielle par injection de fautes électromagnétiques et les contre-mesures associées. Il est mis en évidence que, malgré les différentes recherches à propos de cette attaque, les phénomènes amenant à l'induction de fautes restent encore incertains. De plus, encore peu de systèmes permettent d'assurer la robustesse des circuits face à cette attaque.

Les travaux présentés dans cette thèse essayent donc d'apporter des contributions au niveau de la compréhension des phénomènes physiques conduisant à l'apparition d'une faute lors de l'application d'une EMFI, ainsi que de la modélisation de ces effets, ceci dans l'objectif de développer par la suite de nouvelles contre-mesures face aux EMFIs.

Dans un premier temps, nous avons développé une modélisation du couplage entre le champ EM et les grilles d'alimentations du circuit afin de pouvoir simuler les effets induits. Les résultats de simulations ont montré que l'EMFI induit des perturbations de tension, brèves et de fortes amplitudes, localement sur les réseaux d'alimentations Vdd et Gnd. Dépendamment de la position de la sonde, les variations de tension entre les alimentations Vdd et Gnd peuvent être différentes, ce qui a pour effet de modifier la tension de polarisation (swing) de certaines cellules logiques. Des chutes de swing, pouvant être inférieures à zéro, sont ainsi constatées. Cette modélisation permet de simuler les effets de l'EMFI sur l'intégralité des réseaux d'alimentation d'un circuit donnant la position des principales variations du swing. En outre, cela révèle que les variations induites sont relativement locales, et principalement situées sous les bords de la sonde, dans le cas d'une sonde proche (ou en contact) avec la surface du circuit.

Le troisième chapitre se concentre sur le phénomène d'apparition de fautes, dues à l'EMFI, lors du fonctionnement d'un circuit synchrone. La modélisation précédente est appliquée à un circuit logique lors de simulations, comprenant une bascule D. Un critère F a été défini, permettant de mettre en évidence l'effet d'une perturbation sur la bascule, c'est-à-dire soit un retard des temps de propagation internes soit une faute directe sur la bascule. Les simulations d'EMFIs sur le circuit démontrent dans un premier temps que des retards sont induits sur le circuit (pouvant mener à d'éventuelles fautes de timing sur une bascule en avale), mais également que des fautes d'échantillonnage apparaissent autour du front montant d'horloge. Ces fautes forment une fenêtre de fautes, d'une largeur

de quelques nanosecondes dans notre cas. Ces simulations permettent également de mieux comprendre comment ces fautes d'échantillonnage se forment dans un circuit.

Le modèle de faute développé dans cette thèse est vérifié à l'aide de parallèles expérimentaux sur une puce de test embarquant un AES. Un balayage dans le temps de l'impulsion EM, à différentes fréquences d'horloge, montre que des fenêtres de fautes d'échantillonnage apparaissent avec une période égale à la période de l'horloge. Ces fenêtres sont indépendantes de la fréquence d'horloge et des marges de contraintes de temps. La validité de notre modélisation est ensuite démontrée en comparant l'effet des variations de différents paramètres d'injection (V_{pulse}, PW, Vdd), sur la largeur des fenêtres de fautes, en simulation et expérimentalement. Ainsi, la concordance des résultats obtenus permet de valider la justesse de notre modélisation.

Enfin, le quatrième et dernier chapitre présente des propositions de contre-mesures pouvant être utilisées pour sécuriser les circuits face à l'EMFI. Certaines de ses propositions sont issues d'analyses effectuées avec le modèle défini précédemment. Des règles de conception sont d'abord proposées, ayant pour but d'améliorer la robustesse du circuit. Ces règles concernent le routage des réseaux d'alimentation ainsi que la charge capacitive des entrées D et d'horloge d'une bascule D. Deux détecteurs de fautes EM sont ensuite proposés. Le premier utilise les fils de bonding pour détecter un champ EM au voisinage du circuit, tandis que le deuxième détecte des perturbations temporelles très précises. Enfin le détecteur présenté dans [93] est simulé à l'aide de notre modèle dans le but d'analyser et vérifier son fonctionnement.

Ces travaux constituent une étude approfondie des effets de l'EMFI, permettant d'ouvrir la voie à l'élaboration de nouvelles contre-mesures. Cependant, beaucoup de travail reste encore à accomplir dans le domaine des attaques par EMFI.

Dans un premier temps, la modélisation proposée peut être améliorée. Des calculs plus poussés du couplage entre la sonde d'injection et le circuit seraient intéressants afin d'accroître la précision du modèle. De même, la modélisation d'éléments tels que le boîtier du circuit, les fils de bonding et leurs plots, peut être envisagée. Des analyses pourraient être conduites pour déterminer d'autres éléments couplant le champ EM. Une piste serait, par exemple, la boucle créée par les puits et leurs plots d'alimentation. L'application du modèle à un circuit peut être développée à des circuits logiques plus complexes, ayant des marges de temps différentes, ou même à des circuits analogiques pour déterminer les éléments sensibles à une EMFI. En outre, l'idéal serait d'associer l'emplacement des différentes portes logiques sur la surface du circuit avec la position des différentes variations de tension donnée par les cartographies du modèle.

Nous avons observé que la remontée de la chute de swing était vectrice de l'induction d'une faute dans une bascule. Cette remontée est dépendante des temps de montée/descente de l'impulsion de tension. Ainsi, des mesures peuvent être réalisées en faisant varier ces durées de fronts d'impulsion afin d'analyser leurs effets sur la probabilité d'induire une faute par EMFI dans un circuit. De plus, certaines contre-mesures proposées se doivent d'être vérifiées expérimentalement. Finalement, il est espéré que de nouveaux moyens de défense face à l'EMFI puissent être pensés et développés à partir des éléments fournis dans cette thèse.

Annexe 1

Calcul des valeurs de modélisation de la partie 2.4.1 :

Il est important de rappeler que les valeurs de la modélisation sont dépendantes du circuit étudié pour les parallèles expérimentaux.

La longueur du rail M1, constituant un segment de Std Cell, est L=30µm avec une résistivité linéique de 0,858 $\Omega/\mu m$, pour les rails de Métal supérieurs elle est de 1,036 $\Omega/\mu m$ avec une longueur l=5µm.

- $R_{M1} = 30\mu m \times 0{,}858 = 25{,}75\ \Omega \approx 26\ \Omega$
- $R_{Msup} = 5\mu m \times 1{,}036 = 5{,}18\ \Omega \approx 5\ \Omega$
- $R_{VIA} = 5\ \Omega$

Le facteur de couplage $k_{Vdd/Gnd}$ utilisé dans le calcul du couplage, est déterminé comme un rapport de surface entre la sonde d'injection et une boucle du circuit :

- $k_{Vdd/Gnd} = \frac{30\mu m \times 5\mu m}{300\mu m \times 300\mu m} = 0{,}0017$

Calcul des valeurs de modélisation de la partie 2.4.2 :

On considère un bloc logique de 30µm × 5 µm correspondant à un segment de Std Cell :

- 60% de la surface est occupées par des cellules logiques
- 10% de la surface est occupée par des cellules de capacité de découplage
- 30% de la surface est occupées des cellules de remplissage (Filler cells), utilisées pour remplir les espaces vides du circuit et permettant la continuité des rails de connexion. Ces cellules n'interviennent pas dans la modélisation.

Les cellules de capacités de découplage sont constituées de 50% de de type P et 50% de type N. Leur capacité est de 15fF/□. La surface de l'oxyde est de 50%.

- $C_{DECAP}(Type\ P\ ou\ N) = \frac{0{,}1}{2} \times \frac{30\mu m}{5\mu m} \times 15fF \times 0{,}5 = 2{,}25fF$

La largeur des Nwell est de 1,38µm. Celle du substrat P (ou Pwell) est de 5µm-1,38µm. La résistance du Nwell est de 600Ω /□ et du substrat P de 1500Ω /□. Les plots de polarisation des Nwell et du substrat P sont éloignés de 15µm le long des lignes d'alimentations Vdd et Gnd, donc la distance maximale entre le plot et la cellule polarisée est de 7,5µm.

- $R_{NW} = \frac{7{,}5\mu m}{1{,}38\mu m} \times 600 = 3260\ \Omega$
- $R_{Psub} = \frac{7{,}5\mu m}{5\mu m - 1{,}38\mu m} \times 1500 = 3107\ \Omega$

Le nombre de cellules logiques (Std Cell), d'une taille de moyenne de 1,3µm x 0,5µm (basée sur une NAND2) est de :

- $Nombre\ de\ Std\ Cells = \ 0{,}6\ \times \frac{30\mu m \times 5\mu m}{1{,}3\mu m \times 0{,}5\mu m} = 140\ cells\ (NAND2)$

Une NAND2 comprend 2 NMOS et 2 PMOS donc il y a 280 NMOS et 280 PMOS en moyenne dans un segment de Std Cell. Nous sommes en technologie 40nm et W_N=0,3µm et W_N=0,42µm.

- Surface occupée par les transistors NMOS : $0{,}04\mu m \times 0{,}3\mu m \times\ 280 = 3{,}36\mu m^2$
- Surface occupée par les transistors PMOS : $0{,}04\mu m \times 0{,}42\mu m \times\ 280 = 4{,}7\mu m^2$

La résistance équivalente d'un transistor N passant est de 1kΩ et de 1,8kΩ pour un transistor P. Les transistors sont en parallèles, donc :

- $R_N = 1000/280 = 3{,}6\Omega$
- $R_P = 1800/280 = 6{,}4\Omega$

Pour les capacités de grille, on a :

- $C_{GN} = 15fF\ \times\ 3{,}36\mu m^2 = 50{,}4fF/2 = 25{,}2fF$
- $C_{GP} = 15fF\ \times\ 4{,}7\mu m^2 = 70{,}5fF/2 = 35{,}25fF$

Pour la capacité de l'interface Nwell/Psub, on a 1fF/□ et prennent la moitié d'un segment de Std Cell :

- $C_{NW} = 1fF\ \times\ 0{,}5\ \times 30\mu m \times 1{,}38\mu m = 20{,}7fF$

La diode Nwell a pour valeurs de modélisation : W = 1,8µm (largeur des Nwell dans le circuit), et une longueur de L=30µm.

Le substrat profond est très résistif, 100kΩ/µm. Différentes techniques sont possibles pour calculer R_{sub}, mais étant donné que ces résistances sont très grandes elles n'ont que peu d'influence sur nos simulations, elles ont donc été définies à $R_{sub} = 10k\Omega$

Table des acronymes

AES	*Advanced Encryption Standard*
BEOL	*Back-End-Of-Line*
BBI	*Body Biasing Injection*
CEM	*Compatibilité Électromagnétique*
CI	*Circuit intégré*
CM	*Contre-Mesure*
CMOS	*Complementary Metal Oxyde Silicium*
CPU	*Control Processing Unit*
DES	*Data Encryption Standard*
DIL	*Dual In-Line Package*
EEPROM	*Electrically Erasable Programmable Read Only Memory*
EM	*Électromagnétisme*
EMFI	*Electromagnetic Fault Injection*
EMP	*Electromagnetic Pulse*
fem	*Force Électromotrice*
FEOL	*Front-End-Of-Line*
FIB	*Focus Ion Beam*
FPGA	*Field-Programmable Gate Arrays*
IoT	*Internet of Things*
LDO	*Low DropOut*
MPW	*Multi Project Wafer*
NFC	*Near Field Communication*
PVT	*Process Voltage Temperature*
PW	*Pulse Width*
RAM	*Random Access Memory*
RF	*RadioFréquence*
RO	*Ring Oscillator*
ROM	*Read Only Memory*
RSA	*Rivest Shamir Adleman*
SFW	*Sampling Fault Window*
SIM	*Subscriber Identity Module*
TEG	*Test Element Group*
TRNG	*True Random Number Generator*
UART	*Universal Asynchronous Receiver Transmitter*

Liste des figures

Liste des tableaux

Bibliographie

[1] "Xiaomi Mi Robot vacuum cleaner hacked | Kaspersky official blog." URL: https://www.kaspersky.com/blog/xiaomi-mi-robot-hacked/20632/.

[2] "Karotz, le lapin intelligent : attention au piratage ! - CNET France." URL: https://www.cnetfrance.fr/news/karotz-le-lapin-intelligent-attention-au-piratage-39793818.htm.

[3] "Unpatched Flaws in IoT Smart Deadbolt Open Homes to Danger | Threatpost." URL: https://threatpost.com/unpatched-flaws-in-iot-smart-deadbolt-open-homes-to-danger/146871/.

[4] "La cryptographie militaire. A. Kerckhoffs, *La Cryptogr. Mil.*, vol. IX, pp. 161–191, 1883.

[5] R. Torrance and D. James, "The state-of-the-art in IC reverse engineering," *Lecture Notes Computer Science*, vol. 5747 LNCS, pp. 363–381, 2009.

[6] S. P. Skorobogatov and R. J. Anderson, "Optical Fault Induction Attacks," *Lecture Notes Computer Science*, vol. 2523, pp. 2–12, 2003.

[7] S. P. Skorobogatov, "Semi-invasive attacks-a new approach to hardware security analysis," *Tech. report, Univ. Cambridge, Comput. Lab.*, no. 630, 2005.

[8] U. de Riu, B. Fraboni, S. Lall, and H. Ahmed, "Layout Reconstruction of Complex Silicon Chips," *IEEE J. Solid-State Circuits*, vol. 28, no. 2, pp. 138–145, 1993.

[9] D. Samyde, S. Skorobogatov, R. Anderson, and J. J. Quisquater, "On a new way to read data from memory," *Security in Storage Workshop*, pp. 65–69, 2003.

[10] A. Merle and J. Clediere, "Security testing for hardware products: The security evaluations practice," *On-Line Testing Symposium,* vol. 2005, pp. 122–125, 2005.

[11] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems," *Advanced Cryptology*, 1996.

[12] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Lecture Notes Computer Science*, vol. 1666, pp. 388–397, 1999.

[13] T. Ordas, M. Lisart, E. Sicard, P. Maurine, and L. Torres, "Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits," *Lecture Notes in Computer Science*, vol. 5349, pp. 229–236, 2009.

[14] E. De Mulder *et al.*, "Electromagnetic analysis attack on an FPGA implementation of an elliptic curve cryptosystem," *Computer as a Tool*, vol. II, pp. 1879–1883, 2005.

[15] M. Y. Tay, M. C. Tan, W. Qiu, and X. L. Zhao, "Lock-in thermography application in flip-chip packaging for short defect localization," *Electronics Packaging Technology Conference*, pp. 642–646, 2011.

[16] M. Cozzi, J. M. Galliere, and P. Maurine, "Thermal scans for detecting hardware trojans," *Lecture Notes in Computer Science*, vol. 10815, pp. 117–13, 2018.

[17] D. Binder, E. C. Smith, and A. B. Holman, “Satellite anomalies from galactic cosmic rays,” *IEEE Trans. Nucl. Sci.*, vol. 22, no. 6, pp. 2675–2680, 1975.

[18] D. Boneh, R. A. Demillo, and R. J. Lipton, “On the importance of checking cryptographic protocols for faults,” *Lecture Notes in Computer Science*, vol. 1233, pp. 37–51, 1997.

[19] E. Biham and A. Shamir, “Differential fault analysis of secret key cryptosystems,” *Lecture Notes in Computer Science,* vol. 1294, pp. 513–525, 1997.

[20] G. Piret and J. J. Quisquater, “A differential fault attack technique against SPN structures, with application to the AES and KHAZAD,” *Lecture Notes Computer Science*, vol. 2779, pp. 77–88, 2003.

[21] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, “The Sorcerer’s Apprentice Guide to Fault Attacks.” IEEE, vol. 94, no. 2, pp. 370–382, 2006.

[22] M. Soucarros, C. Canovas-Dumas, J. Clédière, P. Elbaz-Vincent, and D. Réal, “Influence of the temperature on true random number generators,” *Hardware-Oriented Security and Trust* , pp. 24–27, 2011.

[23] P. Maurine, M. Rezzoug, and D. Auvergne, “Output transition time modeling of CMOS structures,” *Circuits and Systems, Conference Proceedings*, vol. 5, pp. 363–366, 2001.

[24] A. Barenghi, G. Bertoni, E. Parrinello, and G. Pelosi, “Low voltage fault attacks on the RSA cryptosystem,” *Fault Diagnosis and Tolerance in Cryptography*, pp. 23–31, 2009.

[25] A. Barenghi, G. M. Bertoni, L. Breveglieri, M. Pellicioli, and G. Pelosi, “Low voltage fault attacks to AES,” *Hardware-Oriented Security and Trust*, pp. 7–12, 2010.

[26] Z. B. Du, Y. Chen, and A. D. Chen, “The impact of the clock frequency on the power analysis attacks,” *Internet Technology and Applications,* 2011.

[27] C. Aumüller, P. Bier, W. Fischer, P. Hofreiter, and J. P. Seifert, “Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures,” *Lecture Notes Computer Science,* vol. 2523, pp. 260–275, 2003.

[28] T. Fukunaga and J. Takahashi, “Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers,” *Fault Diagnosis and Tolerance in Cryptography*, pp. 84–92, 2009.

[29] N. Beringuier-Boher, M. Lacruche, D. El-Baze, J. M. Dutertre, J. B. Rigaud, and P. Maurine, “Body biasing injection attacks in practice,” *ACM International Conference Proceeding Series*, pp. 49–52, 2016.

[30] K. Tobich, P. Maurine, P. Y. Liardet, M. Lisart, and T. Ordas, “Voltage spikes on the substrate to obtain timing faults,” *16th Euromicro Conference on Digital System Design*, pp. 483–486, 2013.

[31] G. Cellere *et al.*, “Total ionizing dose effects in NOR and NAND flash memories,” *Transactions on Nuclear Science*, vol. 54, no. 4, pp. 1066–1070, 2007.

[32] S. Gerardin *et al.*, “Radiation effects in flash memories,” *Transactions on Nuclear Science*, vol. 60, no. 3, pp. 1953–1969, 2013.

[33] H. Li, G. Du, C. Shao, L. Dai, G. Xu, and J. Guo, “Heavy-Ion Microbeam Fault Injection into SRAM-Based FPGA Implementations of Cryptographic Circuits,” *Transactions on Nuclear Science*, vol. 62, no. 3, pp. 1341–1348, 2015.

[34] J. Schmidt and M. Hutter, “Optical and em fault-attacks on crt-based rsa: Concrete results,” *Proc. Austrochip*, pp. 61–67, 2007.

[35] A. Sarafianos *et al.*, “Electrical modeling of the photoelectric effect induced by a pulsed laser applied to an SRAM cell,” *Microelectronics Reliability*, pp.1300-1305, 2013.

[36] A. Sarafianos *et al.*, “Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology," *Physical and Failure Analysis of Integrated Circuits*, pp. 22-27, Apr. 2013.

[37] A. Sarafianos *et al.*, “Building the electrical model of the Photoelectric Laser Stimulation of a PMOS transistor in 90 nm technology,” *Microelectronics Reliability*, vol. 52, no. 9–10, pp. 2035–2038, 2012.

[38] C. Champeix, N. Borrel, J. M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, “SEU sensitivity and modeling using picosecond pulsed laser stimulation of a D Flip-Flop in 40 nm CMOS technology,” *Defect and Fault Tolerance in VLSI and Nanotechnology Systems*, pp. 177–182, 2015.

[39] C. Roscian, J.-M. Dutertre, A. Tria, and A. Tria Frontside, “Laser Fault Injection on Cryptosystems-Application to the AES’ last round," *Hardware-Oriented Security and Trust,* 2013.

[40] B. Selmke, J. Heyszl, and G. Sigl, “Attack on a DFA Protected AES by Simultaneous Laser Fault Injections,” *Fault Diagnosis and Tolerance in Cryptography,* pp. 36–46, 2016.

[41] J. Rodriguez, A. Baldomero, V. Montilla, and J. Mujal, “LLFI: Lateral laser fault injection attack,” *Fault Diagnosis Tolerance in Cryptography,* pp. 41–47, 2019.

[42] S. Anceau, P. Bleuet, J. Clédière, L. Maingault, J. luc Rainard, and R. Tucoulou, “Nanofocused X-ray beam to reprogram secure circuits,” *Lecture Notes in Computer Science,* vol. 10529 LNCS, pp. 175–188, 2017.

[43] H. A. Kalhor, “The Degree of Intelligence of the Law of Biot-Savart,” *IEEE Trans. Educ.*, vol. 33, no. 4, pp. 365–366, 1990.

[44] R. Possamai Bastos *et al.*, “A Bulk Built-in Sensor for Detection of Fault Attacks," *Hardware-Oriented Security and Trust*, pp. 51–54, 2013.

[45] J.-J. Quisquater and D. Samyde, “Eddy current for magnetic analysis with active sensor.” 2002.

[46] F. Vargas, D. L. Cavalcante, E. Gatti, D. Prestes, and D. Lupi, “On the proposition of an EMI-based fault injection approach,” *International On-Line Testing Symposium,* pp. 207–208, 2005.

[47] F. Poucheret, K. Tobich, M. Lisart, and B. Robisson, “Local and Direct Power Injection on CMOS Integrated Circuits,” *Fault Diagnosis and Tolerance in Cryptography,* pp.100-104, 2011.

[48] P. Bayon *et al.*, "Contactless electromagnetic active attack on ring oscillator based true random number generator," *Lecture Notes Computer Science*, vol. 727, pp. 151–166, 2012.

[49] A. Marghescu, D. C. Vasile, P. Svasta, and E. Simion, "Personalized Ring Oscillator-based True Random Number Generator analysis using non-invasive attacks," *Design and Technology in Electronic Packaging,* pp. 98–101, 2016.

[50] L. Riviere, Z. Najm, P. Rauzy, J. L. Danger, J. Bringer, and L. Sauvage, "High precision fault injections on the instruction cache of ARMv7-M architectures," *Hardware-Oriented Security Trust,* pp. 62–67, 2015.

[51] Y. I. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, "Precisely timed IEMI fault injection synchronized with em information leakage," *Electromagnetic Compatibility*, pp. 738–742, 2014.

[52] P. Maurine, "Techniques for EM fault injection: Equipments and experimental results," *Fault Diagnosis Tolerance Cryptography*, pp. 3–4, 2012.

[53] D. Alberto, P. Maistri, and R. Leveugle, "Investigation of Electromagnetic Fault Injection Effects on Embedded Cryptosystems," 2013.

[54] R. Velegalati, R. Van Spyk, and J. Van Woudenberg, "Electro Magnetic Fault Injection in Practice," *International Cryptographic Module Conference*, 2013

[55] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz, "Electromagnetic fault injection: Towards a fault model on a 32-bit microcontroller," *Fault Diagnosis Tolerance Cryptography,* pp. 77–88, 2013.

[56] M. Madau *et al.*, "The impact of pulsed Electromagnetic Fault Injection on true random number generators," *Fault Diagnosis and Tolerance in Cryptography*, pp. 43-48, 2018.

[57] S. K. Bukasa, R. Lashermes, J. L. Lanet, and A. Leqay, "Let's shock our IoT's heart: ARMv7-M under (fault) attacks," *ACM International Conference Proceeding Series*, 2018.

[58] A. Dehbaoui, J. M. Dutertre, B. Robisson, and A. Tria, "Investigation of near-field pulsed EMI at IC level," *Asia-Pacific Symp. Electromagn. Compat,* 2013.

[59] A. Dehbaoui, J. M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of AES," *Fault Diagnosis Tolerance Cryptography,* pp. 7–15, 2012.

[60] P. Maistri *et al.*, "ElectroMagnetic Analysis and Fault Injection onto Secure Circuits," *Conference on VLSI and System-on-Chip*, 2014.

[61] A. Dehbaoui, J.-M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria, "Injection of transient faults using electromagnetic pulses Practical results on a cryptographic system," *Cryptol. ePrint Arch.*, 2012.

[62] S. Ordas, L. Guillaume-Sage, K. Tobich, J. M. Dutertre, and P. Maurine, "Evidence of a larger EM-induced fault model," *Lecture Notes in Computer Science*, vol. 8968, pp. 245–259, 2015.

[63] S. Ordas, L. Guillaume-Sage, and P. Maurine, "Electromagnetic fault injection: the curse of flip-flops," *Journal of Cryptographic Engineering*, vol. 7, no. 3, pp. 183–197, 2017.

[64] S. Ordas, L. Guillaume-Sage, and P. Maurine, “EM injection: Fault model and locality,” *Fault Diagnosis Tolerance Cryptogaphy,* pp. 3–13, 2016.

[65] O. Trabelsi, L. Sauvage, and J. L. Danger, “Impact of Intentional Electromagnetic Interference on Pure Combinational Logic,” *Electromagnetic Compatibility*, pp. 398–403, 2019.

[66] O. Trabelsi, L. Sauvage, and J. L. Danger, “Characterization at logical level of magnetic injection probes,” *Asia-Pacific Int. Symp. Electromagnetic Compatibility*, pp. 625–628, 2019.

[67] A. Menu, S. Bhasin, J. Dutertre, and J. Rigaud, “Precise Spatio-Temporal Electromagnetic Fault Injections on Data Transfers,” *Fault Diagnosis Tolerance Cryptography*, 2019.

[68] M. Ghodrati, B. Yuce, S. Gujar, C. Deshpande, L. Nazhandali, and P. Schaumont, “Inducing Local Timing Fault Through EM Injection,” *Design Automation Conference*, pp. 1–6, 2018.

[69] N. Saga, T. Itoh, Y. H. Takaaki, and H. Sone, “Study on the Effect of Clock Rise Time on Fault Occurrence under IEMI,” *Asia-Pacific Symp. Electromagnetic Compatibility*, p. 9, 2018.

[70] H. Liao and C. Gebotys, “Methodology for em Fault Injection: Charge-based Fault Model,” *Design Automation Test Europe Conference,* pp. 256–259, 2019.

[71] R. Omarouayache, J. Raoult, S. Jarrix, L. Chusseau, and P. Maurine, “Magnetic Microprobe design for EM fault attack," *Electromagnetic Compatibility*, pages 949–954, 2013.

[72] J. Raoult, P. Payet, R. Omarouayache, and L. Chusseau, “Electromagnetic coupling circuit model of a magnetic near-field probe to a microstrip line,” *Electromagnetic Compatibilitys*, no. 978, pp. 29–33, 2015.

[73] S. Jarrix, T. Dubois, R. Adam, P. Nouvel, B. Azais, and D. Gasquet, “Probe characterization for electromagnetic near-field studies,” *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 2, pp. 292–300, 2010.

[74] A. Boyer, B. Vrignon, J. Shepherd, and B. Vrignon, “Near-field injection at die level,” *Asia-Pacific Electromagnetic Compatibility*, pp. 478–481, 2015.

[75] A. Boyer, B. Vrignon, and M. Cavarroc, “Modeling Magnetic Near-Field Injection at Silicon Die Level,” *IEEE Transaction Electromagnetic Compatibility*, vol. 58, no. 1, pp. 257–269, 2016.

[76] A. Boyer, B. Vrignon, J. Shepherd, and M. Cavarroc, “Evaluation of the near-field injection method at integrated circuit level,” *Electromagnetic Compatibility*, pp. 85–90, 2014.

[77] D. Alberto, P. Maistri, and R. Leveugle, “Electromagnetic attacks on embedded devices: A model of probe-circuit power coupling,” *Design Technology Integration Systems Nanoscale Era,* 2014.

[78] P. Laackmann and H. Taddiken, “Apparatus for protecting an integrated circuit formed in a substrate and method for protecting the circuit against reverse engineering,” US Patent 6,798,234 B2, 2003.

[79] J. M. Cioranesco *et al.*, "Cryptographically secure shields," *Hardware-Oriented Security and Trust,* pp. 25–31, 2014.

[80] A. Sarafianos *et al.*, "Robustness improvement of an SRAM cell against laser-induced fault injection," *Defect and Fault Tolerance in VLSI Systems*, pp. 149–154, 2013.

[81] A. Goikoetxea Yanci, S. Pickles, and T. Arslan, "Characterization of a voltage glitch attack detector for secure devices," *Bio-inspired, Learning, and Intelligent Systems for Security,* pp. 91–96, 2009.

[82] N. A. Anagnostopoulos, "Optical fault injection attacks in smart card chips and an evaluation of countermeasures against them," University of Twente, 2014.

[83] A. Sarafianos, "Injection de fautes par impulsion laser dans les circuits sécurisées," Ecole Nationale Supérieure des Mines de Saint-Etienne, 2013.

[84] N. Homma *et al.*, "EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor," *Cryptographic Hardware and Embedded Systems*, vol. 8731, pp. 1–16, 2014.

[85] T. Ordas, A. Sarafianos, F. Marinet, and Stephane Chesnais, "Integrated circuit protection device and method," US Patent 10 , 361 , 164 B2, 2019.

[86] L. Zussa *et al.*, "Efficiency of a glitch detector against electromagnetic fault injection," *Design Automation Test Europe,* pp. 1–6, 2014.

[87] D. Fujimoto, Y. I. Hayashi, A. Beckers, J. Balasch, B. Gierlichs, and I. Verbauwhede, "Detection of IEMI fault injection using voltage monitor constructed with fully digital circuit," *Electromagnetic Compatibility* pp. 753–755, 2018.

[88] N. Miura *et al.*, "PLL to the Rescue : A Novel EM Fault Countermeasure," *Design Automation Conference,* 2016.

[89] N. Miura and S. Bhasin, "Attack sensing against EM leakage and injection," *Int. SoC Des. Conf. Smart SoC Intell. Things*, pp. 201–202, 2016.

[90] J. Breier, S. Bhasin, and W. He, "An electromagnetic fault injection sensor using Hogge phase-detector," *Int. Symp. Qual. Electron. Des.*, pp. 307–312, 2017.

[91] C. R. Hogge, "A Self Correcting Clock Recovery Circuit," *J. Light. Technol.*, vol. 3, no. 6, pp. 1312–1314, 1985.

[92] D. El-Baze, J. Rigaud, and P. Maurine, "An Embedded Digital Sensor against EM and BB Fault Injection," *Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 78–86, 2016.

[93] D. El-baze, J. Rigaud, P. Maurine, and S.- Etienne, "A Fully-Digital EM Pulse Detector," *Design Automation Test Europe,* pp. 439–444, 2016.

[94] C. Deshpande, B. Yuce, L. Nazhandali, and P. Schaumont, "Employing dual-complementary flip-flops to detect EMFI attacks," *Asian Hardware Oriented Security and Trust Symposium,* pp. 109–114, 2018.

[95] S. Kumar, R. Saxena, and V. Garg, "Latch-up Improvement For Tap Less Library Through Modified Decoupling Capacitors Cells." URL : https://www.designreuse.com/articles/32305/latch-up-improvement-for-tap-less-library-through-modified-decoupling-capacitors-cells.html.

[96] A. J. Mondal, J. Talukdar, and B. K. Bhattacharyya, "Estimation of frequency and amplitude of ring oscillator built using current sources," *Ain Shams Eng. Journal*, 2020.

[97] Behzad Razavi, *Fundamentals of Microelectronics*. 2008.

[98] J. Y. Ihm, I. J. Chung, G. Manetas, and A. Cangellaris, "Comprehensive electromagnetic modeling of on-chip switching noise generation and coupling," *IEEE Transaction Advanced Packaging*, vol. 31, no. 4, pp. 841–854, 2008.

[99] S. Jarrix, T. Dubois, R. Adam, P. Nouvel, B. Azais, and D. Gasquet, "Probe characterization for electromagnetic near-field studies," *IEEE Transaction on Instrumentation and Measurement*, vol. 59, no. 2, pp. 292–300, 2010.

[100] Ben Dhia Sonia, Mohamed Ramdani, and S. Etienne, *Electromagnetic Compatibility of Integrated Circuits: Techniques for low emission and susceptibility*. 2006.

[101] Y. P. Su, X. Liu, and S. Y. R. Hui, "Mutual inductance calculation of movable planar coils on parallel surfaces," *IEEE Annu. Power Electron. Spec. Conf.*, pp. 3475–3481, 2008.

[102] R. Panda, S. Sundareswaran, and D. Blaauw, "Impact of low-impedance substrate on power supply integrity," *Design & Test of Computers.*, vol. 20, no. 3, pp. 16–22, 2003.

[103] Y. Wen-Yan, Z. Wen-Sheng, "Modeling and Characterization of On-Chip Interconnects," *Wiley Encyclopedia of Electrical and Electronics Engineering*, 2013.

[104] "Rods - Fair Rite." URL : https://www.fair-rite.com/product/rods-4077375411/.

[105] M. Popovich and E. G. Friedman, "Nanoscale On-Chip Decoupling Capacitors," *SOC Conference*, pp. 51–54, 2008.

[106] B. R. Stanisic, N. K. Verghese, R. A. Rutenbar, L. R. Carley, and D. J. Allstot, "Addressing substrate coupling in mixed-mode IC's: Simulation and power distribution synthesis," *Comput. Design Analog Integr. Circuits Syst.*, vol. 29, no. 3, pp. 477–489, 2002.

[107] N. K. Verghese and D. J. Allstot, "Rapid simulation of substrate coupling effects in mixed-mode ICs," *Proceedings of IEEE Custom Integrated Circuits Conference*, pp. 1–4, 1993.

[108] G. R. Karimi and E. Akbari, "Efficient and accurate modeling and simulation techniques for substrate coupling analysis in deep submicron mixed-signal IC's," *Int. Rev. Model. Simulations*, vol. 3, no. 4, pp. 653–664, 2010.

[109] S. Ben Dhia, A. Boyer, B. Vrignon, M. Deobarro, and T. V. Dinh, "On-chip noise sensor for integrated circuit susceptibility investigations," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 3, pp. 696–707, 2012.

[110] D. Pandini, G. A. Repetto, and V. Sinisi, "Clock distribution techniques for low-EMI design," *Lecture Notes in Computer Science*, vol. 4644, pp. 201–210, 2007.

[111] F. Blaabjerg, T. Dragicevic, P. Davari, *Applications of power electronics : Volume 2.* 2019.

Bibliographie de l'auteur

Articles dans des conférences internationales :

- M. Dumont, M. Lisart, P. Maurine, "Electromagnetic fault injection : How faults occur," *Fault Diagnosis and Tolerance in Cryptography (FDTC 2019)*, pp.9–16, 2019. https://doi.org/10.1109/FDTC.2019.00010

- M. Dumont, P. Maurine, M. Lisart, "Modeling of Electromagnetic Fault Injection," *Electromagnetic Compatibility of Integrated Circuits (EMC COMPO 2019)*, pp.246–248, 2019.
  https://doi.org/10.1109/EMCCompo.2019.8919964

Articles dans des revues internationales :

- M. Dumont, P. Maurine, M. Lisart, "Modeling and Simulating Electromagnetic Fault Injection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD 2020),* 2020.
  https://doi.org/10.1109 /TCAD.2020.3003287

Communication :

- PHISIC 2019, *Workshop on Practical Hardware Innovations in Security Implementation and Characterization,* Campus Georges Charpak Provence, Gardanne, 2019.

- JAIF 2019, *Journée thématique sur les Attaques par Injection de Fautes,* Campus MINATEC, Grenoble, 2019.

Brevet :

- Capteur de champ EM local – M. Dumont; C. Champeix; N. Borrel; M. Lisart. STMicroelectronics

Modélisation de l'injection de faute électromagnétique sur circuits intégrés sécurisés et contre-mesures

Mathieu Dumont

Résumé

Cette thèse est dédiée à l'étude des attaques par injection de faute électromagnétique dans les circuits intégrés sécurisés. De premiers travaux de modélisation électrique ont permis de simuler le couplage entre une sonde d'injection électromagnétique et les grilles d'alimentation et de masse du circuit afin de mieux comprendre les effets de l'impulsion EM. Cette modélisation a ensuite été appliquée à une simulation de circuit logique comprenant une bascule D et ses composants. Les résultats de ces simulations ont permis de déterminer les différentes fautes pouvant être induites par ce type d'attaque et d'en expliquer leur formation. Des mesures sur un circuit de test ont mis en évidence l'apparition de fautes de timing et de fautes d'échantillonnage, ainsi que de valider le modèle expérimentalement. Enfin, des contre-mesures issues du modèle développé sont proposées, afin d'augmenter la robustesse d'un circuit face à une attaque par injection de faute électromagnétique.

Mots-clés : *Sécurité, attaque par injection de fautes, impulsion électromagnétique, modélisation électrique, contre-mesures.*

Abstract

This thesis is devoted to the study of electromagnetic fault injection attack on secure integrated circuits. Electrical modeling permits to simulate the coupling between an EM probe injection and the circuit supply and ground grids in order to understand the effect of the EM pulse. This modeling is then applied on a logic circuit simulation with a D flip-flop and its components. The simulation results were used to determine the various faults that could be induced by this attack and to explain their formation. Measurements on a test circuit revealed the appearance of timing and sampling faults and validated experimentally the proposed model. Finally, some countermeasures based on the model are proposed in order to increase the robustness of a circuit against electromagnetic fault injection.

Keywords: *Security, fault injection attack, electromagnetic pulse, electrical modeling, countermeasures.*