# Évaluation et mitigation du risque d'attaque par injection de fautes électromagnétiques sur plateformes mobiles

Clément Gaine

N° d'ordre NNT : 2022LYSEM013

**THESE de DOCTORAT DE L'UNIVERSITE DE LYON**
opérée au sein de
**L'Ecole des Mines de Saint-Etienne**

**Ecole Doctorale** N° 488
**Sciences, Ingénierie, Santé**

**Spécialité de doctorat** : Microélectronique

Soutenue publiquement le 24/06/2022, par :

**Clément Gaine**

---

# Evaluation et mitigation du risque d'attaque par injection de fautes par perturbations électromagnétiques sur plateformes mobiles

---

Devant le jury composé de :

| | | | |
|---|---|---|---|
| DANGER Jean-Luc | Professeur | Télécom Paris | Rapporteur |
| MAURINE Philippe | Maître de conférences | LIRMM Université de Montpellier | Rapporteur |
| BEROULLE Vincent | Professeur | Université de Grenoble Alpes LCIS | Examinateur |
| ELLÉOUET David | Ingénieur | Direction Générale de l'Armement | Examinateur |
| EL MRABET Nadia | Professeure | Mines de Saint-Etienne | Examinatrice |
| DUTERTRE Jean-Max | Professeur | Mines de Saint-Etienne | Directeur de thèse |
| NIKOLOVSKI Jean-Pierre | Directeur de recherche | CEA-Leti | Co-directeur de thèse |
| ABOULKASSIMI Driss | Ingénieur | CEA-Leti | Encadrant |
| LISART Mathieu | Ingénieur | STMicroelectronics | Invité |

| Spécialités doctorales | Responsables : | Spécialités doctorales | Responsables |
|---|---|---|---|
| SCIENCES ET GENIE DES MATERIAUX | K. Wolski Directeur de recherche | MATHEMATIQUES APPLIQUEES | M. Batton-Hubert |
| MECANIQUE ET INGENIERIE | S. Drapier, professeur | INFORMATIQUE | O. Boissier, Professeur |
| GENIE DES PROCEDES | F. Gruy, Maître de recherche | SCIENCES DES IMAGES ET DES FORMES | JC. Pinoli, Professeur |
| SCIENCES DE LA TERRE | B. Guy, Directeur de recherche | GENIE INDUSTRIEL | N. Absi, Maitre de recherche |
| SCIENCES ET GENIE DE L'ENVIRONNEMENT | V.Laforest, Directeur de recherche | MICROELECTRONIQUE | Ph. Lalevée, Professeur |

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

| | | | | |
|---|---|---|---|---|
| ABSI | Nabil | MR | Génie industriel | CMP |
| AUGUSTO | Vincent | MR | Génie industriel | CIS |
| AVRIL | Stéphane | PR | Mécanique et ingénierie | CIS |
| BADEL | Pierre | PR | Mécanique et ingénierie | CIS |
| BALBO | Flavien | PR | Informatique | FAYOL |
| BASSEREAU | Jean-François | PR | Sciences et génie des matériaux | SMS |
| BATTON-HUBERT | Mireille | PR | Mathématiques appliquées | FAYOL |
| BEIGBEDER | Michel | MA | Informatique | FAYOL |
| BILAL | Blayac | DR | Sciences et génie de l'environnement | SPIN |
| BLAYAC | Sylvain | PR | Microélectronique | CMP |
| BOISSIER | Olivier | PR | Informatique | FAYOL |
| BONNEFOY | Olivier | PR | Génie des Procédés | SPIN |
| BORBELY | Andras | DR | Sciences et génie des matériaux | SMS |
| BOUCHER | Xavier | PR | Génie Industriel | FAYOL |
| BRUCHON | Julien | PR | Mécanique et ingénierie | SMS |
| CAMEIRAO | Ana | PR | Génie des Procédés | SPIN |
| CHRISTIEN | Frédéric | PR | Science et génie des matériaux | SMS |
| DAUZERE-PERES | Stéphane | PR | Génie Industriel | CMP |
| DEBAYLE | Johan | MR | Sciences des Images et des Formes | SPIN |
| DEGEORGE | Jean-Michel | MA | Génie industriel | Fayol |
| DELAFOSSE | David | PR | Sciences et génie des matériaux | SMS |
| DELORME | Xavier | PR | Génie industriel | FAYOL |
| DESRAYAUD | Christophe | PR | Mécanique et ingénierie | SMS |
| DJENIZIAN | Thierry | PR | Science et génie des matériaux | CMP |
| BERGER-DOUCE | Sandrine | PR | Sciences de gestion | FAYOL |
| DRAPIER | Sylvain | PR | Mécanique et ingénierie | SMS |
| DUTERTRE | Jean-Max | PR | Microélectronique | CMP |
| EL MRABET | Nadia | MA | Microélectronique | CMP |
| FAUCHEU | Jenny | MA | Sciences et génie des matériaux | SMS |
| FAVERGEON | Loïc | MR | Génie des Procédés | SPIN |
| FEILLET | Dominique | PR | Génie Industriel | CMP |
| FOREST | Valérie | PR | Génie des Procédés | CIS |
| FRACZKIEWICZ | Anna | DR | Sciences et génie des matériaux | SMS |
| GAVET | Yann | MA | Sciences des Images et des Formes | SPIN |
| GERINGER | Jean | MA | Sciences et génie des matériaux | CIS |
| GONDRAN | Natacha | MA | Sciences et génie de l'environnement | FAYOL |
| GONZALEZ FELIU | Jesus | MA | Sciences économiques | FAYOL |
| GRAILLOT | Didier | DR | Sciences et génie de l'environnement | SPIN |
| GRIMAUD | Frederic | EC | Génie mathématiques et industriel | FAYOL |
| GROSSEAU | Philippe | DR | Génie des Procédés | SPIN |
| GRUY | Frédéric | PR | Génie des Procédés | SPIN |
| HAN | Woo-Suck | MR | Mécanique et ingénierie | SMS |
| HERRI | Jean Michel | PR | Génie des Procédés | SPIN |
| ISMAILOVA | Esma | MC | Microélectronique | CMP |
| KERMOUCHE | Guillaume | PR | Mécanique et Ingénierie | SMS |
| KLOCKER | Helmut | DR | Sciences et génie des matériaux | SMS |
| LAFOREST | Valérie | DR | Sciences et génie de l'environnement | FAYOL |
| LERICHE | Rodolphe | DR | Mécanique et ingénierie | FAYOL |
| LIOTIER | Pierre-Jacques | MA | Mécanique et ingénierie | SMS |
| MEDINI | Khaled | EC | Sciences et génie de l'environnement | FAYOL |
| MOLIMARD | Jérôme | PR | Mécanique et ingénierie | CIS |
| MOULIN | Nicolas | MA | Mécanique et ingénierie | SMS |
| MOUTTE | Jacques | MR | Génie des Procédés | SPIN |
| NAVARRO | Laurent | MR | Mécanique et ingénierie | CIS |
| NEUBERT | Gilles | PR | Génie industriel | FAYOL |
| NIKOLOVSKI | Jean-Pierre | Ingénieur-chercheur | Mécanique et ingénierie | CMP |
| O CONNOR | Rodney Philip | PR | Microélectronique | CMP |
| PICARD | Gauthier | PR | Informatique | FAYOL |
| PINOLI | Jean Charles | PR | Sciences des Images et des Formes | SPIN |
| POURCHEZ | Jérémy | DR | Génie des Procédés | CIS |
| ROUSSY | Agnès | MA | Microélectronique | CMP |
| SANAUR | Sébastien | MA | Microélectronique | CMP |
| SERRIS | Eric | IRD | Génie des Procédés | FAYOL |
| STOLARZ | Jacques | CR | Sciences et génie des matériaux | SMS |
| VALDIVIESO | François | PR | Sciences et génie des matériaux | SMS |
| VIRICELLE | Jean Paul | DR | Génie des Procédés | SPIN |
| WOLSKI | Krzystof | DR | Sciences et génie des matériaux | SMS |
| XIE | Xiaolan | PR | Génie industriel | CIS |
| YUGMA | Gallian | MR | Génie industriel | CMP |

Mise à jour : 04/02/2021

# Remerciements

À l'issue de ces trois années de thèse, je tiens à remercier celles et ceux qui m'ont accompagné ou soutenu dans la réalisation de ces travaux.

Je tiens en premier lieu à remercier mes directeurs de thèse Jean-Max Dutertre et Jean-Pierre Nikolovski ainsi que mon encadrant de thèse Driss Aboulkassimi pour leur disponibilité et la confiance qu'ils m'ont accordée. Leurs conseils me seront précieux pour les prochaines années.

J'adresse mes remerciements à Jean-Luc Danger et Philippe Maurine pour avoir accepté d'être les rapporteurs de ma thèse et pour l'intérêt qu'ils ont porté à mes travaux. Je remercie également Nadia El Mrabet, Vincent Beroulle, David Elleouet et Mathieu Lisart et je leur suis reconnaissant d'être membre de mon jury de thèse.

Au cours de mes 7 années au sein de l'École des Mines de Saint-Etienne en tant qu'élève-ingénieur, ingénieur puis doctorant, j'ai eu l'occasion de côtoyer de nombreuses personnes. Je tiens à les remercier pour la richesse des échanges que j'ai eu avec elles. Ces travaux n'auraient pas pu être menés à bien sans la collaboration de Micro-PackS et Id-Fab et en particulier de l'aide d'Anne-Lise Ribotta, Serge Martinez et François Bernier.

Je souhaite sincèrement remercier Olivier Potin et Simon Pontié pour leur aide au cours de mon stage et de ma thèse et leur accompagnement lors de mes premiers pas dans la recherche.

Je remercie également Joseph Gravellier et Alexandre Menu pour nos discussions du lundi matin et l'ambiance de travail agréable qu'ils ont cultivé. Je tiens aussi à remercier tous les anciens et actuels doctorants et post-doctorants avec qui j'ai partagé mon quotidien ces trois dernières années.

Mes derniers remerciements vont à mes proches qui m'ont épaulé au long de ces travaux. Je remercie enfin Pauline, avec qui je partage ma vie depuis plusieurs années, pour ses encouragements et son soutien ayant facilité la réalisation de cette thèse.

# Glossaire

| | |
|---|---|
| AES | Advanced Encryption Standard - Algorithme de cryptographie symétrique. |
| ARQS | Approximation des Régimes Quasi Stationnaires. |
| ASIC | Application-Specific Integrated Circuit - Circuit intégré propre à une application. |
| BGA | Ball Grid Array - Matrice de bille. |
| CMS | Composant Monté en Surface. |
| CPA | Correlation Power Analysis - Analyse de corrélation sur la consommation. |
| CPU | Central Processing Unit - Processeur. |
| DES | Data Encryption Standard - Algorithme de cryptographie symétrique. |
| DIP | Dual Inline Package - Boîtier sur deux rangées de pattes. |
| DPA | Differential Power Analysis - Analyse de consommation. |
| DRAM | Dynamic Random Access Memory - Mémoire vive dynamique. |
| DVFS | Dynamic voltage and frequency scaling - Ajustement dynamique de la tension. |
| EM | Electromagnétique. |
| EMFI | ElectroMagnetic Fault Injection - Injection de fautes par perturbations électromagnétiques. |
| FIB | Focused Ion Beam - Sonde ionique focalisée. |
| FPGA | Field Programmable Gate Array - Réseau de porte programmable par l'utilisateur. |
| GBF | Générateur Basses Fréquences. |
| GPIO | General Purpose Input/Output - Broche générale d'entrée/sortie. |
| ISA | Instruction Set Architecture - Jeu d'instructions. |
| Laser | Light Amplification by Stimulated Emission of Radiation - Amplification de la lumière par émission stimulée de radiation. |
| MCU | Microcontrôleur Unit - Microcontrôleur. |
| OS | Operating System - Système d'exploitation. |
| PCB | Printed Circuit Board - Circuit imprimé. |
| PoP | Package-on-Package - Boitiers empilés. |
| RISC | Reduced Instruction Set Computer - Processeur à jeu d'instructions réduit. |

| | |
|---|---|
| RO | Ring-Oscillator - Oscillateur en anneau. |
| RSA | Rivest-Shamir-Adleman - Algorithme de cryptographie asymétrique. |
| SEC | Sonde d'Émission ChaXa. |
| SEMA | Simple ElectroMagnetic Analysis - Analyse électromagnétique simple. |
| SoC | Sytem on a chip - Système sur puce. |
| SPA | Simple Power Analysis - Analyse simple de la consommation. |
| SRAM | Static Random Access Memory - Mémoire vive statique. |
| SRC | Sonde de Réception ChaXa. |
| TA | Trusted Application - Application de confiance. |
| TEE | Trusted Execution Environment - Environnement d'exécution de confiance. |
| UART | Universal Asynchronous Receiver-Transmitter - Emetteur-récepteur asynchrone universel. |

# Table des matières

# Introduction

Depuis quelques années, les téléphones mobiles ont évolué et leur utilisation est devenue incontournable. Chacun peut y stocker une quantité importante de données personnelles ou professionnelles telles que des messages, des contacts, des photos, des comptes de réseaux sociaux, etc. Par conséquent, ces dispositifs peuvent être considérés comme une cible privilégiée pour les attaquants. Les attaques physiques, par observation de canaux cachés ou perturbation, sont propices à l'extraction des données et des secrets. Une perturbation volontaire et précise du fonctionnement d'un circuit ou la mesure de son activité par des canaux auxiliaires peuvent être exploitées pour extraire les secrets qu'il contient. Couramment réalisées sur des microcontrôleurs, elles sont en cours d'extension sur des circuits complexes de type processeurs multicœurs. Leur amélioration constante permet de perturber le fonctionnement d'applications de sécurité telles que les implantations logicielles ou matérielles des fonctions de chiffrement. Pour ces raisons, il est primordial que l'intégrité du circuit intégré et la confidentialité des données soient assurées. Il est donc nécessaire d'implanter des mécanismes de protection contre les menaces que représentent les attaques physiques.

En dehors de ces actions illégales, les téléphones portables sont souvent un élément clé dans les affaires judiciaires, car leurs données peuvent contenir des preuves majeures pour résoudre des investigations judiciaires ou prévenir d'autres crimes. Les techniques de recherche d'informations classiques trouvent leurs limites lorsque les téléphones sont protégés par chiffrement. Une partie de ces travaux sont réalisés dans le cadre d'une exploitation touchant au domaine des forces de l'ordre, c'est-à-dire d'une action légale de fouille et d'extraction de données. La combinaison d'attaques matérielles avec les attaques logicielles conduit à de nouvelles possibilités d'analyses pour les forces de l'ordre.

On distingue deux grandes familles d'attaques physiques : les attaques par observation de canaux cachés et celles par perturbation. L'efficacité des attaques par observation, en l'occurrence celles dites par analyse du champ électromagnétique a déjà été prouvée sur des plates-formes mobiles, malgré la complexité de leurs architectures matérielles et logicielles. En revanche, nous nous intéressons plus particulièrement aux attaques par perturbations électromagnétiques dans cette thèse. Elles consistent à produire un champ magnétique impulsionnel à forte intensité sur

la surface d'un circuit intégré afin d'y induire une force électromotrice. En général, l'attaque est d'autant plus efficace que l'injection est précise, à la fois dans l'espace et dans le temps, c'est-à-dire perturbant peu d'éléments du circuit intégré, et durant un court instant. Cela perturbe le fonctionnement d'un circuit provoquant ainsi une modification du flot de contrôle du programme (*control flow*) ou du fonctionnement de modules cryptographiques.

Dans cette thèse, nous travaillerons d'abord sur l'amélioration des paramètres spatio-temporels du banc d'injection par perturbations électromagnétiques afin de rendre plus efficiente l'exploitation de vulnérabilités. Nous étudions ensuite la sensibilité des processeurs de smartphone. Enfin, nous chercherons à proposer des contre-mesures adaptées.

Cette thèse s'est déroulée à la fois dans un contexte académique, industriel et des forces de l'ordre (forensic). Les travaux s'inscrivent dans le cadre du projet FUI CSAFE+ consacré à l'étude des attaques par perturbations électromagnétiques des circuits et systèmes sécurisés, ainsi que dans le cadre du projet européen H2020 EXFILES. Ce dernier vise à fournir aux forces de l'ordre des outils et des protocoles pour extraire des données de smartphones chiffrés.

Ces travaux ont été réalisés au sein de l'équipe commune *Systèmes et Architectures Sécurisés* de l'École des Mines de Saint-Étienne et du CEA-LETI sur le campus Georges Charpak Provence à Gardanne.

Le chapitre 1 présente le contexte général de cette thèse. Nous présentons l'état de l'art des attaques matérielles, puis nous détaillons un ensemble de publications scientifiques présentant les bancs d'injections ainsi que des modèles de fautes. Enfin, nous réalisons une analyse des contremesures par blindage et détection d'attaques.

Le chapitre 2 met en avant l'étude des sondes d'injections, dans le but d'optimiser les perturbations générées sur une cible. Ainsi, après des rappels et une discussion sur la nature des perturbations à partir de quelques expériences élémentaires, nous proposons une modélisation statique des champs magnétiques générés par les sondes. L'étude est ensuite poursuivie de façon dynamique, avec la prise en compte de l'effet des ferrites sur les résultats de l'injection. Nous menons des analyses sur les adaptations d'impédances ainsi que sur les rebonds dus à l'imperfection du générateur d'impulsions. Elles aboutissent à l'obtention d'impulsions monopolaires. Toutes ces travaux conduisent à fournir des préconisations sur la conception des sondes et à fabriquer des sondes avec des performances accrues.

Le chapitre 3 démontre en premier lieu la faisabilité de l'injection de fautes par perturbations électromagnétiques sur des cibles complexes. Nous présentons une méthodologie pour identifier les paramètres d'injection. Nous établissons le modèle des fautes générées. Nous réalisons une exploitation de l'injection de fautes sur une

cible complexe avec une élévation de privilèges sur un système d'exploitation Linux. L'influence de nombreux paramètres est analysée dans l'objectif d'améliorer la compréhension des mécanismes de propagation des fautes et la mise en place d'analyses de vulnérabilités.

Le chapitre 4 propose une solution de contre-mesure aux menaces d'attaques physiques, et en particulier par injections de fautes électromagnétiques. Nous démontrons l'efficacité d'un dispositif de protection et de supervision contre les attaques par canaux auxiliaires. Il détecte de plusieurs types d'attaques physiques et fournit une réponse appropriée pour chaque type de menace. L'efficacité de ce blindage actif est démontrée à la fois sur des microcontrôleurs comme sur des microprocesseurs.

# Chapitre 1 : État de l'Art des attaques par injection de fautes

L'étude des vulnérabilités matérielles des composants électroniques est nécessaire afin de garantir leur sécurité. Ce chapitre propose un état de l'art des attaques matérielles et plus particulièrement de celles par injection de fautes. Les travaux de cette thèse concernent l'évaluation du risque d'attaque par injection de fautes par perturbations électromagnétiques sur des cibles complexes ainsi que leurs contre-mesures. Ainsi, nous présentons la méthode d'injection de fautes par perturbations électromagnétiques et les différents modèles de fautes sur microprocesseurs. Différents mécanismes de protection et de détection des attaques sont ensuite détaillés. Enfin, la dernière partie présentera le contexte ainsi que les objectifs de cette thèse.

## Sommaire du chapitre

## 1.1 Attaques matérielles

Les circuits intégrés utilisent des algorithmes de cryptographie pour sécuriser leurs opérations et leurs communications. Ces algorithmes peuvent être standardisés [94, 93] et sont considérés comme mathématiquement sûrs. Certaines failles logicielles peuvent exister dans ces codes, cependant même en leur absence, ils sont vulnérables aux attaques physiques visant leurs implémentations dans les circuits. Les attaques physiques permettent à un attaquant d'extraire les clés de cryptographie secrètes utilisées par un circuit intégré [59]. Ces attaques physiques, qui nécessitent un accès physique direct à la cible, sont de deux types : les attaques par observation et les attaques par perturbation.

### 1.1.1 Attaques par observation

La première famille d'attaques repose sur l'observation du fonctionnement d'un code logiciel. Cette attaque est donc passive et ne modifie pas l'exécution d'un code. Elle repose sur l'étude des fuites d'informations en analysant la consommation de courant, l'émission électromagnétique ou la variation de température, etc.

Les microcontrôleurs et microprocesseurs sont composés de millions de transistors qui commutent durant leur fonctionnement. Ces changements d'état consomment de l'énergie et peuvent être dépendants des données manipulées.

#### Analyse de la consommation d'énergie

Cette méthode consiste à observer la consommation de courant pendant le fonctionnement d'un composant, car celle-ci peut dépendre des données manipulées par la cible. Les récupérations de clés sont effectuées en analysant statistiquement les courbes de consommations. Les attaques de type Simple Power Analysis (SPA) sont des lectures directes, parfois simplement à l'œil nu, des traces permettant d'identifier les données et clés secrètes. Il peut aussi être nécessaire d'utiliser un outil statique, tel une attaque Differential Power Analysis (DPA) [55, 18] ou Correlation Power Analysis (CPA) [27]. Ces techniques analysent plusieurs traces et leurs données correspondantes (plaintext, ciphertext, etc.) pour identifier les clés secrètes.

Dans le cas de la DPA, un tri des traces est effectué selon la valeur des données manipulées et un secret supposé, puis la différence entre la moyenne des traces de chaque groupe est calculée. Si le secret supposé est correct, alors des pics sont présents dans la trace différentielle. Dans le cas de la CPA, des hypothèses sur les valeurs manipulées sont effectuées afin de calculer leurs émissions de courant selon un modèle théorique. Le coefficient de corrélation de Pearson entre les prédictions de la consommation du circuit et les données mesurées peut être calculé afin de proposer la meilleure hypothèse du secret de la clé de chiffrement. Avec une DPA,

l'hypothèse est réalisée sur un seul bit tandis qu'avec la CPA elle peut aussi l'être sur plusieurs. L'attaquant est alors en mesure de retrouver complètement la clé de chiffrement utilisée.

Il existe aussi des attaques par comparaison des courbes : les attaques par template. Elles nécessitent une copie du composant ciblé. On effectue de nombreuses acquisitions en utilisant plusieurs textes en clair et clés secrètes, définissant le profil du composant. Sur le composant ciblé, on pourra alors faire quelques acquisitions en variant le plaintext, puis comparer ces traces au profil. L'intérêt est de pouvoir trouver la clé secrète d'un composant ciblé avec peu d'acquisitions sur celui-ci.

Les attaques par canaux auxiliaires peuvent être couplées à l'utilisation de machine learning [53] ou deep learning [61] afin de réaliser les calculs statistiques.

### Analyse des émissions électromagnétiques

Cette méthode repose sur l'observation des champs électromagnétiques émis par le fonctionnement d'un composant. L'utilisation des analyses électromagnétiques pour compromettre des systèmes de sécurité date de 1943 quand un ingénieur de Bell Telephone a remarqué des perturbations sur un oscilloscope pendant l'utilisation d'un téléscripteur chiffré. La méthode a ensuite été appliquée pour des cartes à puces, microcontrôleurs et microprocesseurs. Pour réaliser ces attaques, une sonde d'écoute électromagnétique, composée d'un enroulement de fil de cuivre, réalise un couplage par effet inductif avec le circuit sous attaque ce qui mesure les émissions électromagnétiques de la cible.

La découverte des fuites d'informations électromagnétiques a été présentée plusieurs fois dans les années 1990 [85, 86], mais uniquement d'un point de vue théorique. La première mise en place expérimentale des analyses des émissions électromagnétiques pour trouver des clés secrètes a été réalisée par Gandolfi et al. [44] en 2001. Sur trois puces CMOS, avec différents niveaux de protections matérielles, les clés secrètes d'algorithmes tels que le DES ou RSA ont pu être extraites.

La première extraction de clés secrètes d'un AES sur microcontrôleur 32 bits a été publiée par Montminy et al. [71]. L'analyse a été réalisée avec une sonde de champ proche et un récepteur numérique de télévision à bas coût. L'analyse a réussi, malgré des acquisitions réalisées avec des taux d'échantillonnage de quelques MégaHertz, et donc bien inférieurs aux préconisations de Nyquist [88] pour l'acquisition de signaux entre 10 et 70 MHz.

Aboulkassimi et al. [9] ont proposé des approches basées sur la densité de puissance et la resynchronisation par template afin de s'affranchir des distorsions temporelles des acquisitions. Un octet de la clé d'un AES a été retrouvé en une heure (250 acquisitions) sur un processeur RISC 32 bits fonctionnant à 370 MHz.

Longo et al. [59] ont réalisé des analyses différentielles sur l'implémentation d'un AES sur un CPU fonctionnant à 1 GHz. 20 000 acquisitions ont été nécessaires pour retrouver la clé d'un AES logiciel contre 500 millions sur l'implémentation sur co-processeur.

Les circuits de type Package-on-Package (PoP) peuvent aussi être attaqués. Afin d'exécuter des environnements de confiance (TEE, TrustZone, etc.), il est nécessaire que leur initialisation soit sécurisée afin qu'elle ne puisse pas être corrompue. Pour ce faire, différents chargeurs d'amorçage du système (bootloader) sont présents et vérifient l'intégrité des codes chargés. Le code du bootloader de premier niveau (BL1) est chargé par la BootROM, depuis la mémoire externe vers la SRAM interne, puis l'authenticité de BL1 est vérifiée. Vasselle et al. [105] ont réussi à extraire la clé de déchiffrement de BL1, autorisant le chargement de code malicieux. Pour cela, la mémoire DRAM a été retirée du SoC car elle engendre un bruit supérieur aux fuites du SoC principal. Cependant, cette attaque n'autorise pas directement un contournement du secure boot.

#### Autres canaux alternatifs

L'écoute des émissions électromagnétiques et des consommations d'énergie constitue les attaques par canaux auxiliaires les plus courantes. Mais d'autres techniques peuvent aussi être utilisées. Lors du fonctionnement d'un composant, des bruits peuvent être émis en fonction des opérations effectuées. Genkin et al. [46] ont extrait la clé de chiffrement d'un algorithme RSA exécuté sur un PC et un smartphone. Les émissions de température des composants [51] peuvent aussi être mesurées.

### 1.1.2 Attaques par perturbation

La seconde famille d'attaques repose sur la perturbation de l'environnement de fonctionnement d'une cible. Cette modification des paramètres physiques engendre une modification de l'exécution d'un code. Ces attaques peuvent être réalisées par des augmentations de température, des modifications des tensions d'alimentation, d'horloges, des perturbations laser ou électromagnétiques par exemple. L'exécution des instructions est alors corrompue, ce qui entraîne la non-exécution d'une ou plusieurs instructions, un phénomène appelé saut d'instruction. Les instructions manquantes créent alors des erreurs (encore appelées fautes) dans les calculs de l'algorithme visé. Un attaquant peut alors contourner des mécanismes de sécurité comme des environnements d'exécution de confiance (TEE) ou Secure Boot pour obtenir des données personnelles et clés secrètes d'algorithmes de chiffrement. On parvient à ce type de perturbations en générant des perturbations électromagnétiques [35] à proximité du composant ou en l'illuminant avec un laser [33].

Afin de réaliser certaines attaques, il peut être nécessaire de préparer le circuit cible.

Les attaques utilisant une sonde ionique focalisée (FIB) nécessitent d'avoir accès au silicium du circuit intégré. Ce type d'attaques modifiant ou observant directement le système est donc *invasif* et demande de décapsuler les composants. Pour cela, le package doit être fraisé mécaniquement ou dissout chimiquement avec des acides. Les attaques utilisant des laser nécessitent une ouverture du boîtier. Les attaques par perturbations électromagnétiques peuvent nécessiter une préparation de la cible, comme les décapsulations, afin de faciliter l'injection. On classe ce type d'attaques comme *semi-invasive*. Enfin, certaines attaques ne demandent aucune modification du circuit, comme les glitchs de tensions. On considère que ces attaques sont *non-invasive*.

Certains types d'injection vont modifier le comportement de tout le système, comme une modification de la tension d'alimentation, de l'horloge de fonctionnement ou de la température. On parle alors de fautes avec un *effet global*. Au contraire, les perturbations électromagnétiques et laser peuvent générer des fautes ayant des *effets locaux*, apportant une précision spatiale.

#### Injection de fautes par perturbation de la tension

Cette méthode d'injection de fautes consiste à modifier la tension d'alimentation d'un composant. En sous-alimentant, sur-alimentant ou réalisant un court-circuit de l'alimentation, on introduit des variations d'alimentation, ce qui engendre des fautes sur des bits. Le fonctionnement du processeur pourra être corrompu ou réaliser des sauts d'instructions.

Une des premières attaques sur une cible pouvant être utilisée dans les mobiles a été réalisée par Barenghi [19, 20]. L'attaque consiste à sous-alimenter le processeur pendant des chargements mémoires ce qui peut modifier des instructions (AND en EOR, ADDNE en ADDEQ ou BNE en BEQ par exemple). Le fonctionnement de l'algorithme RSA est alors modifié en substituant une condition NOT EQUAL en condition EQUAL. Cependant, la clé de chiffrement n'a pas pu être récupérée. Une seconde attaque permet quant à elle d'extraire la clé de chiffrement d'un AES.

L'utilisation des glitchs de tension peut être utilisée pour réaliser des élévations de privilèges. Pour ce faire, Timmers et Mune [96] décrivent trois scénarios d'attaque. Le premier consiste à réaliser une injection lors de l'appel système OPEN durant l'ouverture de /DEV/MEM pour autoriser une application non privilégiée à mapper des adresses arbitraires en mémoire physique. Le second consiste à modifier le registre pointeur d'instruction (Program Counter), de façon similaire à [97]. La dernière attaque vise l'appel système SETRESUID afin d'assigner l'identifiant d'un processus non privilégié à ROOT. Les taux de succès de chacune de ces attaques sont proches de 0.5 %.

Enfin, l'attaque VoltJockey [80] exploite une vulnérabilité du Dynamic Voltage and

Frequency Scaling (DVFS). Cette technique de gestion de la tension consiste à adapter la tension du processeur en fonction de la charge. Dans cette attaque, les tensions d'alimentations sont réduites pendant l'exécution du code cible pour réaliser des fautes. Une application non signée a pu être exécutée par une TrustZone sur un smartphone Nexus 6 en modifiant l'exécution de sa signature RSA.

### Injection de fautes par perturbation de l'horloge

Le fonctionnement des circuits intégrés est cadencé par des fronts montants du signal d'horloge. Une introduction de front montant supplémentaire crée de mauvaises lectures de données ou erreurs sur les instructions.

Sur des microcontrôleurs ATMega256 et ARM Cortex-M0, Korak et Hoelfer [56] ont réalisé des sauts d'instructions arithmétiques, de branchements et mémoires. Pour certaines de ces attaques, les modifications de tensions d'alimentation sont combinées avec des perturbations d'horloge.

Sur les processeurs de type SoC, l'attaque CLKScrew [95] consiste à réaliser un overclocking logiciel pour créer des fautes dans un TEE. La clé secrète d'un AES logiciel sur un environnement TEE est récupérée, et la vérification de signature RSA exécutée sur une Trusted Application (TA) est corrompue.

### Injection de fautes par perturbation laser

Les attaques par illumination ont été présentées par Skorobogatov et Anderson [90], en utilisant un flash d'appareil photo pour changer individuellement les bits d'une SRAM.

Cette méthode s'est ensuite améliorée en utilisant des laser. Vasselle et al. [104] ont réussi à contourner un secure boot d'un processeur ARM Cortex-A9, après une préparation du circuit. Colombier et al. [33] ont modifié des bits d'une mémoire flash sur un ARM Cortex-M3. Grâce à cela, ils ont extrait la clé secrète d'un AES 128 bits.

### Injection de fautes par perturbation électromagnétique

La génération de champs électromagnétiques pour modifier le comportement d'un circuit a été réalisée expérimentalement par Schmidt et Hutter [84] sur un microcontrôleur 8 bits. Une onde impulsionnelle est générée en utilisant un allume-gaz, générant un arc électrique. La distance entre les deux électrodes fait varier l'intensité du champ électromagnétique. La localité spatiale et temporelle de ces techniques a ensuite été améliorée.

Deux types d'ondes électromagnétiques [63] peuvent être utilisés :

- **Ondes harmoniques** Un générateur de fréquence couplé à un amplificateur afin de perturber des réseaux d'horloge ou des générateurs de nombres aléatoires (TRNG) [78]
- **Ondes impulsionnelles** Un générateur capable de délivrer des tensions de plusieurs centaines de volts pendant des durées de quelques nanosecondes.

Dans le cadre de cette thèse, seules les injections de fautes par perturbations électromagnétiques impulsionnelles seront étudiées.

Dehbaoui et al. [35] ont réalisé la première injection de fautes avec une impulsion électromagnétique sur un AES logiciel et matériel sur une cible 32 bits ARM Cortex-M3. L'impulsion est générée entre le $9^{\text{ème}}$ et $10^{\text{ème}}$ tour de l'AES et vise le compteur de boucle afin de réaliser un tour supplémentaire. Ainsi, la clé de chiffrement peut être trouvée avec deux paires de textes chiffrés corrects et fautés.

Majéric et al. [62] ont montré que des analyses par canaux auxiliaires électromagnétiques permettent d'identifier les paramètres spatiaux et temporels pour l'injection électromagnétique. Sur un microprocesseur ARM Cortex-A9, le $9^{\text{ème}}$ tour d'un AES matériel a été fauté, ce qui permet d'extraire la clé de chiffrement en utilisant la méthode de Piret et Quisquater [77].

Menu et al. [66] ont présenté des corruptions de données lors du transfert de la mémoire flash vers le buffer de donnée sur un microcontrôleur ARM Cortex-M3. Un nombre contrôlable de bits a ainsi été mis à zéro.

Elmohr et al. [39] ont réalisé des corruptions au niveau du pipeline sur un microcontrôleur ARM Cortex-M0. Une perturbation durant la phase d'exécution d'instructions de chargement autorise l'accès à des données non autorisées.

Les attaques sur des microprocesseurs sont plus récentes du fait de leur complexité plus importante. Ces cibles comportent plusieurs cœurs, des fréquences de fonctionnement élevées ($> 1\,\text{GHz}$), des pipelines et plusieurs niveaux de mémoire cache ainsi que des systèmes d'exploitation complexes. La première injection sur un SoC de téléphone portable a été démontrée par Cui et Housley [34]. L'exploitation BADFET consiste à générer des fautes qui vont se propager dans un composant, appelées *attaques de second ordre*. Les attaques par injections de fautes présentées précédemment, reposent sur l'exploitation des fautes du composant perturbé, ainsi on peut les considérer comme *attaques de premier ordre*. Ces attaques demandent une résolution spatiale et temporelle qui est difficile à atteindre sur des processeurs modernes fonctionnant au-dessus de 1 GHz [34]. BADFET contourne cette difficulté en créant des fautes dans des composants connectés avec la cible. Par exemple, au lieu de cibler la cache instruction d'un processeur, il est possible de corrompre le code stocké en mémoire, ce qui perturbera le fonctionnement du processeur dans un second temps. Ces composants ont des fréquences de fonctionnement différentes et utilisent des bus de communication (i2c, SPI, etc.) ouvrant la possibilité à de

nouvelles attaques.

L'ensemble des attaques précédentes visaient des cibles sans technologie Package-on-Package. Aït el Mehdi [65] a montré que des cibles avec cette technologie pouvaient être sensible à l'injection. Cependant, l'objectif de désactiver la protection anti-bruteforce de l'écran de déverrouillage d'Android n'a pu être atteint.

Trouckine et al.[102] ont détaillé une méthode permettant de caractériser un modèle de faute sur des CPUs. Grâce à elle, il est possible de déterminer si les fautes perturbent les registres du CPU, le pipeline ou les mémoires. Expérimentalement, l'emplacement des fautes sur des SoC Broadcom BCM2837 (ARM Cortex A53) et Intel Core i3 a pu être identifié dans respectivement 95% et 80% des cas.

Un état de l'art de l'exploitation des injections de fautes par perturbations électromagnétiques sur cibles microcontrôleur et SoC est représenté sur le tableau 1.1. Ce tableau, non exhaustif, représente l'évolution des cibles : du microcontrôleur vers des microprocesseurs avec systèmes d'exploitation. Afin d'étudier la possibilité d'attaques dans un contexte d'utilisation par les forces de l'ordre, l'utilisation d'un signal de synchronisation (trigger) est notée. La répétabilité des attaques, c'est-à-dire le taux de succès par tentatives d'attaques, est présentée dans la colonne des résultats.

TABLEAU 1.1 – Récapitulatif des exploitations des injections de fautes par perturbations électromagnétiques.

| Publication | Année | Cible | Trigger | Résultats | Exploitation |
|---|---|---|---|---|---|
| Dehbaoui et al. [36] | 2013 | ARM Cortex-M3 | Oui | 2 ciphertexts modifiés et 2 corrects | Récupération de clé AES |
| Majéric et al. [62] | 2016 | ARM Cortex-A9 | Oui | 0.03 % | Récupération de clé sur AES matériel |
| Menu et al. [66] | 2019 | Atmel SAM3X8E ARM Cortex-M3 | Oui | Jusqu'à 100 % | Récupération et mise à zéro de clé AES |
| Elmohr et al. [39] | 2020 | NXP LPC1114 ARM Cortex-M0 E31 RISC-V SiFive FE310-G002 | Oui | Entre 12 et 31 % | Contournement de vérifications Chargement de données non autorisées en RAM |
| BADFET [34] | 2017 | Cicso 8861 IP Phone Broadcom BCM11125 Soc | Non | 72 % | Contournement de vérification de secure boot Chargement de bootloader non autorisé Accès privilégié au TEE |
| Aït el Mehdi [65] | 2019 | Puce Package-on-Package Android 8.0 | Oui | Pas de réussite | Désactivation de la protection anti-bruteforce de l'écran de déverrouillage Android |

#### Autres méthodes d'injections de fautes

Une méthode invasive et coûteuse d'injection de fautes consiste à utiliser des faisceaux d'ions focalisés (FIB) afin de forcer un signal sur un point précis du circuit, ou de couper et recréer des interconnexions. Torrance et James [98] l'ont utilisé pour retrouver des clés de chiffrements sur un ASIC.

Les attaques par injections de fautes peuvent se réaliser en chauffant l'environnement d'une puce. Skorobogatov [89] a montré que le chauffage de mémoire EEPROM et Flash pouvait modifier leurs contenus. Hutter et Schmidt [51] ont chauffé à 150°C un microcontrôleur ATMega162 pendant des déchiffrements RSA-CRT, générant une faute et de retrouver les nombres premiers $p$ et $q$ permettant de déchiffrer les messages.

## 1.2 Injection de fautes par perturbations électromagnétiques

Les attaques par injections de fautes par perturbations électromagnétiques reposent sur l'utilisation de générateurs d'impulsions de tension et de sondes d'injection. Une analyse des différents bancs d'injection de l'état de l'art est proposée. Ces perturbations produisent différents types de fautes, ainsi les différents modèles de fautes sont aussi présentés.

### 1.2.1 Bancs d'injections de fautes par perturbations électromagnétiques

Les bancs d'injection électromagnétiques se composent de générateurs d'impulsions connectés à des sondes, ces deux éléments requis pour l'injection de fautes sont étudiés successivement.

#### Générateurs d'impulsions

Une perturbation électromagnétique est créée en faisant circuler une impulsion de courant à travers une bobine (ou sonde) d'injection. Le générateur doit alors fournir un signal impulsionnel, ce qui peut se réaliser à partir de la décharge d'un condensateur. Cependant afin d'obtenir des intensités et tensions de sorties plus importantes, d'autres circuits doivent être utilisés. La majorité des travaux de l'état de l'art ont été réalisés avec des générateurs de marque Avtech [15, 16], capable de délivrer des impulsions de tension avec des amplitudes de plusieurs centaines de volts, sur une plage de quelques nanosecondes avec des fronts montants de 1.5 à 5 ns sous une impédance de 50 Ω. Des solutions commerciales comme la Burst Power Station BPS202 de Langer ou l'EM-FI Transient Probe de Riscure peuvent aussi

être utilisées dans l'injection de fautes. Leurs caractéristiques sont proches de celles de la plateforme Avtech.

Il est possible de classer les générateurs selon leur architecture tel que présenté sur la figure 1.1. L'impulsion est créée en déchargeant un condensateur à haute tension (C_HT) dans un circuit de décharge comprenant (direct) ou non (couplé) la sonde d'injection [74].

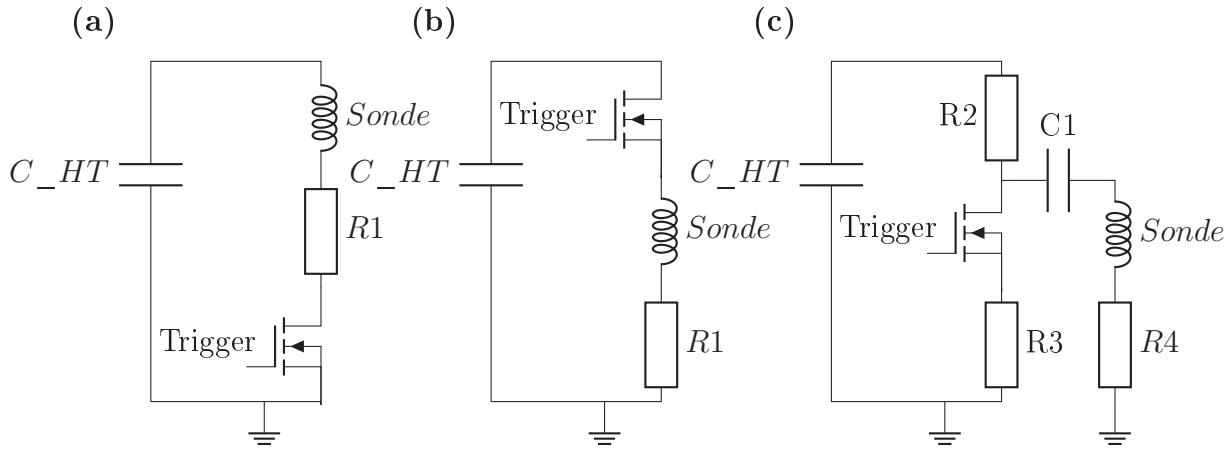



FIGURE 1.1 – Couples générateurs/sondes à architectures directes **(a et b)** ou couplées **(c)** [74].

Les deux schémas de gauche représentent des générateurs d'impulsions avec une architecture directe. En plus d'avoir une simple conception, cette architecture est fonctionnelle avec toutes les sondes, quelle que soit leur impédance. Le condensateur haute tension C_HT délivre l'énergie électrique. La résistance R1 sert à limiter le courant dans le transistor en cas de court-circuit au niveau de la sonde, ce qui l'endommagerait.

Le premier schéma représente un circuit *low-side switching*, tel que présenté par SiliconToaster [8]. Ce générateur est capable de délivrer des tensions jusqu'à 1200 V. Comme illustré sur la figure 1.2, ce dispositif est compact, la sonde est ainsi positionnée directement en sortie du générateur.

L'efficacité de ce dispositif a été montrée sur une cible microcontrôleur sur laquelle la configuration de la protection du firmware a été cassée. Le générateur présenté par Cui [34] propose la même architecture, cependant l'inconvénient de cette architecture réside dans le fait que la sonde est toujours connectée à la source haute tension. Si une personne touche la sonde, elle risque alors une électrisation, et ce peu importe l'état de la commande du transistor.
Une architecture *high-side switching*, présentée sur le schéma 1.1.b, évite ce problème. Le transistor est placé entre le condensateur et la sonde. Le courant circule donc dans la sonde uniquement lorsque le transistor est fermé, c'est-à-dire durant la

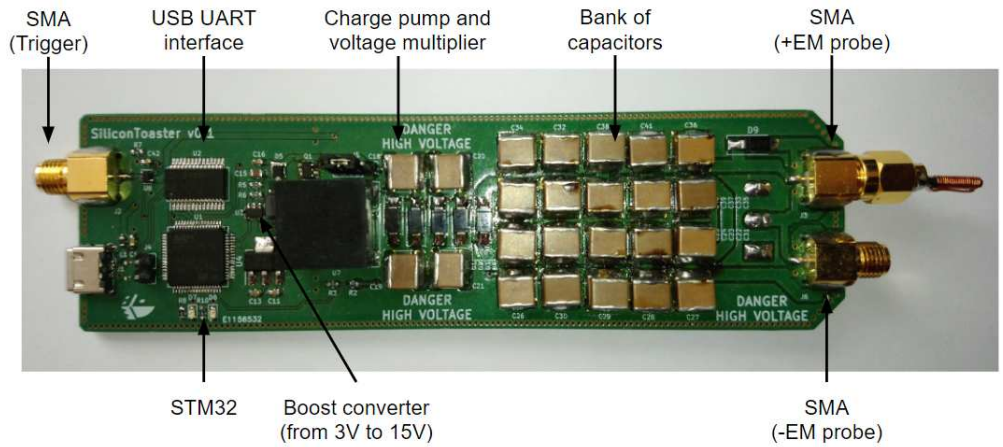



FIGURE 1.2 – Illustration du SiliconToaster [8].

génération de l'impulsion de tension. NewAE a développé le générateur ChipSHOUTER qui est basé sur ce principe. Le coût de ce générateur est d'environ 3 k€. Son efficacité a été prouvée en contournant le mot de passe d'un calculateur moteur (ECU - Engine Control Unit) [42].

Enfin, la dernière architecture de la figure 1.1.c est couplée, avec un condensateur. Cela garanti aussi la présence de la tension uniquement durant l'instant d'injection. Cette architecture est utilisée par Beckers [25], cependant elle demande une adaptation du circuit d'injection (R4 et C1) en fonction de la sonde utilisée.

L'architecture des générateurs d'impulsions de tension de marque Avtech est différente des schémas précédents et est détaillée dans la documentation [15, 16]. Par exemple, sur l'Avtech AVL-5-B, un réseau de mise en forme d'impulsion (Pulse Forming Network), basé sur un câble coaxial de grande longueur, produit des impulsions électriques de courtes durées.

Balasch et al. [17] ont développé un générateur capable de fournir des courants de 20 Ampères. La plateforme a été validée en récupérant la clé secrète d'un AES sur un microcontrôleur 8 bits.

Plus récemment, NewAE a présenté le générateur ChipSHOUTER-PicoEMP dédié à l'auto-apprentissage. La figure 1.3 illustre ce générateur, capable de produire une impulsion d'environ 200 V durant quelques dizaines de nanosecondes. L'ensemble des documents de fabrication sont présentés dans un répertoire GitHub [73] et le coût de fabrication est inférieur à 50 €.

La preuve de concept de ce générateur a été réalisée en corrompant le chargement du bootloader du porte-feuille de crypto-monnaie Trezor One.

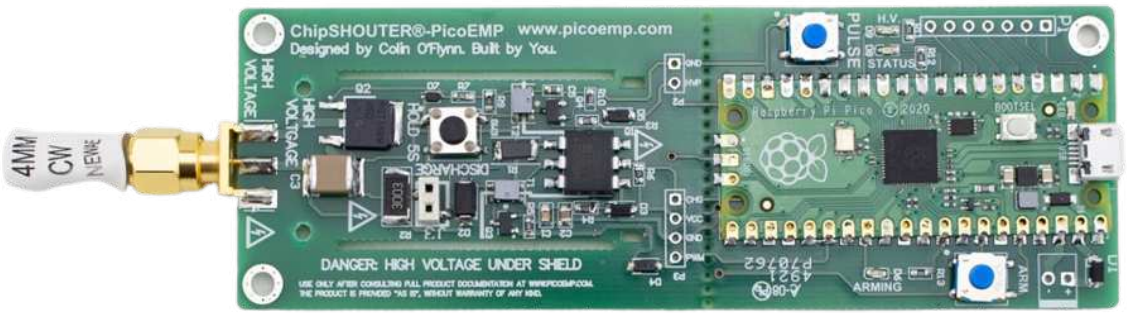



FIGURE 1.3 – Illustration du ChipSHOUTER-PicoEMP [73].

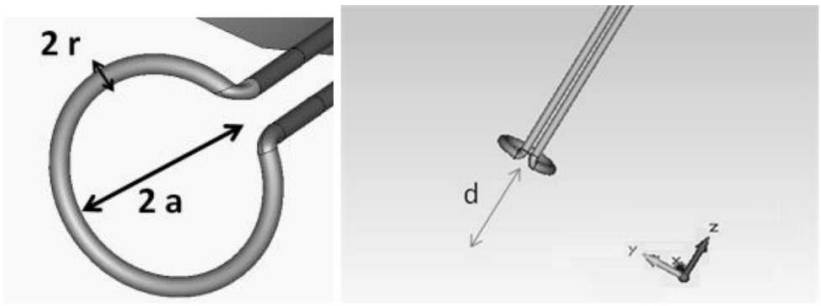
### Sondes d'injections

La perturbation électromagnétique permettant d'injecter une faute est créée en faisant circuler une impulsion de courant dans une bobine. Beaucoup de travaux portent sur la modélisation et la caractérisation des sondes d'injection électromagnétique. Jarrix [52] a présenté les premières caractérisations de sondes en 2010. Les sondes sont basées sur des câbles coaxiaux. Les mesures de coefficient de réflexion S11 réalisées avec un analyseur de réseau montrent que des pics de résonance sont observés lorsque la longueur de la sonde est proche de $\frac{\lambda}{4}$. L'étude d'une sonde, considérée comme de type magnétique, avec une spire montre que l'effet magnétique est dominant pour des fréquences en dessous de 1 GHz, mais qu'au-delà, le champ électrique généré doit aussi être pris en compte. Ainsi, il est préconisé d'utiliser des sondes basées sur un câble coaxial. Cependant, ces études sont réalisées pour des fréquences de l'ordre d'une dizaine de GigaHertz et ces sondes sont assimilables à des antennes quart d'onde pour des champs électromagnétiques. Les fréquences observées dans nos cas d'usages sont plus proches de quelques dizaines de MégaHertz.

Omarouayache et al. [75] ont simulé des sondes magnétiques pour l'injection de fautes afin d'en déduire les effets de différents paramètres. Ils ont pu mettre en évidence que l'intensité du flux dépend de la distance entre la sonde et le circuit. Ils évoquent l'idée qu'une seule boucle optimise l'intensité du flux. L'ajout d'une ferrite taillée en pointe, comme représenté sur la figure 1.4, améliore l'intensité et la localité du champ magnétique engendré. Or, dans les expériences que j'ai menées, l'utilisation d'une seule boucle au lieu de plusieurs spires (entre 5 et 10) perturbait moins les circuits.

Sauvage et al. [83] ont testé différentes sondes électriques. Une sonde large et plate (2 mm de longueur et 500 µm de largeur) semble la meilleure pour réaliser des injections de fautes. Les mesures sont effectuées sur une ligne microstrip et le couplage est électrique et non magnétique. Cependant, aucune attaque n'a été réalisée avec ce type de sonde dans l'état de l'art.

Chusseau et al. [31] ont mis en évidence que le couplage est de type magnétique




(a) (b)

Fig. 1. Basic probe geometry. (a) close view, (b) general view.

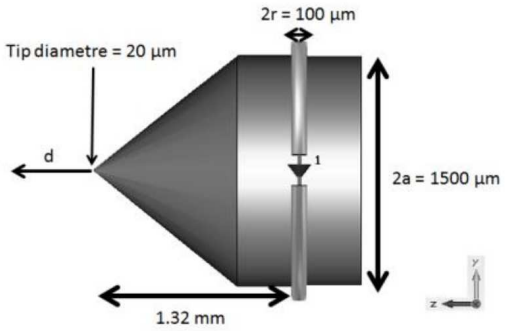



Fig 16. Sharpened ferrite in the loop and geometrical parameters.

FIGURE 1.4 – Illustration des sondes d'Omarouayache [75].

et non électrique. Ils ont montré que plusieurs tours couplent mieux à basses fréquences et que l'ajout d'une ferrite améliore l'intensité du flux magnétique créé.

Raoult et al. [81] ont proposé un modèle électrique de la sonde sur la base d'un couplage capacitif entre la sonde et le circuit. Le couplage entre des sondes et une ligne microstrip a été analysé et est dépendant du nombre de spires. La hauteur entre une sonde et un circuit est présentée comme ayant un rôle mineur sur l'efficacité de l'injection.

Trabelsi et al. [101] ont caractérisé des sondes en utilisant des buffers en cascade sur un FPGA. Les meilleures localités spatiales sont obtenues avec des noyaux de ferrites de diamètres fins.

Beckers et al. [24] ont étudié les sondes et les injecteurs. Ils ont montré que le matériau de ferrite utilisé a un impact significatif sur la réponse aux impulsions. Ils montrent qu'une augmentation du nombre de tours diminue l'amplitude de l'impulsion, mais cela se compense légèrement par une augmentation du champ magnétique généré. En revanche, la durée de l'impulsion de tension induite est allongée, comme présenté sur la figure 1.5. Une augmentation du diamètre de la ferrite réduit l'amplitude de la perturbation, car l'inductance et le champ magnétique dépendent du rayon du solénoïde. Une superposition des fils de la bobine augmente l'amplitude

du champ généré par rapport à une juxtaposition.

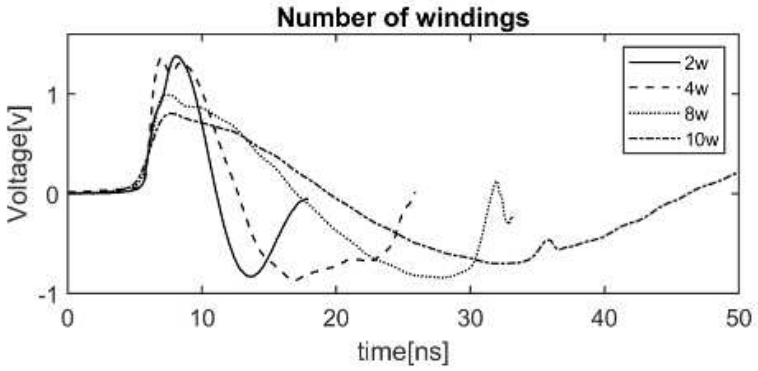



FIGURE 1.5 – Tension induite dans le dispositif de mesure après une excitation impulsionnelle en fonction du nombre de spires [24].

Toulemont et al. [99] ont montré que la tension induite dans une sonde d'écoute présente des oscillations. L'amplitude du second pic est d'environ 30 % de celle du premier. Le système d'adaptation d'impédance AVX-M4-H développé par Avtech est utilisé pour limiter les rebonds. Cependant, il engendre une division de l'amplitude de l'impulsion d'un facteur 2. Cela est justifié par une mauvaise adaptation d'impédance de sortie du dispositif de $3\,\Omega$ ; or celle de la sonde est inférieure à $1\,\Omega$. Une diode transil est alors utilisée en tant que système anti-rebond. Les effets ont été analysés via une sonde d'écoute Langer et montrent que la première impulsion est transmise tandis que les suivantes sont complètement supprimées.

### 1.2.2 Mécanismes d'injection de fautes électromagnétiques et modèles de fautes

Les perturbations électromagnétiques produisent des fautes au sein des circuits. Différentes études ont permis d'identifier les mécanismes de fautes ainsi que les modèles de fautes sur microcontrôleurs et sur microprocesseurs.

Dehbaoui et al. [35] ont présenté des résultats d'injection en utilisant des impulsions électromagnétiques sur deux types de circuits : microcontrôleur et FPGA. Ils décrivent que la perturbation modifie le déroulement d'un programme et que les effets sont similaires à une non-exécution des instructions ou bien d'un remplacement par l'instruction NOP (No Operations). L'effet est obtenu par une violation des contraintes temporelles de la cible, ce qui est montré par l'évolution entre le nombre de fautes et la tension d'injection. Une chute de tension suffisamment importante augmente les délais de propagation des données, créant une violation des temps d'établissement (*timing faults*).

Ordas et al. [76] ont présenté un modèle basé sur des modifications d'amplitude des signaux entrants des Flip Flop de type D pendant leur commutation, et donc

au moment du front montant du signal d'horloge. Ainsi, la contrainte de temps d'établissement ou de maintien au niveau de la porte est violée. Cela entraîne un échantillonnage et/ou transfert erroné des données (*sampling faults*). Cela est justifié par l'apparition d'une fenêtre de susceptibilité d'une largeur constante et indépendante de la période d'horloge. La durée des zones ne produisant pas d'injection augmente linéairement avec la période d'horloge, ce qui confirme l'existence d'un autre phénomène que les violations de contraintes temporelles.

Maurine et al. [64] ont mis en évidence la possibilité de forcer la sortie de Flip Flop de type D (DFF) à un état haut ou un état bas indépendamment de l'état d'entrée. Le premier type de fautes est appelé *bit-set* (la valeur du signal est forcée à 1) et le second *bit-reset* (la valeur du signal est forcée à 0). Le terme de *bit-flip* (inverser la valeur d'un signal) a été introduit.

Moro et al. [72] ont proposé une caractérisation au niveau du jeu d'instruction sur des microcontrôleurs ARM 32 bits Cortex-M3 où ils étudient les transferts depuis la mémoire flash. Des corruptions de données et des remplacements d'instructions ont été réalisés, dans 25 % des cas le comportement produit est identique à des sauts d'instructions.

Riviere et al. [82] ont ciblé la cache instruction d'un microcontrôleur ARM Cortex-M4. Ils ont montré qu'il est possible de sauter l'exécution de 4 instructions et de rejouer les 4 suivantes. Cela serait possiblement dû à la présence d'un cache d'instruction ou « prefetch buffer ».

Beckers et al. [23] ont montré que sur le microcontrôleur 8 bits ATmega328P les fautes sont obtenues sur les fronts d'horloge lors du chargement des données depuis la mémoire flash. En initialisant la flash avec différentes valeurs choisies, il est possible de générer des bits-sets mais pas de bit-reset. Un modèle similaire a été présenté dans [72].

Dumont et al. [37] ont proposé une modélisation de l'induction électromagnétique sur des circuits intégrés lors de fautes d'échantillonnage. La perturbation électrique provoque des variations sur le réseau d'alimentation. Le front de l'inversion de la polarité de l'alimentation de la Flip Flop durant un court instant la met dans un état « gelé », puis le front inverse permet un rétablissement rapide. La faute apparaît lorsque le front d'horloge est rétabli avant la stabilisation du signal d'entrée.

Proy et al. [79] ont travaillé sur un processeur ARM 32 bits Cortex-A9 qui a été bridé à 80 MHz. Ils proposent une méthodologie pour caractériser les fautes au niveau du jeu d'instruction (ISA), et identifient 4 modèles de fautes (saut d'instructions, mise-à-zéro du demi-mot le plus significatif d'un registre, corruption de registre et substitution des opérandes sources) ou une combinaison de ces modèles.

Trouchkine et al. [103] ont réalisé des injections de fautes sur des processeurs ARM Cortex-A53 et Intel Core i3. Ils ont identifié différents comportements (*bit-reset*, *bit-set*, *bit-flip*, observation de la valeur d'un autre registre, complémentaire de la valeur d'un autre registre, AND, XOR, OR ou ADD avec un autre registre ou deux autres registres.). Leurs travaux montrent que la localisation des fautes se situe entre la cache L2 et l'exécution d'une instruction par le processeur.

On constate ainsi que les effets des perturbations électromagnétiques ne sont pas triviaux, probablement dû à la complexité et la cohabitation de nombreux phénomènes dans les circuits. Différents cibles et bancs d'injections produisent des résultats potentiellement différents bien que cohérent entre eux. Plusieurs modèles de fautes sont présentés, cependant la conséquence de l'injection majoritairement décrite est un phénomène de saut d'instruction. Les exploitations présentées dans le tableau 1.1 imposent donc de protéger les circuits.

## 1.3 Contre-mesures à l'injection de fautes électromagnétiques

Afin de conserver l'intégrité et la confidentialité des données manipulées, il existe plusieurs types de protections notamment par blindages passifs et détecteurs d'attaques.

Les protections contre les injections de fautes peuvent être implémentées de façon logicielle, par exemple en doublant et vérifiant les instructions [21]. Ces contre-mesures logicielles sont plus faciles à mettre en œuvre sur des circuits déjà existants, mais elles peuvent être mises en défaut. En général, on utilise plusieurs niveaux de contre-mesures pour fiabiliser la sécurité des composants. On peut par exemple ajouter un blindage et des détecteurs d'attaque. Les deux types de protections consistent :

— À bloquer le chemin d'attaque en ajoutant un blindage bloquant le mécanisme physique à l'origine de l'attaque

— À détecter l'attaque en surveillant les paramètres environnementaux via un capteur de perturbation électromagnétique ou laser, par exemple.

La protection contre les injections électromagnétiques par blindage est connue par les experts de la sécurité matérielle et fait l'objet de publications scientifiques et de brevets. Il en va de même de la détection des attaques notamment par perturbation au moyen d'impulsions électromagnétiques.

### 1.3.1 Blindages contre les attaques par observation ou perturbation

Les dispositifs de blindage électromagnétique sont majoritairement destinés à des protections contre les interférences électromagnétiques et non pas contre les attaques par injection de fautes. Un brevet de Gemplus [45] déposé en 2006 propose cependant un dispositif de protection d'un composant électronique contre les attaques. Le circuit est encapsulé par un matériau présentant des variations aléatoires d'indices de réfraction, ce qui est représenté sur la figure 1.6. Le matériau déforme ainsi temporellement toute impulsion électromagnétique d'attaque, de façon à réduire sa localité temporelle.

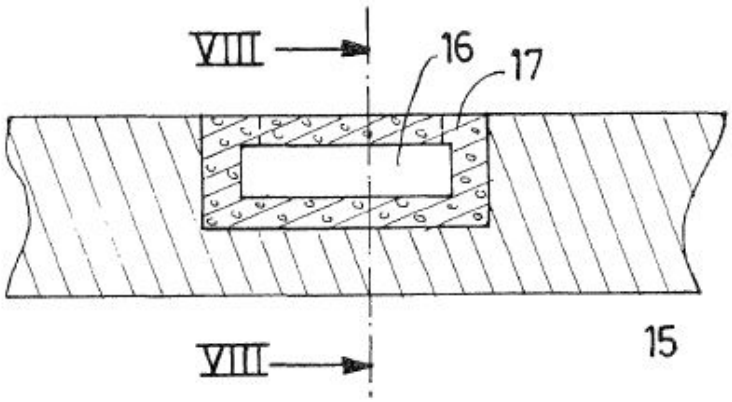



FIGURE 1.6 – Description du dispositif de Gemplus extrait de [45].

L'efficacité est relative dans la mesure où la protection est uniquement passive, elle ne détecte pas les attaques.

Apple [14] a déposé en 2015 un brevet proposant d'ajouter une couche de blindage magnétique composée de particules de ferrite sur des puces électroniques. L'utilisation de ce dispositif est prévue pour limiter les interférences électroniques sur une puce, générées par les antennes intégrées dans les smartphones.

Une protection par blindage contre les injections de fautes laser est l'ajout d'une couche de métal sur le composant comme montré par Anderson et al. [13]. Cependant, cette solution n'est viable qu'en face avant. En face arrière, les lasers de type infrarouge (longueur d'onde de 1064 nm) peuvent traverser le substrat de silicium et créer des fautes.

### 1.3.2 Détecteurs de perturbations électromagnétiques

Différents détecteurs d'impulsions électromagnétiques ont été réalisés en utilisant des éléments de logiques reconfigurables (FPGA). Zussa et al. [48] ont par

exemple développé un capteur détectant les perturbations de tension d'alimentation et électromagnétiques. Afin de couvrir la surface du circuit et maximiser la détection, il est nécessaire d'implémenter plusieurs capteurs. El-Baze et al. [22] ont développé un capteur entièrement numérique utilisant 5 bascules D. Ils ont montré que le détecteur était aussi efficace pour détecter les injections de type « Body-Biasing ». Miura et al. [70] ont conçu un capteur exploitant le fait qu'une perturbation modifie la phase et la fréquence de l'horloge interne du circuit cible, ce qui entraîne un déverrouillage de la boucle à verrouillage de Phase (PLL) et ainsi une détection de la perturbation. Breier et al. [26] ont utilisé un détecteur Hogge Phase et un oscillateur en anneau (RO) pour capter les modifications de fréquence induites par les ondes électromagnétiques.

Homma et al. [50] présentent une protection plus complète, à la fois contre les écoutes side-channel et les injections de fautes, en utilisant un capteur à double bobine. Lors de l'approche d'une sonde d'attaque à effet inductif, cette dernière se couple à une bobine de détection disposée à la surface du circuit à protéger. Le couplage maximal étant obtenu lorsque les deux bobines se retrouvent dans le même plan, la mutuelle inductance qui se crée a alors une valeur maximale et renseigne sur l'approche de la sonde d'attaque. Une description du dispositif est effectuée sur la figure 1.7.

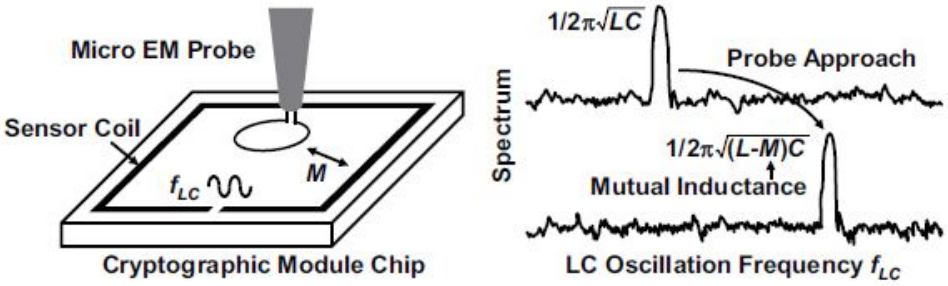



FIGURE 1.7 – Description du dispositif de Homma et al. [50].

Cependant, ils ne proposent pas de blindage, ni de moyens réduisant l'amplitude de l'induction magnétique, ni de contrôle de l'intégrité du dispositif de protection. Dans le cas d'attaques de forte intensité, la bobine de détection peut alors devenir une source de perturbation, pouvant endommager ou fauter le circuit à protéger, par induction dans les réseaux d'alimentation électrique du circuit.

Un état de l'art de détecteurs d'impulsions laser est présenté, car leurs fonctionnements en tant que dispositifs de contrôle d'intégrité peuvent être adapté en les rendant efficaces pour toute détection d'injection semi-invasive telle que les injections de fautes par perturbations électromagnétiques. Champeix et al. [30] ont validé l'utilisation d'un détecteur de courant (Bulk Current) pour la détection du courant induit par des tirs laser. He et al. [49] proposent une contre-mesure au niveau logique sur un FPGA en utilisant un RO et une PLL pour surveiller l'ondulation des

fréquences dans le RO et ainsi détecter une impulsion laser.

Afin de réaliser une attaque par injection laser, il est nécessaire de décapsuler le composant pour avoir accès à la puce [69]. Cela peut être fait de façon chimique ou mécanique. Les composants peuvent aussi être analysés par sondage afin de déterminer leur fonctionnement et leurs moyens de protections. Ces techniques demandent aussi l'abrasion du matériau d'encapsulation. Il est donc important de vérifier l'intégrité du circuit cible afin de garantir la confidentialité et intégrité des données manipulées.

Sharhrjerdi et al. [87] ont mis au point un composant électronique contre la rétro-ingénierie via sondage et les attaques par injections de fautes. Ils exploitent des photodétecteurs au niveau du circuit intégré chargé de détecter une illumination seuil et des capteurs à poutre micro ou nano-piézoélectriques montés sur le circuit intégré sensible aux vibrations induites par les procédés d'abrasion mécanique. Les dispositifs sont décrits dans la figure 1.8.

Le premier dispositif est composé d'éléments photovoltaïques qui vont absorber les radiations incidentes et générer une énergie électrique. Celle-ci va déclencher l'effacement du circuit afin d'empêcher un attaquant de voler des informations confidentielles. Le second dispositif est composé d'un microsystème électromécanique (MEMS) en porte-à-faux qui convertit les vibrations mécaniques vers une énergie électrique, et peut déclencher l'effacement du circuit.

Plusieurs contre-mesures dans le domaine des attaques par observation consistent à masquer (en modifiant l'algorithme de façon à ce que les variables soient indépendantes de la clé secrète) ou cacher (en générant du bruit) les informations. Nous nous intéressons principalement aux contre-mesures nécessitant le moins de modifications du code à protéger. Liu et al. [58] ont par exemple proposé un générateur de bruit adaptatif contre les attaques par écoute électromagnétiques sur une plateforme ARM. Il est basé sur la vidange et le rechargement d'une mémoire cache. Cette méthode logicielle est uniquement adaptée pour l'architecture ARM. La contre-mesure surcharge les performances du système de moins de 5 % et diminue l'efficacité des écoutes side-channel à 70 %.

## 1.4 Contexte et objectifs de la thèse

Les circuits intégrés peuvent contenir de nombreuses données personnelles, ce qui est accentué lorsque les composants sont implémentés sur des plateformes de type smartphone. Les attaques par injection de fautes permettent d'extraire des secrets tels que des clés de chiffrement ou des propriétés intellectuelles. Ainsi, la sécurité de ces circuits intégrés est primordiale afin de garantir la confidentialité et intégrité des données. Les attaques par injection de fautes électromagnétiques induisent des fautes

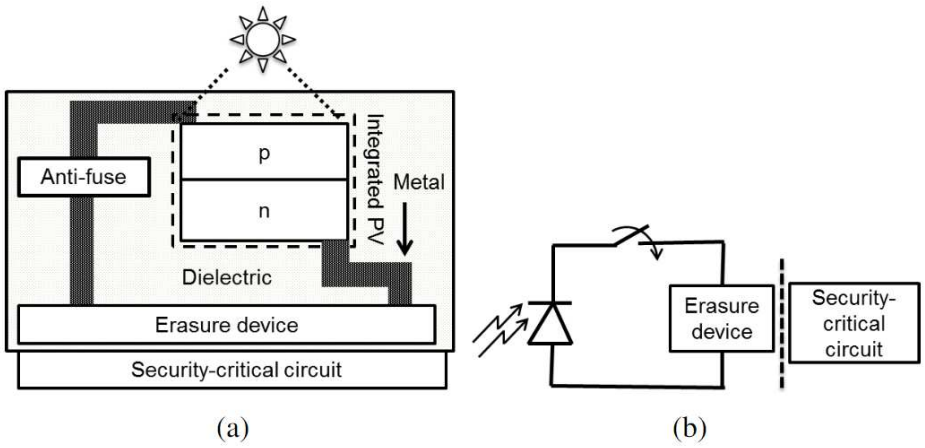



Fig. 3. (a) Side-view of an IC using energy-harvesting PV cells to detect optical attacks [4]. (b) Equivalent circuit diagram.

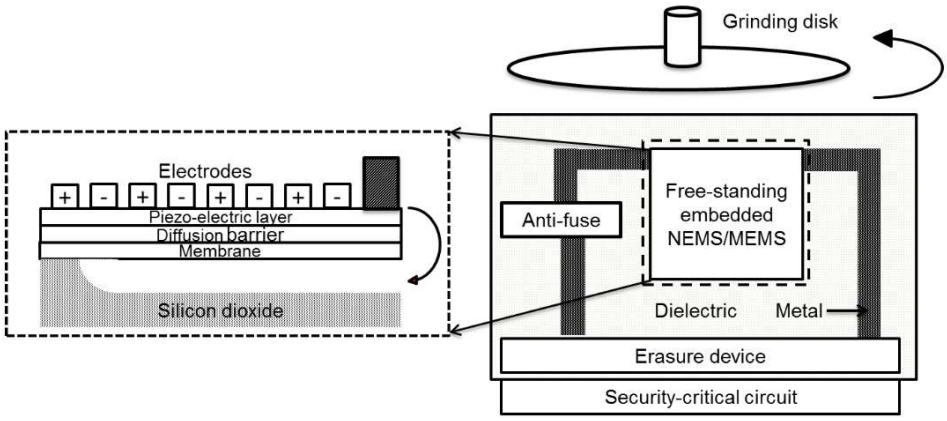



Fig. 5. Side-view of an IC using NEMS/MEMS-based devices to detect mechanical attacks. The inset shows the structure of a NEMS/MEMS cantilever.

FIGURE 1.8 – Description du dispositif de Shahrjerdi et al. [87].

dans un circuit afin d'en corrompre le fonctionnement. Ces attaques sont principalement dirigées contre des microcontrôleurs et dans des contextes académiques. Les travaux de cette thèse s'intéressent aux cibles complexes, telles que celles utilisées dans des smartphones. Cette thèse s'inscrit aussi dans un contexte industriel, au travers du projet CSAFE+ [1] et des forces de l'ordre, avec le projet européen EXFILES.

Afin de réaliser ces injections sur des processeurs complexes avec plusieurs cœurs et des fréquences de fonctionnement élevées, les bancs d'injection électromagnétiques doivent être adaptés. Les travaux de ma thèse portent dans un premier temps à la compréhension des phénomènes de génération et de propagation des ondes électromagnétiques ainsi qu'à leur optimisation. Nous pouvons ainsi évaluer la capacité d'attaque afin de définir l'efficacité maximale d'un attaquant. La mise en place des injections sur un SoC est réalisée dans un second temps. La compréhension des mécanismes d'injection fait progresser l'efficacité des mécanismes de défense, ainsi des solutions de protection des circuits intégrés face aux attaquants les plus performants sont proposées.

L'objectif de ces travaux est d'améliorer la mise en place des injections de fautes sur cibles mobiles afin d'en assurer leur protection. Pour cela, il est dans un premier temps nécessaire d'améliorer les sondes et générateurs d'impulsions afin d'optimiser les perturbations électromagnétiques. Les injections de fautes sur cibles complexes seront alors réalisées. Les résultats de la perturbation pourront être exploités pour mener à bien une élévation de privilèges. Enfin, les cibles de type microprocesseur devront être protégées des injections de fautes par perturbations électromagnétiques.

1. Circuit Sécurisé contre les Attaques par injection de Fautes Électromagnétiques avancées

# Chapitre 2 : Caractérisation du dispositif d'injection de fautes par induction magnétique

En fournissant une étude détaillée du couple (sondes d'injection électromagnétiques et générateur d'impulsions), ce chapitre s'intéresse aux bancs d'injection électromagnétiques. L'analyse des sondes est réalisée en régime statique afin de caractériser leur géométrie et donc leur localité spatiale. Dans un second temps, l'étude s'effectue en régime dynamique permettant d'analyser la résolution temporelle des sondes sous test. Les sondes étant constituées d'un noyau en ferrite, une partie des travaux est donc dédiée à l'identification du meilleur compromis entre localité et puissance transmise. Enfin, différentes solutions pour adapter les impédances de sortie des générateurs et limiter les rebonds sont évaluées.

## Sommaire du chapitre

## 2.1 Phénomènes physiques et dispositifs expérimentaux

La mise en place d'injections de fautes par perturbations électromagnétiques sur des circuits intégrés requiert l'utilisation d'un dispositif d'injection électromagnétique composé d'un générateur d'impulsions de tension. Ce dispositif ainsi que les cibles évaluant les propriétés des phénomènes physiques rencontrés sont décrits. Grâce à cela, la nature de l'injection électromagnétique est déterminée.

### 2.1.1 Dispositifs d'injection de fautes par perturbation électromagnétique et plateformes de test

Les résultats présentés dans ce chapitre ont nécessité la mise en place de nombreuses expérimentations. Les dispositifs d'injections de fautes par perturbations électromagnétiques utilisés se composent de bancs d'injections et de différentes cibles.

#### Banc d'injection électromagnétique

Les campagnes d'injections électromagnétiques présentées dans l'ensemble de cette thèse ont été réalisées grâce à des générateurs d'impulsions de tension de marque Avtech [15, 16], de sondes d'injection placées sur un bras motorisé et d'une unité de contrôle tel que présenté sur la figure 2.1.

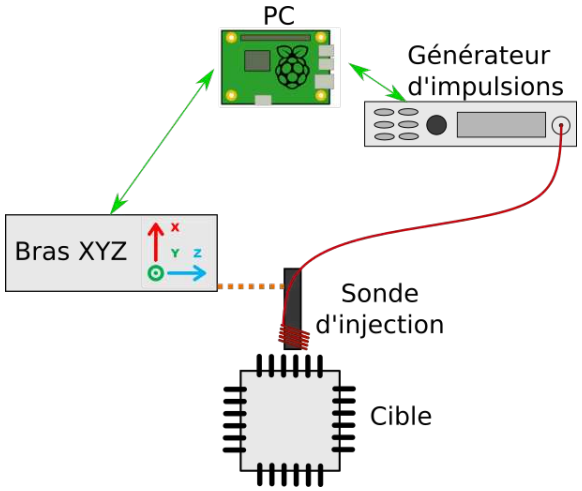



FIGURE 2.1 – Banc d'injection de fautes par perturbations électromagnétiques.

Les générateurs d'impulsions de tension utilisés dans cette thèse délivrent des impulsions avec une force électromotrice maximale de 800 V crête et une impédance de sortie de 50 Ω, soit un courant pic de court-circuit de 16 A. Les tensions présentées dans ce manuscrit correspondent aux consignes d'amplitudes fournies au générateur, et sont donc égales à la moitié de la force électromotrice créée. En effet, afin de produire une tension U aux bornes du générateur, il est nécessaire de fournir une force électromotrice $E = U + R * i$ où R est la résistance interne du générateur,

égale à 50 Ω, et i l'intensité dans le circuit. Ainsi, une tension affichée de 400 V est équivalente à une force électromotrice de 800 V. Les temps de montée et de descente sont compris entre 1.5 et 5 ns, tandis que la durée de l'impulsion varie entre 6 et 100 ns.

La sonde est le deuxième élément clé pour le dispositif d'injections électromagnétiques. Elle est composée d'une bobine de fil enroulée autour d'une tige de ferrite, que l'on connecte au générateur. Elle est positionnée au plus près du circuit cible via un bras motorisé XYZ d'une précision de 0.1 µm. Les sondes utilisées dans ces travaux de thèse sont réalisées à la main, et sont présentées en annexe. La figure 2.2 illustre une sonde d'injection composée d'un connecteur SMA, d'une ferrite et de 5 spires. Des gaines thermorétractables peuvent être ajoutées afin de maintenir de la ferrite et de faciliter l'identification des sondes.

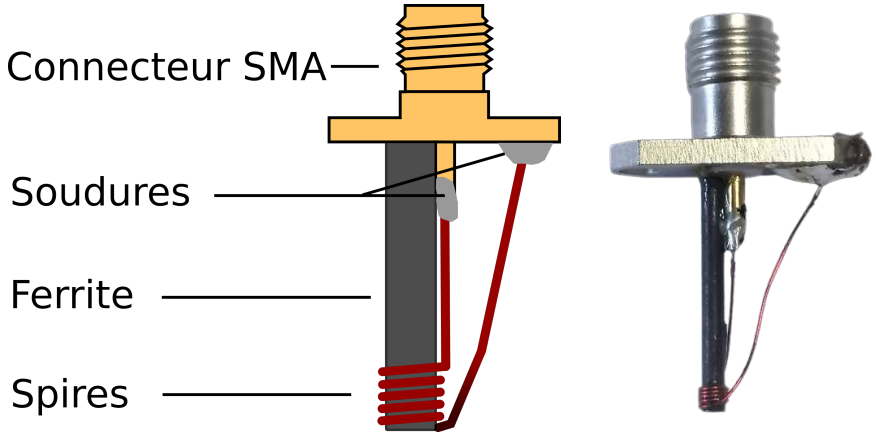



FIGURE 2.2 – Sonde d'injection électromagnétique, composée d'une ferrite et de 5 spires.

Quatre cibles sont majoritairement utilisées dans les travaux présentés dans ce chapitre : une sonde d'écoute de diamètre 250 µm, un microcontrôleur ATmega328P, un FPGA Zynq-7010 et un système sur puce (SoC) décrit dans le chapitre 3.

### Sonde d'écoute de diamètre 250 µm

Le premier dispositif servant à mesurer le champ $\vec{B}$ émis par la sonde d'injection est une sonde d'écoute. Elle est composée de 2 spires de fil de diamètre 40 µm autour d'un support en polymère de diamètre 170 µm. Elle est donc d'un diamètre extérieur de 250 µm. La figure 2.3 présente la sonde d'écoute mesurant le champ $\vec{B}$ émis par une sonde d'injection, composée de 5 spires autour d'une ferrite de diamètre 750 µm.

Cette sonde est utilisée pour évaluer le champ $\vec{B}$ qu'émettent les sondes d'injection électromagnétique. Pour cela, un oscilloscope est connecté à ses bornes pour mesurer sa tension induite. Son diamètre inférieur à l'ensemble des sondes d'injections étudiées permet de la considérer comme suffisamment ponctuelle pour réaliser des mesures spatiales du champ $\vec{B}$ émis par la sonde d'injection.

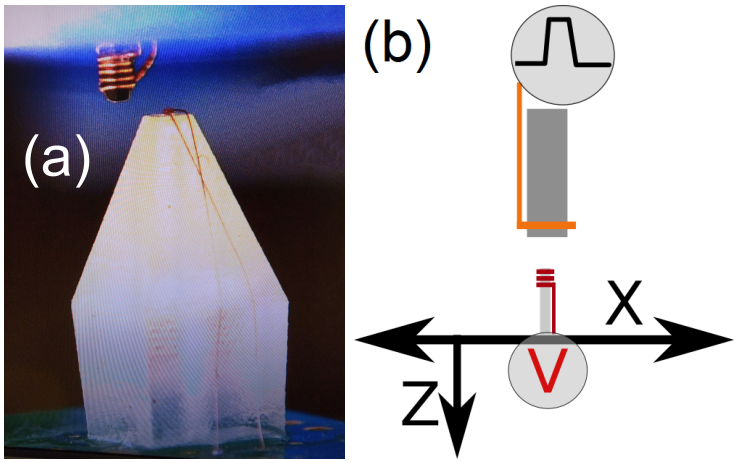



FIGURE 2.3 – **a.** Sonde d'écoute de diamètre 250 µm (bas) caractérisant une sonde de diamètre de ferrite 750 µm (haut) **b.** Manipulation réalisant des cartographies XZ du champ $\vec{B}$ émis, avec une sonde d'écoute.

### Cible microcontrôleur ATmega328P

La seconde cible utilisée pour caractériser le dispositif d'injection est un microcontrôleur ATmega328P-PU. Ce microcontrôleur 8 bits RISC est présent sur les plateformes de prototypage Arduino Uno, tel que présenté sur la figure 2.4. La technologie est CMOS 0,35 µm et la fréquence de fonctionnement est de 16 MHz. Il comporte 20 ko de mémoire flash, 2 ko de SRAM et 1 ko d'EEPROM. Ce circuit âgé d'une quinzaine d'années a une conception simple propice à une interprétation facile des résultats de l'injection de fautes. De nombreuses publications étudiant ce composant ont été effectuées au sein du laboratoire *SAS*, ce qui justifie son utilisation actuelle.


FIGURE 2.4 – Plateforme de développement Arduino Uno embarquant un microcontrôleur ATmega328P.

Les essais d'injection sont menés lors de l'utilisation d'un programme de test simple permettant la caractérisation des fautes injectées. Ce programme, présenté sur le code source 2.1, est une manipulation des registres qui sera soumise à une perturbation.

```
//Initialisation des registres : r16 a r25 = 0x55
ldi r16,0x55
ldi r17,0x55
...
ldi r25,0x55

//Levee du trigger
sbi %[portb],%[portb0]

//Manipulation des registres = Instructions cibles
ld r16,Z+
ld r17,Z+
...
ld r25,Z+

//Descente du trigger
cbi %[portb],%[portb0]

//Lecture des valeurs contenues dans les registres
```

Code 2.1 – Extrait du programme en langage assembleur pour détecter la présence de fautes sur ATmega328P.

L'instruction *ld Rd, Z+* charge un mot de 8 bits de la mémoire SRAM vers le registre de destination *Rd*. Les mots à charger sont inscrits dans un tableau. Le registre *Z* pointe initialement vers le premier élément du tableau puis est incrémenté afin de charger les éléments suivants. L'injection de fautes est réalisée lors de l'exécution des instructions de chargement des registres. Les valeurs contenues dans les registres sont ensuite relues et comparées avec celles obtenues sans perturbations. L'effet des perturbations est un saut d'une (ou plusieurs) instruction, nous pouvons alors lire la valeur d'initialisation *0x55* dans un des registres. Cet outil est utilisé avec un générateur d'impulsions de tension de marque Avtech. La tension de consigne minimale du générateur d'impulsions permettant de réaliser des fautes est appelée seuil de fautes. La comparaison des seuils de fautes obtenus avec différentes sondes sert à évaluer l'intensité des perturbations produites. L'étendue de la zone du microcontrôleur sensible aux perturbations électromagnétiques est utilisée pour déterminer la localité spatiale des sondes.

**Cible FPGA Zynq-7010**

La troisième cible testée dans ces travaux de thèse est un FPGA Zynq-7010 présent sur une carte de développement Zybo Z7. Le bloc fonctionnel implanté dans la logique programmable visé sur le FPGA est un capteur à base d'oscillateur en anneau (RO) développé par Gravellier et al. [47] et présenté sur la figure 2.5. Une perturbation électromagnétique engendre une variation de la tension d'alimentation des composants du FPGA. Ainsi, les délais de propagation des portes logiques évoluent en fonction de l'intensité de la perturbation. Le capteur est composé d'un inverseur provoquant une oscillation infinie de la sortie, qu'on lit à une fréquence fixe. Les fluctuations des valeurs en sortie du capteur permettent donc d'avoir une image de la variation de tension dans la cible.

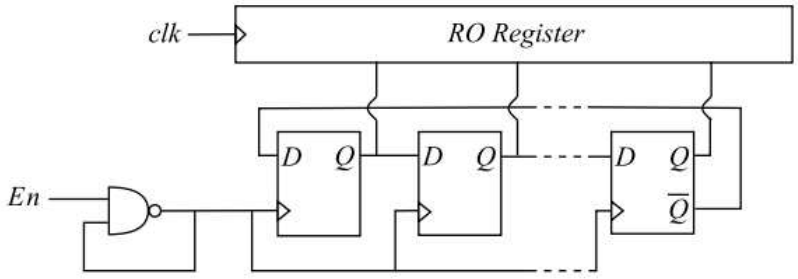



FIGURE 2.5 – Schéma du capteur à base d'oscillateurs en anneaux [47].

En comptant le nombre d'oscillations de l'oscillateur en anneau dans un temps donné, on mesure les variations internes de tension du FPGA. Ce capteur est donc assimilable à un oscilloscope embarqué pour mesurer les variations de tension interne dans la cible, à une fréquence de 200 MHz.

### 2.1.2 Étude de la nature de l'injection électromagnétique : capacitive ou inductive

La première question a été de déterminer si les perturbations engendrées par le banc d'injection reposent sur un effet capacitif ou inductif. En effet, nous retrouvons différentes utilisations de sondes électriques dans l'état de l'art [83]. Pour cela, nous réalisons un montage avec une sonde inductive d'injection électromagnétique composée d'une bobine, générant un champ $\vec{B}$, et une sonde capacitive composée d'une pointe, générant un champ $\vec{E}$.

Nous commençons les expérimentations par des campagnes d'injections utilisant une sonde capacitive sur un ATmega328P, comme présenté dans la figure 2.6.

Avec la sonde d'injection utilisant uniquement l'effet capacitif, il n'a pas été possible d'obtenir des fautes avec les mêmes paramètres de tension, de durée d'impulsion et de front montant qu'utilisés avec la sonde d'injection inductive. De même, en exploitant tout le potentiel du générateur d'impulsions de tension, i.e. pour des

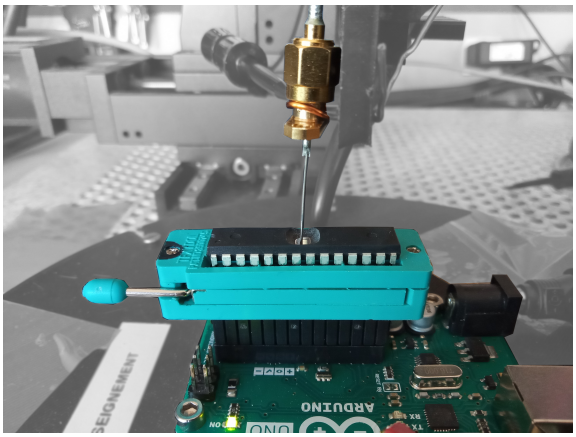



FIGURE 2.6 – Montage pour l'injection avec une sonde capacitive sur ATmega328P.

tensions de 280 V, une durée d'impulsion de 10 ns et un front montant de 2.5 ns, aucune faute n'a été obtenue.

Nous réalisons aussi des injections sur l'oscillateur en anneau du FPGA Zybo. Les variations des valeurs retournées sont présentées sur la figure 2.7.

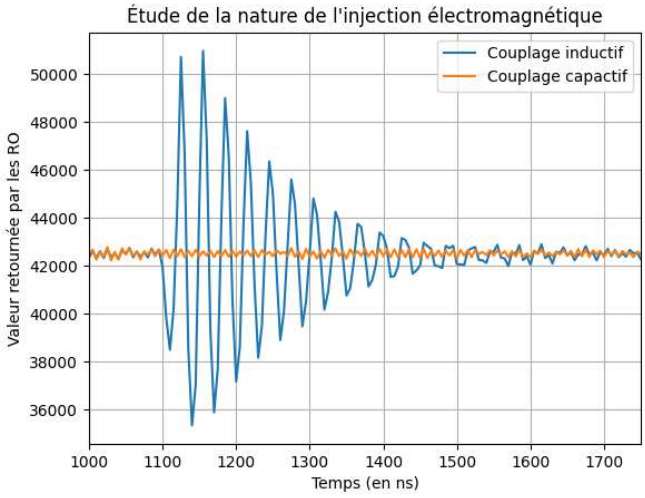



FIGURE 2.7 – Comparaison de l'effet induit dans la logique d'un FPGA par couplage inductif et capacitif.

Nous observons des variations notables de la valeur retournée par l'oscillateur en anneau avec la sonde inductive. Cependant, avec la sonde capacitive, aucune variation ne sort du niveau de référence. Nous en concluons donc que le couplage n'est pas capacitif et que la composante inductive a l'effet dominant dans notre cas. La tension nécessaire aux attaques par couplage capacitif sera probablement beaucoup plus élevée qu'avec des attaques par couplage inductif. Ainsi, nous étudierons seulement les sondes d'injection à effet inductif.

### 2.1.3 Rappels d'électromagnétisme

Un champ électromagnétique représente l'ensemble des forces électromagnétiques appliquées sur une particule chargée. Nous exprimons cette force de Lorentz par $\vec{F} = q(\vec{E} + \vec{v} \wedge \vec{B})$ où $q$ est la charge de la particule, $\vec{E}$ est le champ électrique, $\vec{v}$ est la vitesse de la particule et $\vec{B}$ est le champ magnétique.

Dans le cas de l'injection de fautes, une impulsion de courant est réalisée dans un solénoïde. La variation du courant électrique crée un champ magnétique (théorème de Maxwell-Ampère).

Le circuit de réception est donc soumis à un flux magnétique variable $\Phi$, qui produit, d'après la loi de Lenz-Faraday, une force électromotrice $e = -\frac{d\Phi}{dt}$. $\Phi$ est défini par $\Phi = \oint_S \vec{B} \cdot d\vec{S}$, avec $\vec{S}$ la surface orientée du circuit de réception.

Ainsi, nous analyserons dans la suite de l'étude la force électromotrice engendrée dans le circuit cible. Cela implique d'étudier la variation de $\frac{d\Phi}{dt}$, et donc du champ $\vec{B}$ produit par une sonde.

## 2.2 Étude des sondes d'injection

Une sonde d'injection est généralement constituée de quelques spires autour d'une ferrite cylindrique. Dans cette section, nous étudions la géométrie afin d'identifier les paramètres importants et les réglages qui optimisent l'effet d'une perturbation électromagnétique.

### 2.2.1 Géométrie pour une sonde composée d'une seule spire

Pour simplifier la compréhension et l'étude du mécanisme d'injection électromagnétique ainsi que l'effet de la géométrie d'une sonde inductive, nous effectuons l'étude sur une sonde composée d'une seule spire. Afin d'étudier la géométrie des sondes d'injection, nous réalisons l'étude théorique de façon statique. Dans un premier temps, nous ne prendrons en compte qu'une spire circulaire sans présence d'une tige de ferrite. Pour cela, nous considérons une spire, de rayon R, et un point M dans l'espace comme représenté sur la figure 2.8.

Un courant I circule dans la spire et nous définissons en un point P une portion élémentaire de fil $\vec{dl}$ orientée. Notons $\theta$ l'angle xOP et $d\vec{B}$ la portion élémentaire de fil produit un champ élémentaire en un point M. La représentation selon le plan XZ est présentée sur la figure 2.9. La zone en pointillé de la figure 2.9.a représente l'emplacement d'une ferrite, ou dans le cas de l'étude, de l'air. Nous voulons écrire le champ magnétique produit par la spire. D'après la loi de Biot et Savart, le champ magnétique produit par un courant constant sur une longueur de spire élémentaire $\vec{dl}$ intégré sur le contour de la spire est :

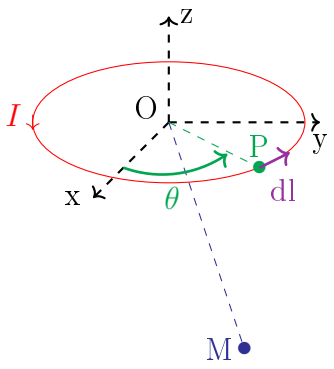



FIGURE 2.8 – Schéma d'une spire circulaire (en rouge).

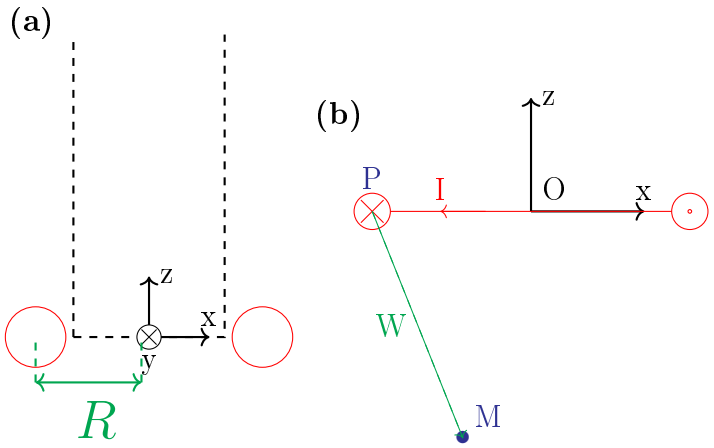



FIGURE 2.9 – Schéma d'une sonde composée d'une spire (en rouge).

$$\boxed{B(\vec{r}) = \frac{\mu_0 I}{4\pi} \oint_C \frac{\vec{dl} \wedge \vec{W}}{|\vec{W}|^3}} \tag{2.1}$$

$\vec{dl}$ est le vecteur déplacement élémentaire tangent au contour de la spire C au point P et $\vec{W}$ est le vecteur entre le fil et le point M. P est sur le fil et M dans l'espace. $\mu_0$ est la perméabilité magnétique du vide et vaut $4\pi * 10^{-7} kg.m.A^{-2}.s^{-2}$.

Le vecteur déplacement élémentaire dl s'écrit $\vec{dl} = \begin{pmatrix} dx \\ dy \\ dz \end{pmatrix} = R \begin{pmatrix} -\sin\theta \\ \cos\theta \\ 0 \end{pmatrix} d\theta$

et $\vec{W} = \begin{pmatrix} x - R\cos\theta \\ y - R\sin\theta \\ z \end{pmatrix}$.

En utilisant la loi de Biot et Savart, nous obtenons :

$$B_x(x,y,z) = \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{Rz\cos\theta d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + z^2]^{\frac{3}{2}}}$$

$$B_y(x,y,z) = \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{Rz\sin\theta d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + z^2]^{\frac{3}{2}}}$$

$$B_z(x,y,z) = \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R^2 - Ry\sin\theta - Rx\cos\theta)d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + z^2]^{\frac{3}{2}}}$$

Nous cherchons le flux produit sur la surface $S$ d'une autre spire distante et parallèle au plan (0xy) : $\Phi = \int_{S_C} \vec{B} \cdot \vec{dS}$.

Nous nous plaçons dans un cas d'une spire de réception dans le plan XY, ainsi S est dans le plan XY, donc $\vec{dS} = \begin{pmatrix} 0 \\ 0 \\ dS \end{pmatrix}$.

Nous obtenons $\Phi = \int_{S_C} B_z \cdot dS$.

Nous considérons donc uniquement la composante en z du champ $\vec{B}$, d'où :

$$\boxed{B_z(x,y,z) = \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R^2 - Ry\sin\theta - Rx\cos\theta)d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + z^2]^{\frac{3}{2}}}} \tag{2.2}$$

La figure 2.10 affiche les résultats de l'application de l'équation 2.2 pour différentes distances entre les spires. Cette équation a été tracée en utilisant le langage Python. Une sonde d'un rayon de spire R=850 µm a été utilisée pour ce test. Cela correspond à une sonde réalisée avec un fil de 200 µm de diamètre autour d'un support de 1500 µm de diamètre. Le courant circulant dans les spires est proposé arbitrairement à 1 A. L'intensité du champ $\vec{B}$, proportionnelle au courant, est donnée en millitesla ($mT$).

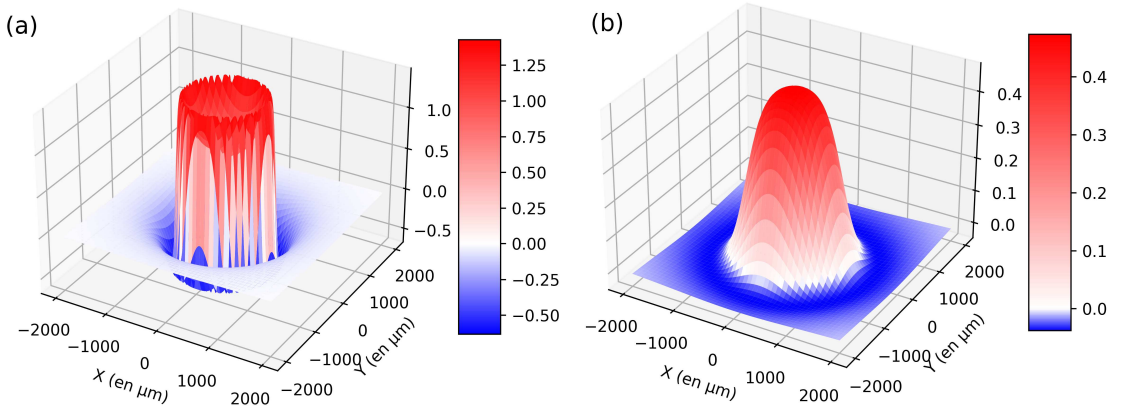



FIGURE 2.10 – Évolution du champ $\vec{B}$ (en mT), en fonction de x et y pour R=850 µm à z=-100 **(a)** et -500 µm **(b)** .

Nous constatons que le champ $\vec{B}$ est de forme cylindrique lorsque la distance z est petite comparée au rayon, puis forme une cloche lorsque la distance z augmente. Son amplitude décroît lorsque l'on s'éloigne de la spire d'injection, passant d'un maximum à 1.25 mT à 100 µm de distance à 0.45 mT à 500 µm.

### Étalement spatial

La représentation du champ $\vec{B}$ en 3 dimensions pour une spire de rayon R=850 µm est projetée sur le plan XZ, car il existe une symétrie cylindrique par rapport à l'axe z.

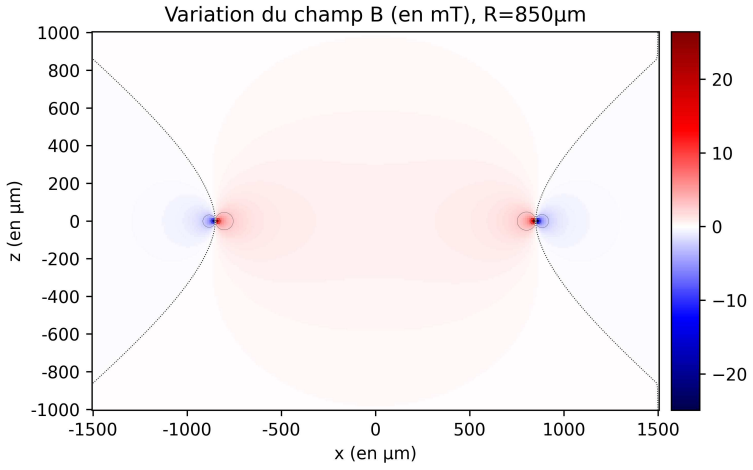



FIGURE 2.11 – Évolution du champ $\vec{B}$, en fonction de x pour R=850 µm.

Trois zones sont créées, soit une positive entre les deux sections de fil et deux

négatives à l'extérieur. L'intensité du champ $\vec{B}$ est maximale à la périphérie de la spire, puis décroît lorsque l'on s'en éloigne. Afin d'étudier cette décroissance en fonction de la distance, nous nous positionnons à une « hauteur » z par rapport à la spire. Nous avons alors :

$$\boxed{B_z(x) = \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R^2 - Rx\cos\theta)d\theta}{[(x - R\cos\theta)^2 + (R\sin\theta)^2 + z^2]^{\frac{3}{2}}}}. \tag{2.3}$$

La représentation de l'étalement spatial du champ $\vec{B}$ en fonction de la distance z est illustrée sur la figure 2.12. La simulation est effectuée pour une sonde d'un rayon de 1600 µm et le champ B est tracé en fonction de la position x pour différentes hauteurs z.

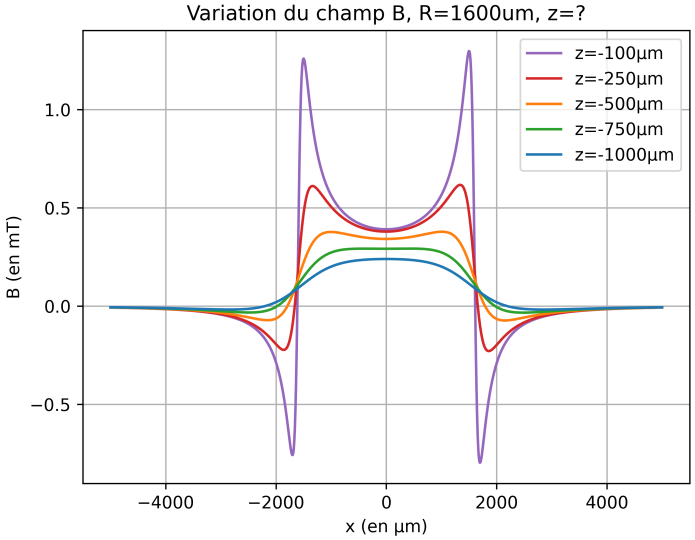



FIGURE 2.12 – Champ $\vec{B}$ engendré en fonction de x pour R=1600 µm.

Lorsque la hauteur est très faible par rapport au diamètre de la spire (de l'ordre de 100 µm), nous observons des valeurs élevées du champ juste au-dessous de la spire. Dans la pratique, la distance entre la spire et un circuit est au minimum de 200 µm, ce qui correspond à des champs générés inférieurs à 1 mT.

La comparaison avec les valeurs expérimentales est réalisée en mesurant le champ $\vec{B}$ émis par la spire via une sonde d'écoute d'un diamètre de 250 µm, tel que décrit sur la figure 2.13.a. La sonde d'attaque est conçue avec un fil de 200 µm de diamètre autour d'un support de 3 mm de diamètre. Le diamètre de la spire étant de 3.2 mm, nous considérons la sonde d'écoute comme ponctuelle. La spire est excitée par un signal impulsionnel produit par un générateur d'impulsions de tension de marque Avtech. Nous notons la tension maximale reçue dans la sonde d'écoute. Les résultats expérimentaux sont comparés selon la figure 2.13.b avec la simulation d'une sonde

d'un rayon de 1600 µm et d'une distance z=600 µm, correspondant à la distance entre les deux sondes lors de l'expérience.

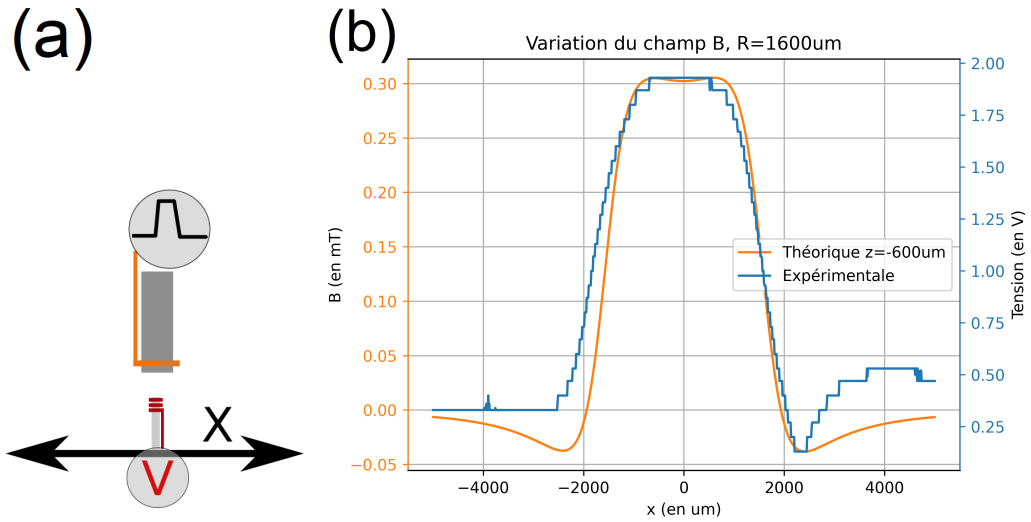



FIGURE 2.13 – **a.** Montage mesurant expérimentalement le champ $\vec{B}$ produit par une sonde **b.** Profil du champ $\vec{B}$ engendré en fonction de x, théoriquement et expérimentalement (en supposant la sonde d'écoute quasi-ponctuelle).

Les valeurs du champ $\vec{B}$ simulé atteignent un maximum de 0.31 mT sur une largeur de 1600 µm. La tension mesurée atteint un maximum de 1.9 V sur une largeur de 1400 µm. Les données théoriques et expérimentales sont assez similaires. Il y a une légère perte de symétrie sur la courbe expérimentale, car le plan de la spire n'est pas rigoureusement perpendiculaire à l'axe z.

### Effet du diamètre de la spire

Nous cherchons à étudier l'effet du diamètre des spires sur les champs $\vec{B}$ produits. L'influence du rayon de la spire sur le champ $\vec{B}$ engendré à une distance de 500 µm est illustrée sur la figure 2.14.

Nous constatons que le rayon de la spire influence l'intensité et l'étalement spatial des champs $\vec{B}$ engendrés. Le champ maximum est engendré pour un rayon de 750 µm, soit environ 1.4 fois la distance z. Pour les sondes de rayon inférieur à cette valeur, nous obtenons des champs en forme de cloche, et pour des sondes d'un rayon supérieur, nous observons une forme cylindrique puis l'apparition de deux pics.

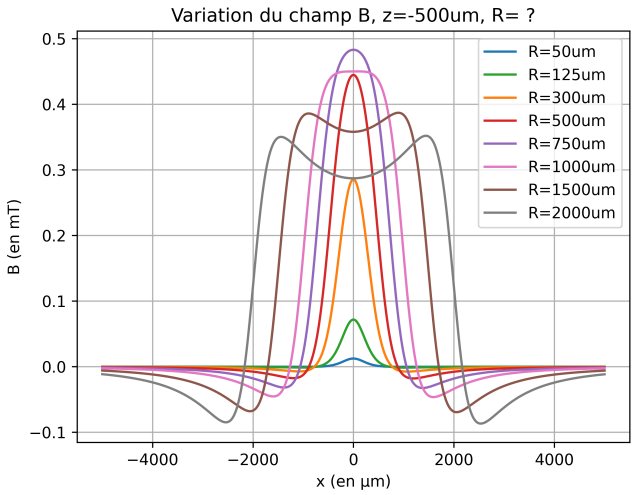



FIGURE 2.14 – Champ $\vec{B}$ engendré en fonction de x pour différents rayons de la spire d'émission à une distance de 500 µm.

### Loi de décroissance en z

Nous nous plaçons sur l'axe z, et nous cherchons à calculer le flux à travers une surface de 250 µm*250 µm :

$$\Phi = \int_{S_C} B_z \cdot dS = \int_{-125um}^{+125um} \int_{-125um}^{+125um} B_z dx dy \quad (2.4)$$

$$= \int_{-125um}^{+125um} \int_{-125um}^{+125um} \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R^2 - Ry\sin\theta - Rx\cos\theta)d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + z^2]^{\frac{3}{2}}} dxdy. \quad (2.5)$$

Nous obtenons une loi de décroissance du flux en $\frac{1}{z^2}$, tandis que celle du champ est en $\frac{1}{z^3}$. La décroissance théorique est comparée avec les valeurs expérimentales de la figure 2.15.

Les valeurs de la courbe théorique sont proches de celles de la courbe expérimentale. Nous notons que la courbe expérimentale débute avec un décalage de 300 µm par rapport à la courbe théorique, car il est en pratique impossible d'avoir une distance z = 0 µm.

Ces courbes montrent que le positionnement en z de la sonde a une influence importante sur la valeur du champ $\vec{B}$. Ainsi, lors d'un positionnement manuel de la sonde, la répétabilité des expériences n'est pas bonne pour des distances z où la pente est la plus forte, typiquement autour de 1 mm (trait vert sur la figure 2.15). Par exemple, à z=600 µm, une erreur de positionnement à +/-300 µm engendre une variation de flux de l'ordre de 35 %.

La décroissance en z varie également en fonction du rayon de la spire comme représenté sur la figure 2.16.

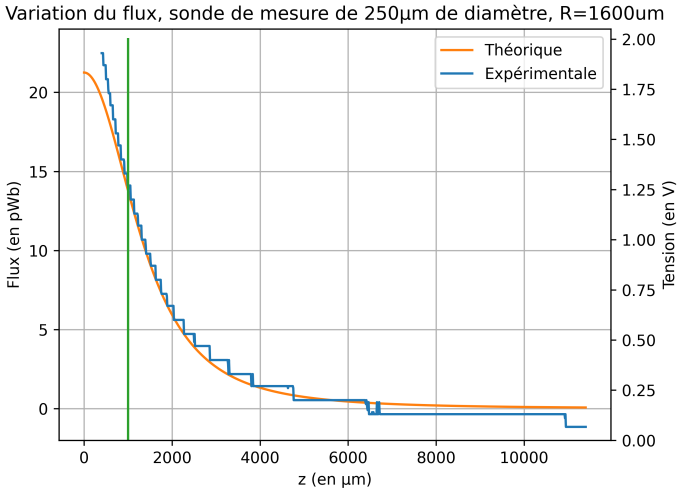



FIGURE 2.15 – Décroissance du flux, en fonction de la hauteur z pour différents rayons de spires, théorique et expérimentale.

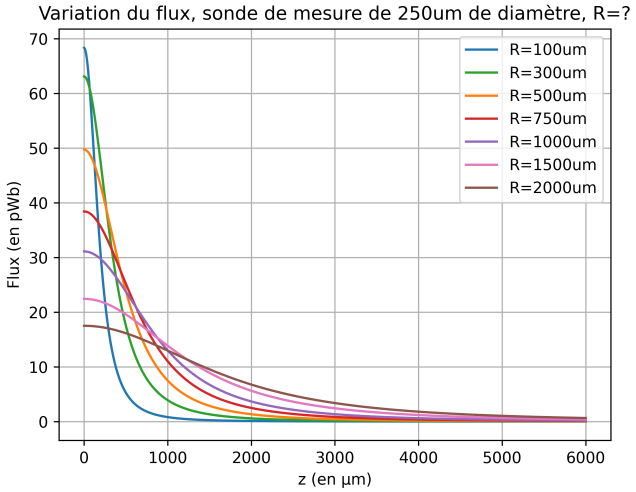



FIGURE 2.16 – Décroissance du flux, en fonction de la hauteur z pour différents rayons de spires.

Le flux reçu par la sonde d'écoute pour une sonde d'émission d'un rayon de 200 µm est le plus intense. En revanche, sa décroissance en fonction de la distance est la plus grande. Le flux mesuré à une distance z=0 mm est de 68 pWb tandis qu'il n'est que de 1 pWb à une distance z=1 mm. L'atténuation est ainsi de 99 %. La mesure de flux pour une sonde ayant un rayon de 2000 µm est de 18 pWb au contact de la sonde de réception, ce qui est plus faible que pour les autres sondes. En revanche, l'atténuation est moins importante ; nous mesurons 13 pWb pour une distance de 1 mm. Nous remarquons que les sondes avec de petits diamètres décroissent plus rapidement qu'avec de gros diamètres, cependant les valeurs de flux reçu sont aussi plus importantes. Ces courbes mettent en évidence que pour une distance z fixée, nous maximisons le flux en utilisant la sonde adaptée.

### Relation entre la distance z et le diamètre de la spire

La relation entre la distance z et le diamètre de la spire maximisant le flux reçu est illustrée sur la figure 2.17.

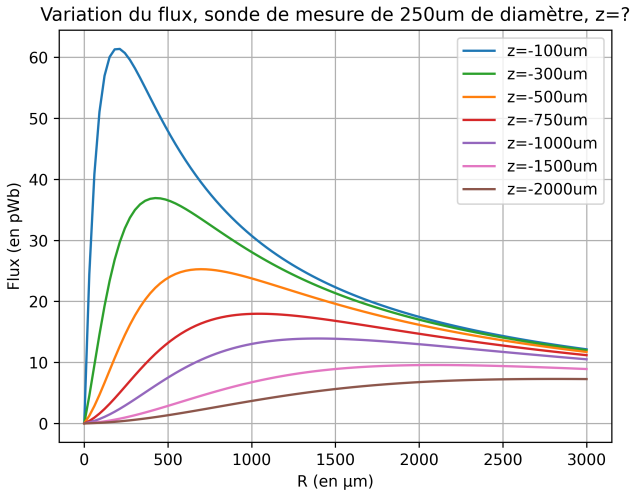



FIGURE 2.17 – Décroissance du flux, en fonction du rayon des spires pour différentes hauteurs z.

Nous observons que le flux est plus intense lorsque la distance z est faible. Le flux maximal à une distance de 100 µm est obtenu pour un rayon de 150 µm et vaut 60 pWb, tandis qu'à une distance de 750 µm il est obtenu pour un rayon de 1050 µm et vaut 18 pWb. Le rapport entre la distance et le rayon de la spire pour le pic de flux reçu semble égal à 1.4, ce qui signifie que pour une distance z fixée, la sonde la plus adaptée a un rayon de z*1.4.

Nous vérifions cela d'un point de vue théorique. Pour ce faire, nous choisissons une sonde « infiniment petite » afin de mesurer le flux reçu. La figure 2.18 illustre la hauteur z correspondant au maximum du flux reçu pour différents rayons.

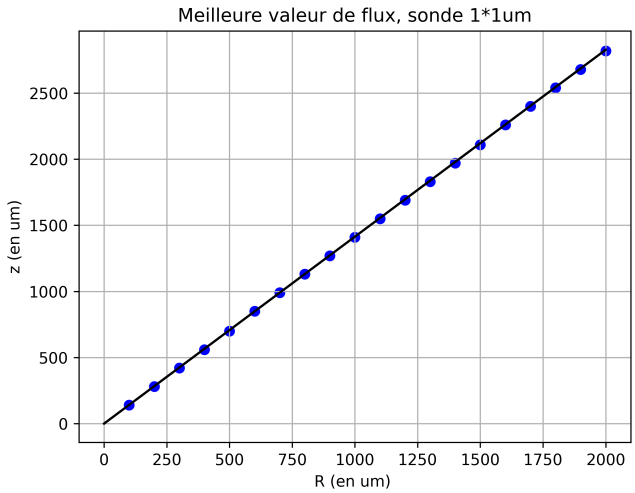



FIGURE 2.18 – Hauteur correspondant à la plus forte valeur de flux pour différents rayons.

Les points sont sur la droite linéaire de pente $\sqrt{2}$. Une préconisation est donc de limiter la distance z dans un premier temps. Dans le cas d'une sonde composée d'une seule spire et d'une distance z fixe, il convient donc d'optimiser le rayon de la sonde afin que $R = \sqrt{2}z$.

La vérification expérimentale est difficilement réalisable, car la répétabilité du positionnement en z n'est pas bonne, ainsi une erreur de positionnement de quelques dizaines de micromètres fausse le résultat.

### 2.2.2 Géométrie pour une sonde multispire de rayon constant

La majorité des sondes présentées dans l'état de l'art sont constituées de plusieurs spires. L'étude de la géométrie est donc poursuivie pour des sondes multispire. Nous cherchons à mettre en équation le champ $\vec{B}$ émis par plusieurs spires superposées et distantes de $\delta$, en un point M dans l'espace. La figure 2.19 est une représentation de la sonde en coupe ZX.

Chacune des spires est traversée par un courant $I_x$. Nous considérons que les intensités parcourant chaque spire sont égales, ainsi $I_0 = .. = I_{N-1} = I$. En utilisant la loi de Biot et Savart, nous obtenons :

$$B_x(x,y,z) = \sum_{n=0}^{N-1} \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{Rz\cos\theta d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + (z + n * \delta)^2]^{\frac{3}{2}}}$$

$$B_y(x,y,z) = \sum_{n=0}^{N-1} \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{Rz\sin\theta d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + (z + n * \delta)^2]^{\frac{3}{2}}}$$

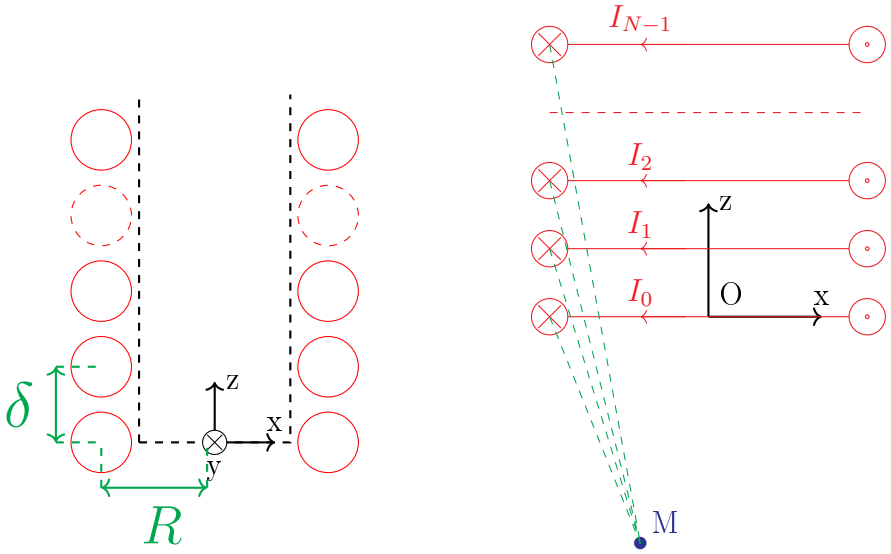



FIGURE 2.19 – Schéma d'une sonde composée de N spires.

$$B_z(x,y,z) = \sum_{n=0}^{N-1} \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R^2 - Ry\sin\theta - Rx\cos\theta)d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + (z + n * \delta)^2]^{\frac{3}{2}}}$$

Nous étudierons uniquement la composante en z du champ $\vec{B}$, car nous cherchons à quantifier le flux à travers la surface S située dans le plan XY :

$$\boxed{B_z(x,y,z) = \sum_{n=0}^{N-1} \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R^2 - Ry\sin\theta - Rx\cos\theta)d\theta}{[(x - R\cos\theta)^2 + (y - R\sin\theta)^2 + (z + n * \delta)^2]^{\frac{3}{2}}}} \quad (2.6)$$

**Influence du nombre de spires et du pas interspire sur la propagation du champ**

Étant donné qu'il existe une symétrie cylindrique par rapport à l'axe Z, la représentation du champ $\vec{B}$ en 3 dimensions est projetée sur le plan XZ. Nous définissons un courant I constant à 1 A, un rayon de spire de 850 µm et une distance verticale entre les spires $\delta = 200$ µm.

Nous constatons la création de trois zones, une positive entre les deux sections de fil et deux négatives à l'extérieur. Sur les deux figures, le champ $\vec{B}$ est maximal au centre des spires, mais il s'atténue en dehors de cette zone. En revanche, sur la figure avec 5 spires, l'intensité du champ est plus importante. Nous cherchons à déterminer l'influence du nombre de spires sur l'étalement et l'intensité du champ $\vec{B}$ produit. La figure 2.21 montre ces effets pour un rayon des spires R=1600 µm et une distance z=500 µm, ainsi qu'une distance verticale entre des spires $\delta$ égale à 200 µm. Cela signifie que les fils de diamètre 200 µm sont jointifs.

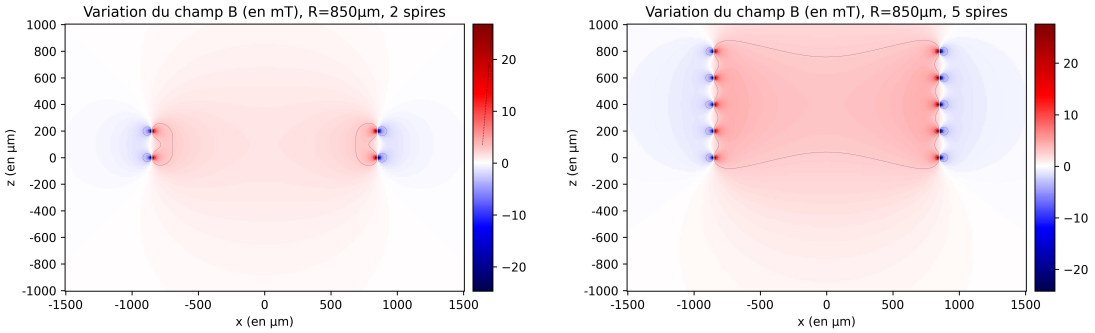



FIGURE 2.20 – Champ $\vec{B}$ engendré pour 2 et 5 spiresa, en fonction de x et de z pour une bobine de rayon R=850 µm.

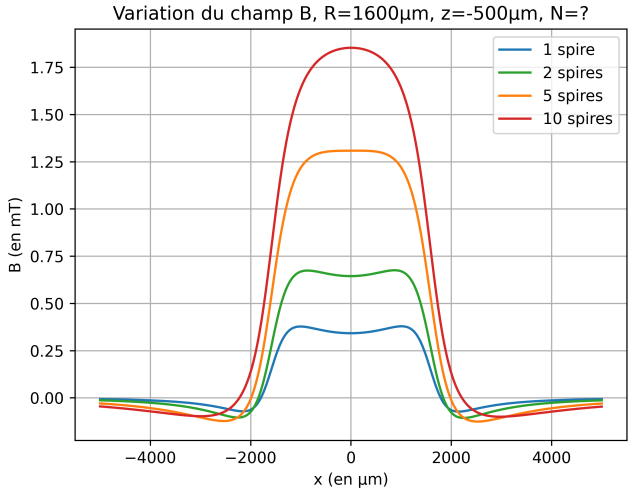



FIGURE 2.21 – Étalement du champ $\vec{B}$ pour différents nombres de spires.

L'augmentation du nombre de spires accroît les valeurs des champs produits, mais a peu d'influence sur la largeur d'effet des sondes. Le champ $\vec{B}$ mesuré en x=0 vaut 0.34 mT pour 1 spire, 0.65 mT pour 2 spires (1.9 fois plus), 1.6 mT pour 5 spires (4.7 fois plus qu'avec une seule spire) et 1.85 mT pour 10 spires (5.4 fois plus qu'avec une seule spire). Nous constatons donc que le champ $\vec{B}$ augmente avec le nombre de spires, mais que cette évolution n'est pas linéaire et elle s'atténue avec le nombre de spires. Dans la pratique, avec un générateur de tension non idéal, un nombre important de spires pourra augmenter la résistance de la sonde, ce qui entraînera une diminution de l'intensité I. Cependant, des mesures ont montré que cette atténuation était limitée pour des sondes allant jusqu'à 10 spires.

Nous mesurons le champ $\vec{B}$ engendré par une sonde de diamètre de ferrite 3 mm et de diamètre de fil 200 µm avec une sonde de diamètre 250 µm. Nous pouvons ainsi considérer qu'elle est ponctuelle par rapport au diamètre de la sonde d'injection caractérisée. La sonde d'injection est excitée par un signal impulsionnel de 8 V, avec un temps de montée de 5 ns et une durée d'impulsion de 10 ns, produit par un GBF Tektronix AFG3102. Afin de comparer les mesures expérimentales et les simulations, nous traçons sur la figure 2.22 l'étalement spatial pour une sonde de 5 spires à une distance z=600 µm avec un rayon R=1600 µm et une distance verticale interspire $\delta$=250 µm.

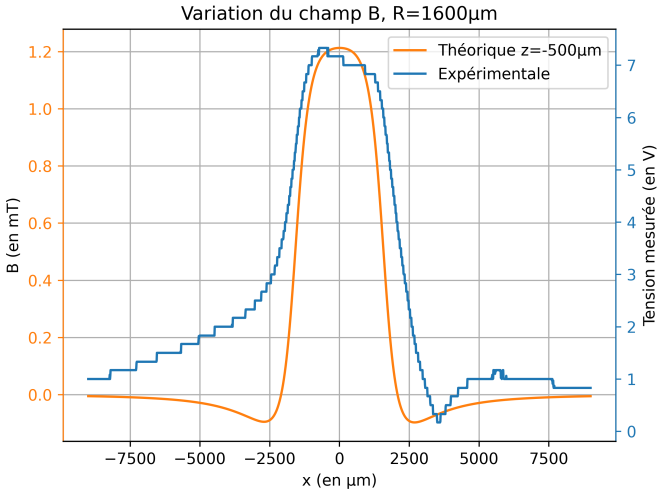



FIGURE 2.22 – Profil du champ $\vec{B}$ engendré en fonction de x, théorique et expérimentale (en supposant la sonde d'écoute quasi-ponctuelle).

Les valeurs du champ $\vec{B}$ simulé atteignent un maximum de 1.2 mT sur une largeur de 800 µm. Les valeurs de la tension mesurée atteignent un maximum de 7 V sur une largeur de 1600 µm. Les courbes théoriques et expérimentales sont assez similaires. Le profil du champ $\vec{B}$ expérimental est environ 30 % plus large que le théorique, ce qui peut être dû à un bobinage qui n'est pas au contact total de la ferrite. Il y a une légère perte de symétrie sur la courbe expérimentale, car le plan de la spire n'est

pas rigoureusement perpendiculaire à l'axe z. L'écart avec la théorie est relativement faible.

La figure 2.23 met en évidence l'effet de la variation du pas interspire, c'est-à-dire la variation de la distance verticale entre les spires $\delta$. Le rayon de la sonde est de 1600 µm et le nombre de spires varie entre 1 et 10.

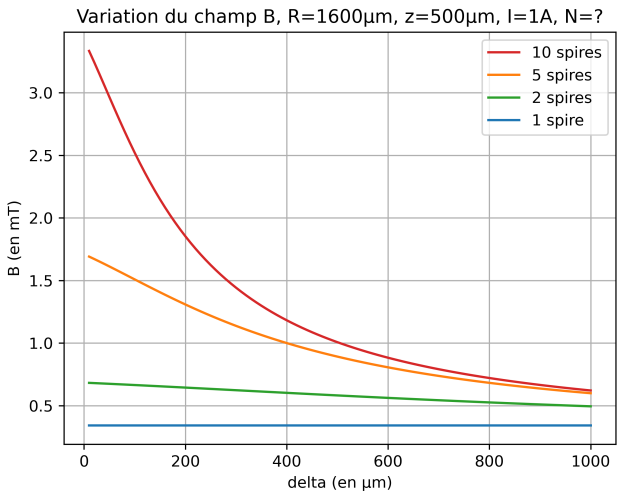



FIGURE 2.23 – Champ $\vec{B}$ engendré en fonction de la distance interspire verticale $\delta$ différents nombres de spires.

Pour un pas interspire vertical entre les spires $\delta$ égal à 100 µm, le champ $\vec{B}$ mesuré pour deux spires vaut 0.6 mT, 1.5 mT pour 5 spires et 2.5 mT pour 10 spires. Lorsque ce pas est égal à 200 µm, nous mesurons un champ $\vec{B}$ de 0.6 mT pour 2 spires, 1.3 mT pour 5 spires (13 % d'atténuation par rapport à $\delta$=100 µm) et 1.8 mT pour 10 spires (28 % d'atténuation). Par conséquent, le pas interspire a davantage d'incidence sur l'efficacité des sondes composées d'un nombre élevé de tours. Quel que soit le nombre spires, lorsque le pas interspire augmente, le champ $\vec{B}$ généré est plus faible. Cela montre que nous devons minimiser le pas interspire et donc réaliser des spires jointives. L'utilisation d'un fil verni avec un isolant est alors nécessaire.

Nous avons vu précédemment qu'un rapport de $\sqrt{2}$ entre le rayon et la distance avec la cible maximise le champ émis dans le cas d'une sonde avec une spire. Pour une sonde composée de 2 spires, les valeurs maximales de flux en fonction du pas interspire $\delta$ sont représentées sur la figure 2.24.

Nous observons qu'une augmentation du pas interspire $\delta$ impose de diminuer le rayon de la spire pour optimiser le champ reçu à une distance z. Si nous souhaitons réaliser une injection à une distance de 1 mm avec un fil de 200 µm de diamètre, nous pourrons utiliser une sonde avec 2 spires jointives d'un diamètre de 1000 µm ou 2 spires non jointives d'un diamètre de 400 µm ($\delta$=500 µm).

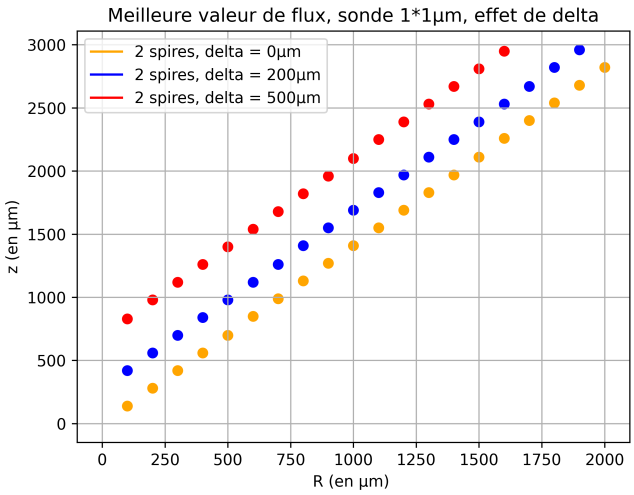



FIGURE 2.24 – Hauteur correspondant à la meilleure valeur de flux pour différentes valeurs de pas interspire $\delta$.

### 2.2.3 Géométrie pour une sonde multispire conique

Certaines sondes présentées dans l'état de l'art sont constituées de plusieurs spires arrangées non pas selon une forme cylindrique, mais plutôt en forme de cône comme illustré sur la figure 2.25. Le but est d'affiner le profil du champ $\vec{B}$ produit afin de gagner en résolution spatiale. Nous continuons donc l'étude de la géométrie avec des sondes multispire coniques. Nous cherchons à mettre en équation le champ $\vec{B}$ émis par plusieurs spires, superposées, distantes de $\delta$ et de rayons croissants $(R+\zeta)$ en un point M dans l'espace. La figure 2.25 est une représentation de la sonde en coupe ZX.

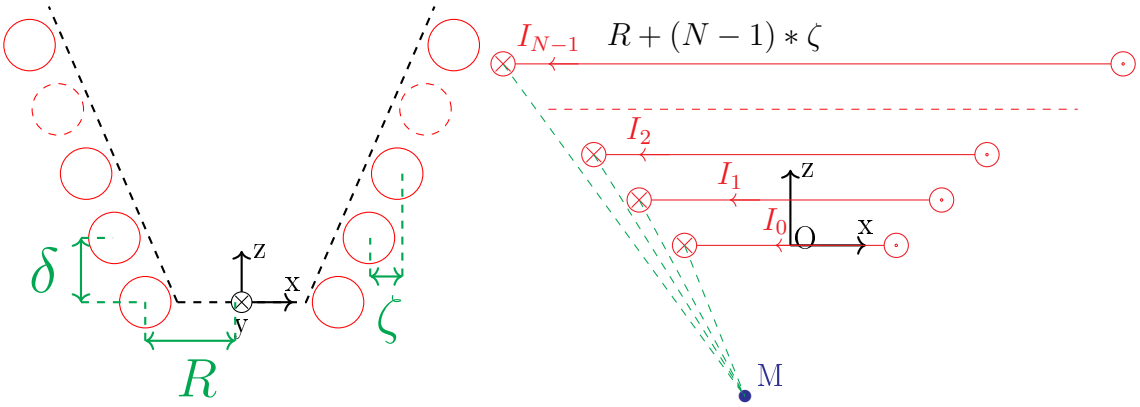



FIGURE 2.25 – Schéma d'une sonde et du champ magnétique autour de N spires coniques.

Chacune des spires est traversée par un courant $I_x$. Nous considérons que ces

intensités parcourant chaque spire sont égales, ainsi $I_0 = .. = I_{N-1} = I$. En utilisant la loi de Biot et Savart, nous avons :

$$B_x(x,y,z) = \sum_{n=0}^{N-1} \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R+n*\zeta)*z\cos\theta d\theta}{[(x-(R+n*\zeta)*\cos\theta)^2+(y-(R+n*\zeta)*\sin\theta)^2+(z+n*\delta)^2]^{\frac{3}{2}}}$$

$$B_y(x,y,z) = \sum_{n=0}^{N-1} \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{(R+n*\zeta)*z\sin\theta d\theta}{[(x-(R+n*\zeta)*\cos\theta)^2+(y-(R+n*\zeta)*\sin\theta)^2+(z+n*\delta)^2]^{\frac{3}{2}}}$$

$$B_z(x,y,z) = \sum_{n=0}^{N-1} \frac{\mu_0 I}{4\pi} \int_0^{2\pi} \frac{((R+n*\zeta)^2-(R+n*\zeta)*y\sin\theta-(R+n*\zeta)*x\cos\theta)d\theta}{[(x-(R+n*\zeta)*\cos\theta)^2+(y-(R+n*\zeta)*\sin\theta)^2+(z+n*\delta)^2]^{\frac{3}{2}}}$$

Nous étudierons uniquement la composante en z du champ $\vec{B}$, car nous cherchons à quantifier le flux à travers la surface S située dans le plan XY :

$$\boxed{B_z(x,y,z) = \frac{\mu_0 I}{4\pi} \sum_{n=0}^{N-1} \int_0^{2\pi} \frac{((R+n*\zeta)^2-(R+n*\zeta)*y\sin\theta-(R+n*\zeta)*x\cos\theta)d\theta}{[(x-(R+n*\zeta)*\cos\theta)^2+(y-(R+n*\zeta)*\sin\theta)^2+(z+n*\delta)^2]^{\frac{3}{2}}}} \quad (2.7)$$

### Étalement spatial

La représentation du champ $\vec{B}$ en 3 dimensions est projetée sur le plan XZ étant donné qu'il existe une symétrie cylindrique par rapport à l'axe z. Dans les deux exemples de la figure 2.26, le rayon de la spire à la pointe est de R=1600 µm, et $\delta = \zeta = 140$ µm.

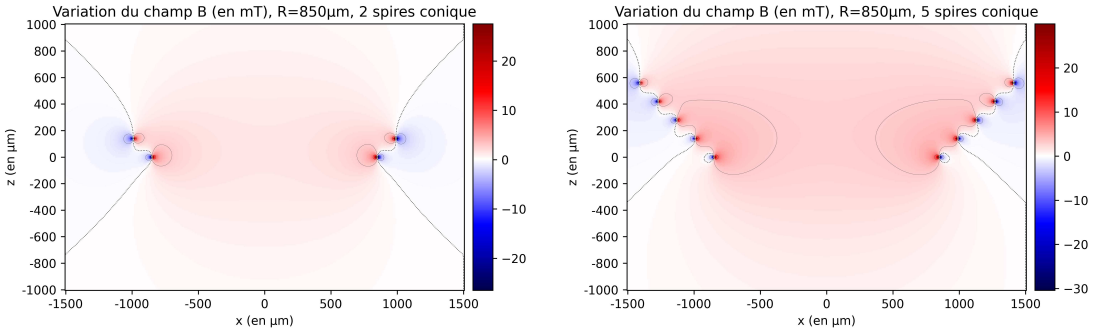



FIGURE 2.26 – Évolution du champ $\vec{B}$ pour 2 et 5 spires coniques, en fonction de x pour R=850 µm.

Nous constatons la présence de trois zones, une positive entre les deux sections de fil et deux négatives à l'extérieur. Le champ $\vec{B}$ produit par la sonde avec 5 spires

est plus intense que celui avec la sonde de 2 spires. Nous cherchons à déterminer l'influence de la géométrie conique sur l'étalement et l'intensité du champ $\vec{B}$ engendré. La figure 2.27 illustre l'effet des sondes coniques comparé aux sondes cylindriques pour un diamètre R=1600 µm. Pour les sondes coniques, le diamètre R=1600 µm est celui de la spire ayant le plus grand diamètre et positionnée au-dessus des autres. Les spires sont jointives et constituées d'un fil de diamètre 200 µm. Ainsi, dans le cas des sondes cylindriques $\delta$=200 µm, tandis que dans le cas des sondes coniques $\delta = \zeta = \frac{200\,\mu m}{\sqrt{2}} \approx 140$ µm. Les simulations sont effectuées pour un nombre de spires variant de 1 à 10.

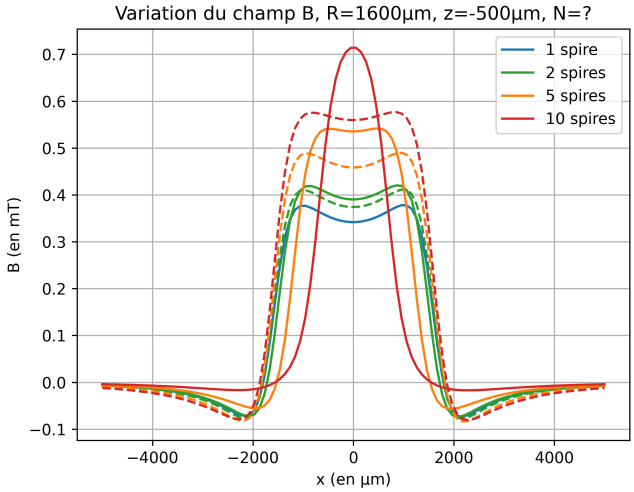



FIGURE 2.27 – Profil du champ $\vec{B}$ engendré en fonction de x pour des géométries cylindriques (traits pleins) et coniques (traits pointillés) avec 1, 2, 5 et 10 spires.

Les traits pleins représentent les spires coniques et en pointillés les cylindriques. Le champ $\vec{B}$ obtenu en x=0 avec 10 spires de géométrie conique est de 0.7 mT tandis qu'avec la géométrie cylindrique, il est de 0.55 mT, soit une atténuation de 21 %. Dans l'ensemble, les intensités des champs $\vec{B}$ obtenues avec des sondes coniques sont toujours supérieures à celles des sondes cylindriques. La largeur du profil du champ $\vec{B}$ est également réduite avec l'utilisation des sondes coniques plutôt que cylindriques. Pour les sondes composées de 10 spires, les largeurs des profils des champs $\vec{B}$ générés à 50 % du maximum d'intensité sont de 1400 µm avec la sonde conique et 3200 µm avec la sonde cylindrique. Dans l'ensemble, les largeurs obtenues pour les profils de champs $\vec{B}$ des sondes coniques sont toujours inférieures à celles des sondes cylindriques. Cela montre qu'une sonde avec une géométrie conique engendre un champ plus concentré et plus intense qu'une géométrie cylindrique.

L'évolution du champ $\vec{B}$ engendré par une sonde conique de 5 spires est représentée sur la figure 2.28 et comparée avec des sondes cylindriques de diamètre 1200 µm et 1600 µm correspondant aux diamètres minimaux et maximaux des spires de la sonde conique.

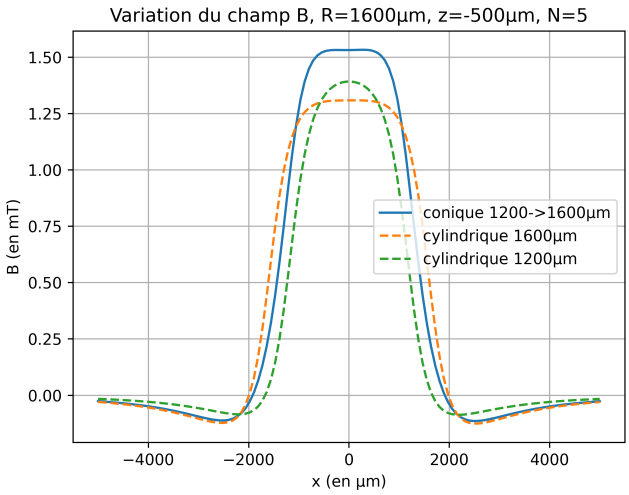



FIGURE 2.28 – Profil du champ $\vec{B}$ engendré en fonction de x pour des géométries cylindriques et coniques avec 5 spires.

Nous constatons que le champ $\vec{B}$ est plus intense avec la sonde conique qu'avec les deux autres types de sondes. L'augmentation est d'environ 9 % pour la sonde cylindrique de rayon 1200 µm et de 15 % pour celle de rayon 1600 µm. La localité spatiale de la sonde est améliorée par rapport à la sonde du diamètre 1600 µm. Cela montre que tailler en pointe l'extrémité d'une ferrite localise mieux le flux et augmente l'intensité de champ $\vec{B}$ produit.

L'étude de la variation de l'angle au sommet pour une sonde 5 spires et un rayon de 1600 µm est représentée sur la figure 2.29.

Pour une valeur de distance interspire horizontale $\zeta$=200 µm, le champ $\vec{B}$ mesuré vaut 0.47 mT, et diminue lorsque la distance $\zeta$ varie. Il existe donc une distance $\zeta$ optimale générant un champ $\vec{B}$ avec la plus forte intensité. Par conséquent, il existe un angle au sommet optimal pour maximiser le champ engendré. Pour les fils en cuivre que nous utilisons, il est proche de $\delta$ = 200 µm et $\zeta$ = 200 µm. Nous constatons que la largeur du champ $\vec{B}$ rayonné diminue lorsque l'angle au sommet augmente.

Pour une sonde composée de 2 spires, les valeurs maximales de flux en fonction de la distance $\zeta$ sont représentées sur la figure 2.30.

Nous observons qu'une augmentation du pas interspire $\zeta$ impose d'augmenter le rayon de la spire pour optimiser le champ reçu à une distance z. Si nous souhaitons réaliser une injection à une distance de 1 mm avec un fil de 200 µm de diamètre, il est préférable d'utiliser une sonde conique avec 2 spires espacées de $\delta$=200 µm et $\zeta$=50 µm avec un diamètre de 1200 µm ou une sonde conique avec 2 spires espacées de $\delta$=200 µm et $\zeta$=350 µm avec un diamètre de 2000 µm. La relation entre le rayon R, le nombre de spires n, $\delta$, $\zeta$ et la distance z optimisant le flux n'a pas été déterminée.

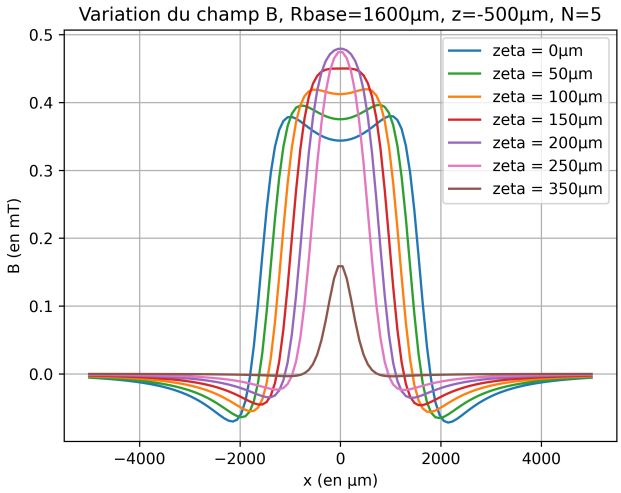



FIGURE 2.29 – Profil du champ $\vec{B}$ engendré en fonction de x pour différentes distances interspire horizontales $\zeta$.

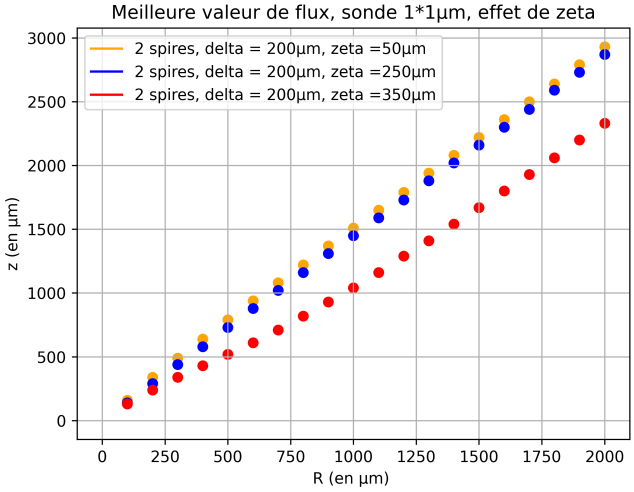



FIGURE 2.30 – Hauteur correspondant à la meilleure valeur de flux pour différentes valeurs de $\zeta$.

Cependant, la simulation permet d'aboutir par itération aux valeurs optimales.

### 2.2.4 Effet d'une ferrite sur le champ magnétique engendré par une sonde d'injection électromagnétique

Les simulations présentées dans les précédentes parties ont été effectuées avec un bobinage dans l'air. Dans la pratique, le bobinage est réalisé autour d'une ferrite afin d'augmenter l'intensité des champs produits. Cette section s'intéresse à l'effet de l'ajout d'un matériau ferromagnétique. Or, la présence de ferrite est l'un des paramètres limitant la réduction des diamètres des sondes. Ici, nous montrons que la présence d'une ferrite est nécessaire à la génération d'un champ magnétique suffisamment intense pour engendrer des fautes dans un circuit cible, et nous quantifions son apport.

Dans le cas d'absence de ferrite, c'est-à-dire dans l'air, la perméabilité magnétique vaut $\mu = \mu_0 * \mu_r(air) = \mu_0$. Avec les ferrites, la perméabilité magnétique vaut $\mu = \mu_0 * \mu_R(ferrite)$, elle est donc supérieure à $\mu_0$. Nous cherchons à en obtenir une estimation. Nous admettons que les lignes de champ sont canalisées le long des ferrites et qu'elles sortent orthogonalement à l'interface, comme représenté sur la figure 2.31.

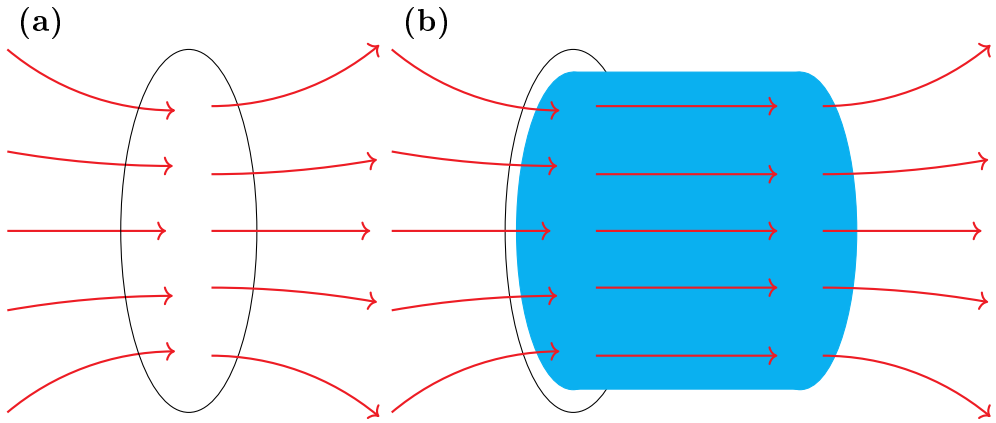



FIGURE 2.31 – Schéma du champ magnétique autour d'une spire circulaire sans **(a)** et avec une ferrite **(b)**.

Les lignes de champ à travers la ferrite se propagent orthogonalement à la spire, tandis que dans l'air, seules les lignes de champ situées au centre de la spire se propagent orthogonalement au plan de la spire.

Afin de quantifier l'apport de l'utilisation d'un noyau de ferrite, nous mesurons de façon expérimentale l'effet de la ferrite sur des sondes de diamètre 3 mm et composées d'une seule spire, avec et sans ferrite, comme représenté sur la figure 2.32.

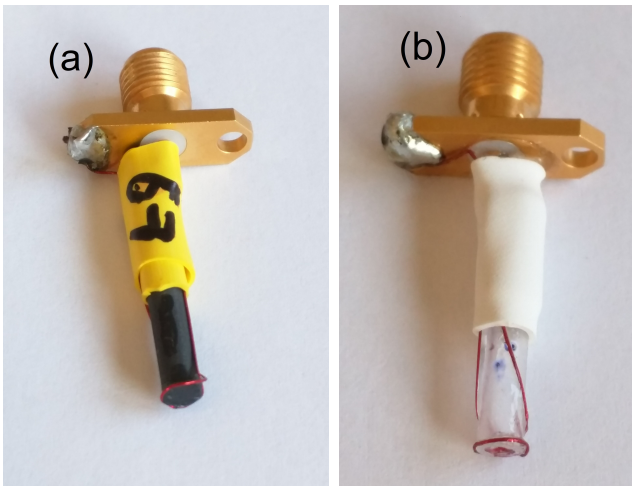



FIGURE 2.32 – Sondes d'injection constituées d'une spire unique d'un diamètre 3 mm avec et sans ferrite.

Cette étude commence par l'utilisation d'une sonde d'écoute comme cible pour caractériser la sonde. La sonde d'écoute est ensuite remplacée par un FPGA.

### Caractérisation de l'effet de la ferrite sur une sonde fine

Nous mesurons le champ $\vec{B}$ engendré par une sonde de diamètre 3 mm, avec et sans ferrite, à l'aide d'une sonde de diamètre 250 µm. Ainsi, nous pouvons considérer qu'elle est ponctuelle par rapport au diamètre de la sonde d'injection caractérisée. La sonde d'injection est excitée par un signal impulsionnel de 8 V, avec un temps de montée de 5 ns et une durée d'impulsion de 10 ns, produit par un GBF Tektronix AFG3102, comme représenté sur la figure 2.33.a.

Sur la figure 2.33.b, les courbes sont normalisées, ce qui permet de constater qu'elles ont des localités spatiales similaires. Les valeurs mesurées pour la sonde sans ferrite sont inférieures d'un facteur 2.2 à celles avec ferrite, signifiant que la perméabilité relative $\mu_R$ en régime d'excitation impulsionnel est de l'ordre de 2.2. Nous en concluons que l'ajout d'une ferrite augmente l'intensité du champ $\vec{B}$ d'un gain supérieur à 2 et que l'ajout d'une ferrite ne modifie pas l'étalement spatial des sondes.

L'évolution du champ magnétique dans la ferrite est représentée sur la figure 2.34. Le champ $\vec{B}$ est mesuré dans un premier cas lorsqu'une impulsion est émise aux bornes d'une spire située à l'extrémité de la ferrite. Dans un second cas, une spire est placée à 20 mm de la première spire, à l'autre extrémité de la ferrite, comme représenté sur la figure 2.34.a. L'excitation est une impulsion similaire à celle utilisée précédemment, mais la sonde a un diamètre de ferrite 1.5 mm avec 5 spires.

Les tensions mesurées en x=0 µm pour des spires à l'extrémité de la ferrite où à son centre avoisinent toutes les deux 0.95 V. Lorsque la spire est au contact de la sonde, le champ est très localisé. En revanche, il est davantage étalé lorsque la spire

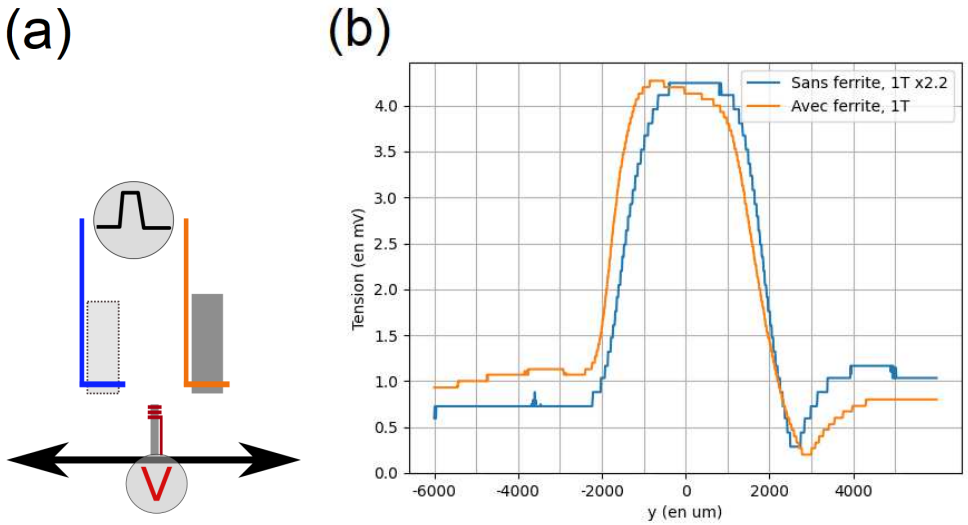



FIGURE 2.33 – **a.** Montage mesurant le champ $\vec{B}$ produit par une sonde **b.** Évolution du champ $\vec{B}$, en fonction de x, avec et sans ferrite.

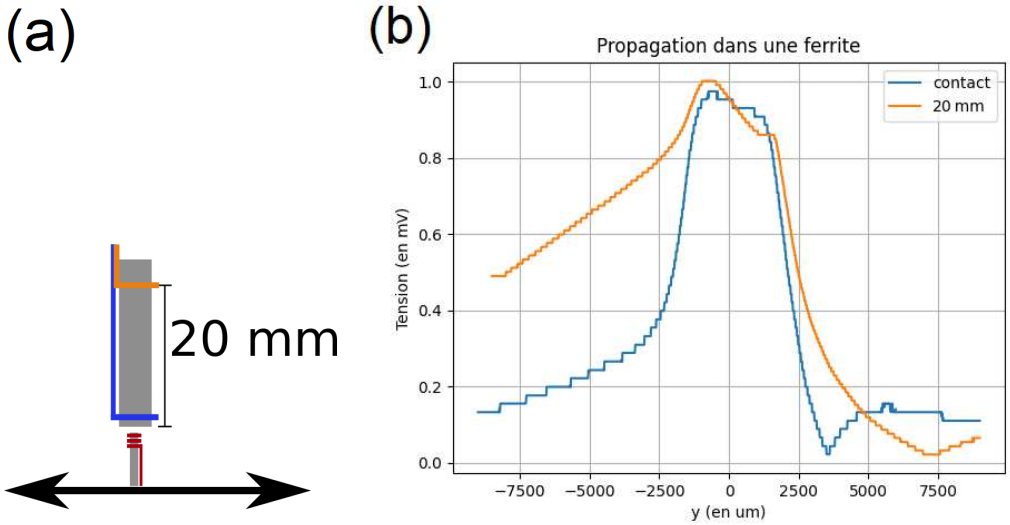



FIGURE 2.34 – Schéma du montage **(a)** pour mesurer le guidage du champ dans une ferrite **(b)**.

est éloignée. Ce phénomène est cependant sans impact sur l'intensité du champ, le champ est donc guidé dans la ferrite de façon uniforme.

Les mesures de champ ont été effectuées grâce à une sonde fine de diamètre 250 µm. Des mesures sont également effectuées sur un FPGA pour analyser l'effet de la présence d'une tige de ferrite sur une cible réelle.

### Caractérisation de l'effet de la ferrite sur une cible de type FPGA

Nous souhaitons caractériser les sondes avec la cible FPGA, décrite au paragraphe 2.1.1. Cette cible sert à mesurer les variations internes de tension du FPGA en comptant le nombre d'oscillations de l'oscillateur en anneau dans un temps donné. La valeur est d'autant plus élevée que la perturbation est importante. Nous utilisons deux types de sondes avec et sans ferrites. Les premières sont de diamètres 790 µm composées d'un fil de diamètre 40 µm autour d'un support (ferrite ou plastique) de diamètre 750 µm. Les secondes sont de diamètres 1700 µm composées d'un fil de diamètre 200 µm autour d'un support (ferrite ou plastique) de diamètre 1500 µm. Les effets de la perturbation sur la cible FPGA avec et sans ferrite sont présentés sur la figure 2.35. L'excitation est une impulsion de tension réalisée depuis un générateur Avtech d'amplitude 150 V pour le premier cas et 70 V pour le second. La durée du front montant (entre 20 et 80 % du signal) est de 2.5 ns et celle de l'impulsion de 10 ns.

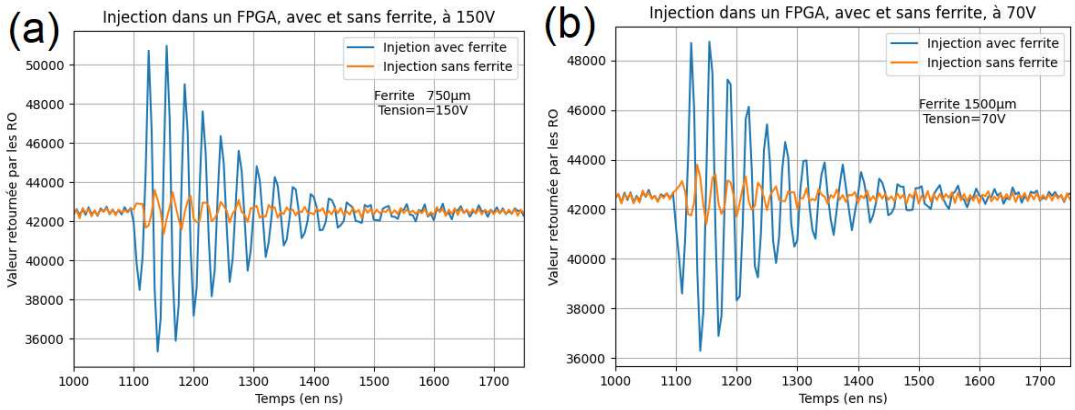



FIGURE 2.35 – Comparaison de l'injection électromagnétique avec et sans ferrites pour des diamètres de support (ferrite ou plastique) 750 µm **(a)** et 1500 µm **(b)**.

Lors de l'injection avec une ferrite de 1500 µm, la variation mesurée par l'oscillateur en anneau est de 8500 tandis qu'elle n'est que de 1000 sans ferrite. Cela signifie que la tension interne du FPGA est plus perturbée avec la présence d'une ferrite. En revanche, le capteur ne mesure pas les perturbations linéairement sur toute sa plage de mesure. Cela est vérifié en analysant la figure 2.36, représentant la variation retournée par le capteur en fonction de la tension de perturbation. Les mesures sont réalisées avec deux sondes de diamètres 1700 µm composées d'une tige de ferrite et de plastique.

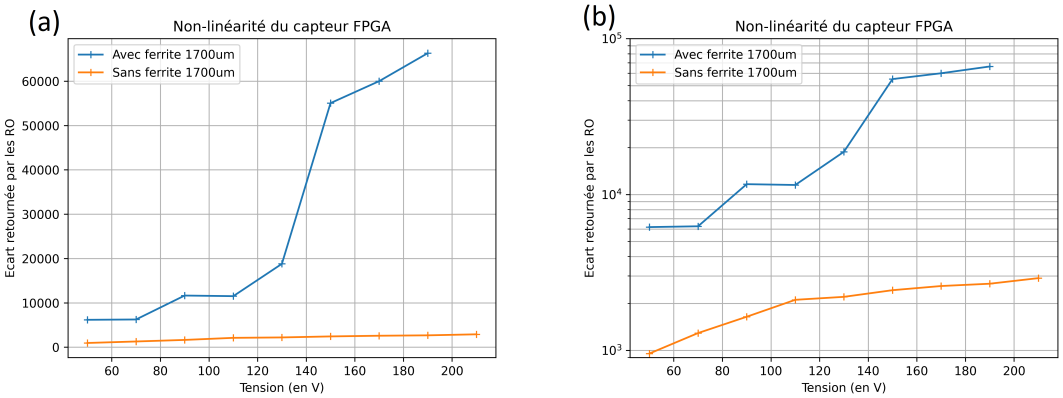



FIGURE 2.36 – Évolution des variations mesurées par le capteur embarqué dans le FPGA en fonction de la tension d'excitation, pour une sonde de diamètre 1700 µm, avec une représentation linéaire **(a)** et semi-logarithmique **(b)**.

Les variations obtenues avec la sonde composée d'une ferrite n'évoluent pas de façon linéaire avec l'augmentation de la tension de perturbation. Pour une tension de 90 V, on mesure une variation de 12000, en revanche pour une tension deux fois plus importante, soit 180 V, l'écart est proche de 63000. On observe donc un facteur 5 sur l'écart alors que théoriquement il est attendu uniquement un facteur 2. De même, on constate sur la figure 2.36.b que l'évolution n'est pas linéaire pour des perturbations faibles. On mesure une variation proche de 2000 pour une tension 100 V sans ferrite, et elle reste inférieure à 3000 pour une tension de 200 V. L'évolution de la perturbation étant linéaire avec la tension de perturbation, la non-linéairité provient de la variation de la tension interne du FPGA ou du capteur lui-même.

Nous en concluons toutefois que la présence d'une ferrite augmente le flux magnétique transitoire et la puissance transmise à la cible. Après avoir étudié l'intensité des champs $\vec{B}$ produits par les sondes, nous cherchons à caractériser et à améliorer leurs étalements spatiaux.

### 2.2.5 Validation expérimentale des résultats théoriques

L'utilisation de la loi de Biot et Savart a mis en évidence l'effet des différents paramètres de façon théorique. Nous cherchons désormais à les valider d'un point de vue expérimental.

#### Cartographie 3D du champ $\vec{B}$ engendré par une sonde d'injection

Des cartographies ont été réalisées pour chacune des sondes en injectant un signal impulsionnel de 8V avec un temps de montée de 5 ns produit par un GBF Tektronix AFG3102 dans la sonde à caractériser. Les mesures sont effectuées par une sonde de diamètre 250 µm, telle que présentée sur la figure 2.37.

Une sonde conique composée de 10 spires autour d'une ferrite d'un diamètre de base 1500 µm est cartographiée selon une coupe XY et XZ. Les coupes sont

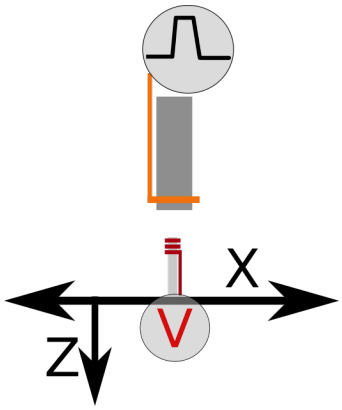



FIGURE 2.37 – Schéma de la manipulation réalisant la cartographie XZ.

présentées sur la figure 2.38. Elles représentent la tension maximale mesurée par la sonde d'écoute, en Volts.

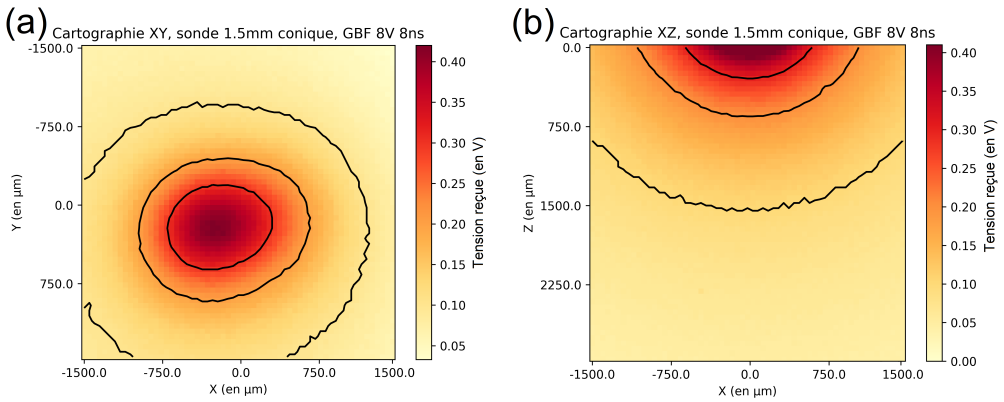



FIGURE 2.38 – Cartographie d'une sonde de diamètre 1500 µm, dite de référence, au moyen d'une sonde de diamètre 250 µm : XY **(a)** et XZ **(b)**.

Les courbes équipotentielles, tracées en noir, montrent l'évolution de la tension en fonction de la position. Elles sont placées pour des tensions induites de 100 mV, 200 mV et 300 mV. L'amplitude maximale de la tension induite dans la sonde de mesure est de 400 mV. Sur la première figure (2.38.a), nous observons que la zone d'influence en coordonnées XY est circulaire et qu'il existe un axe de symétrie, ce qui limitera l'étude à 2 dimensions. Ces résultats sont valables pour l'ensemble des sondes réalisées. Sur la seconde figure (2.38.b), nous observons que la tension induite dans la sonde décroît rapidement, et qu'elle n'est que de 100 mV à une distance de 1500 µm.

### Dispersion du champ $\vec{B}$ engendré par une sonde d'injection

L'étude des champs $\vec{B}$ créés par des sondes définit leurs zones d'influences. Les profils du champ $\vec{B}$ engendrés par différentes sondes d'injection ont été tracés sur

la figure 2.39.a. Ils ont été obtenus en injectant un signal impulsionnel de 10V, avec un temps de montée de 5 ns et une durée de 8 ns, produit par un GBF Tektronix AFG3102 dans la sonde à caractériser, et en notant la valeur maximale de la tension mesurée à travers une sonde de diamètre 250 µm. Les types de ferrite utilisés sont présentés dans la légende, et correpondent à ceux détaillés dans le paragraphe 2.4.1. Les profils des champs $\vec{B}$ normalisés sont présentés sur la figure 2.39.b. La normalisation est obtenue en divisant les tensions mesurées par la tension maximale obtenue pour chaque sonde.

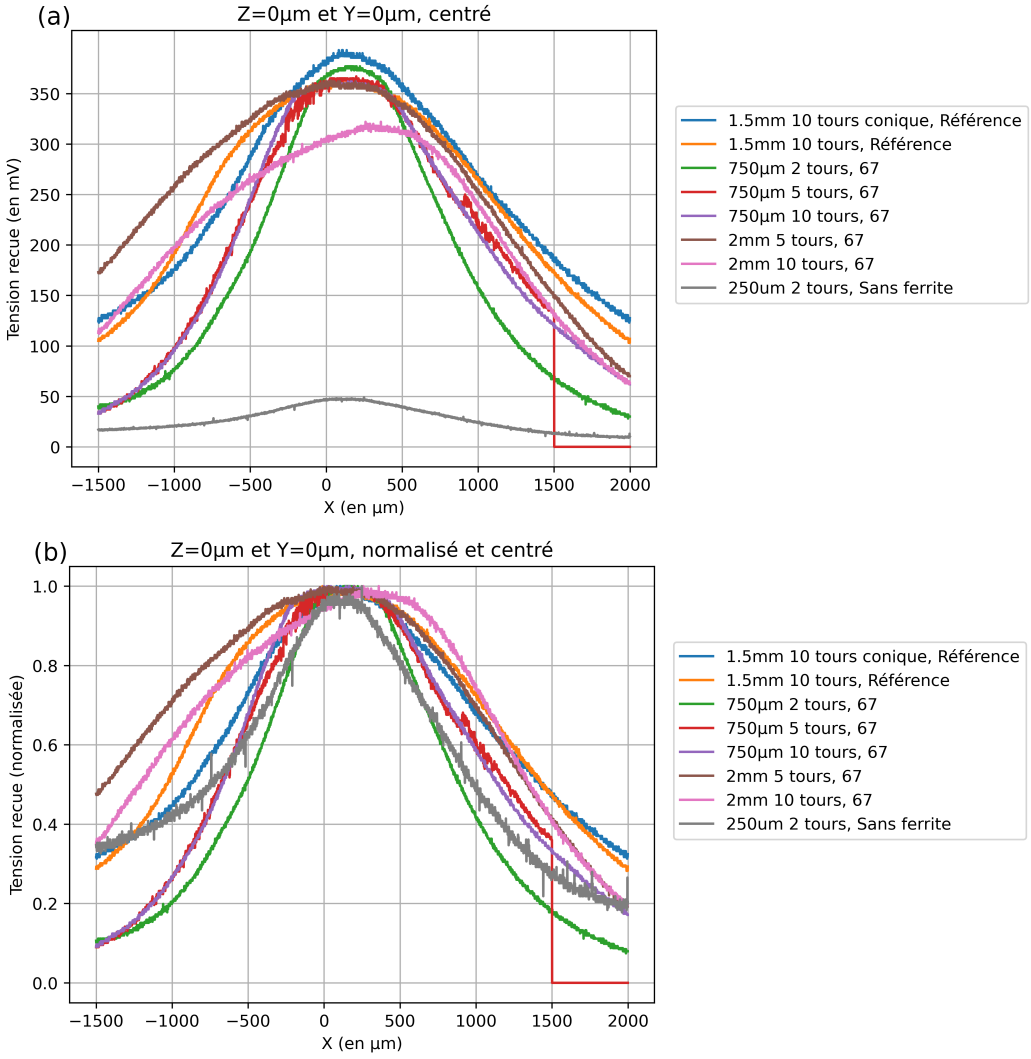



FIGURE 2.39 – Comparaison de la dispersion du champ $\vec{B}$ engendré par des sondes d'injection (centré **(a)** et normalisé **(b)**).

Les profils du champ magnétique créé avec des ferrites de diamètre 750 µm, mais avec un nombre de spires différent, sont assez similaires. Pour les sondes de ferrites de diamètre 2 mm, l'augmentation du nombre de spires accroît les valeurs des tensions mesurées. Ces légères différences de tensions mesurées sont difficilement in-

terprétables, car une variation de quelques micromètres selon l'axe Z a une influence importante sur les tensions mesurées. En revanche, nous constatons que l'augmentation du nombre de spires n'a qu'un effet minime sur la largeur du flux de la sonde.

La sonde de référence et la sonde cylindrique sont toutes les deux conçues à partir de ferrites de diamètre 1500 µm, dont l'extrémité a été taillée en pointe pour la sonde de référence. Nous constatons une diminution de la zone d'effet entre la sonde cylindrique et celle conique. Ainsi, cela confirme expérimentalement l'intérêt de concevoir des sondes coniques afin d'améliorer leur localité spatiale.

Pour la sonde de diamètre 250 µm, l'absence de ferrite et un diamètre petit provoquent une importante diminution du signal mesuré. La tension induite dans la sonde de mesure est environ 7 fois inférieure à l'ensemble des autres sondes caractérisées, passant de 350 mV à 50 mV.

Afin de comparer la localité des sondes, nous mesurons la largeur de la zone d'effet correspondant à un signal à 50 % de la valeur maximale. Ces valeurs d'étalement spatial à 50 % sont représentées au tableau 2.1.

| Diamètre de la ferrite et nombre de spires | Étalement spatial à 50 % |
|---|---|
| 2 mm, 5 spires | 2725 µm |
| 2 mm, 10 spires | 2500 µm |
| 1.5 mm, 10 spires = Cylindrique | 2475 µm |
| 1.5 mm, 10 spires, conique = Référence | 2250 µm |
| 750 µm, 5 spires | 1850 µm |
| 750 µm, 10 spires | 1775 µm |
| 250 µm, 2 spires | 1700 µm |
| 750 µm, 2 spires | 1350 µm |

TABLEAU 2.1 – Dispersion à 50 % en fonction des sondes.

La résolution spatiale d'une sonde de diamètre de ferrite 2000 µm est comprise entre 2500 et 2750 µm tandis qu'elle diminue entre 2250 µm et 2475 µm pour des sondes de diamètre de ferrite 1500 µm. Lorsque le diamètre de ferrite est de 750 µm, l'étalement est compris entre 1350 et 1850 µm. Nous constatons qu'une diminution du diamètre améliore la localité.

Nous en concluons que le meilleur compromis entre la puissance et la localité est obtenu avec de petits diamètres et une ferrite conique. Le nombre de spires n'influe pas significativement sur la localité. La sonde sans ferrite de diamètre 250 µm est caractérisée par une puissance transmise très inférieure à celle obtenue avec ferrite.

## 2.3 Étude dynamique des sondes et du générateur

La première partie de l'étude des sondes a été réalisée en régime statique afin d'étudier l'effet de leur géométrie. Il convient ensuite d'analyser le comportement des sondes en régime dynamique, puis la modélisation électrique d'une sonde et des générateurs d'impulsions de tension.

### 2.3.1 Étude dynamique théorique

Dans les parties précédentes, nous avons conclu que le champ magnétique selon l'axe Oz s'exprimait :
$B_z(x,y,z) = \frac{\mu_0 I}{4\pi} \sum_{n=0}^{N-1} \int_0^{2\pi} \frac{((R+n*\zeta)^2-(R+n*\zeta)*y\sin\theta-(R+n*\zeta)*x\cos\theta)d\theta}{[(x-(R+n*\zeta)*\cos\theta)^2+(y-(R+n*\zeta)*\sin\theta)^2+(z+n*\delta)^2]^{\frac{3}{2}}}$ pour les sondes coniques.
Cependant la loi de Biot et Savart ne s'applique qu'en régime continu ou approximation des régimes quasi-stationnaires (ARQS). Ainsi, nous devons vérifier que nous respectons ces conditions dans le cas de l'étude dynamique. Les phénomènes électromagnétiques dans les sondes se propagent à une vitesse de $\frac{2}{3}c$, soit un chemin parcouru de l'ordre de 20 cm en 1 ns. Les déphasages sont alors négligeables compte tenu des petites dimensions des sondes. Nos cas d'études permettent ainsi d'appliquer la loi de Biot et Savart.

La force électromotrice engendrée dans le circuit cible vaut :

$$e = -\frac{d\Phi}{dt} \tag{2.8}$$

où $\Phi$ est le flux magnétique à travers le circuit cible, d'une surface S, et vaut

$$\Phi = \int_S \frac{\mu_0 I}{4\pi} \sum_{n=0}^{N-1} \int_0^{2\pi} \frac{((R+n*\zeta)^2-(R+n*\zeta)*y\sin\theta-(R+n*\zeta)*x\cos\theta)d\theta}{[(x-(R+n*\zeta)*\cos\theta)^2+(y-(R+n*\zeta)*\sin\theta)^2+(z+n*\delta)^2]^{\frac{3}{2}}} dS. \tag{2.9}$$

Nous avons aussi aussi

$$e = -L\frac{di}{dt} \tag{2.10}$$

avec L l'inductance du circuit, exprimée en Henry (H), et i le courant dans le circuit.

En identifiant membre à membre, nous avons :

$$\boxed{L = \frac{\mu_0}{4\pi} \sum_{n=0}^{N-1} \int_S \int_0^{2\pi} \frac{((R+n*\zeta)^2-(R+n*\zeta)*y\sin\theta-(R+n*\zeta)*x\cos\theta)d\theta}{[(x-(R+n*\zeta)*\cos\theta)^2+(y-(R+n*\zeta)*\sin\theta)^2+(z+n*\delta)^2]^{\frac{3}{2}}} dS}. \tag{2.11}$$

Dans le cas d'une spire, nous obtenons :

$$\boxed{L = \int_S \frac{\mu_0}{4\pi} \int_0^{2\pi} \frac{(R^2 - R * y \sin\theta - R * x \cos\theta) d\theta}{[(x - R * \cos\theta)^2 + (y - R * \sin\theta)^2 + z^2]^{\frac{3}{2}}} dS}. \quad (2.12)$$

Nous émettons l'hypothèse que la spire d'émission et la spire d'écoute sont confondues (c'est-à-dire de taille identique et avec z=0).
Pour une sonde composée d'une spire avec un rayon de 1700 µm (1500 µm de diamètre de ferrite et 200 µm de diamètre de fil), nous obtenons une inductance de 33 nH. En sachant que l'utilisation d'une ferrite augmentait l'inductance d'un facteur $\mu_r \approx 2.2$, ainsi cette même sonde composée d'une ferrite aurait une inductance de 73 nH. Pour une sonde composée de 5 spires avec ferrite, nous obtenons une inductance de 425 nH.

Nous pouvons comparer ces valeurs avec celles obtenues par les formules empiriques de Wheeler [106] :

$$\boxed{L = \frac{0.8 * N^2 * \mu_R * R^2}{6 * R + 9 * l + 6 * Rfil}}. \quad (2.13)$$

L'inductance L est en microhenry, les mesures en pouces et $l$ représente la longueur de la bobine.

Pour 5 spires, un rayon de 1500 µm, un fil de 100 µm de rayon et un coefficient de perméabilité relative $\mu_r$ de 2.2, nous obtenons une inductance de 204 nH.

Les valeurs d'inductances pour différentes caractéristiques de sondes sont détaillées dans le tableau 2.2.

| Diamètre de sonde et de fil | Formule d'inductance 2.11, en considérant $\mu_r = 2.2$ | Formule de Wheeler [106], en considérant $\mu_r = 2.2$ |
|---|---|---|
| 3000 µm, 200 µm, 5 spires | 425 nH | 204 nH |
| 2000 µm, 200 µm, 5 spires | 290 nH | 111 nH |
| 1500 µm, 200 µm, 5 spires | 223 nH | 72 nH |
| 1000 µm, 200 µm, 5 spires | 154 nH | 43 nH |
| 750 µm, 40 µm, 5 spires | 77 nH | 45 nH |

TABLEAU 2.2 – Inductance calculée pour différentes sondes.

Les inductances calculées à l'aide de la formule 2.11 sont environ deux fois plus élevées que celles calculées avec la formule de Wheeler. La formule 2.11 prend en compte la géométrie de la sonde et permet facilement d'avoir les valeurs d'inductance en fonction du pas interspire vertical et horizontal. Bien que ces valeurs soient différentes, elles donnent une approximation de la valeur d'inductance. La comparaison de ces valeurs théoriques avec des mesures est effectuée dans le paragraphe 2.4.4.

Nous cherchons à maximiser la force électromotrice engendrée dans le circuit cible. Pour cela, nous maximisons la variation de flux $\frac{d\Phi}{dt}$. Or $\Phi = L_{mutuelle} * I_{generateur}$. Nous devons donc chercher à maximiser la variation $\frac{dI_{generateur}}{dt}$. Nous pouvons approximer le circuit injecteur/sonde par un générateur de tension, une résistance de charge et une inductance en série. La variation du courant vaut donc $I(t) = I_0(1 - \exp(-\frac{t}{\tau}))$ avec $\tau = \frac{L}{R_{charge}}$.

Ainsi,

$$\frac{dI}{dt} = \frac{dI_0(1 - \exp(-\frac{t}{\tau}))}{dt} = I_0 \frac{1}{\tau} \exp(-\frac{t}{\tau}) = \frac{U_0}{L} \exp(-\frac{t}{\tau}). \tag{2.14}$$

Nous en concluons qu'une augmentation de tension $U_0$ accroît la perturbation au niveau du circuit cible. Une diminution de l'inductance $L$ augmenterait aussi la perturbation. En revanche, si nous souhaitons conserver un temps de montée relativement court, 2 ns dans le cas de l'Avtech, l'inductance doit être inférieure à 100 nH. Ces résultats sont valables pour un $\mu_r = 2.2$. Si les ferrites sont différentes, les valeurs d'inductances sont différentes.

### 2.3.2 Étude dynamique des sondes

Nous cherchons à modéliser le circuit électrique équivalent à la sonde d'attaque. Pour cela, nous réalisons deux modifications : le générateur d'impulsions Avtech est remplacé par un GBF, et la sonde par une inductance de valeur fixe. Dans la pratique, la sonde est équivalente à une inductance en série avec une résistance dont les valeurs dépendent de la fréquence d'excitation. Si les modèles électriques du générateur d'impulsions de tension et de la sonde sont cohérents avec la pratique, nous pouvons simuler des modifications pour maximiser la variation de courant $\frac{di}{dt}$.

#### Inductance connectée à un GBF

La première expérience est réalisée à partir d'une sonde composée d'une inductance CMS, équivalente à une sonde de 1.2 µH en série avec une résistance de 150 Ω, connectée à la sortie d'un GBF Tektronix AFG3102. Le GBF produit un signal impulsionnel d'amplitude 7 V avec un temps de montée de 5 ns, de plateau de 30 ns et de descente de 5 ns. La figure 2.40 présente la sonde et les mesures obtenues via un oscilloscope.

La tension mesurée aux bornes du GBF est représentée en bleu, celle aux bornes de la résistance en orange et la différence entre les deux tensions en vert. La courbe verte est donc le signal aux bornes de la sonde. Nous constatons lors du front montant de l'impulsion que la tension au sein de la sonde est positive et d'une amplitude maximale de 10 V. Ensuite, durant le front descendant de l'impulsion, la tension au sein de la sonde est négative et d'une amplitude de -11 V.

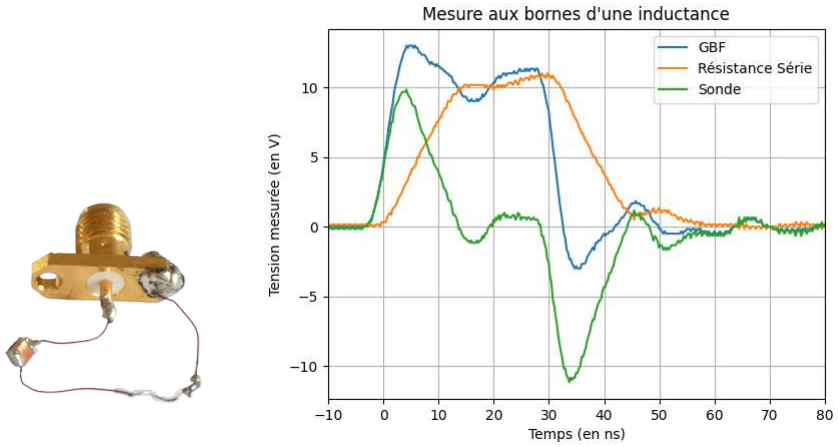



FIGURE 2.40 – Évolution des tensions dans un circuit composé d'une inductance CMS, lors d'un signal impulsionnel produit par un GBF.

Le circuit a été saisi sur le logiciel de conception de schémas électroniques : Kicad. Le schéma électrique est donné sur la figure 2.41.

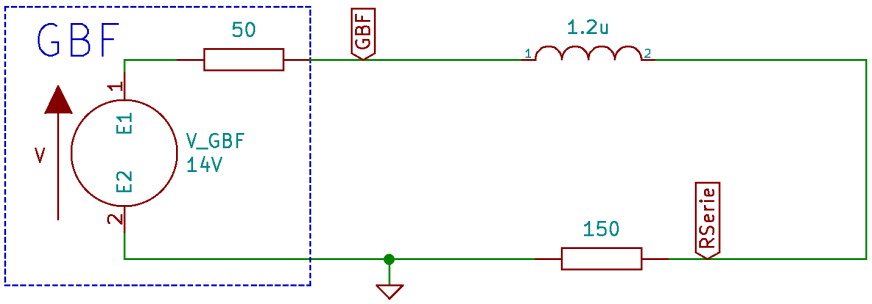



FIGURE 2.41 – Schéma électrique d'un GBF couplé à une inductance.

La tension aux bornes de la source de tension ($E$) est de 14 V, alors que la tension de consigne du générateur est de 7 V. La tension de sortie du générateur ($U_{sortie}$) est donnée pour charge $R_{charge}$ de 50 Ω, d'où $E + 50 * i = U_{sortie} = R_{charge} * i_{charge}$. D'après la loi des nœuds, nous avons $i = -i_{charge}$. Ainsi, la force électromotrice vaut $E = (R_{charge} + 50) * i_{charge} = 2 * R_{charge} * i_{charge} = 2 * U_{sortie}$. Le fonctionnement du circuit électrique est simulé en utilisant le moteur de simulation SPICE : ngspice. Le circuit électrique est séparé en composants élémentaires modélisés par un ensemble d'équations à l'aide des lois de Kirchhoff. Cela permet d'obtenir une visualisation des courbes des signaux analogiques en tous points d'un circuit électrique. La figure 2.42 est le résultat de la simulation SPICE.

La tension aux bornes du GBF est représentée en bleu, celle aux bornes de la résistance en orange et celle aux bornes de l'inductance en vert. De façon similaire à

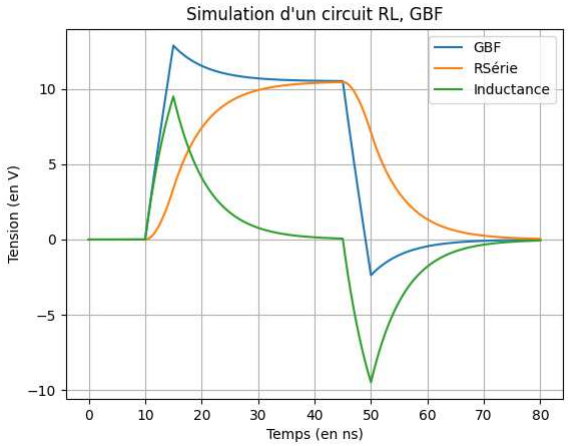



FIGURE 2.42 – Simulation des tensions dans un circuit composé d'une inductance CMS, lors d'un signal impulsionnel produit par un GBF.

la figure 2.40, nous constatons que la tension dans l'inductance est positive durant le front montant de l'impulsion et négative durant le front descendant. Nous observons des réponses aux bornes de l'inductance relativement similaires entre le signal simulé et expérimental. Afin de l'améliorer, il est possible de prendre en compte une capacité parasite de 5 pF entre les fils de la bobine. La résistance du circuit de 0.5 Ω est aussi considérée, comme présenté sur la figure 2.43.

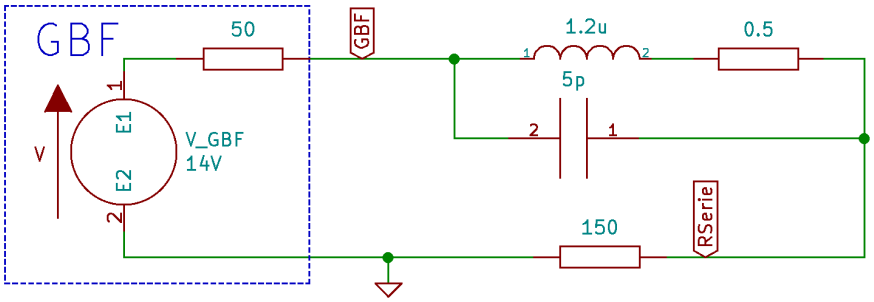



FIGURE 2.43 – Amélioration du schéma électrique d'un GBF couplé à une inductance.

Ces résultats sont comparés avec ceux obtenus expérimentalement sur la figure 2.44.

Les variations de tensions entre les mesures expérimentales et théoriques sont inférieures à 500 mV. Nous estimons que le modèle théorique est conforme aux résultats expérimentaux. Ainsi, nous remplaçons dans la suite la sonde, composée d'une inductance CMS, par une sonde d'injection.

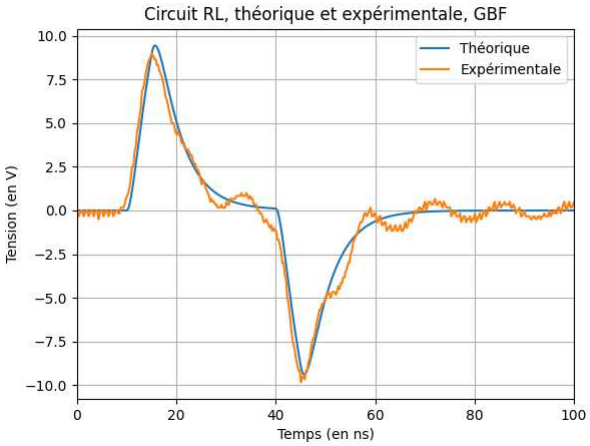



FIGURE 2.44 – Évolution des tensions dans un circuit RL lors d'un signal impulsionnel produit par un GBF, théoriquement et expérimentalement.

### Sonde d'injection électromagnétique connectée à un GBF

La modélisation SPICE de la partie précédente est réutilisée afin de tracer la variation de tension aux bornes de la sonde. Le résultat est comparé à celui obtenu expérimentalement sur la figure 2.45. Une sonde de diamètre de ferrite 1500 µm et composée de 5 spires est utilisée.

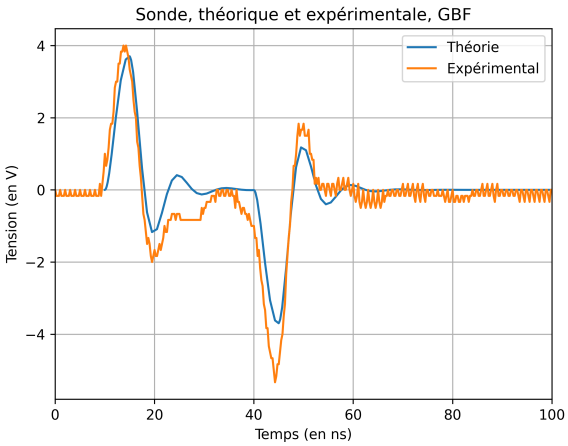



FIGURE 2.45 – Évolution des tensions dans une sonde d'injection lors d'un signal impulsionnel produit par un GBF, théoriquement et expérimentalement.

La tension mesurée aux bornes de la sonde augmente jusqu'à 4 V puis diminue jusqu'à -5.25 V. La tension simulée suit les mêmes variations mais atteint son maximum à 3.7 V et son minimum à -3.7 V. L'évolution des deux tensions reste similaire, nous considérons donc le modèle équivalent de la sonde comme satisfaisant. Il se compose d'une inductance de 200 nH en série avec une résistance de 0.1 Ω et en

parallèle avec une capacité de 10 pF.

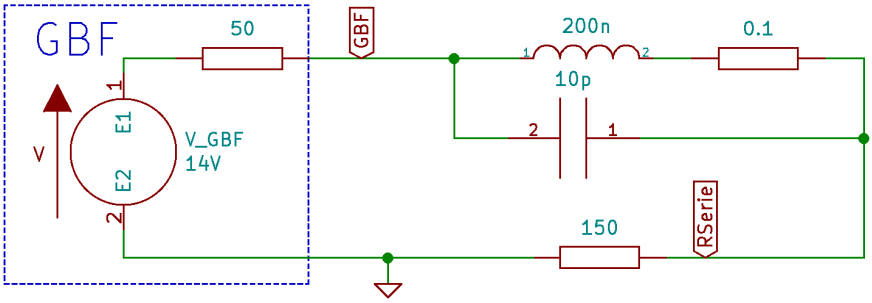



FIGURE 2.46 – Schéma électrique d'un GBF couplé à une sonde.

Le circuit équivalent de la sonde de ferrite de diamètre 1500 µm et composée de 5 spires est représenté sur la figure 2.46. Nous disposons donc du circuit électrique équivalent pour le GBF, le circuit composé d'une inductance cms et la sonde d'injection.

### 2.3.3 Étude dynamique du générateur de marque Avtech avec une sonde

La partie précédente a permis d'obtenir un modèle électrique d'un GBF. Cependant, les injections de fautes sont réalisées avec un générateur d'impulsions de tension de marque Avtech. Afin d'obtenir son modèle électrique, nous comparons les résultats de simulation et expérimentaux. Nous nous plaçons dans un cas simple avec une sonde composée d'une inductance fixe, puis dans un cas réel avec une sonde d'injection.

#### Inductance connectée à un générateur d'impulsions de tension de marque Avtech

Nous utilisons le circuit composé d'une inductance et d'une résistance en série de la partie précédente, en utilisant cette fois un générateur d'impulsions de tension de marque Avtech pour générer le signal d'excitation. Ce type de générateur est souvent utilisé dans l'état de l'art de l'injection électromagnétique pour fournir le signal d'excitation. Le schéma électrique du circuit composé de l'inductance produisait une simulation correcte à la partie précédente, donc elle est réutilisée. Nous réglons les caractéristiques du signal impulsionnel aux valeurs de l'Avtech, c'est-à-dire une impulsion d'amplitude 40 V et d'une durée de 10 ns avec un front montant et descendant d'une durée de 2.5 ns. Les résultats de la simulation sont présentés sur la figure 2.47.

La tension théorique aux bornes de la sonde est représentée en bleu, celle mesurée expérimentalement en orange et le signal de consigne en vert. Nous constatons

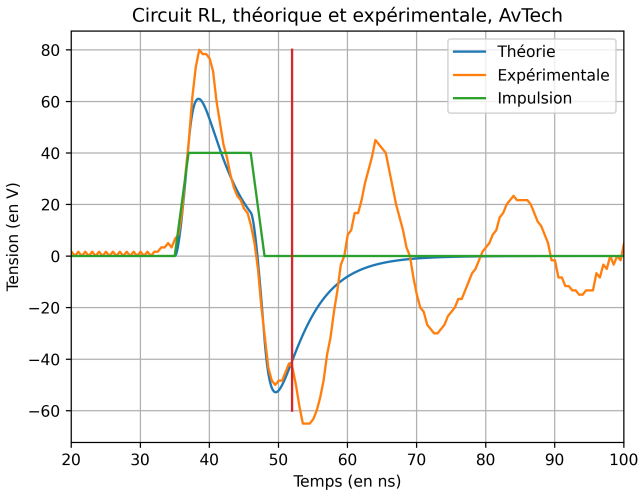



FIGURE 2.47 – Évolution des tensions dans un circuit RL lors d'un signal impulsionnel produit par un Avtech, théoriquement et expérimentalement.

que la tension maximale mesurée aux bornes de la sonde est de 80 V, tandis qu'elle est de 60 V en simulation pour une tension de consigne de 40 V. Nous remarquons aussi qu'à partir de 52 ns, marqué par un trait rouge sur la figure 2.47, la tension mesurée observe une discontinuité (un changement de son sens de variation puis des oscillations amorties). En revanche, la tension simulée ne subit pas de changement et remonte à 0 V.

La simulation ne correspond pas à la réalité car nous observons expérimentalement des variations supplémentaires de la tension. Or, les résultats de simulation de la sonde étaient corrects, nous émettons donc l'hypothèse que l'incohérence provient de la source : environ 2 ns après la fin de l'impulsion, nous remarquons une discontinuité de la variation de tension. Des manipulations ont montré que l'impédance du générateur n'était pas fixe à 50 Ω mais qu'elle est augmentée après l'impulsion. Nous décidons de modifier la simulation et d'inclure à cet instant une modification de l'impédance du générateur de 50 Ω à 1 000 Ω pour simuler une impédance plus élevée. Le schéma électrique est présenté sur la figure 2.48.

Le changement d'impédance est simulé en modifiant la résistance d'un interrupteur. Le logiciel de simulation ne permet pas de contrôler temporellement un interrupteur. Nous réalisons donc un montage composé d'un interrupteur contrôlé par tension elle même maîtrisée temporellement. Les résultats de cette simulation sont présentés sur la figure 2.49. La programmation de l'interrupteur est détaillée dans le texte de la figure 2.48.

La tension simulée n'est pas modifiée jusqu'à l'instant t=52 ns, et malgré un écart d'amplitude de 25 % avec le signal mesuré à la fin du front montant, la différence de tension est ensuite inférieure à 5 V. Nous constatons la présence d'une variation de tension similaire entre les signaux expérimentaux et théoriques au moment du

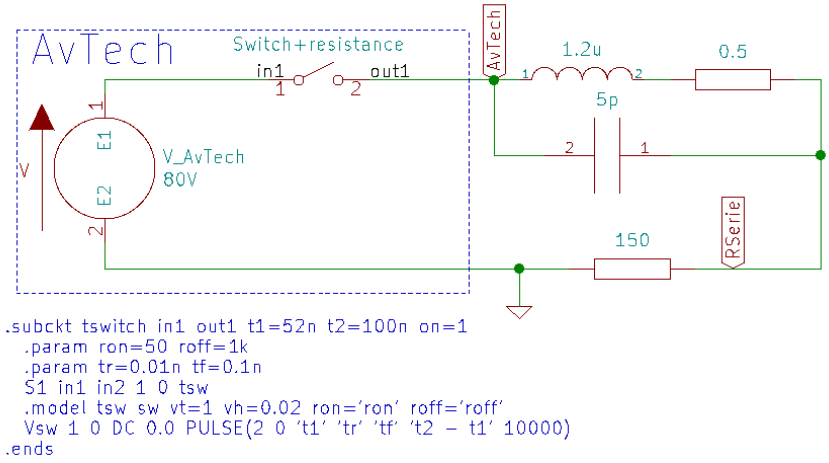



FIGURE 2.48 – Schéma du circuit électrique du générateur AvTech couplé à une inductance.

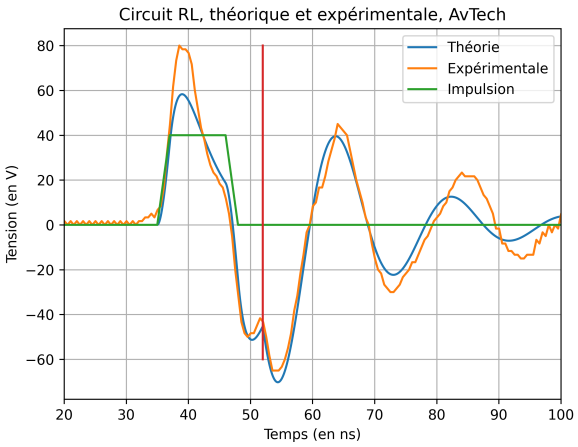



FIGURE 2.49 – Évolution des tensions dans un circuit RL lors d'un signal impulsionnel produit par un Avtech, théoriquement et expérimentalement.

changement d'impédance, matérialisée par un trait vertical rouge sur la figure. À l'instant t=50 ns, les deux tensions valent -50 V, puis augmentent à -45 V à t=52 ns et diminuent entre -65 et -70 V. Les oscillations amorties sur la tension simulée sont aussi similaires à celles de la tension mesurée.

Nous pourrons considérer la modélisation de l'Avtech présentée dans la figure 2.48 comme correcte. Ce générateur n'a pas une impédance de sortie fixe, mais commute entre une impédance de sortie de 50 Ω et une impédance de sortie haute impédance 2 ns après la fin de l'impulsion. Nous souhaitons désormais simuler le couple sonde/Avtech.

### Sonde connectée à un générateur d'impulsions de tension de marque Avtech

Le circuit électrique de la sonde présenté sur la figure 2.46 et celui du générateur d'impulsions de tension AvTech décrit sur la figure 2.48 sont utilisés pour simuler la combinaison d'un générateur Avtech et d'une sonde d'injection. Les tensions simulées aux bornes de la sonde sont représentées sur la figure 2.50. La durée de l'impulsion de tension a été augmentée de 2 ns lors de l'expérience, ainsi, la durée du signal impulsionnel engendré est agrandie de 2 ns.

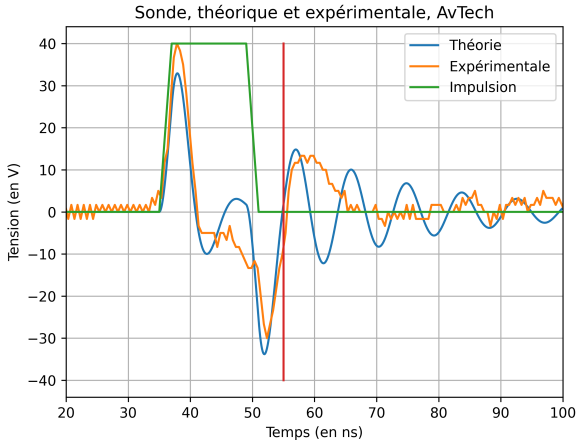



FIGURE 2.50 – Évolution des tensions aux bornes de la sonde d'injection lors d'un signal impulsionnel produit par un Avtech, théoriquement et expérimentalement.

À la fin du front montant de l'impulsion, la tension mesurée aux bornes de la sonde atteint sont maximum à 40 V et alors que la tension théorique vaut 32 V. Nous observons donc une tension simulée inférieure de 20 % à celle mesurée. La tension simulée présente 5 oscillations amorties, tandis qu'une seule est constatée expérimentalement. Cependant, les tensions observent des comportements similaires. Nous avons une simulation cohérente avec l'expérience pendant la durée de l'impulsion, que l'on peut donc utiliser pour étudier l'effet de la variation de différents paramètres tels que l'inductance et la résistance de la sonde. Cela permettra dans un premier

temps de mieux comprendre l'influence de ces paramètres puis d'en optimiser leurs valeurs pour maximiser l'intensité du champ $\vec{B}$ produit par la sonde.

Pour ce faire, la résistance série permettant de réaliser les mesures de tensions aux bornes des sondes est enlevée de la simulation. Ainsi, nous nous plaçons dans le cas des injections électromagnétiques et nous étudions le courant dans la sonde, comme représenté sur la figure 2.51.


FIGURE 2.51 – Simulation du courant à travers une sonde, lors d'un signal impulsionnel produit par un Avtech.

Nous constatons que le courant augmente durant l'impulsion et atteint son maximum à 1.5 A au début du front descendant de l'impulsion. Au moment du changement d'impédance de sortie du générateur, à t=55 ns, le courant diminue brusquement jusqu'à 50 mV. Nous observons des discontinuités dans la variation de courant lors des débuts et fins des fronts montants et descendants.

### 2.3.4 Simulation de la variation des paramètres du dispositif d'injection

Nous disposons d'un modèle électrique équivalent à celui d'une sonde et de son générateur d'impulsions de tension. Ainsi, nous pouvons l'utiliser pour simuler l'effet de différents paramètres tels que la valeur de l'inductance de charge, c'est-à-dire l'inductance de la sodne d'injection, ou la présence d'une résistance en série.

#### Effet de l'inductance de charge

Il a été démontré dans la partie théorique 2.3.1 qu'une diminution de l'inductance augmente l'intensité de la perturbation. Les valeurs des inductances des sondes utilisées variant de 50 nH à 500 nH, selon la méthode de calcul, nous traçons sur la figure 2.52 le courant pour ces valeurs.

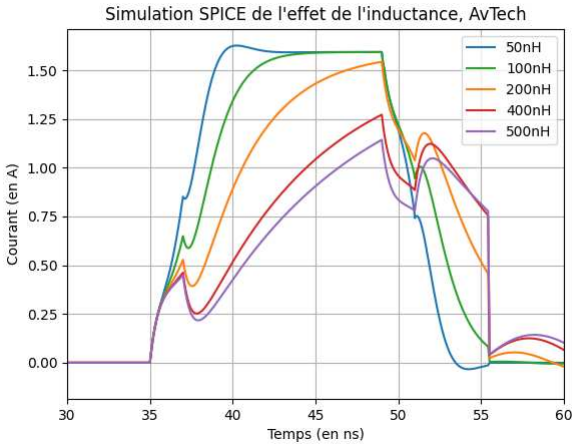



FIGURE 2.52 – Simulation de l'effet de l'inductance sur le courant à travers une sonde.

Pour une sonde d'inductance 50 nH, le courant varie de 0 à 1.6 A en 5 ns, tandis qu'il faut 8 ns pour une sonde d'inductance 100 nH. Le courant maximal pour une sonde de 200 nH est de 1.5 A, tandis qu'il est de 1.25 A pour une sonde de 400 nH et 1.15 A pour une de 500 nH. La diminution de l'inductance augmente le courant traversant la sonde. La durée nécessaire pour que le courant atteigne son maximum est plus importante lorsque l'inductance de la sonde augmente. Cela confirme qu'une valeur d'inductance comprise entre 50 et 100 nH provoque le plus intense et court pic de variation de courant. Ainsi, pour maximiser la tension induite dans la cible, les sondes doivent avoir des valeurs d'inductance de cet ordre de grandeur.

### Effet d'une résistance en série

Changer la longueur ou le diamètre du fil de la sonde modifie sa résistance. La réponse attendue lorsque la résistance de la sonde augmente est décrite sur la figure 2.53. Des valeurs de résistances série comprises entre 0 et 100 Ω ont été utilisées pour les simulations. L'inductance L vaut 200 nH durant la simulation.

Le courant maximal à travers une sonde est obtenu en l'absence de résistance série, le courant vaut alors 1.5 A. Lorsque la résistance augmente à 5, 10 puis 50 et 100 Ω, le courant maximal vaut respectivement 1.4 A, 1.3 A puis 800 mA et 500 mA. Pour des résistances supérieures à 50 Ω, nous observons que le courant atteint une limite maximale.

Lorsque nous ajoutons une résistance en série, la variation de courant diminue. Il faut donc limiter la résistance de la sonde. Cependant, entre 0 et 10 Ω, la chute n'est que de 5 %, ce paramètre n'a donc qu'une influence négligeable sur la variation de courant. Un des facteurs limitant la réduction du diamètre du fil est que cela augmente sa résistance. La résistance de fil pour la longueur d'une sonde avec un diamètre de 250 µm est de 30 mΩ. Elle est de 200 mΩ pour un fil de 100 µm et 1.38 Ω

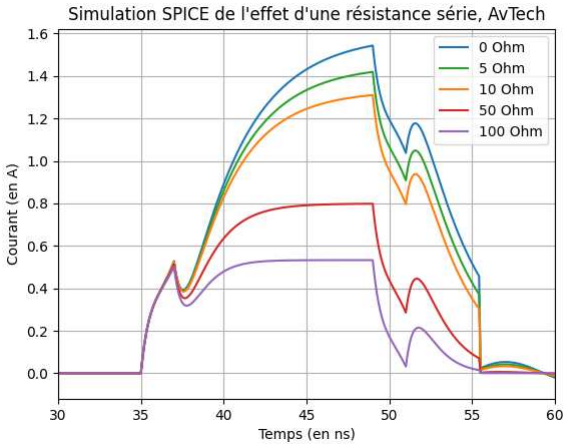



FIGURE 2.53 – Simulation de l'effet d'une résistance série sur le courant traversant une sonde.

pour un fil de diamètre 40 µm. La réduction du diamètre du fil, et donc du solénoïde, est une forme d'optimisation. Il faut cependant s'assurer que le fil ne s'échauffe pas excessivement. Ces effets sont étudiés expérimentalement en partie 2.6.3.

## 2.4 Étude des ferrites

Il a été démontré que la présence d'une ferrite apporte un gain de 2.2 sur l'intensité des champs magnétiques créés. Leur présence est donc appréciable pour perturber les circuits. Cette section s'intéresse aux avantages de la ferrite dans le dispositif d'injection électromagnétique. Elle sera donc étudiée pour déterminer les paramètres favorisant la création de perturbations dans le circuit cible.

### 2.4.1 Présentation des ferrites

Pour réaliser cette étude, 3 types de ferrite ont été étudiés :

- **Référence** Des ferrites initialement utilisées dans le laboratoire SAS et présentes dans plusieurs publications [67]
- **Fair-rite 67 [40]** Des ferrites de marque Fair-Rite contenant un alliage de Nickel et du Zinc, avec une perméabilité stable et peu de pertes jusqu'à 50 MHz.
- **Fair-rite 78 [41]** Des ferrites de marque Fair-Rite contenant un alliage de Manganèse et du Zinc, pour des applications en puissance jusqu'à 200 kHz

Nous cherchons à maximiser la perturbation engendrée par la sonde d'injection sur le circuit cible. Pour cela, nous étudions les pertes dans les ferrites. Une sonde peut être approximée par un modèle RL série : $\bar{Z} = R + jL\omega = j\omega(L - i\frac{R}{\omega}) = j\omega(K\frac{\mu_R}{l} - i\frac{R}{\omega})$ avec $K = \frac{Ll}{\mu_R}$ et l la longueur de la bobine en mètre.

La perméabilité complexe s'obtient en retranchant la résistance du bobinage de résistivité linéique $R_0$, d'où :

$\bar{\mu} = \mu_R - i(R - R_0)l = \mu' - i\mu''$, avec $\mu'$ qui représente la composante purement inductive et $\mu''$ les pertes.

Cela demande donc d'étudier la perméabilité relative complexe des matériaux afin de choisir le matériau avec le moins de pertes résistives.

### 2.4.2 Perméabilité complexe

Les courbes de perméabilités complexes fournies par le fabricant Fair-Rite sont présentées sur la figure 2.54. Les courbes sont obtenues en appliquant un régime sinusoïdal aux extrémités d'un fil bobiné sur un tore.

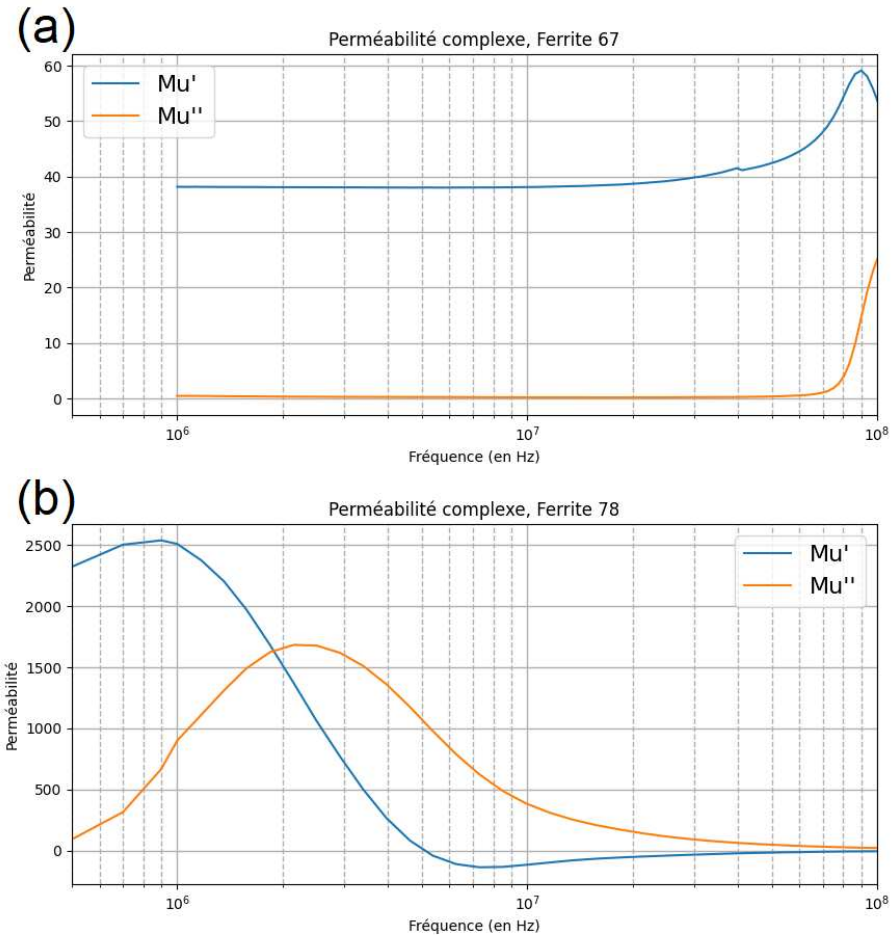



FIGURE 2.54 – Perméabilité complexe de la ferrite 67 **(a)** et 78 **(b)**.

Nous en déduisons que la ferrite 78 est plus adaptée pour des applications basses fréquences ($< 1\,\text{MHz}$), tandis que la 67 l'est pour des fréquences de plusieurs dizaines de MHz (50 MHz). Les valeurs de perméabilités sont assez élevées et très

différentes selon les matériaux. Dans le cas de la ferrite de type 67, à une fréquence de 30 MHz, la perméabilité vaut $\mu_R = 40$. Pour la ferrite 78, la perméabilité à 1 MHz vaut $\mu_R = 2500$. Cependant, il a été montré dans la partie 2.2.4 que la valeur de perméabilité $\mu_R$ était de l'ordre de 2 pour une sonde de diamètre 2 mm. La différence entre les valeurs théoriques et expérimentales ne peut pas être ignorée. L'étude doit donc être approfondie.

La perméabilité d'un matériau varie considérablement selon que la géométrie exploitée conserve un champ magnétique comme dans un tore, ou implique un changement du matériau propageant le champ comme dans le cas d'une tige. Dans ce dernier cas, le champ se propage dans une ferrite et dans l'air, ce qui l'atténue. La différence entre les valeurs de perméabilité des matériaux et des tiges de ferrites a déjà été rapportée dans différentes publications comme [54]. D'après le site du fabricant Fair-rite, nous obtenons les courbes de la figure 2.55 lors d'une caractérisation par un signal sinusoïdal à 10 kHz.

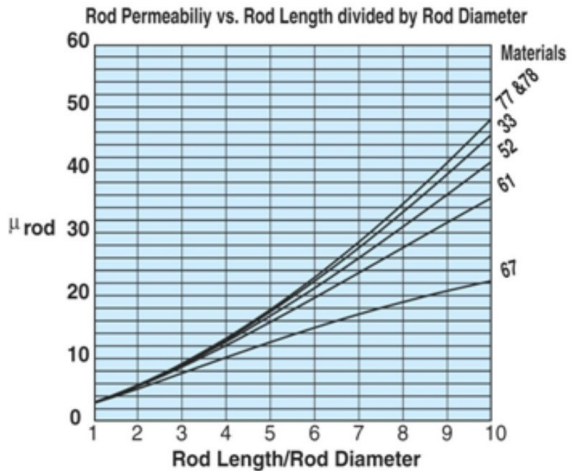



FIGURE 2.55 – Perméabilité d'une tige de ferrite Fair-rite.

Les valeurs de perméabilité sont donc très dépendantes du rapport longueur/ diamètre de la tige et beaucoup plus proches de celles obtenues (de l'ordre de 5 à 10). Ces mesures sont réalisées avec une excitation sinusoïdale à une fréquence de 10 kHz. Dans notre cas, la valeur de $\mu_R$ de 2.2 a été obtenue dans le cas d'une excitation impulsionnelle. Certains domaines magnétiques, c'est-à-dire des régions des ferrites, sont responsables de la perméabilité relative. Dans cette zone, les moments magnétiques sont orientés dans la même direction. La diminution de cette perméabilité en régime impulsionnel traduit alors un retard à l'alignement de ces domaines magnétiques. La perméabilité initiale a donc une influence très réduite sur l'inductance de la bobine.

Nous cherchons à estimer les valeurs de perméabilité relative correspondant à un régime impulsionnel.

### 2.4.3 Perméabilité relative impulsionnelle

Pour obtenir ces valeurs de $\mu_R$ en régime impulsionnel, nous mesurons le champ $\vec{B}$, via une sonde d'écoute de diamètre 250 µm, sans ferrite, lors d'une excitation impulsionnelle d'amplitude 5 V et d'un temps de montée de 5 ns. Le montage est illustré sur la figure 2.56.

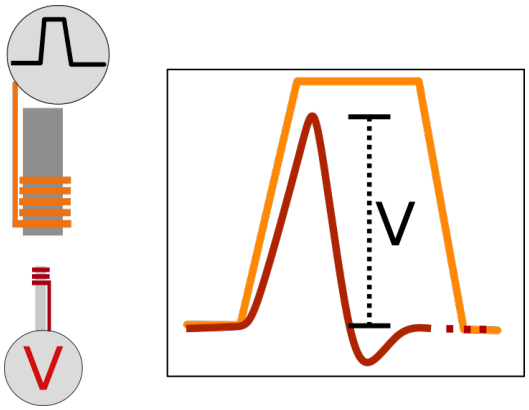



FIGURE 2.56 – Montage mesurant la perméabilité relative impulsionnelle.

La valeur de perméabilité relative de l'air est égale à 1. Ainsi, nous pouvons effectuer le rapport des amplitudes pour en déduire la valeur de perméabilité relative impulsionnelle du matériau.

| Diamètre de la ferrite, du fil, nombre de spires et matériau | Amplitude mesurée | $\mu_R$ |
|---|---|---|
| 3000 µm, 200 µm, 1 spire, Air | 21 mV | 1 |
| 3000 µm, 200 µm, 1 spire, 67 | 36 mV | 1.7 |
| 2000 µm, 200 µm, 5 spires, Air | 41 mV | 1 |
| 2000 µm, 200 µm, 5 spires, 67 | 90 mV | 2.2 |
| 2000 µm, 200 µm, 5 spires, 78 | 92 mV | 2.2 |
| 1500 µm, 200 µm, 5 spires, Air | 27 mV | 1 |
| 1500 µm, 200 µm, 5 spires, 67 | 103 mV | 3.8 |
| 1500 µm, 200 µm, 5 spires, 78 | 116 mV | 4.3 |
| 1000 µm, 200 µm, 5 spires, Air | 25 mV | 1 |
| 1000 µm, 200 µm, 5 spires, 67 | 130 mV | 5.2 |

TABLEAU 2.3 – Amplitude de la tension mesurée aux bornes de la sonde et $\mu_R$ calculé pour différentes sondes.

La différence de perméabilité relative impulsionnelle entre les ferrites 67 et 78 est faible, inférieure à 10 %. Nous constatons qu'une diminution du diamètre de la ferrite augmente la valeur de perméabilité relative $\mu_R$ dans le cas d'une excitation impulsionnelle. Par exemple, la perméabilité relative est de l'ordre de 1.7 pour une sonde de diamètre 3000 µm et de 5.2 pour un diamètre 1000 µm. Cette augmentation

de la valeur de perméabilité relative impulsionnelle implique une augmentation de l'intensité du champ $\vec{B}$ engendré. Cependant, cela ne signifie pas que la tension induite dans une sonde ou un circuit soit plus importante, car elle dépend aussi de la distance entre la cible et la sonde.

### 2.4.4 Inductances des sondes

Les inductances de différentes sondes ont été mesurées à une fréquence de 10 kHz à l'aide d'un multimètre LCR SmartTweezers ST-5S. Leurs valeurs sont présentées dans le tableau 2.4.

| Diamètre de la ferrite, du fil, nombre de spires et matériau | Inductance mesurée à 10 kHz |
|---|---|
| 3000 µm, 200 µm, 5 spires, 67 | 536 nH |
| 2000 µm, 200 µm, 5 spires, 67 | 370 nH |
| 2000 µm, 200 µm, 5 spires, 78 | 360 nH |
| 1500 µm, 200 µm, 5 spires, 67 | 360 nH |
| 1500 µm, 200 µm, 5 spires, 78 | 325 nH |
| 1500 µm conique, 200 µm, 10 spires, référence | 540 nH |
| 1000 µm, 200 µm, 5 spires, 67 | 275 nH |

TABLEAU 2.4 – Inductance mesurée pour différentes sondes.

Nous constatons que l'inductance diminue également avec le diamètre de la sonde, et les ferrites 78 ont une inductance plus élevée que les 67 pour des caractéristiques identiques. Les valeurs diffèrent de celles présentées dans le tableau 2.2, où la perméabilité relative $\mu_R$ était estimée à 2.2. L'inductance d'une bobine ne dépend pas de sa fréquence d'utilisation, cependant, dans le cas des bobines avec ferrites, le comportement non linéaire des ferrites introduit une variation de la perméabilité relative. Les calculs effectués précédemment ne prennent pas en compte l'effet de la variation de la perméabilité relative en fonction de la fréquence. De plus, lors de la fabrication des sondes, la distance entre les spires n'est pas régulière, ce qui ne peut être pris en compte dans l'étude théorique. L'évolution des inductances en fonction du diamètre de la sonde et du nombre de spires reste cohérente avec l'étude théorique dynamique.

Les résultats entre les sondes avec une ferrite de type 67 ou 78 sont relativement similaires en régime continu. En revanche, l'excitation est impulsionnelle, donc à spectre large, il faut étudier la réponse fréquentielle des sondes en mesurant leur diagramme de Bode.

### 2.4.5 Réponse fréquentielle des ferrites

La réponse fréquentielle des perméabilités relatives $\mu r$ est tracée en réalisant des mesures des tensions aux bornes de trois sondes de diamètre 1.5 mm avec 5 spires.

Elles sont composées de ferrites 67 et 78 et d'air. L'excitation est réalisée par un signal sinusoïdal d'amplitude crête-crête 5 V et de fréquence entre 100 kHz et 100 MHz, en utilisant un GBF Tektronix AFG3102, tel que présenté sur la figure 2.57.

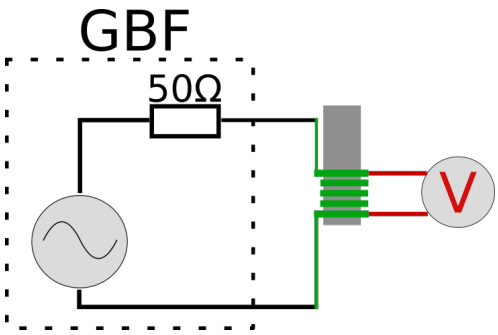



FIGURE 2.57 – Montage mesurant la réponse fréquentielle de la perméabilité relative des ferrites.

Le rapport des amplitudes entre des sondes avec ferrite et avec air permet d'en déduire une réponse fréquentielle de la perméabilité relative $\mu r$. La perméabilité relative des matériaux 67 et 78 en fonction de la fréquence de l'excitation est tracée sur la figure 2.58.

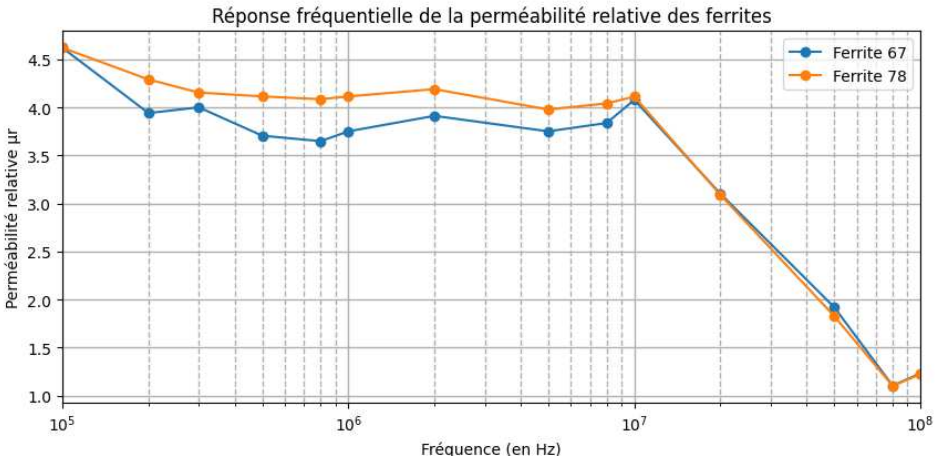



FIGURE 2.58 – Réponse fréquentielle de la perméabilité relative des ferrites 67 et 78.

Nous constatons que les réponses fréquentielles des sondes à base de ferrite 67 et 78 ont des comportements similaires. La perméabilité de la ferrite 78 est légèrement supérieure à celle de la 67, mais elles restent proches de 4 jusqu'à 10 MHz puis chutent. D'après les documentations des ferrites Fair-rite de type 67 [40] et 78 [41], les réponses fréquentielles devraient être différentes, avec une perméabilité relative plus importante à 200 kHz pour la ferrite 78 et à 50 MHz pour la ferrite 67. Ces valeurs sont obtenues pour des ferrites toriques et non des tiges, tel que nous

l'utilisons. Cela montre donc que les caractéristiques des ferrites varient en fonction de la géométrie. La simple lecture de la documentation technique ne peut donc pas être réalisée afin de déterminer la ferrite la plus adaptée pour réaliser des injections de fautes.

Nous regardons alors la réponse des sondes à une impulsion via un générateur Avtech.

### 2.4.6 Courants consommés par une sonde

Nous comparons les courants circulant dans les sondes à base de ferrites 67 et 78 lors d'une injection. Une sonde ayant une variation de courant plus grande générera une perturbation plus intense dans la cible. Pour réaliser la comparaison, une résistance de shunt de 1 Ω est placée en série avec la sonde, tel que présenté sur la figure 2.59.a. Cela permet d'obtenir la valeur du courant dans la sonde, en mesurant la tension aux bornes de la résistance. L'excitation est une impulsion de tension réalisée depuis un générateur Avtech d'amplitude 400 V. La durée du front montant, entre 20 et 80 % du signal, est de 2.5 ns et celle de l'impulsion est de 8 ns. Les résultats sont présentés dans la figure 2.59.b.

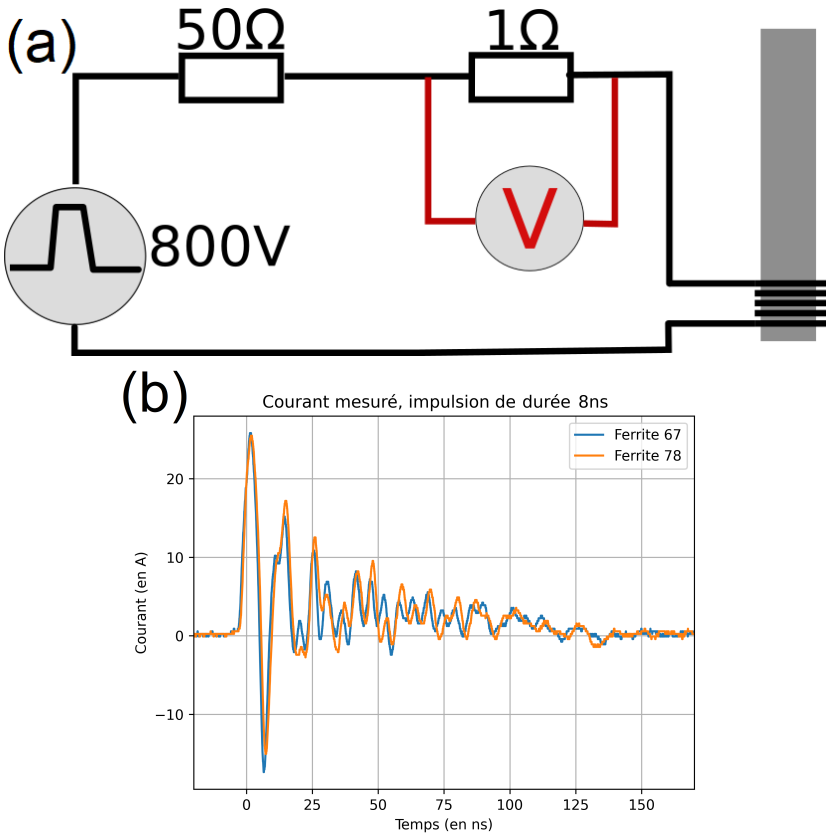



FIGURE 2.59 – Montage **(a)** mesurant le courant dans une sonde composée de ferrite 67 et 78 pour une impulsion de durée 8 ns **(b)**.

Les courants mesurés avec des sondes à base de ferrite 67 et 78 sont similaires. Nous en concluons que sur cet aspect, il y a peu de différences entre les deux types de ferrites. Le fabricant fournit des caractéristiques de bandes passantes de 50 MHz pour la sonde 67 et de 200 kHz pour la sonde 78. Ces valeurs, fournies pour des ferrites de formes toriques, sont donc également modifiées pour des utilisations avec des tiges de ferrite.

Sachant que ces deux matériaux sont normalement caractérisés par des pertes variables avec la fréquence, nous regardons dans le paragraphe suivant la décroissance du flux magnétique en fonction de la longueur de ferrite.

### 2.4.7 Décroissance du champ $\vec{B}$ dans les ferrites

Nous cherchons à obtenir une loi de décroissance du champ magnétique dans les ferrites. Pour cela, des enroulements de 5 spires sont réalisés sur les ferrites avec du fil de 40 µm. La figure 2.60 illustre les enroulements avec leurs distances relatives.

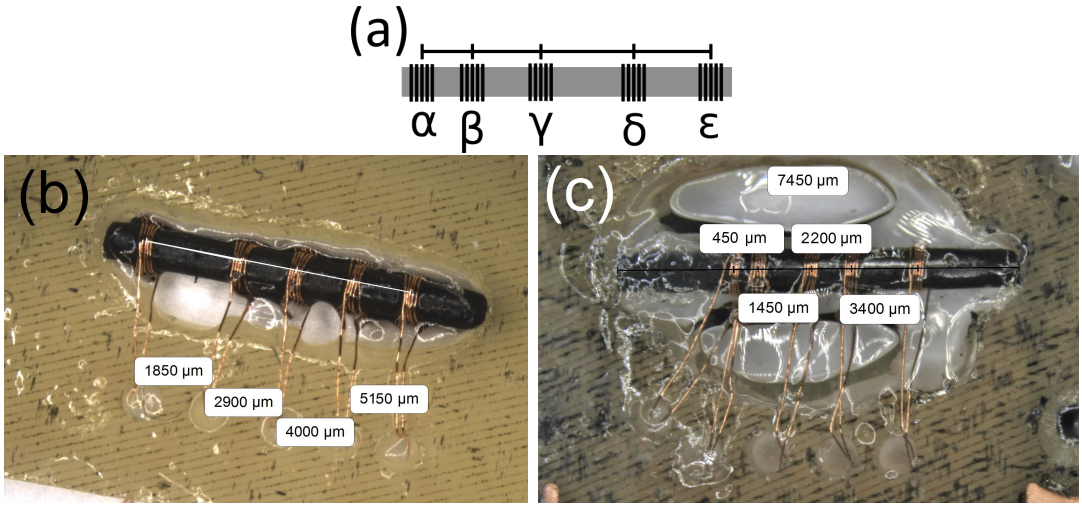



FIGURE 2.60 – Schéma d'une ferrite avec plusieurs enroulements **(a)**, montages composés de ferrites de type 67 **(b)** et 78 **(c)**, de longueur 7.5 mm et de diamètre 750 µm.

Nous injectons un signal impulsionnel sur une bobine et nous mesurons aux bornes des autres bobines leur tension, comme représenté sur la 2.61. Chaque bobine (de $\alpha$ à $\epsilon$) est donc utilisée en tant qu'émetteur et récepteur durant l'expérience. L'excitation est une impulsion de tension d'amplitudes entre 100 V et 400 V réalisée depuis un générateur de marque Avtech. La durée du front montant est de 2.5 ns et celle de l'impulsion est de 6 ns.

La figure 2.62 représente les tensions maximales mesurées en fonction de la distance entre les bobines pour les ferrites 67 et 78.

Nous observons que la décroissance est assez forte : en 1 mm le signal est diminué de 20 % et en 4 mm de 80 %. Ainsi, pour optimiser les paramètres d'injection, il est préconisé d'utiliser des spires jointives au plus près de l'extrémité de la tige de ferrite.

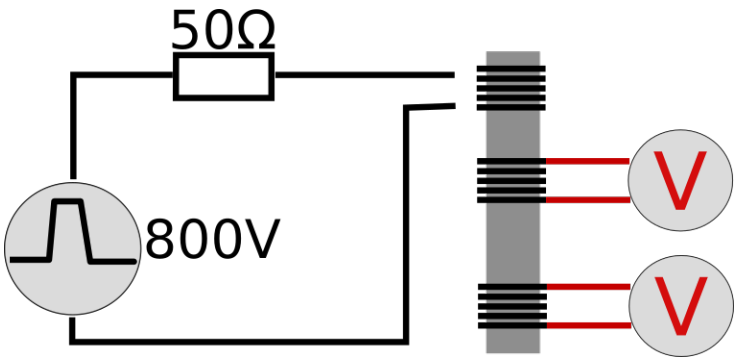



FIGURE 2.61 – Manipulation mesurant la décroissance du champ $\vec{B}$ dans les ferrites.

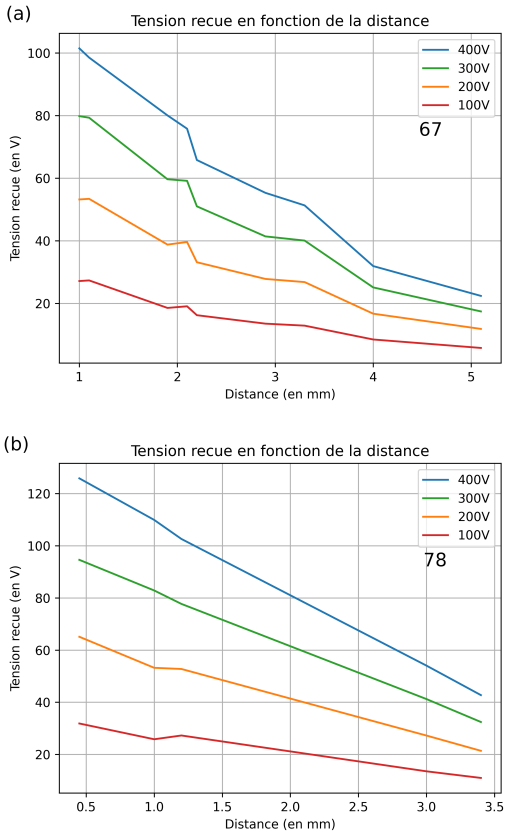



FIGURE 2.62 – Tension mesurée en fonction de la distance entre deux enroulements pour la ferrite 67 **(a)** et 78 **(b)**.

La figure 2.63 décrit les lois de décroissances pour des ferrites 67 et 78.

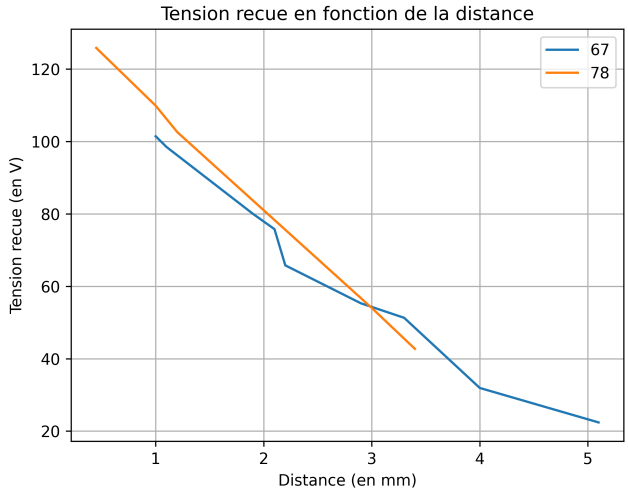



FIGURE 2.63 – Comparaison de la décroissance du champ $\vec{B}$ dans les ferrites 67 et 78.

La décroissance du champ $\vec{B}$ en fonction de la distance semble linéaire dans les deux matériaux, même si la tension reçue par le matériau 78 est plus élevée. La comparaison des lois de décroissance dans la ferrite montre que les deux matériaux ont des décroissances comparables. Cette figure montre aussi qu'il n'y a pas de saturation lorsque l'on utilise des ferrites 750 µm avec 5 spires et un générateur Avtech fournissant une impulsion de tension d'amplitude 400 V et de durée 6 ns. Une expérience similaire a également montré que cette loi de décroissance est valable pour des durées d'impulsions jusqu'à 100 ns sous une force électromotrice de 800 V. De même, il n'a pas été possible d'obtenir de saturation des ferrites pour les deux types de ferrites.

La ferrite de type 78 a de meilleures caractéristiques pour réaliser des injections de fautes que celle de type 67. Ces résultats sont confirmés dans la prochaine section, en comparant les effets de ces différentes ferrites sur une cible réelle.

### 2.4.8 Étude des effets des différentes ferrites sur la perturbation de tension induite

Le circuit de test basé sur un FPGA est utilisé pour réaliser des mesures de la perturbation de la tension interne à des fins de comparaison entre les sondes à base de ferrites 67 et 78 pour des diamètres de 750 µm, 1500 µm et 2000 µm. Les mesures présentées sur la figure 2.64 montrent la valeur maximale renvoyée par l'oscillateur en anneau. Dans le cas des ferrites de diamètres 1500 µm, les résultats de la sonde de référence (ferrite conique de diamètre 1500 µm et 10 tours) sont aussi

présentés. L'excitation est une impulsion de tension d'amplitude 70 V durant 6 ns réalisée depuis un générateur de marque Avtech.

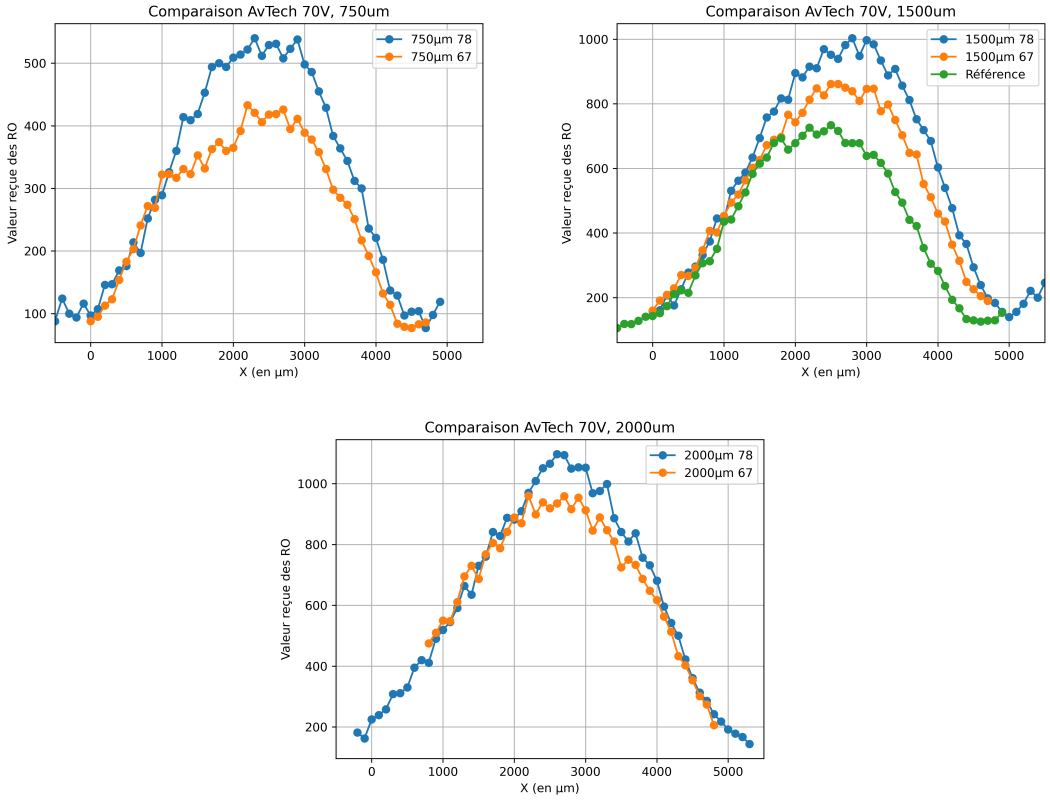



FIGURE 2.64 – Variations maximales mesurées par l'oscillateur en anneau d'un FPGA lors d'injection avec des ferrites de diamètres 750 µm **(a)**, 1500 µm **(b)** et 2000 µm **(c)**.

Nous constatons que la variation des valeurs reçues lors d'un déplacement latéral de la sonde n'évolue pas en fonction du diamètre de la sonde. Ainsi, nous n'utiliserons pas ce capteur afin de caractériser les variations de résolution spatiale, mais uniquement pour étudier l'intensité des variations de la tension interne. Dans le cas de la ferrite de diamètre 1500 µm, la variation des valeurs reçues de l'oscillateur en anneau est supérieure de 15 % avec le matériau 78 par rapport au 67 et de 30 % avec le matériau 78 par rapport à celui de référence. Nous constatons que les variations de tensions internes sont plus grandes avec des sondes composées de noyaux de ferrites de matériaux 78 qu'avec des matériaux 67 ou une ferrite dite de référence.

Nous en concluons que l'utilisation d'une ferrite 78 est plus avantageuse qu'une ferrite 67. Elle optimise l'injection. La suite de l'étude consiste à déterminer si certains paramètres ont une influence sur les champs magnétiques engendrés par les sondes.

### 2.4.9 Effet de la longueur d'une ferrite

Nous cherchons à déterminer l'effet de la longueur d'une ferrite sur les lignes de champs. Pour cela, le champ magnétique engendré par une ferrite de diamètre 3 mm comprenant 10 spires est mesuré via une sonde Langer RF-R 50-1. Les spires sont à l'extrémité de la ferrite, et la longueur h de la ferrite est raccourcie au fur et à mesure de l'expérience, tel que présenté sur la figure 2.65.a. L'excitation est une impulsion de tension réalisée depuis un générateur Avtech d'amplitude 200 V, avec une durée d'impulsion de 10 ns.

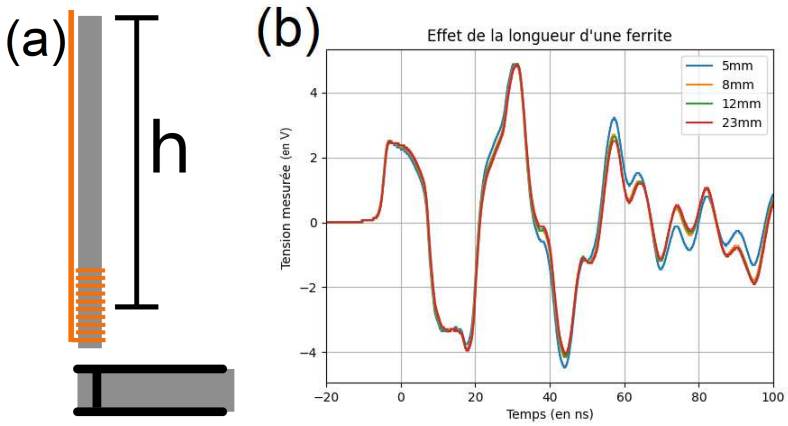



FIGURE 2.65 – Montage **(a)** étudiant l'effet de la longueur d'une tige de ferrite mesuré par une sonde Langer **(b)**.

Les variations de tensions aux bornes de la sonde Langer sont présentées dans la figure 2.65.b. Nous observons de très légères variations d'amplitudes en fonction de la longueur de ferrite. Elles sont inférieures à 100 mV tandis que l'amplitude de la perturbation est de 8 V. Nous les considérons ainsi comme peu significatives. La longueur de la ferrite n'a donc pas d'influence sur l'intensité du champ $\vec{B}$ produit. Nous pouvons tester cette affirmation sur la cible de type FPGA.

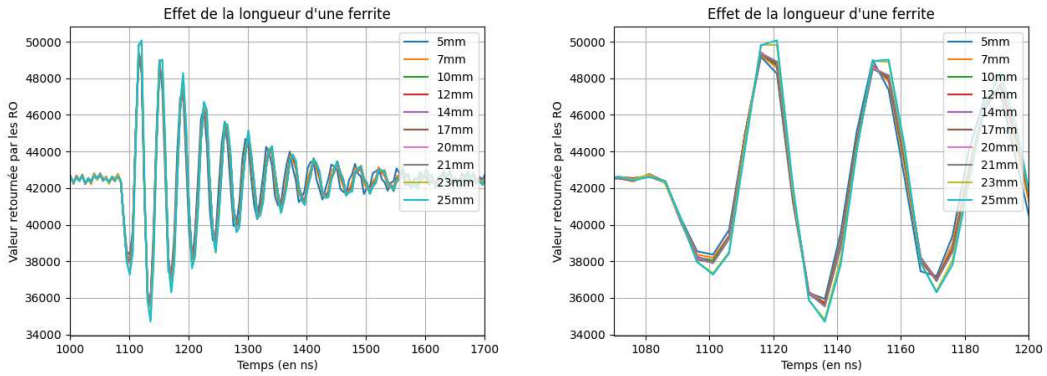



FIGURE 2.66 – Effet de la longueur d'une tige de ferrite mesuré par un FPGA.

Nous observons de légères variations d'amplitudes, qui peuvent être dues aux limites du dispositif de mesures : une fréquence d'échantillonnage basse, de l'ordre de 200 MHz. Dans tous les cas, la variation est inférieure à 5 %. Nous avons conclu que la longueur de la ferrite a une influence négligeable sur les perturbations engendrées.

## 2.5 Adaptation d'impédance et rebonds

La première partie du chapitre s'est concentrée sur l'étude des sondes. Cependant, nous avons vu au paragraphe 2.3.3 que le comportement du générateur d'impulsions de tension Avtech n'était pas évident à modéliser. Ainsi, cette partie s'attache à adapter les sondes au générateur d'impulsions afin d'optimiser l'injection et de réduire les oscillations présentes aux bornes de la sonde à la suite des impulsions.

### 2.5.1 Adaptation de l'impédance vers une impédance plus basse

L'impédance de sortie du générateur est de 50 Ω et l'impédance ohmique de la sonde est d'environ 0.1 Ω, tandis que son impédance inductive est directement dépendante du temps de montée de l'impulsion et de la capacité du générateur à fournir du courant pour les faibles charges. Lorsque nous cherchons à transférer le maximum de puissance à une charge plus petite que l'impédance de sortie du générateur, nous pouvons utiliser un transformateur d'impédance. Pour cela, le dispositif AVX-M4 développé par Avtech peut être utilisé. Il réalise une adaptation de l'impédance 50 Ω du générateur d'impulsions vers une charge 3 Ω. Ainsi, la résistance est divisée par 16, le courant doit alors être quadruplé en sortie du transformateur. La figure 2.67 montre le dispositif couplé à une sonde de diamètre 1500 µm soudée directement dessus. Bien que l'utilisation d'un connecteur de type SMA en sortie du transformateur simplifie le montage des sondes, elle est à proscrire, car ces connecteurs sont adaptés pour des charges 50 Ω et cela provoquerait une perte de transmission du signal.

Nous pouvons utiliser le dispositif de caractérisation des sondes basé sur le FPGA afin de mesurer l'effet des perturbations en fonction du temps. Pour cela, nous réalisons des injections avec une sonde 1500 µm (ferrite 78) au contact du FPGA, puis nous faisons de même avec le dispositif AVX-M4 soudé directement à la sonde. La figure 2.68 montre l'impact du dispositif sur la tension interne du FPGA pour des tensions d'injection de 70 et 150 V, avec une durée d'impulsion de 10 ns.

Nous constatons que pour les deux tensions, la variation de la valeur mesurée par l'oscillateur en anneau est 2 fois moins élevée avec le dispositif pour une injection à 70 V. Si nous voulons obtenir des variations de tensions équivalentes à une injection avec une amplitude de 50 V, il est nécessaire d'utiliser des tensions de 150 V lorsque le dispositif est présent, tel que le montre la figure 2.69.

Nous constatons une augmentation de la période des oscillations amorties et une diminution de leur amplitude. L'amortissement des oscillations est marginal et ne

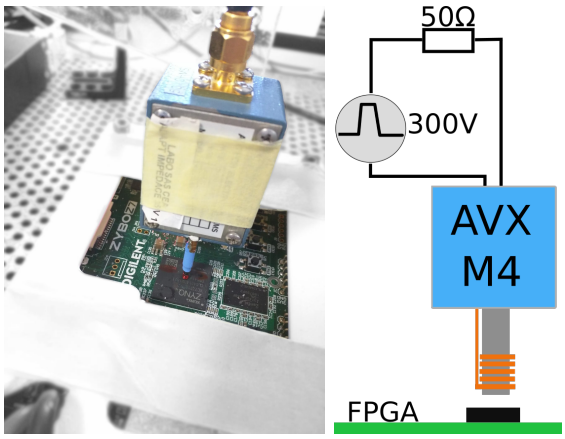



FIGURE 2.67 – Transformateur d'impédance AVX-M4 avec sonde d'injection électromagnétique.

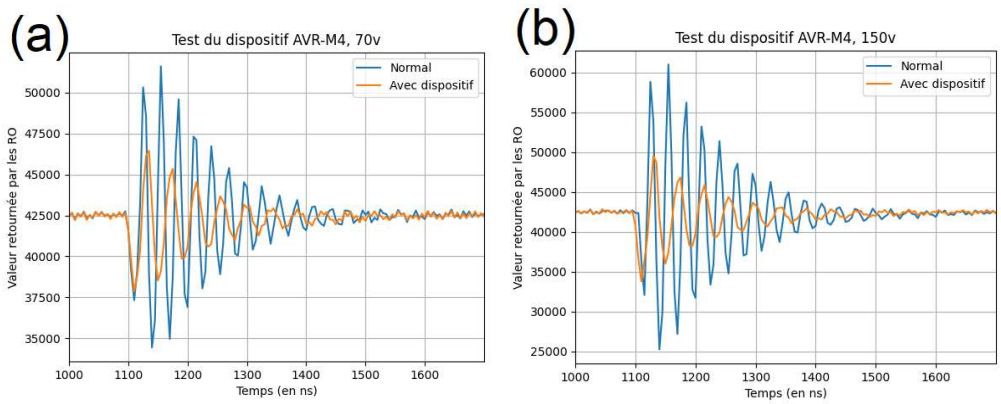



FIGURE 2.68 – Influence du dispositif AVX-M4 à 70 **(a)** et 150 V **(b)** avec une sonde 1500 µm.

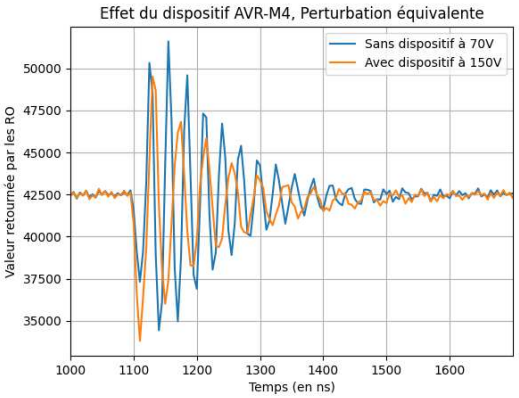



FIGURE 2.69 – Effet du dispositif adaptateur d'impédance AVX-M4.

permet pas de conserver une impulsion monopolaire aux bornes de la sonde telle qu'on l'observe dans une charge 50 Ω. Ce dispositif n'apporterait pas d'intérêt pour réaliser des injections de fautes. Afin de déterminer l'origine d'une diminution si importante de la variation de tension interne au FPGA, nous étudions l'efficacité énergétique du dispositif AVX-M4.

Dans un premier temps, nous cherchons à mesurer la puissance maximale que fournit le générateur Avtech. Pour cela, nous connectons une charge 50 Ω en sortie du générateur et nous mesurons la tension à ses bornes, tel que présenté sur la figure 2.70.a. Lorsqu'une impulsion d'amplitude 200 V et de durée 10 ns est demandée, nous mesurons une amplitude maximale de 250 V aux bornes de la charge. Cela signifie que la puissance fournie est de $P_{fournie} = \frac{200^2}{50} = 1250\,W$.

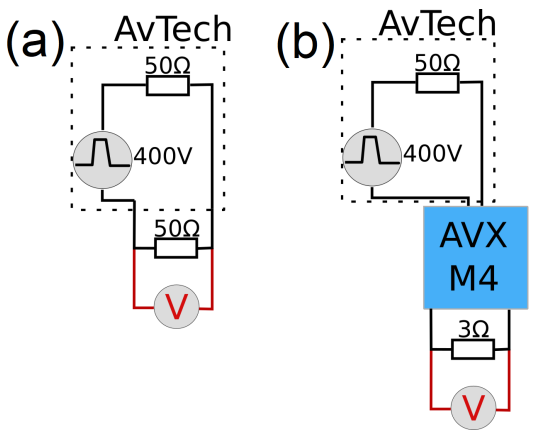



FIGURE 2.70 – Montages mesurant l'efficacité énergétique du dispositif adaptateur d'impédance AVX-M4.

Nous cherchons ensuite à mesurer la puissance que nous pouvons récupérer dans une charge adaptée en sortie du dispositif. Pour cela, nous connectons le dispositif AVX-M4 au générateur, avec une charge de 3 Ω à sa sortie, tel que présenté sur la figure 2.70.b. Nous réalisons la mesure de la tension de sortie du dispositif AVX-M4 lors d'une impulsion de mêmes caractéristiques que précédemment. La tension maximale mesurée est de 30 V, ainsi la puissance maximale fournie à la charge est d'environ 300 W. L'efficacité énergétique du transformateur est alors de 24 %. Les pertes du transformateur d'impédance sont relativement importantes (76 %), et ont pour conséquence la diminution de variation de la tension interne du FPGA mesurée précédemment.

Afin de limiter les oscillations de la tension interne des circuits visés, nous cherchons à estimer l'impédance des sondes pour adapter le couple générateur/sonde.

### 2.5.2 Estimation de l'impédance de la sonde en régime sinusoïdal

Selon le raisonnement précédent, la sonde a été considérée comme une charge résistive d'impédance ohmique d'environ 0.1 Ω au lieu d'une impédance complexe. Nous avons établi au paragraphe 2.3.2 un circuit équivalent de la sonde. Nous pouvons donc calculer l'impédance pour une fréquence donnée.
Nous obtenons $\bar{Z_{Sonde}} = Ze^{j\theta}$ avec $|\bar{Z}| = \frac{1}{\sqrt{\frac{R^2}{R^2+L^2\omega^2}+\omega^2(C-\frac{L}{R^2+L^2\omega^2})^2}}$ et

$\theta = -\arctan\left(\frac{C\omega(R^2+L^2\omega^2)-L\omega^2}{R}\right)$.
Le temps de montée d'un signal impulsionnel de 2 ns correspond à celui d'une sinusoïde de fréquence 50 MHz. Pour la sonde utilisée dans la simulation (1500 µm, 5 spires), nous obtenons une impédance de 80 Ω à 50 MHz. La valeur est donc bien supérieure à la résistivité linéique du fil de cuivre d'impédance ohmique de 0.1 Ω, et de l'impédance de sortie du générateur de 50 Ω.

### 2.5.3 Estimation de l'impédance de la sonde en régime impulsionnel

Nous cherchons ici à mettre en évidence le rôle de l'impédance complexe de la sonde dans le cas d'un générateur Avtech. Nous plaçons une charge 50 Ω en parallèle de la sonde et nous mesurons la perturbation au niveau de l'oscillateur en anneau du FPGA. Nous recommençons ensuite l'expérience en ajoutant aussi une résistance en série de la sonde de 4.7 Ω. Le circuit final est représenté sur la figure 2.71. L'impulsion de tension, réalisée depuis un générateur Avtech, a une amplitude de 70 V avec une durée du front montant de 2.5 ns et d'impulsion de 10 ns.

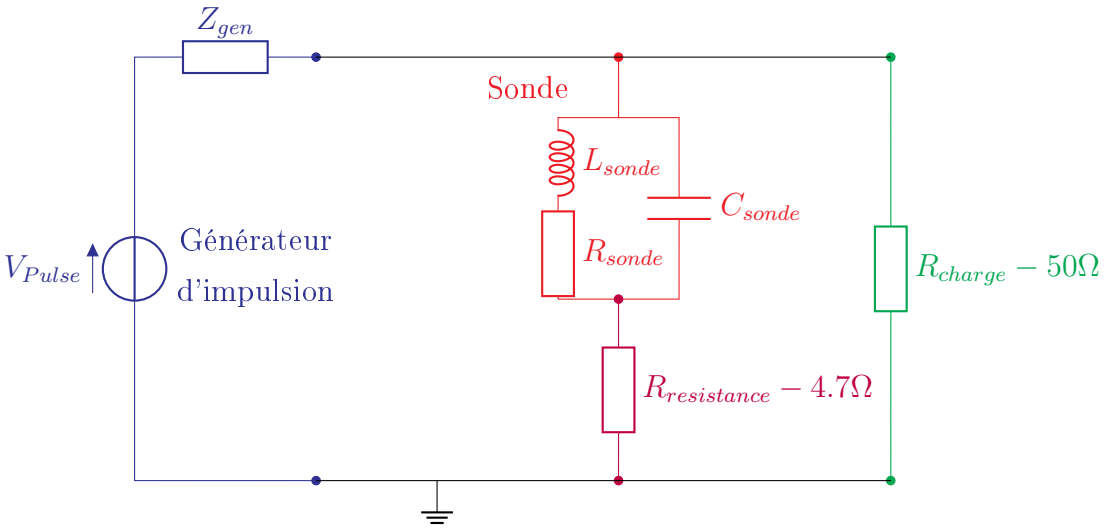



FIGURE 2.71 – Représentation du circuit électrique mesurant l'impédance de la sonde.

L'impulsion de tension réalisée depuis un générateur Avtech a une amplitude de 70 V avec une durée du front montant de 2.5 ns et d'impulsion de 10 ns. La figure 2.72 met en évidence l'effet d'une résistance de 4.7 Ω en série avec la sonde. Une charge de 50 Ω en parallèle de la sortie du générateur est présente durant les expériences.

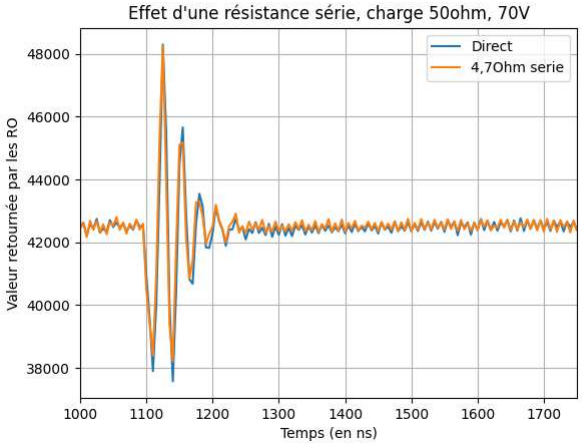



FIGURE 2.72 – Effet de l'ajout d'une résistance série.

Nous remarquons que les deux signaux sont assez similaires. Les valeurs retournées par l'oscillateur en anneau oscillent entre 38 000 et 48 000 en l'absence de résistance série. Lorsque la résistance série est ajoutée, ces valeurs oscillent entre 38 500 et 48 000, soit une diminution de 5 % des variations. Si la sonde avait une impédance comparable à la résistance série, nous obtenons une amplitude divisée par un facteur 2. Dans notre cas, elle est peu modifiée, ce qui montre que la sonde a une impédance plus élevée que 4.7 Ω.

Nous cherchons à estimer l'impédance de cette sonde durant le front montant de l'impulsion. Pour cela, nous réalisons le montage présenté sur la figure 2.71. Nous développons alors la loi des mailles : $U_R + U_{sonde} = U_{50}$. Nous obtenons ainsi $U_{50} - U_R = Z_{sonde} * i$, d'où $U_{50} - U_R = Z_{sonde} * \frac{U_R}{R}$. Nous écrivons alors : $Z_{sonde} = (\frac{U_{50}}{U_R} - 1) * R$

La figure 2.73 présente les tensions aux bornes de la résistance série, en bleu, et de la charge 50 Ω, en orange, lors d'une impulsion de tension de 70 V. L'échelle de la première courbe est multipliée par un facteur 20.

La tension aux bornes de la charge augmente jusqu'à 70 V, puis diminue jusqu'à -45 V. À la fin du front montant de l'impulsion, nous constatons qu'on obtient les tensions maximales aux bornes des résistances. Ces signaux sont en phase, nous pouvons alors mesurer les tensions à la fin de l'impulsion : $U_{50} = 70\,V$ et $U_R = 2.2\,V$. Nous savons que $R = 4.7\,\Omega$, nous estimons alors le module de l'impédance de la sonde lorsqu'il atteint son maximum : $Z_{Sonde\_impulsion} = (\frac{70}{2.2} - 1) * 4.7 = 145\,\Omega$.

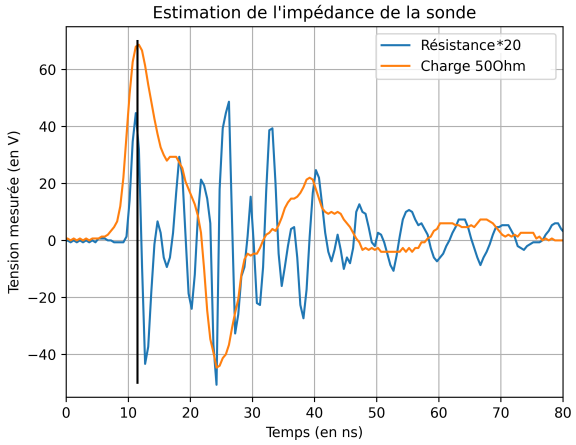



FIGURE 2.73 – Tensions aux bornes de la résistance série (bleu) et de la charge 50 Ω (orange).

Nous cherchons alors à comparer le module de l'impédance de cette sonde avec celle d'une résistance de 150 Ω en réalisant le circuit présenté sur la figure 2.74.

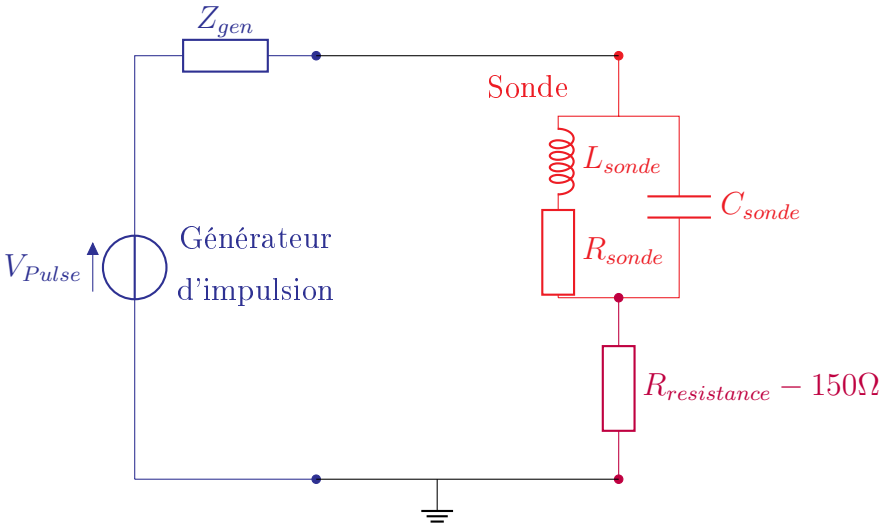



FIGURE 2.74 – Représentation du circuit.

La figure 2.75 représente les signaux aux bornes de l'Avtech (en bleu), de la résistance (en orange) et leur différence (en vert).

Les tensions aux bornes de la sonde augmentent jusqu'à 80 V, puis diminuent jusqu'à -75 V. Lors de la fin du front montant de l'impulsion, à l'instant t=13 ns, nous obtenons le maximum d'amplitude de la tension aux bornes de la résistance. La tension aux bornes de l'Avtech est de 140 V et de 70 V aux bornes de la résistance. À cet instant, la tension aux bornes de la résistance est équivalente à la moitié de celle du circuit total, ce qui signifie que l'impédance de la résistance est équivalente

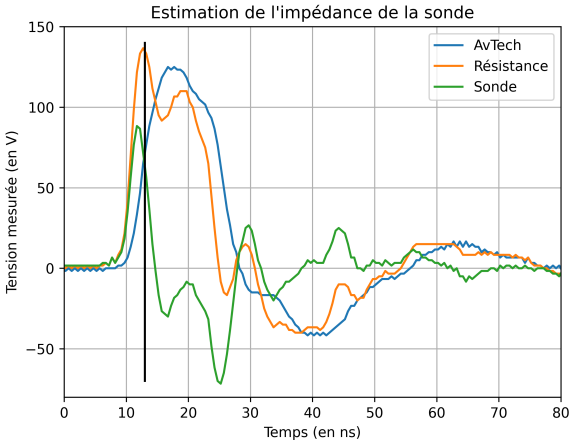



FIGURE 2.75 – Tensions aux bornes de l'Avtech (en bleu), aux bornes de la résistance (en orange) et leur différence (en vert).

à celle de la sonde à la fin du front montant de l'impulsion.

Ainsi, nous validons une valeur approximative du module de l'impédance de la sonde à 150 Ω à la fin du front montant de l'impulsion, pour une ferrite 78 de diamètre 1.5 mm et 5 spires. Pour transférer le maximum de puissance, il faut donc réaliser une adaptation d'impédance de 50 Ω vers 150 Ω.

### 2.5.4 Circuit élévateur d'impédance

Pour augmenter l'impédance de sortie du générateur Avtech, nous exploitons un transformateur 2 spires - 6 spires autour d'une ferrite torique du matériau 67, tel que présenté sur la figure 2.76.a. Ce transformateur d'impulsions est exploité ici pour sa capacité d'adaptation d'impédance. Ces caractéristiques sont généralement utilisées à des fréquences beaucoup plus basses en raison des pertes magnétiques élevées aux fréquences hautes. Ce transformateur divise l'impédance perçue par le générateur par un facteur 9. Les effets sur l'oscillateur en anneau d'un FPGA pour des impulsions de 70V sont représentés sur la figure 2.76.b.

Les variations de valeurs retournées par l'oscillateur en anneau obtenues avec le transformateur sont inférieures d'environ 50 % à celles obtenues par une connexion directe de la sonde à l'Avtech. Cela signifie que le transformateur a une efficacité limitée : la puissance transmise est réduite et l'adaptation d'impédance n'est pas effectuée.

Afin de mieux comprendre les problématiques liées à la conception de transformateurs d'impédance en régime impulsionnel, un transformateur 20 spires - 60 spires est réalisé. Il est caractérisé par un burst de 6 périodes d'un sinus avec une amplitude de 4 Vpp de force électromotrice à l'aide d'un GBF Tektronix AFG3102. Dans un premier temps, afin de déterminer sa fréquence de fonctionnement optimale, nous

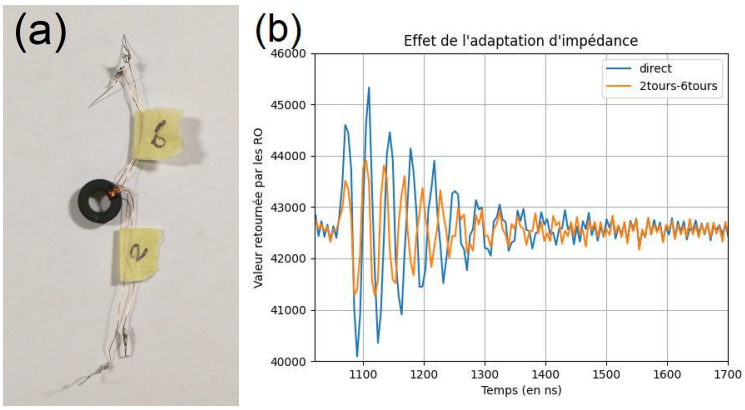



FIGURE 2.76 – Transformateur 2 spires - 6 spires **(a)** et effet du transformateur adaptateur d'impédance **(b)**.

cherchons la fréquence permettant d'obtenir 50 % du signal d'entrée en circuit ouvert sur le primaire du transformateur. La tension en circuit ouvert est de 1.96 V, et celle aux bornes du primaire de 0.98 V pour une fréquence de 330 kHz, tel que présenté sur la figure 2.77.

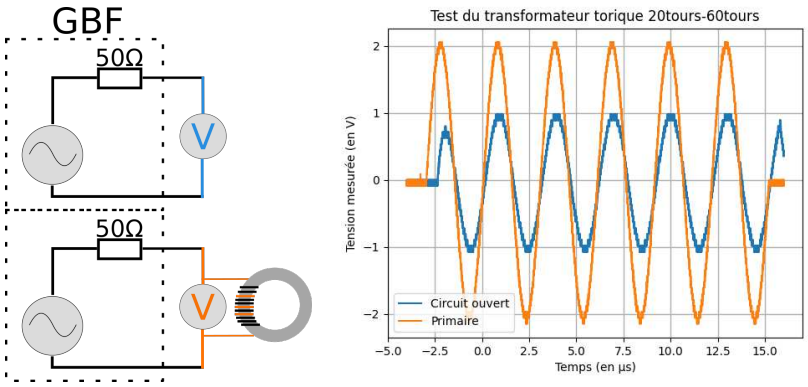



FIGURE 2.77 – Recherche de la fréquence de fonctionnement optimale du transformateur.

Dans un second temps, nous cherchons à calculer le gain en tension du transformateur, c'est-à-dire le rapport entre la tension de sortie et d'entrée pour sa fréquence de fonctionnement optimale. Le gain obtenu à 330 kHz est de 1.8, tel que montré sur la figure 2.78.

Cette valeur est inférieure au gain de 3 qui était attendu. Avec une charge de 130 Ω, la tension aux bornes du secondaire est égale à 50 % de celle en circuit ouvert. Cela signifie que le transformateur adapte les impédances de 50 Ω vers 130 Ω ce qui correspond à un gain de 2.4, au lieu de 9 attendu. La puissance mesurée aux bornes du primaire est de 20 mW et elle est de 7.7 mW aux bornes du secondaire. Les pertes de ce transformateur sont ainsi de 61 %.

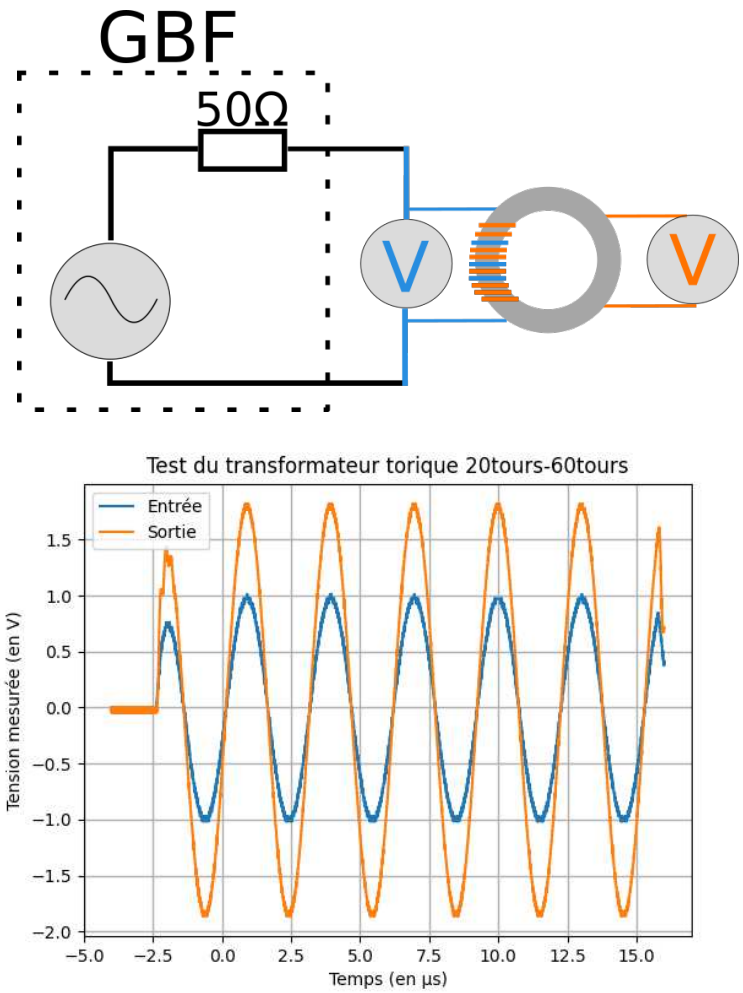



FIGURE 2.78 – Calcul du gain en tension du transformateur à 330 kHz.

Les pertes d'un transformateur de ce type sont donc relativement importantes. De plus, ce transformateur est conçu pour fonctionner à une fréquence de 330 kHz, mais dans le cas de l'injection de fautes la fréquence de fonctionnement devra être de l'ordre de plusieurs dizaines de MégaHertz. Cela oblige à diminuer le nombre de tours du primaire, augmentant les pertes. L'adaptation d'impédance est donc difficilement réalisable en utilisant des transformateurs. De plus, un montage de ce type ne présente que peu d'intérêt dans notre situation étant donné que nous cherchons aussi à limiter la force électromotrice des générateurs permettant de réaliser des fautes. Enfin, il n'a pas été observé de réduction des oscillations, ce qui n'apporte pas de gain dans la qualité et la précision des fautes.

Deux types de circuits adaptateurs d'impédances ont été utilisés, mais les pertes engendrées par ces transformateurs sont entre 61 et 76 % ce qui est relativement élevé. Afin de limiter les résonances observées sur la figure 2.76, nous étudions dans le paragraphe suivant un montage suppresseur de rebonds sans adaptations d'impédance.

### 2.5.5 Montage suppresseur des rebonds sans adaptation d'impédance

Nous avons jusqu'ici cherché à supprimer les oscillations en jouant sur l'adaptation d'impédance en sortie du générateur d'impulsions. Nous utilisons ici une autre approche, basée sur les travaux de Toulemont et al. [100] qui a présenté une première méthode de suppression des rebonds. La suppression des rebonds est obtenue par l'ajout d'une diode de suppression de tensions transitoires (ou diode transil) en parallèle de la sonde, comme représenté sur la figure 2.79. La diode choisie est de type P6KE600A dont la tension de claquage est de 570 V.

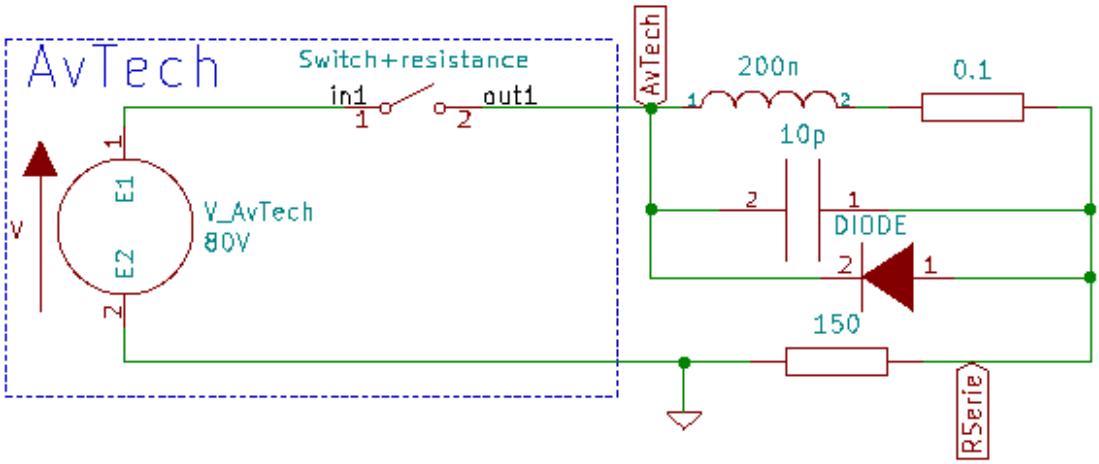



FIGURE 2.79 – Schéma du circuit électrique d'un générateur Avtech et d'une sonde d'injection électromagnétique avec l'ajout d'une diode transil.

Étant donné qu'il est impossible d'avoir une adaptation d'impédance, le recours à une diode est nécessaire pour obtenir une impulsion magnétique monopolaire. L'ajout de cette diode est simulé sur SPICE et les résultats de la simulation électrique sont présentés sur la figure 2.80.


FIGURE 2.80 – Simulation pour une diode transil montée en inverse, en parallèle de la sonde d'injection.

Nous constatons que l'ajout de la diode conserve uniquement l'impulsion électrique positive, ce qui revient à obtenir une impulsion de tension monopolaire aux bornes de la sonde, et non bipolaire. Le champ magnétique produit par la sonde est donc une impulsion magnétique monopolaire. Des essais ont été réalisés en injectant un signal depuis un GBF dans une sonde et en mesurant la variation de tension dans une sonde Langer RF-R 0.3-3. Ces résultats sont présentés sur la figure 2.81. L'excitation est une impulsion de tension réalisée depuis un générateur Tektronik AFG3102, d'amplitude 10 V, avec une durée du front montant de 5 ns et d'impulsion de 10 ns. La sonde utilisée est composée d'une tige de ferrite, de matériau Fair-rite 78, de diamètre 1500 µm et de 5 spires de fil de diamètre 200 µm.

Nous observons en bleu la tension dans la sonde de mesure lors d'une injection sans présence de diode et en orange avec une diode. En l'absence de diode, la tension mesurée dans la sonde atteint son maximum à 110 mV, puis son minimum à -110 mV. Avec une diode, la tension atteint toujours son maximum à 110 mV, et son minimum à -30 mV. Conformément à la simulation, nous observons que seule l'impulsion positive est conservée. Ce résultat est significatif, car nous obtenons pour la première fois de nouvelles conditions d'injection où l'on peut espérer mettre en évidence l'influence de la polarité de l'impulsion sur le dispositif d'injection électromagnétique.

Les effets de la présence de cette diode sur la tension interne d'un FPGA sont présentés sur la figure 2.82. Un signal impulsionnel d'amplitude 70 V avec une durée

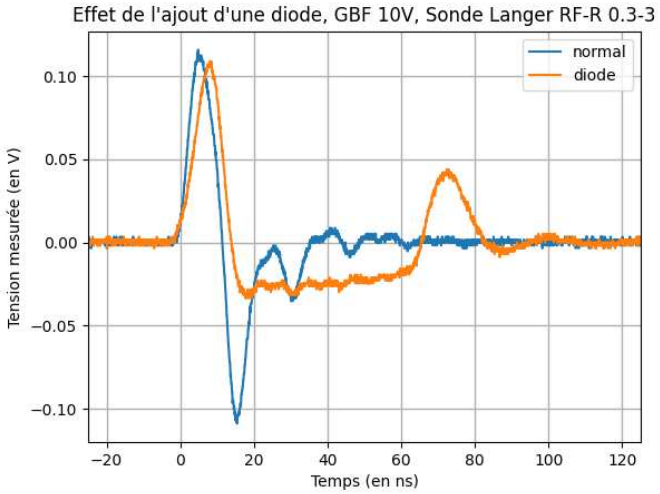



FIGURE 2.81 – Tension aux bornes d'une sonde d'écoute Langer avec et sans diode en parallèle de la sonde d'injection.

de 10 ns est produit depuis un générateur Avtech.

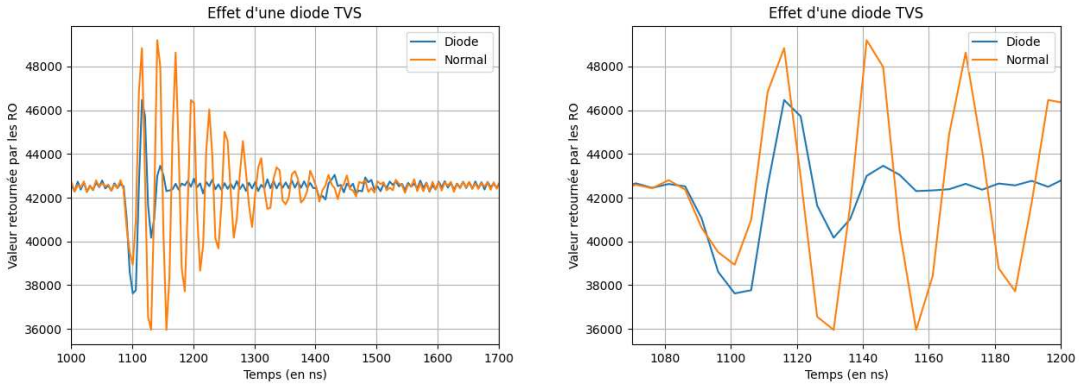



FIGURE 2.82 – Effet d'une diode transil sur l'oscillateur en anneau.

Sur la première figure, nous constatons que les oscillations des valeurs retournées par l'oscillateur en anneau ont disparu. Nous remarquons que l'amplitude des variations des valeurs est diminuée d'environ 5 %. Le dispositif limite donc les oscillations des tensions internes de la cible, tout en conservant l'intensité des perturbations.

Les effets de la présence de cette diode sont aussi visibles sur une cible microcontrôleur ATmega328P. Des injections de fautes sont réalisées lors de l'exécution du code de test décrit au paragraphe 2.1.1. Un générateur d'impulsions de tension Avtech est utilisé avec une sonde composée d'une tige de ferrite, de matériau Fair-rite 78, de diamètre 1000 µm et de 5 spires de fil de diamètre 200 µm. Une cartographie spatiale sur la surface du circuit est réalisée afin de détecter les zones produisant

des fautes dans l'exécution du programme. La cartographie est réalisée sur une zone de 3200*1800 µm avec un pas de 100 µm et 10 itérations sont effectuées pour chaque position. Une première cartographie est obtenue pour une utilisation de la sonde de façon classique, puis une seconde avec la diode montée en inverse et la troisième avec la diode montée en direct mais avec une impulsion de polarité négative, tel que présenté sur la figure 2.83.

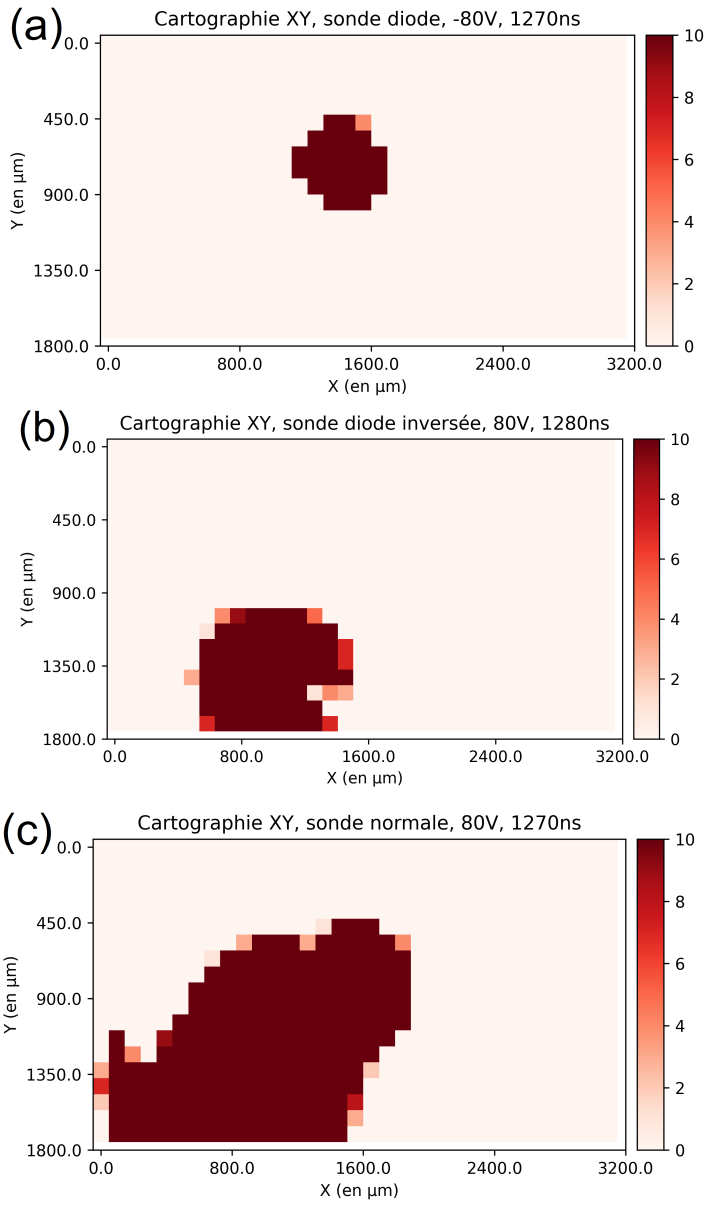



FIGURE 2.83 – Effet d'une sonde avec diode transil sur un ATmega328P **(a)**, d'une sonde avec une diode inversée **(b)** et d'une sonde sans diode **(c)**.

L'amplitude de l'impulsion de tension est de 80 V lors des trois expériences. Dans le cas de l'utilisation d'une sonde sans diode, le délai entre le déclenchement de l'injection par le microcontrôleur et la génération de l'impulsion est de 1270 ns. Dans

le cas de l'expérience avec la sonde montée en direct et de la tension négative, les fautes sont obtenues pour un délai retardé de 10 ns par rapport à celui des deux autres expériences. Aucune faute n'a pu être réalisée avec le délai de 1270 ns.

Nous remarquons qu'il est possible de réaliser des injections de fautes sur un ATmega328P avec une impulsion de tension monopolaire aux bornes de la sonde, qu'elle soit positive ou négative. Le seuil de tension produisant des fautes est de 60 V sans diode et 70 V avec diode. Avec la sonde sans diode, 32 % de la surface explorée est sensible et le nombre de fautes obtenu est de 1910. Pour le montage avec une diode en direct et une tension négative, la surface sensible est de 4 % et le nombre de fautes est de 264, tandis que pour le montage avec une diode en inverse et une tension positive, la surface sensible est de 12 % et on obtient 1292 fautes. Les surface sensibles avec les sondes avec diodes sont disjointes. Les types de fautes obtenus sont différents sur les trois cartographies. Cela signifie deux choses : la première est que nous avons désormais un nouvel outil de discrimination de fautes en jouant sur la polarité de l'impulsion ; la seconde est qu'on ne peut pas décomposer l'impulsion bipolaire en deux impulsions monopolaires. L'effet produit par une impulsion bipolaire ne peut être obtenu en combinant plusieurs impulsions monopolaires.

Cette modification assez simple permet d'obtenir un nouvel outil qui pourra servir à mieux comprendre les mécanismes et les modèles de fautes. Les résultats sur une cible de type SoC sont présentés dans le chapitre 3 au paragraphe 3.5.3.

## 2.6 Conception de nouvelles sondes

L'ensemble des précédents résultats ont permis de comprendre les mécanismes de génération des phénomènes inductifs et de définir des règles de conception des sondes. Dans cette dernière partie, nous présentons un outil simulant les champs magnétiques engendrés par les sondes. Quelques exemples sont proposés.

### 2.6.1 Outil d'aide à la conception des sondes

Dans les paragraphes précédents, nous avons montré que l'optimisation d'une sonde d'injection dépendait de nombreux paramètres. Nous présentons ici un programme utilitaire Polaris, simulant les effets étudiés précédemment par visualisation de l'influence de certains paramètres. Cet utilitaire est réservé à un usage interne du laboratoire SAS de l'École des Mines de St-Étienne et du CEA. Une capture d'écran est présentée sur la figure 2.84.

Cette interface fournit instantanément l'étalement spatial, la décroissance en z et une visualisation en 3D du champ magnétique engendré par une sonde. Ces résultats sont obtenus en fonction du nombre de spires, du rayon de la ferrite et du fil souhaité, de la distance verticale et horizontale entre les spires, du coefficient de perméabilité relative de la ferrite et du courant d'excitation. L'inductance de la sonde est alors calculée en fonction de ces paramètres. L'optimisation du diamètre de la

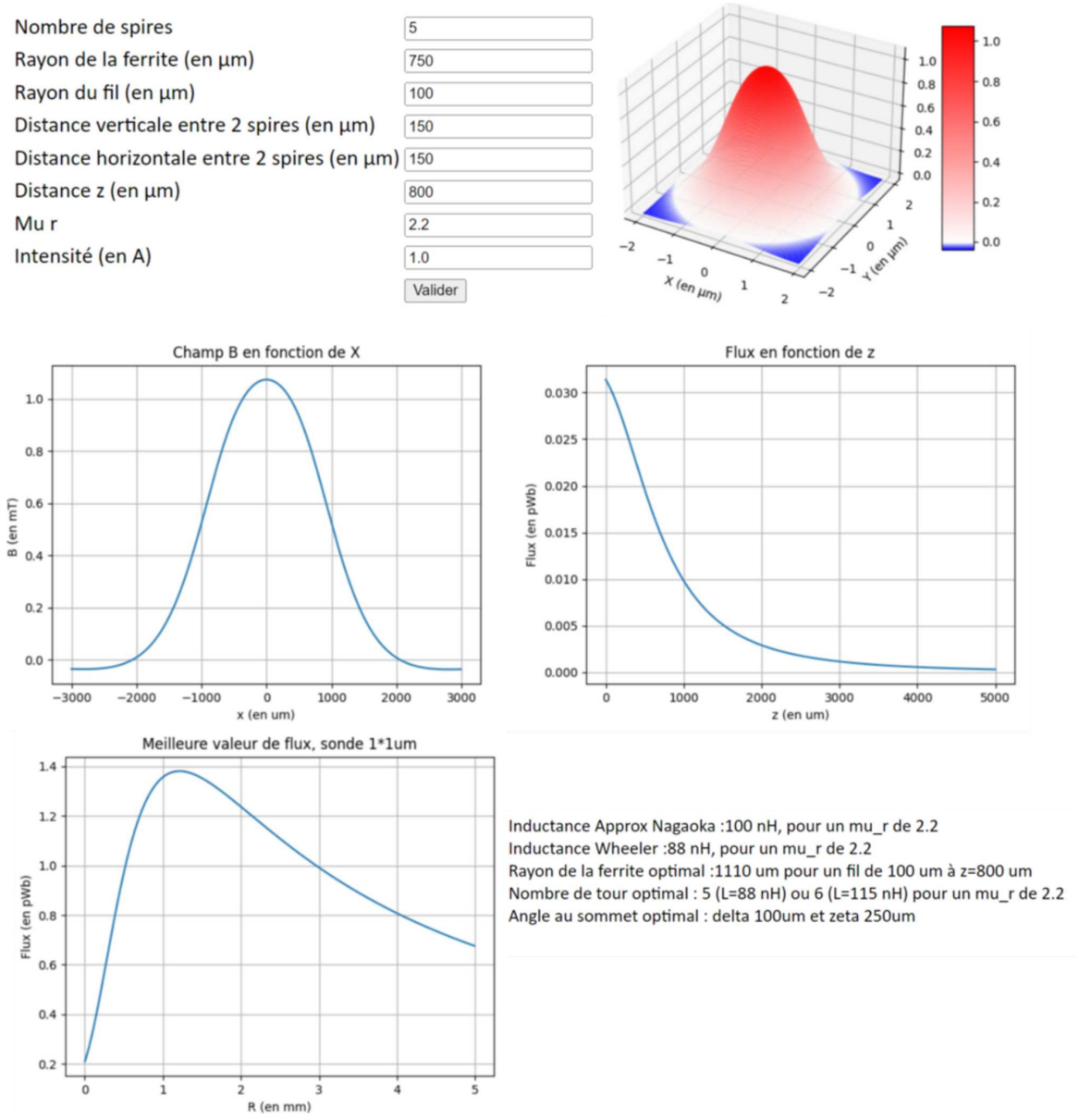



FIGURE 2.84 – Interface pour le paramétrage des sondes d'injection.

ferrite, du nombre de spires et de l'angle au sommet maximise le champ magnétique à une distance z donnée.

Par exemple, si l'on souhaite réaliser une injection sur une cible dont la distance entre le haut du boîtier et la puce est de 800 µm, il est plus adapté d'utiliser une sonde avec 5 tours de fil de diamètre 200 µm sur une ferrite de diamètre 2000 µm taillée de forme conique ayant une distance interspire verticale de 100 µm et horizontale de 250 µm. L'inductance de cette sonde est proche de 100 nH, et l'angle au sommet maximise l'intensité du champ $\vec{B}$ engendré à une distance de 800 µm.

### 2.6.2 Nouvelles géométries de sonde

Il a été montré plus haut qu'une géométrie de ferrite de forme conique était plus efficace pour réaliser des injections de fautes qu'une géométrie cylindrique simple. Avec Polaris, il est possible d'envisager de nouvelles géométries de sondes et de simuler rapidement leurs effets et leurs intérêts éventuels.

#### Superposition de spires

La tension maximale du générateur est un des paramètres limitant l'efficacité des bancs d'injections. En réalisant des sondes plus compactes, c'est-à-dire en réduisant la hauteur d'une bobine, il est possible d'augmenter l'intensité des perturbations engendrées pour une même tension source. Pour cela, nous proposons ici une nouvelle géométrie de sondes consistant à superposer les spires d'une bobine comme présenté sur la figure 2.85.

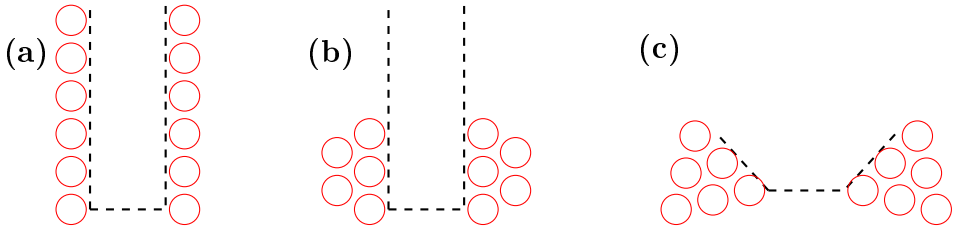



FIGURE 2.85 – Schéma d'une sonde cylindrique **(a)**, à couches cylindriques superposées **(b)** et conique avec une double superposition **(c)**.

Les équations du champ $\vec{B}$ s'obtiennent de façon analogue aux parties précédentes. La figure 2.86 est la représentation du champ $\vec{B}$ en 3 dimensions projetée sur le plan XZ pour différents types de géométries. Le diamètre de la spire en z=0 µm vaut 850 µm et les spires sont jointives avec un fil de diamètre 200 µm.

Le champ $\vec{B}$ engendré par la sonde avec 5 spires superposées est réparti de façon uniforme de part et d'autre de la bobine, c'est-à-dire de l'axe z, tandis que celui produit par la sonde avec 5 spires coniques superposées n'observe pas cette symétrie selon l'axe z. Ces figures ne montrent pas l'influence de la géométrique

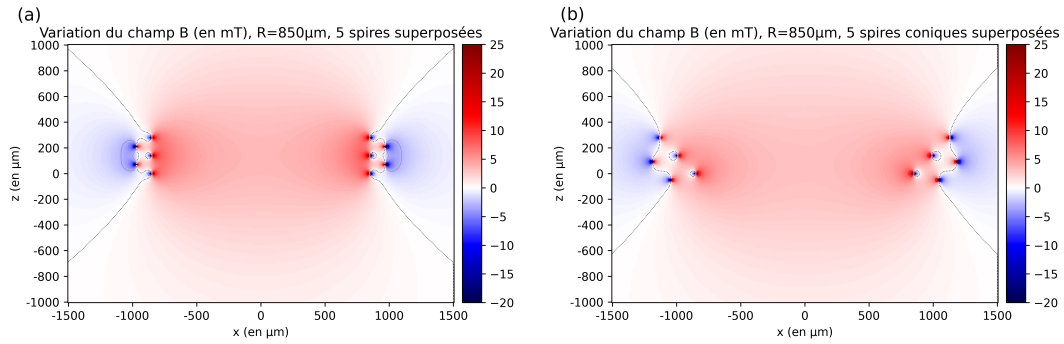



FIGURE 2.86 – Représentation du champ $\vec{B}$ pour des sondes de 5 spires cylindriques **(a)** et coniques **(b)** avec superposition.

conique sur l'étalement et l'intensité du champ $\vec{B}$ engendré. Les outils de simulation représentent, sur la figure 2.87, l'effet des sondes coniques et cylindriques à une distance z=800 µm de la spire la plus basse. La spire la plus étroite a un rayon 1600 µm et l'ensemble des spires sont jointives. Le courant est considéré comme constant et égal à 1 A.

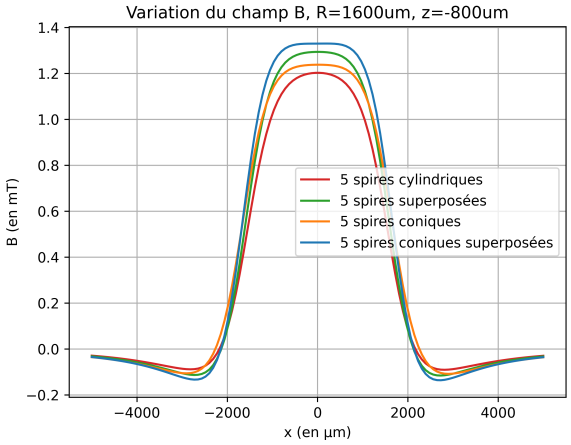



FIGURE 2.87 – Étalement du champ $\vec{B}$ lors de superpositions des spires.

L'intensité des champs $\vec{B}$ émis par les sondes avec des spires superposées est supérieure de 10 % à celle sans superposition. La superposition des spires augmente l'intensité du champ $\vec{B}$ engendré tout en conservant la même étendue spatiale.

Lorsque le nombre de spires est élevé, il est possible de réaliser une double superposition. Le champ $\vec{B}$ engendré par différentes sondes composées de 9 spires, avec une ferrite de diamètre 2000 µm et de diamètre de fil 200 µm est représenté sur la figure 2.88.

L'intensité du champ magnétique produit à z=250 µm avec la sonde cylindrique

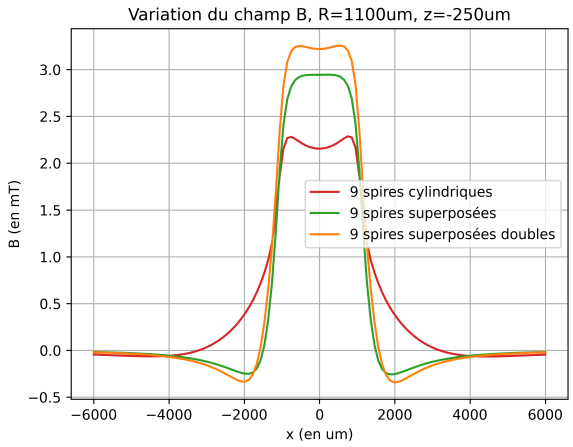



FIGURE 2.88 – Simulation du profil spatial du champ $\vec{B}$ lors de la superposition des spires pour une sonde composée de 9 spires, d'une ferrite de diamètre 2 mm et d'un fil de diamètre 200 µm.

croît de 30 % lorsque nous réalisons une superposition et de 43 % avec une double superposition. D'après les simulations, la superposition des spires est intéressante et cela est maintenant vérifié de façon expérimentale.

Les champs $\vec{B}$ émis par différentes sondes sont mesurés au moyen d'une sonde Langer RF-R 0.3-3. Les sondes sont composées de 9 spires avec une ferrite de diamètre 2000 µm et d'un fil de diamètre 200 µm. La première est cylindrique, la seconde est composée d'une superposition des spires (5 + 4 spires) et la dernière d'une double superposition de spires (4 + 3 + 2 spires). Les photographies de ces sondes et de l'ensemble de celles exploitées dans le manuscrit sont présentes en annexe. Les champs $\vec{B}$ mesurés lors d'une excitation par une impulsion de tension, réalisée depuis un générateur Tektronik AFG3102 d'amplitude 10 V, avec une durée du front montant de 5 ns et d'impulsion de 10 ns sont présentées sur la figure 2.89.

Nous constatons qu'une superposition des spires augmente l'intensité de la perturbation. Le gain est d'environ 3 % pour une superposition et 14 % pour une double superposition. Ces augmentations sont plus faibles qu'en théorie, car il est plus difficile en pratique d'obtenir un bobinage parfait.

Afin d'étudier les profils du champ magnétique créé avec ces sondes, nous mesurons les variations de champ à l'aide d'une sonde de diamètre 250 µm. Les caractéristiques de l'impulsion sont identiques à celles utilisées précédemment. Les résultats du balayage latéral des sondes sont présentés sur la figure 2.90.

Nous constatons que la superposition simple n'apporte qu'un gain limité, d'environ 2 %. En revanche, la double superposition permet de gagner 18 % de la puissance pour une étendue spatiale similaire.

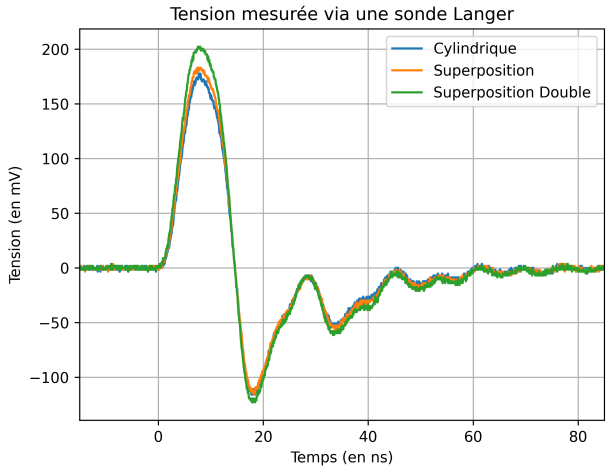



FIGURE 2.89 – Évolution du champ $\vec{B}$ lors de la superposition des spires pour une sonde composée de 9 spires, d'une ferrite de diamètre 2 mm et d'un fil de diamètre 200 µm mesurée au moyen d'une sonde Langer.

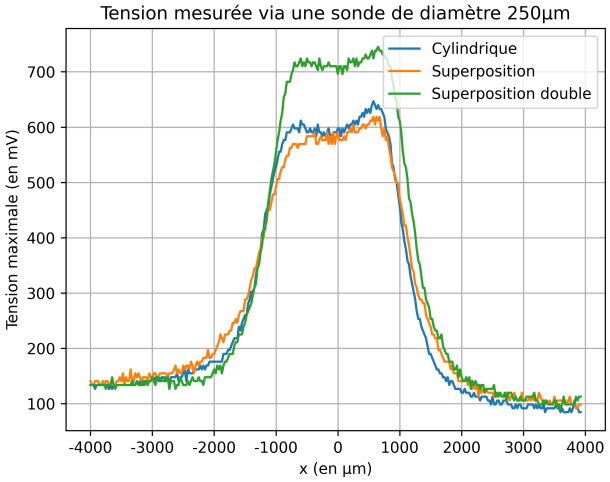



FIGURE 2.90 – Évolution du champ $\vec{B}$ lors de la superposition des spires pour une sonde composée de 9 spires, d'une ferrite de diamètre 2 mm et d'un fil de diamètre 200 µm mesurée au moyen d'une sonde de diamètre 250 µm.

Le microcontrôleur ATmega328P a servi de cible de test pour comparer l'effet des perturbations produites par différentes sondes. Lorsque l'intensité de la perturbation électromagnétique est suffisamment importante, le fonctionnement du microcontrôleur est altéré. La tension de commande minimale du générateur d'impulsion de tension permettant de réaliser des fautes sert à évaluer l'intensité des champs $\vec{B}$ produits par une sonde. La durée de l'impulsion est de 8 ns. La tension de consigne minimale du générateur d'impulsions de tension produisant des fautes est de 80 V avec une sonde cylindrique composée de 9 spires et d'un diamètre 2000 µm. Avec une sonde ayant une double superposition, des fautes apparaissent pour une consigne de 60 V. La consigne nécessaire pour obtenir des fautes avec la sonde ayant une simple superposition est similaire à celle de la sonde cylindrique. Nous pouvons constater l'effet du travail d'optimisation sur la tension de seuil d'apparition des fautes. La géométrie la plus compacte constituée de plusieurs superpositions de fils réduit le seuil des fautes d'environ 25 %.

### Sondes radiales

Si l'on poursuit l'idée de réduire la longueur du solénoïde, nous aboutissons à la superposition de toutes les spires. La représentation du champ $\vec{B}$ en 3 dimensions est projetée sur le plan XZ sur la figure 2.91.b. La sonde est composée de 5 spires, dont le rayon de la spire la plus étroite est de 850 µm, et la distance interspire $\delta$ de 200 µm. Cette simulation ne prend pas en compte la présence de la ferrite.

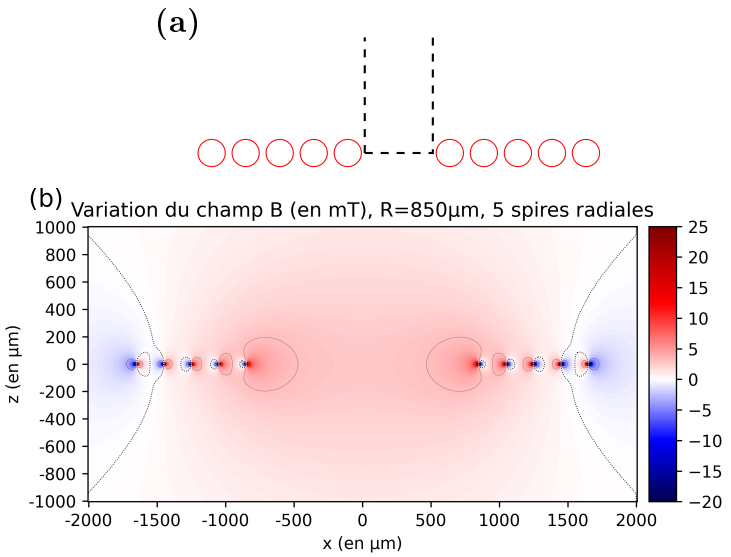



FIGURE 2.91 – Sonde radiale **(a)** et Évolution du champ $\vec{B}$ pour une sonde radiale de 5 spires **(b)**.

La figure 2.92 est une simulation spatiale des profils des champs magnétiques produits par une sonde cylindrique, une sonde avec une double superposition et une sonde radiale. Ces sondes sont composées de 9 spires de diamètre 200 µm et le rayon

de la spire la plus étroite est de 1100 µm, ce qui correspond à une sonde composée d'une tige de ferrite de diamètre 2000 µm. Le profil est réalisé pour une distance de 250 µm avec la sonde.

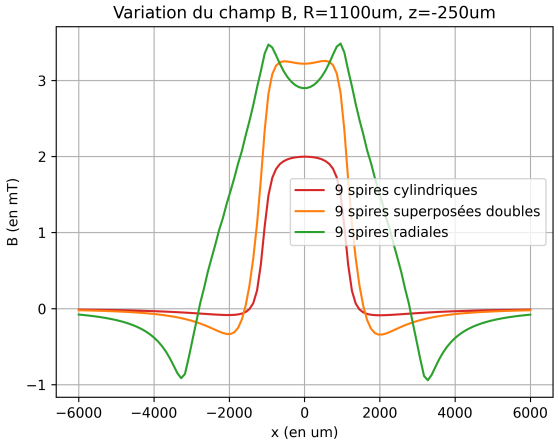



FIGURE 2.92 – Simulation du profil spatial du champ $\vec{B}$ pour différentes géométries de sondes de 9 spires.

Nous constatons que la perturbation engendrée par la sonde radiale a une étendue spatiale beaucoup plus importante que celle des sondes cylindriques. La largeur de la zone d'effet correspondant à un signal à 50 % de son maximum est de 4000 µm pour la sonde radiale contre 2100 µm et 2400 µm pour les sondes cylindriques et avec une superposition des spires. L'intensité du champ $\vec{B}$ produit est en revanche similaire à celui de la sonde avec une superposition des spires. Un compromis peut être alors de répartir les spires sur deux niveaux. La simulation d'une sonde de ce type est ajoutée à la figure précédente et représentée sur la figure 2.93.

Les caractéristiques de cette sonde, représentée en bleu, correspondent au meilleur compromis. Elle a été réalisée et une photo de la sonde est présentée sur la figure 2.94.a. Les résultats expérimentaux sont présentés pour une caractérisation avec une sonde de diamètre 250 µm sur la figure 2.94.b. Les caractéristiques de l'impulsion sont identiques à celles utilisées précédemment (impulsion produite par un GBF avec une amplitude de 10 V, avec une durée du front montant de 5 ns et d'impulsion de 10 ns).

Les résultats obtenus correspondent à ceux de la simulation. La sonde radiale engendre des perturbations plus importantes qu'une sonde de géométrie cylindrique ou comportant une double superposition. En revanche, la largeur de la zone d'effet correspondant à un signal à 50 % de son maximum est augmentée d'environ 15 % par rapport à la sonde de géométrie cylindrique.

Le microcontrôleur ATmega328P a servi de cible de test pour comparer l'effet des perturbations produites par cette sonde et celles avec les sondes avec superpositions. La tension de consigne minimale du générateur d'impulsions de tension produisant

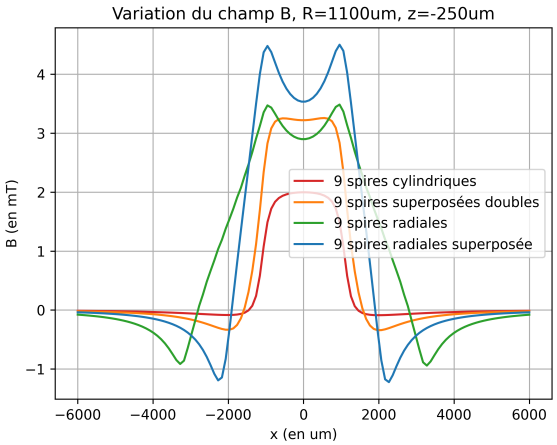



FIGURE 2.93 – Simulation du profil spatial du champ $\vec{B}$ pour différentes géométries de sondes de 9 spires.

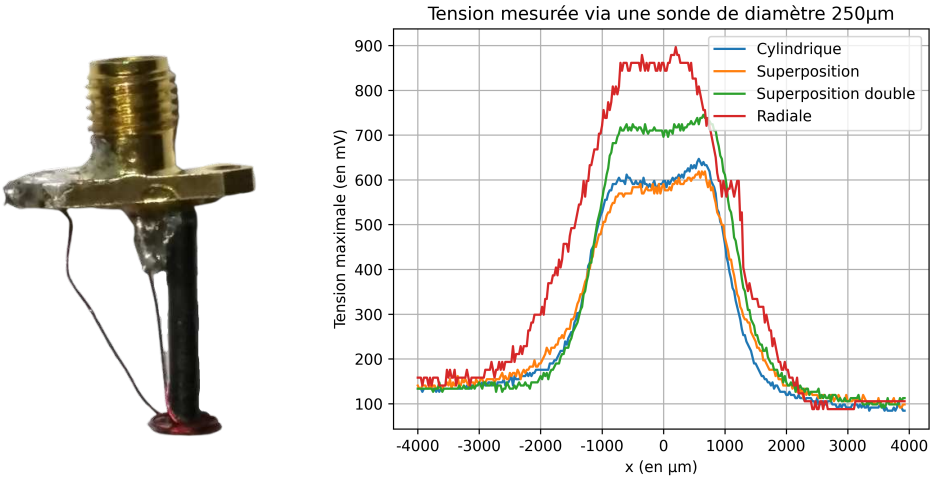



FIGURE 2.94 – Bénéfice du compactage des solénoïdes, obtenus avec une sonde composée de 9 spires, d'une ferrite de diamètre 2 mm et de fil 200 µm.

des fautes est de 80 V avec une sonde cylindrique composée de 9 spires et d'un diamètre 2000 µm. Pour la sonde radiale, la tension seuil est de 60 V. Cette valeur est inférieure à celle de la géométrie cylindrique et identique à celle avec les sondes cylindriques comportant une double superposition des fils. En revanche, l'utilisation expérimentale des sondes radiales est plus complexe. L'encombrement de la sonde étant assez important, il est difficile d'être au contact de la cible.

### Sondes ruban

La superposition des fils présente des caractéristiques intéressantes, cependant leur fabrication manuelle n'est pas aisée. Une solution pour faciliter la fabrication consiste à remplacer le fil de cuivre par un ruban de cuivre, d'épaisseur 35 µm. Trois sondes d'un diamètre de 2000 µm avec 1, 5 et 9 spires ont été réalisées et sont présentées sur la figure 2.95.

FIGURE 2.95 – Sondes composées d'un ruban de 1, 5 et 9 spires.

Les résultats expérimentaux des profils des champs magnétiques créés avec ces sondes sont présentés sur la figure 2.96. Les variations de champ $\vec{B}$ sont mesurées à l'aide d'une sonde de diamètre 250 µm. Les caractéristiques de l'impulsion sont identiques à celles utilisées précédemment.

Nous constatons que les profils des sondes sont symétriques et que leur étalement à 90 % du signal maximal est très réduit comparé à une sonde cylindrique. Les différences d'intensité de champ mesurées sont inférieures à 15 %. Les différences entre les sondes de 1, 5 et 9 spires sont relativement faibles, ce qui montre un effet d'écrantage des spires extérieures par les spires intérieures. Nous constatons que les sondes avec 5 et 9 spires sont symétriques. La localité de la sonde composée d'une seule spire est améliorée tout en conservant des valeurs de transmissions satisfaisantes.

Le microcontrôleur ATmega328P a servi de cible de test pour comparer l'effet des perturbations produites par des sondes composées de rubans de cuivre au lieu de fils de cuivre. Des sondes, composées de 9 tours autour d'une ferrite de diamètre 2000 µm, avec un ruban et un fil de cuivre, sont utilisées. Avec la sonde de 9 spires

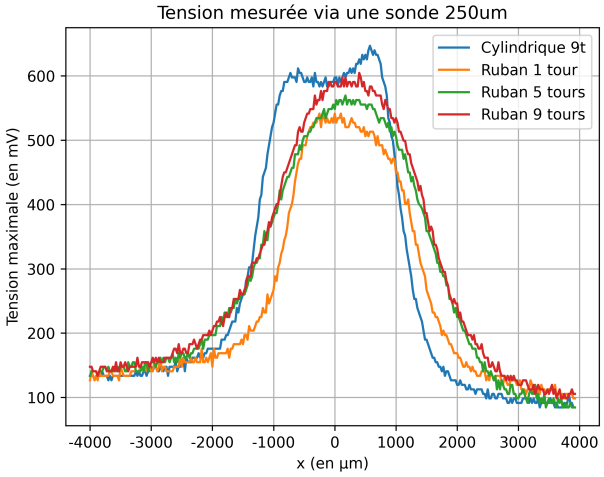



FIGURE 2.96 – Évolution du champ $\vec{B}$ lors de la superposition des spires pour des spires composées de ruban de cuivre superposé à une ferrite de diamètre 2 mm mesurée au moyen d'une sonde de diamètre 250 µm.

ruban, le seuil de tension réalisant des fautes est de 75 V tandis qu'il est de 80 V avec une sonde composée d'un fil. Les perturbations produites ont donc un effet similaire. Dans le cas des attaques par injections de fautes par perturbations électromagnétiques, ces sondes n'apportent pas d'avantages.
Par ailleurs, un autre intérêt d'utiliser ce type de sonde est que leurs inductances sont 20 % plus faibles que celles des sondes réalisées avec un fil de cuivre de 200 µm.

### Sondes chemisées

Les géométries des sondes précédentes ont permis d'améliorer la puissance transmise par une sonde. Cependant, nous pouvons également chercher à réduire leur étendue latérale. Pour cela, il est possible d'envelopper la sonde dans une couche de ferrite (MHLL12060) et d'y ajouter éventuellement une fine couche de cuivre (d'épaisseur 35 µm). Ces sondes sont présentées sur la figure 2.97.

Les résultats expérimentaux des profils des champs magnétiques créés avec ces sondes sont présentés sur la figure 2.98. Les variations de champ $\vec{B}$ sont mesurées à l'aide d'une sonde de diamètre 250 µm. Les caractéristiques de l'impulsion sont identiques à celles utilisées précédemment.

L'utilisation des sondes chemisées de ferrite ou de ferrite et de cuivre réduit l'étendue latérale du champ $\vec{B}$, bien que cela nécessite d'augmenter la puissance d'injection. La largeur de la perturbation à la moitié de sa valeur maximale est de 2500 µm pour la sonde cylindrique, 2300 µm pour la sonde enveloppée avec de la ferrite et de 2100 µm pour la sonde enveloppée avec de la ferrite et du cuivre. Les pertes d'intensité de la perturbation sont de 28 % avec une chemise en ferrite et de 60 % avec l'ajout de la ferrite et du cuivre.

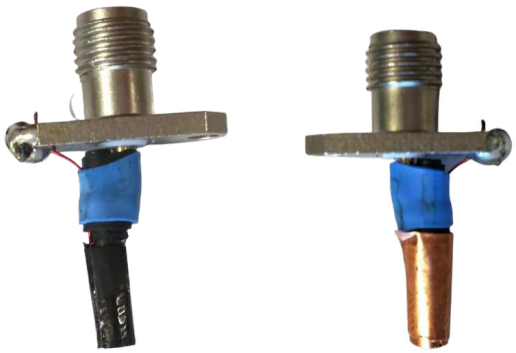


FIGURE 2.97 – Photographie des sondes avec chemises de ferrite et ferrite + feuille de cuivre.

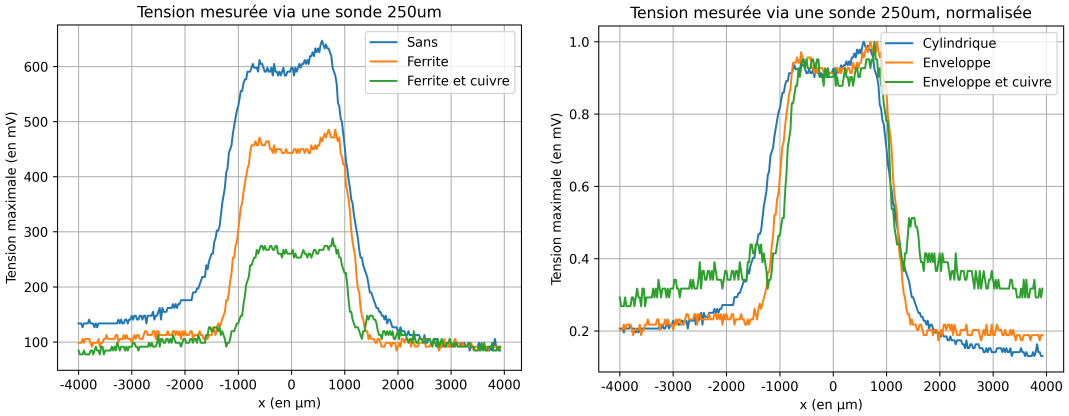



FIGURE 2.98 – Évolution du champ $\vec{B}$ lors d'un enveloppement avec des feuilles de ferrite et de cuivre pour des spires composées fils de diamètre 200 µm autour de ferrites de diamètre 1500 µm mesurée au moyen d'une sonde de diamètre 250 µm.

### Sondes à champ projeté à travers le circuit intégré

Les lignes de champ magnétique circulant au centre de la ferrite doivent se refermer en circulant à l'extérieur de la bobine. La cible positionnée à l'extrémité de la sonde est donc perturbée par une partie du champ magnétique sortant de la ferrite. Afin de maximiser la transmission vers la cible, nous forçons les lignes de champ à se projeter plus loin avant de reboucler en traversant la cible. Le flux est alors maximisé au niveau de la cible.

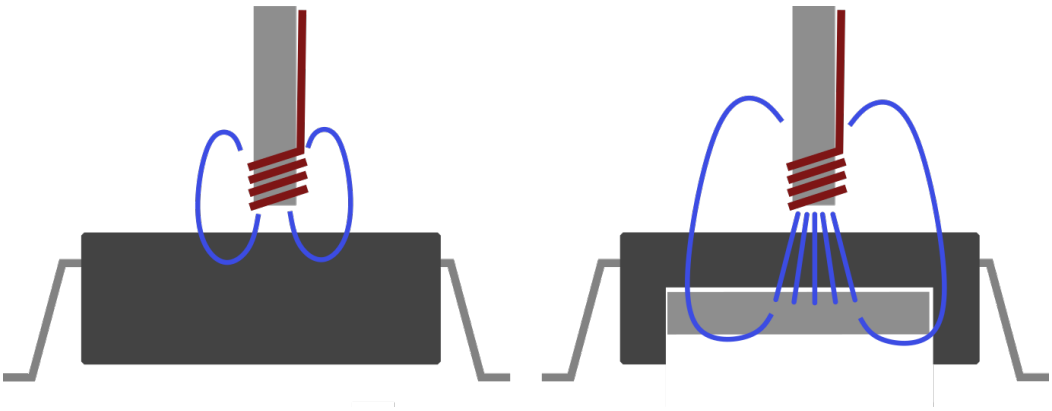


FIGURE 2.99 – Schéma de principe d'une sonde à champ projeté à travers le circuit cible au moyen d'une ferrite disposée sous le circuit cible.

Ce principe a été mis en œuvre sur une cible ATmega328P dont la partie arrière a été décapsulée et recouvert d'une couche horizontale de feuille de ferrite de type MHLL12060. Une représentation est réalisée en figure 2.99. Une sonde conique, dite de référence, d'un diamètre de ferrite 1500 µm et composée de 10 spires est utilisée pour réaliser les injections de fautes. La tension de commande minimale du générateur d'impulsions de tension réalisant des fautes sans feuille de ferrite est de 62 V, tandis qu'elle est abaissée à 57 V avec la présence de cette ferrite. Le guidage des lignes de champ à travers le circuit apporte donc une diminution de la tension seuil réalisant des fautes. Nous constatons une réduction de 10 % sur la tension de consigne du générateur. Cette technique peut être additionnée à l'utilisation de sondes plus performantes minimisant encore les tensions seuils de fautes.

L'ajout d'un aimant permanent sur la face arrière guide les lignes de champ, cependant l'inductance de la sonde est très fortement réduite en raison de la saturation de la ferrite. Des tests ont été réalisés avec des sondes à fortes inductances, c'est-à-dire avec un nombre de spires important. Cependant, le seuil de fautes sur un ATmega328P n'a pas été amélioré significativement.

### 2.6.3 Diamètre du fil

L'ensemble des sondes réalisées avec des ferrites d'un diamètre supérieur à 1 mm l'ont été avec des fils d'un diamètre de 200 µm. La figure 2.100 présente des sondes avec différents diamètres de fil. Des ferrites de type 78 et d'un diamètre 1500 µm sont utilisées.

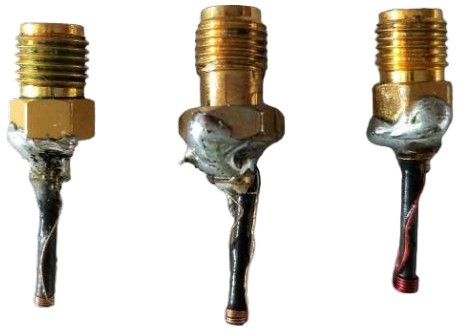


FIGURE 2.100 – Sondes avec diamètres de fil de 100 µm, 150 µm et 200 µm.

Le fil de diamètre 40 µm est très cassant, ce qui rend la conception et l'utilisation difficile. En revanche, les fils de diamètre supérieur à 100 µm sont suffisamment résistants. Ils permettent aussi plus facilement de réaliser les enroulements à l'extrémité de la ferrite. Comme présenté au paragraphe 2.3.4, la diminution du diamètre du fil augmente sa résistance linéaire, mais les effets sont négligeables pour une utilisation en injection de fautes.

Les résultats expérimentaux des profils des champs magnétiques créés avec ces sondes sont présentés sur la figure 2.101. Les variations de champ $\vec{B}$ sont mesurées à l'aide d'une sonde d'écoute de diamètre 250 µm. Les caractéristiques de l'impulsion sont identiques à celles utilisées précédemment.

La tension maximale mesurée par la sonde lors de la génération d'un champ $\vec{B}$ est de 950 mV pour les sondes avec un diamètre de fil de 100 et 150 µm, et de 900 mV pour un diamètre de fil de 200 µm. Nous constatons que la sonde avec un diamètre de fil de 100 µm est légèrement plus locale. Ce diamètre de fil paraît être le meilleur compromis entre facilité de réalisation, d'utilisation et efficacité d'injection.

En procédant à un test sur microcontrôleur ATmega328P, la tension seuil produisant des fautes est de 55 V avec le fil de 200 µm tout comme avec le fil de 100 µm. Le diamètre de fil n'a pas d'effet sur la tension seuil de fautes.

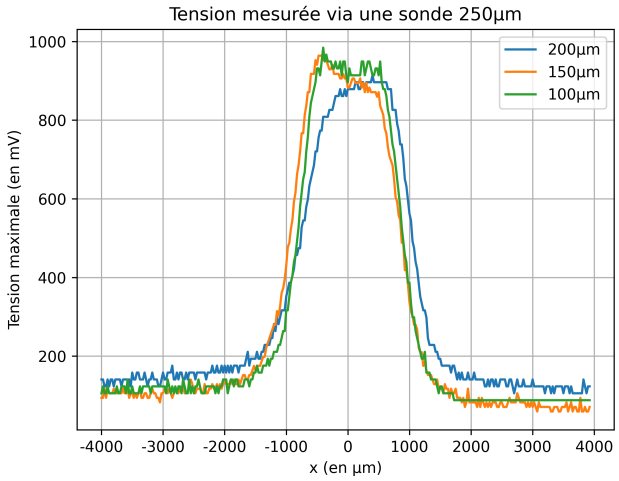



FIGURE 2.101 – Influence du diamètre de fil.

### 2.6.4 Utilisation des nouvelles sondes en écoute électromagnétique

Les travaux ont mené à une meilleure caractérisation des sondes pour les injections de fautes. Ils peuvent également s'appliquer aux sondes d'écoute pour les attaques par canaux auxiliaires. Lors du fonctionnement d'un circuit, les portes logiques le constituant émettent des émanations électromagnétiques lors de leurs commutations. Ces changements d'état de portes sont liés aux informations qu'elles transmettent. Ainsi une mesure du champ magnétique émis pendant l'exécution d'un algorithme permet d'en déduire les données manipulées.

La technique utilisée est celle des analyses du courant par corrélation (CPA) qui consiste à trouver une relation entre les émissions mesurées et le comportement au niveau logique. Cette attaque nécessite la connaissance des opérations effectuées par l'algorithme ainsi que des messages d'entrée (les textes en clair dans le cas d'un chiffrement) [27].

Dans ces travaux, nous cherchons à trouver la clé secrète, composée de 16 octets, d'un algorithme AES. Pour chaque hypothèse de sous-clé, c'est-à-dire d'un octet de la clé secrète, nous établissons des prédictions de consommation. L'analyse est menée sur la sortie du bloc *SubBytes* lors du premier tour de l'AES. Nous calculons les 256 valeurs possibles de sous-clé pour chacun des textes clairs chiffrés pendant la campagne. Le poids de Hamming de chacune des valeurs obtenues est calculé, puis nous réalisons le calcul de la corrélation de Pearson entre ces différents poids de Hamming et les signaux acquis. Lorsque l'hypothèse de sous-clé est correcte, les consommations prédites corrèlent avec le signal acquis.

Dans notre cas, nous vérifions que ces sondes présentent un intérêt pour les écoutes side-channel, en effectuant des acquisitions et attaques CPA sur un AES logiciel

exécuté par un ATmega328P fonctionnant à 16 MHz. Pour trouver la clé secrète de chiffrement, une campagne d'acquisitions est réalisée avec une sonde Langer RF-B 3, utilisée couramment au sein du laboratoire pour faire ce type de mesures. Nous utilisons également une sonde Langer LF-U 2.5 et une sonde expérimentale constituée de 5 spires de fil de diamètre 100 µm et de ferrite de diamètre 1,5 mm.

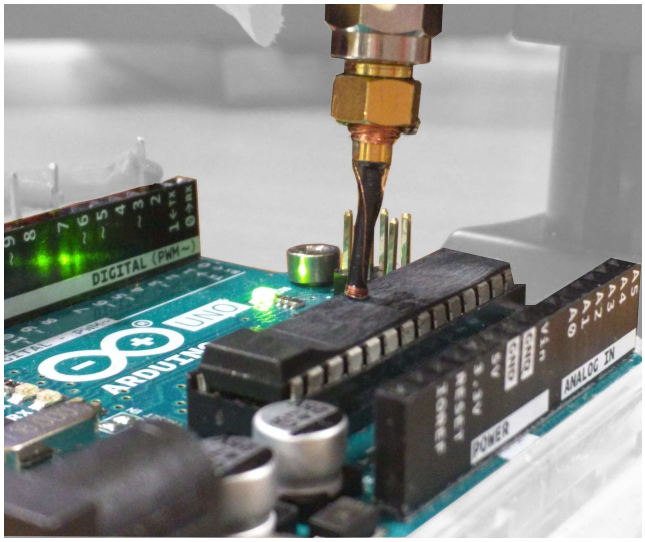



FIGURE 2.102 – Banc d'écoute side-channel avec une sonde expérimentale.

La figure 2.103 montre la corrélation de chaque candidat de clé en fonction du nombre d'acquisitions analysées. Chaque courbe représente l'évolution de la corrélation d'un octet avec les données expérimentales. Initialement, chaque octet a une corrélation de 1, mais celle-ci doit diminuer pour l'ensemble des clés candidates sauf pour la clé correcte. Les résultats de l'attaque CPA sont présentés pour un octet de la clé, l'octet 0. L'évolution de la corrélation d'un octet est représentée pour la sonde Langer sur la figure 2.103.a, la Langer LF sur la figure 2.103.b et pour la sonde d'injection expérimentale sur la figure 2.103.c.

En utilisant une attaque CPA, 50 acquisitions sont nécessaires pour retrouver tous les octets de la clé de chiffrement avec les sondes Langer, et 35 sont nécessaires avec la sonde expérimentale. Cela signifie que l'utilisation de ces sondes est envisageable avec une efficacité comparable à celle des sondes commerciales. L'étude réalisée sur les sondes pour l'injection est donc aussi valable pour les sondes d'écoute.

Nous expliquons cette amélioration des résultats par des bandes passantes différentes entre les sondes. Dans le cas de la sonde Langer RF, la sensibilité est constante entre 50 MHz et 3 GHz et entre 100 kHz et 50 MHz pour la sonde Langer LF. Dans le cas de la sonde d'injection expérimentale, la sensibilité est maximale entre 5 et 30 MHz. Ceci est vérifié avec un analyseur de réseau vectoriel NanoVNA. Les signaux de fréquence supérieure à 50 MHz sont atténués de 5 dB par rapport à ceux à 15 MHz. Ce filtrage limite les perturbations dues à des signaux qui ne proviennent pas de fuites électromagnétiques. Par ailleurs, les sondes de type Langer LF et RF ont des dia-

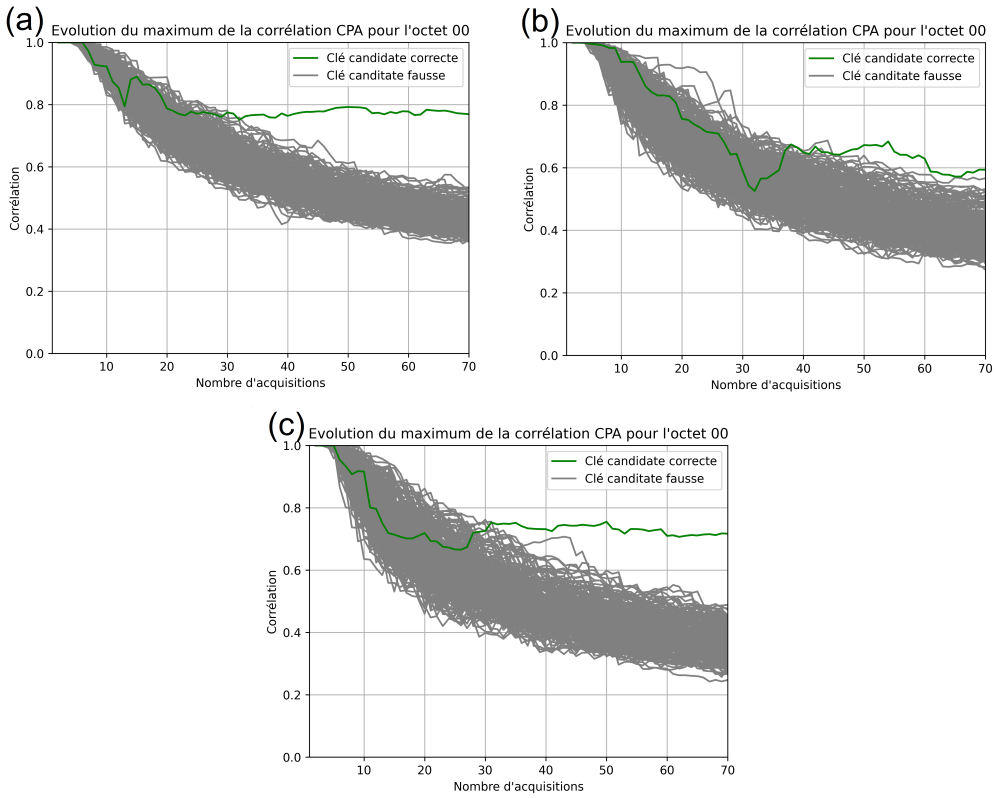



FIGURE 2.103 – Résultats de l'attaque CPA pour l'octet 0x00 avec une sonde Langer RF **(a)**, LF **(b)** et d'injection expérimentale **(c)**.

mètres minimaux de 4 mm. Les sondes expérimentales réduisent l'étendue spatiale de l'écoute tout en conservant des caractéristiques idéales pour les écoutes électromagnétiques. Cette réduction de diamètre atténue le bruit provenant d'émissions parasites du microcontrôleur.

## 2.7 Conclusion

Ce chapitre a démontré que les injections électromagnétiques sont de natures inductives. Afin d'évaluer les champs $\vec{B}$ engendrés, différents essais utilisant des capteurs composés de sondes d'écoute et de circuits réels (microcontrôleurs et FPGA) ont été réalisés.

À partir de la loi de Biot et Savart, le diagramme de rayonnement et la décroissance du champ magnétique engendré par une sonde ont été modélisés. Cette étude a été réalisée avec des sondes constituées d'un petit nombre de spires agencées de diverses façons : cylindriques et coniques. Les géométries cylindriques et coniques ont été envisagées avec une ou plusieurs couches et un espace interspire variable. Les simulations montrent qu'il faut privilégier la compacité des spires et qu'il faut les disposer à l'extrémité d'une tige. Les résultats des simulations ont pu être vérifiés

expérimentalement au moyen d'une sonde de petite taille, réalisant un échantillonnage spatial du flux magnétique engendrée par une sonde de plus grande taille. Ils ont également pu être vérifiés au moyen d'un capteur de mesure de tension interne réalisé avec un oscillateur en anneau programmé directement dans un FPGA.

Une étude dynamique du comportement des sondes et du générateur a permis de déterminer leurs circuits électriques équivalents, et de constater une discontinuité de l'impédance de sortie des générateurs d'impulsions de tension de marque Avtech. L'influence de l'inductance et de la résistance des sondes a été étudiée.

Une analyse théorique et expérimentale de ferrites composées de différents alliages a été menée. Malgré des différences de perméabilités relatives importantes entre deux ferrites, leurs caractéristiques pour réaliser des perturbations électromagnétiques restent proches. Les ferrites de marque Fair-rite et de référence 78 sont cependant plus adaptées à l'utilisation dans un banc d'injection de fautes.

La génération d'une perturbation électromagnétique avec les générateurs d'impulsions de tension de marque Avtech engendre des phénomènes d'oscillations de la tension interne des cibles, tel que constaté avec le capteur embarqué sur un FPGA. L'estimation de l'impédance d'une sonde d'injection électromagnétique a montré qu'elle était désadaptée avec celle de sortie des générateurs. La réduction des phénomènes d'oscillations n'a pas été possible en réalisant des adaptations d'impédance. La discontinuité de l'impédance de sortie de l'Avtech et les différentes manipulations ont mis en évidence que ces dispositifs ne sont pas utilisables dans le cas de l'injection de fautes par perturbations électromagnétiques. Un montage suppresseur des rebonds sans adaptation d'impédance a été testé sur plusieurs cibles et permet de supprimer l'impulsion négative tout en conservant l'impulsion positive.

Enfin, la simulation de sondes avec géométries alternatives a été réalisée. Elles augmentent l'intensité des champs $\vec{B}$ produits par une sonde, autorisant la diminution de la tension de consigne des générateurs d'impulsions tout en conservant l'efficacité des injections. La localité spatiale des sondes a aussi pu être réduite. Les sondes conçues ont ainsi des caractéristiques pour l'injection de fautes plus intéressantes que celles de l'état de l'art.

L'ensemble de ces travaux définissent des préconisations sur la conception des sondes. La présence d'une ferrite est nécessaire pour maximiser le flux magnétique et éviter d'utiliser des tensions trop importantes. Une ferrite de petit diamètre limite la portée du champ magnétique engendré par la sonde à une distance z fixée. Le rayon R de la sonde doit être choisi avantageusement lorsque l'on connaît la hauteur à laquelle la sonde doit être positionnée au-dessus de la cible. Une règle simple préconise que le rayon soit voisin de $\sqrt{2}z$ pour une sonde monospire. En outre, la ferrite peut être taillée en pointe selon un certain angle au sommet afin de réduire encore la localité spatiale, par exemple entre 90° et 120°. Une sonde type se compose de

plusieurs spires produisant une inductance qui devrait rester inférieure à 100 nH afin de conserver une bonne localité temporelle. Ces spires sont de préférence jointives afin de maximiser l'intensité du champ. La ferrite du type Fair-Rite 78 fournit les meilleurs résultats pour des injections de fautes. Le fil utilisé doit être le plus fin possible, ainsi des diamètres entre 40 µm et 100 µm sont idéaux.

Afin d'améliorer les caractéristiques des sondes, un outil a été créé pour calculer les paramètres optimaux. Par exemple, si l'on souhaite créer une perturbation sur une cible dont la distance entre le haut du boîtier et la puce est de 500 µm, une sonde avec 5 tours de fil de diamètre 100 µm sur une ferrite de diamètre 1500 µm taillée en forme conique, ayant une distance interspire verticale de 200 µm et horizontale de 200 µm, est la plus adaptée.

Ce chapitre a donc proposé des améliorations des sondes et générateurs afin d'optimiser les perturbations électromagnétiques. Ces résultats vont ainsi servir à perturber le fonctionnement de cibles plus complexes, tels que des systèmes sur puce.

# Chapitre 3 : Injections de fautes par perturbations électromagnétiques sur cibles de type System On a Chip

Dans ce chapitre, nous présentons une méthode pour réussir des injections de fautes par perturbations électromagnétiques sur les cibles complexes de type System On a Chip. Nous proposons ensuite une modélisation des fautes engendrées, puis nous envisageons une exploitation de ces perturbations. Une étude au niveau microarchitectural propose des pistes de compréhension des mécanismes provoquant les fautes, allégeant alors les conditions expérimentales.

## Sommaire du chapitre

## 3.1 Identification d'une vulnérabilité physique

La mise en évidence de fautes par perturbations électromagnétiques sur cibles de type System On a Chip est plus complexe que sur microcontrôleurs. Nous commençons par définir les spécifications de la cible utilisée dans ce chapitre, puis nous proposons une méthode pour identifier une vulnérabilité physique.

### 3.1.1 Cible

La cible de test est une puce de type System On a Chip embarquant 4 cœurs ARM Cortex A53. Ce composant complexe embarque sur le même circuit intégré un processeur (CPU), de la mémoire et des périphériques d'entrées/sorties. Cette puce est présente sur une carte de développement pour plateforme mobile. La largeur de bus est de 64 bits et la fréquence de fonctionnement est réglable entre 200 MHz et 1.2 GHz. Le jeu d'instructions est aarch64. Ce processeur est présent sur une centaine de types de téléphones d'entrée/milieu de gamme des années 2015/2016. La technologie est CMOS 28 nm, soit une dizaine de fois inférieure à celle du microcontrôleur utilisé pour les essais décrits dans le chapitre 2.

Ce type de SoC est généralement utilisé avec un système d'exploitation Android, cependant afin de mieux maîtriser la couche logicielle, un système Linux Yocto [107] a été installé. La version du noyau Linux utilisé est la 4.14 et celle de Yocto est Sumo.

Le SoC n'utilise pas la technologie Package-on-Package (PoP), ce qui signifie que la mémoire DRAM n'est pas au-dessus des CPUs, mais implantée ailleurs sur la carte. La puce est *flip chip*, ainsi la face arrière est accessible telle que présentée dans la figure 3.1.

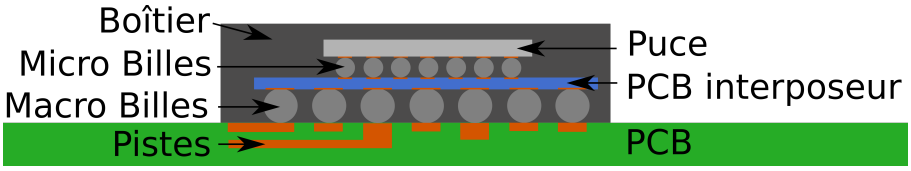



FIGURE 3.1 – Coupe du boîtier de la puce étudiée.

Les pistes du circuit imprimé sont connectées via une matrice de billes (Ball Grid Array - BGA) à un second circuit imprimé interne au boîtier. Une seconde matrice de billes fait le contact avec le circuit intégré.

La sonde d'injection électromagnétique peut donc être positionnée directement au-dessus des CPUs et à faible distance. Les premières cibles ont été décapsulées, cependant différents essais ont montré qu'il n'est pas nécessaire d'enlever le package plastique de la puce ou de modifier la carte pour réaliser les injections de fautes. La synchronisation de l'impulsion électromagnétique avec le code sous attaque est réalisée au moyen d'un signal marquant le début de son exécution et accessible via une sortie GPIO de la carte de développement. Une carte d'adaptation de tension est

présente pour convertir la tension de sortie du GPIO de 1.8V à 5V, tension nécessaire pour déclencher le générateur d'impulsions de tension Avtech. Un Raspberry Pi est utilisé pour communiquer avec le SoC via un premier UART pour la console de contrôle et via un second UART pour les données. Le premier UART peut, par exemple, servir au démarrage d'un code de test et à l'initialisation de ses paramètres, puis le second déclenchera son exécution et permettra d'en récupérer ses valeurs de sortie.

### 3.1.2 Méthode

Induire des fautes sur un SoC semble plus compliqué que sur microcontrôleur pour différentes raisons. Tout d'abord, le nœud technologique étant plus petit, les cartographies spatiales doivent être réalisées avec une plus grande résolution et avec une sonde électromagnétique de petit diamètre. De plus, la taille de la puce ($55\,mm^2$ pour notre cible) est plus grande que celle des microcontrôleurs (de l'ordre d'une dizaine de $mm^2$). Cela ralentit donc la recherche et l'identification des positions spatiales permettant l'injection de fautes. À cause de la vitesse de fonctionnement plus élevée, la période d'horloge est aussi plus courte ce qui demande d'augmenter la résolution temporelle des cartographies. Par ailleurs, de nombreuses sources de désynchronisation sont présentes. Enfin, le champ $\vec{B}$ nécessaire pour injecter des fautes s'est révélé plus important, ce qui demande des équipements plus puissants. Les temps de démarrage et de chargement d'un système d'exploitation sur SoC sont aussi plus longs ce qui rallonge les campagnes de tests.

Nous montrons ci-après comment identifier une vulnérabilité physique. La première partie de notre méthodologie est d'apprendre à injecter des fautes dans le SoC ciblé. Pour cette partie, un code de test simple détermine 3 paramètres importants : le temps, la position de la sonde et l'intensité de l'injection. La position et l'intensité de la perturbation sont liées, cela signifie que deux défis sont à relever : l'identification de l'instant et de la position d'injection.

#### Identification de l'instant temporel de l'injection

La cible étudiée étant complexe, nous forçons sa fréquence de fonctionnement à 1.2 GHz. Sinon, la fréquence d'horloge pourrait changer de façon aléatoire, ce qui modifierait le délai entre le déclenchement du signal de synchronisation et l'instruction visée. Ceci améliore la répétabilité et facilite l'interprétation des fautes obtenues.

Concernant le code de test, il doit être assez long (300 ns), afin de limiter les contraintes de synchronisation temporelles. Cela offre une plage temporelle suffisamment longue et supérieure à la gigue temporelle. Nous sommes alors certains de réussir à synchroniser une perturbation électromagnétique avec le code en cours d'exécution. Sur ce dernier, nous faisons en sorte qu'il soit possible de cibler n'importe laquelle de ses instructions. Ce code consiste en une série de soustractions

unitaires à partir d'une valeur initiale passée successivement à dix registres et répétée 32 fois, comme présenté sur le code source 3.1. L'instruction assembleur SUB soustrait à un registre une valeur immédiate et stocke le résultat dans un autre registre. Afin de déterminer l'effet des fautes sur les registres plutôt que des altérations du *control flow* de la boucle, qui sont plus difficiles à interpréter, il n'y a pas de boucle dans le code de test. La répétition de la séquence de 10 soustractions est spécifiée au compilateur par une directive PRAGMA, permettant au précompilateur C de réaliser la répétition.

```
//Initialisation
mov x19, #0x55555555    //r0 = 0x55555555
...
mov x27, #0x55555555    //r8 = 0x55555555
mov x28, #0x170          //r9 = 0x170
//Sequence suivante repetee 32 fois
sub x19, x28, #0x1      //r0 = r9 - 1
sub x20, x19, #0x1      //r1 = r0 - 1
sub x21, x20, #0x1      //r2 = r3 - 1
...
sub x28, x27, #0x1      //r9 = r8 - 1
```

Code 3.1 – Code de test avec dépendance de données.

Avant l'exécution du code de test, les registres sont initialisés à la valeur 0X5555 5555 afin d'être toujours dans les mêmes conditions initiales. Le registre X28 est initialisé à la valeur 0x170. En fin d'expérience, les 10 registres 64 bits, de X19 à X28 sont transférés en mémoire afin d'être relus. La signature électromagnétique du code testé peut être identifiée afin de déterminer le délai entre la commutation du signal de synchronisation et le déclenchement de l'impulsion de tension pour une injection efficace. Ce n'est pas obligatoire, mais pour gagner du temps, une analyse électromagnétique simple (SPA) peut être utilisée. Cela consiste à enregistrer une image de l'activité de la cible à travers ses émissions électromagnétiques telle que présentée sur la figure 3.2. La capture est effectuée à l'aide d'une sonde électromagnétique passive connectée à un oscilloscope. Dans le cas de cette manipulation, l'injection électromagnétique pendant l'écoute est difficilement réalisable car elle peut endommager le système d'acquisition.

Nous observons sur la figure 3.2, en couleur verte, la trace électromagnétique capturée via une sonde positionnée à proximité du processeur. Le déclenchement de l'acquisition est réalisé en utilisant un trigger produit par un GPIO de la carte de développement, représenté en couleur bleue. Il est déclenché, des instructions No Opérations sont exécutées, suivi du code de test et d'autres NOP, puis finalement le trigger est abaissé. Les instructions NOP sont des instructions nulles, n'effectuant aucune action. Cela isole le code testé, ce qui facilite également sa visualisation dans une capture électromagnétique temporelle. Les émissions électromagnétiques

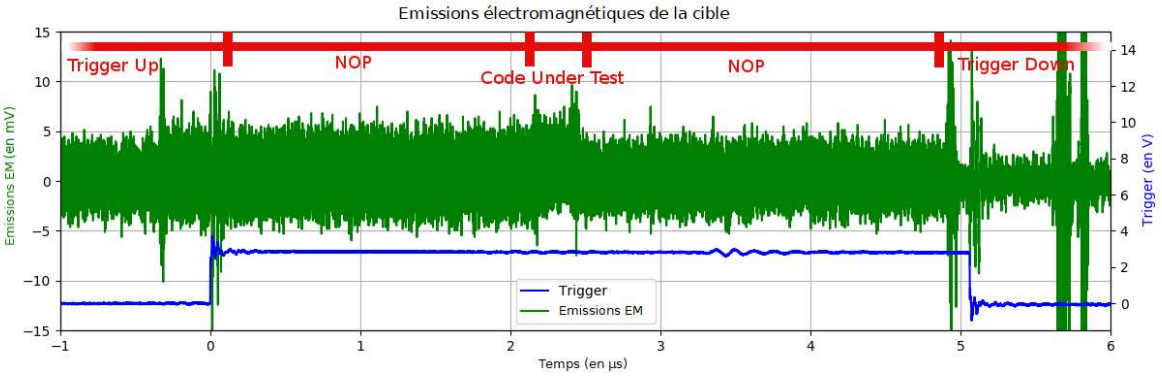



FIGURE 3.2 – Identification du délai via analyse électromagnétique simple (SEMA), sans impulsion électromagnétique.

produites par le code de test sont observées 2.1 µs après la levée du trigger, durent environ 300 ns et ont une gigue de 50 ns.

La vérification de la présence d'une faute se fait lors de la relecture des registres. Pour connaître l'instant de l'injection, il est nécessaire de connaître le moment où est exécuté le code de test. Pour cela, le délai entre la levée du trigger et l'exécution du code de test est relevé via la SEMA. Ensuite, nous recherchons par dichotomie le délai de tir du générateur d'impulsion de tension rapprochant le début de la perturbation avec la valeur précédemment notée. Afin de visualiser le début de la perturbation, une trace de la perturbation électromagnétique est capturée en réalisant une bobine autour du câble reliant le générateur à la sonde d'attaque.

Dans un premier temps nous souhaitons perturber l'une des 300 instructions du code de test. La largeur de la plage d'injection est alors de 250 ns. La contrainte temporelle est donc assez limitée, ce qui permet de se concentrer sur le positionnement fin de la sonde. L'étape suivante consiste à identifier tous les emplacements qui permettent d'injecter des fautes dans la cible.

### Identification des zones de vulnérabilités

L'injection électromagnétique est locale, ce qui signifie que la sonde doit être positionnée au-dessus du composant ciblé. Pour trouver les emplacements efficaces pour l'injection de fautes, il est plus facile de conserver des paramètres identiques tout au long d'une campagne. Pour cela, nous avons choisi d'exécuter les programmes de test uniquement sur un seul des quatre CPUs, le CPU 3. Injecter une faute sans connaître les CPUs actifs est néanmoins possible, mais cela allonge la durée des campagnes. Un code qui n'est pas exécuté sur un CPU déterminé en changera de façon aléatoire et généralement assez lentement, c'est-à-dire après plusieurs milliers d'exécutions. Lorsque le processeur est fortement sollicité, nous avons constaté qu'un code consommant peu de ressources est déplacé de façon régulière entre les 4 CPUs. Ainsi,

il est possible de réaliser un programme de stress afin de solliciter le processeur pour que le code sous attaque se déplace entre les différents CPUs.

Cette augmentation de la charge des CPUs a aussi pour effet de faire fonctionner la puce à la fréquence maximale lorsque le DVFS est activé. Le Dynamic and Voltage Frequency Scaling (DVFS) est une technique réduisant la consommation électrique en abaissant la tension d'alimentation des CPUs lorsque la fréquence diminue. Étant donné que l'injection électromagnétique repose sur la génération de forces électromotrices parasites dans les circuits, une variation de la tension d'alimentation pendant une campagne perturbe sa reproductibilité.

Un exemple de programme de stress consiste à réaliser des compressions de données en boucle comme présenté sur le code source 3.2.

```
#!/bin/bash
DATA="$(dd if=/dev/urandom bs=1024 count=4096 2>/dev/null
    | tr -d '\0')"
while true; do
    echo "$DATA" | gzip -9 >/dev/null
done
```

Code 3.2 – Code sollicitant fortement un processeur.

Grâce à ce système, le programme sous attaque est exécuté de façon uniforme sur tous les CPUs. Des expériences ont montré que la fréquence des fautes avec ce système est 4 fois plus faible que celle obtenue avec un seul CPU, ce qui correspond bien à une exécution du code répartie sur 4 CPUs.

Les tests ont été réalisés à la tension maximale des amplitudes du générateur d'impulsions de tension disponible et avec une sonde d'un diamètre de 1.5 mm pour identifier rapidement les zones sensibles. La zone est considérée comme sensible lorsqu'elle produit un gel ou un redémarrage de la carte. L'objectif est d'abord de provoquer un dysfonctionnement quelconque par effet du couplage entre la sonde et le circuit plutôt que des fautes précises. L'apparition des redémarrages est à éviter, car la durée de chargement du système d'exploitation est d'environ 20 secondes, ce qui réduit la cadence des perturbations. Nous nous assurons que la carte n'est pas gelée en envoyant des messages sur les UARTs pour vérifier que l'application de test n'a pas été fermée. S'il n'est pas possible de relancer l'application, alors l'alimentation de la carte est réinitialisée afin de redémarrer la carte.

Une fois une zone de sensibilité identifiée, la sonde est remplacée par une plus fine et l'amplitude des impulsions de tension est diminuée pour localiser le point le plus sensible, afin de rechercher d'éventuelles fautes exploitables. Une sonde composée de 5 tours de fil autour d'une ferrite de diamètre 750 µm et du matériau 78 de Fair-Rite, présentée sur la figure 3.3, est un bon compromis entre puissance et localité. La meilleure configuration a été obtenue avec une amplitude d'impulsion de 360 V. La

durée de l'impulsion de tension est de 6 ns. Il est normalement préférable de placer la sonde au plus près du silicium. Pour cela, le boîtier plastique du SoC peut être aminci, mais cela n'est pas nécessaire sur cette cible.

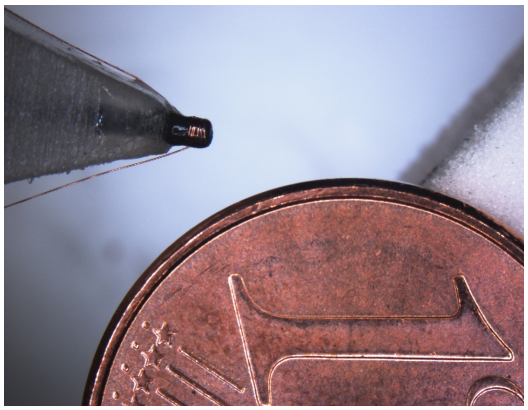


FIGURE 3.3 – Sonde d'injection électromagnétique composée d'une ferrite de diamètre 750 µm.

La zone de vulnérabilité mesure 1 mm*1 mm et la zone intéressante, caractérisée par des fautes lors de la manipulation des registres, est inférieure à 0.4 $mm^2$, soit environ 0.7 % de la surface de la puce. Cette zone est représentée en vert sur la figure 3.4.

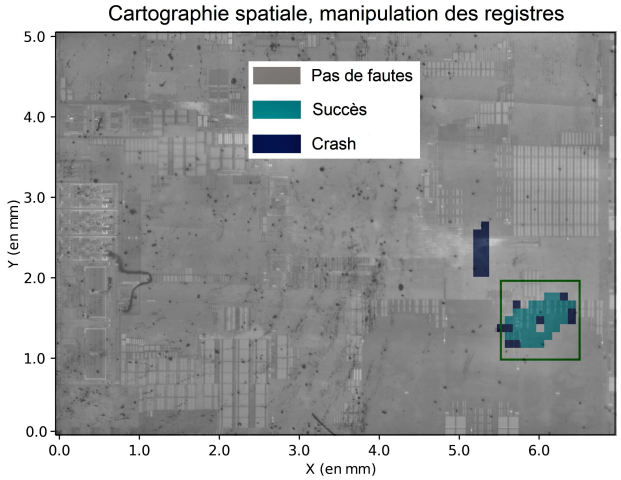



FIGURE 3.4 – Cartographie spatiale des résultats superposée à une vue infrarouge de la puce de dimensions 7.1 mm*7.8 mm.

On remarque dans le coin inférieur droit la présence de deux zones symétriques, correspondant aux 4 CPUs. La zone de sensibilité est proche d'un CPU. La meilleure configuration de position de la sonde est obtenue par itérations successives jouant sur le délai entre le trigger et l'impulsion de tension ainsi que son amplitude.

### 3.1.3 Résultats

Les résultats présentés au tableau 3.1 sont ceux d'une campagne d'injection dont le délai d'injection est incrémenté progressivement de 1600 à 1900 ns par pas de 10 ns. Les résultats sont classés par types de fautes.

| Ref. | Nombre d'occurrences | Résultats (x19, ..., x28) | Taux d'occ. | Délai (en ns) |
|---|---|---|---|---|
| A | 27287 | 39,38,37,36,35,34,33,32,31,30 | 71.0 % | 1600 - 1900 |
| B | 5314 | Perte de communication | 13.8 % | 1600 - 1900 |
| C | 4899 | 43,42,41,40,3F,3E,3D,3C,3B,3A | 12.7 % | 1650 - 1890 |
| D | 48 | 39,38,37,36,35,3E,3D,3C,3B,3A | 0.1 % | 1900 |
| E | 28 | 39,42,41,40,3F,3E,3D,3C,3B,3A | 0.1 % | 1900 |
| ... | ... | ... | ... | ... |

TABLEAU 3.1 – Résultats d'une cartographie avec le code 3.1.

Lorsqu'il n'y a pas de fautes, le résultat attendu correspond à une suite décroissante de nombres hexadécimaux de 0x39 à 0x30, comme indiqué en ligne A du tableau 3.1. C'est statistiquement le résultat obtenu le plus fréquemment avec un taux d'occurrence de 71 %. Des fermetures de l'application de test et des redémarrages de la carte créent des pertes de communication, ce qui survient dans 14 % des cas (ligne B). La ligne C correspond aux injections effectuées lors des 310 premières instructions. Les valeurs renvoyées sont plus élevées qu'en l'absence de fautes. Cela est interprétable comme au moins une instruction non exécutée, c'est-à-dire un saut d'instruction. La chaîne de 10 soustractions successives réalisée sur 10 registres est alors cassée. Les valeurs retournées sont donc plus élevées qu'attendu (augmentées de 0x0A). Ce code ne permet pas de conclure sur le nombre de sauts d'instructions effectués, car le résultat obtenu est identique, qu'il y ait entre 1 et 9 sauts. Les 2 dernières lignes correspondent à des fautes induites lors des 10 dernières opérations `sub`. La première partie des résultats correspond à ceux attendus, mais les suivants sont incrémentés de 10 (écrits en rouge). Cela signifie que l'exécution d'une instruction n'a pas été effectuée, et les valeurs du tour précédent sont affichées. Les lignes D et E ont des fréquences d'apparition d'environ 0.1 %, cependant la zone temporelle cible est plus réduite que celle de la ligne C, ce qui justifie le fait qu'il y en ait moins. L'analyse des répartitions temporelles des fautes est présentée sur la figure 3.5.

Les pertes de communication sont majoritairement obtenues avant le délai de 1650 ns. Nous ne constatons que peu de pertes de communication entre les délais de 1660 et 1880 ns, ce qui est favorable au bon déroulement des campagnes. Les fautes des lignes D et E se produisent au voisinage de 1900 ns, juste après après celles de la ligne C.

Ces résultats montrent qu'il est possible de corrompre le fonctionnement d'un SoC

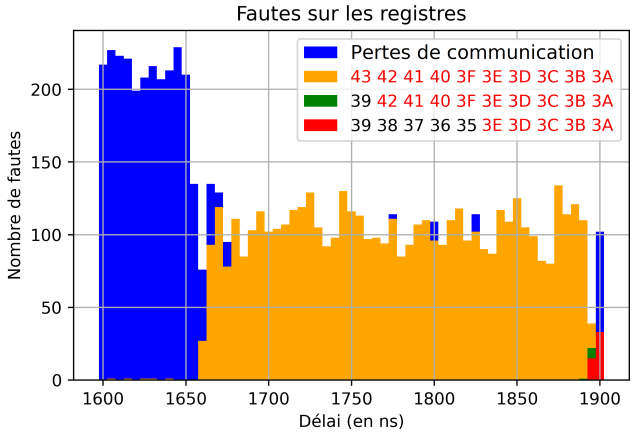



FIGURE 3.5 – Nombre de fautes classé par type en fonction du délai d'injection.

selon un modèle de fautes par saut d'instruction. La suite des travaux consiste à analyser les effets des perturbations au niveau du jeu d'instructions.

## 3.2 Effet des fautes

Dans la partie précédente, une méthodologie pour réussir des injections de fautes sur des cibles complexes a été présentée. Dans cette partie, nous étudions les effets des fautes. Pour cela, différents codes de tests ont été utilisés.

### 3.2.1 Essais préliminaires

Le premier test réalisé avec le code source 3.1 et ses résultats sont présentés dans le tableau 3.1. Ces premiers travaux montrent que la perturbation électromagnétique provoque entre 1 et 10 sauts d'instructions. Cependant, l'ensemble des instructions sont dépendantes, c'est-à-dire qu'une instruction utilise le résultat de l'instruction précédente. Afin de déterminer plus précisément le nombre de registres perturbés par une injection électromagnétique, un code sans dépendance de données doit être réalisé.

### 3.2.2 Évaluation du nombre de registres fautés

Un second code utilisé supprime la dépendance de données et permet de savoir si plusieurs registres sont fautés simultanément pendant le même tir électromagnétique, ou si certains sont plus sensibles que d'autres. Le code utilisé est une instruction de soustraction (SUB) d'un registre par 1 dont le résultat est stocké dans le registre, pour les registres X19 à X28. Il est présenté dans le code source 3.3.

Durant la campagne d'injection, la position de la sonde est fixe, l'amplitude de l'impulsion de tension est de 360 V et le délai est celui déterminé dans la partie 3.1.2. Sur 150 000 injections, 1 439 fautes sont obtenues, dont 42 sont des fautes de

```
//Initialisation des 10 registres
mov x19, #0x59      //r0 = 0x59
mov x20, #0x58      //r1 = 0x58
...
mov x27, #0x51      //r8 = 0x51
mov x28, #0x50      //r9 = 0x50

//Sequence suivante repetee 32 fois
sub x19, x19, #0x1 //r0 = r0 - 1
sub x20, x20, #0x1 //r1 = r1 - 1
sub x21, x21, #0x1 //r2 = r2 - 1
...
sub x28, x28, #0x1 //r9 = r9 - 1
```

Code 3.3 – Code de test sans dépendance de données.

communication, 757 des fautes monoregistres et 303 des fautes sur 2 registres. Ainsi, nous pouvons dans un premier temps considérer que l'injection perturbe majoritairement une seule instruction. Les valeurs des 10 registres de X19 à X28 dont un registre a été modifié par l'injection sont présentées à la figure 3.6.

```
143 0x39 0x38 0x37 0x36 0x35 0x30 0x33 0x32 0x31 0x30
133 0x39 0x38 0x37 0x36 0x35 0x34 0x33 0x33 0x31 0x30
52  0x39 0x38 0x37 0x37 0x35 0x34 0x33 0x32 0x31 0x30
36  0x39 0x38 0x37 0x36 0x35 0x35 0x33 0x32 0x31 0x30
15  0x39 0x39 0x37 0x36 0x35 0x34 0x33 0x32 0x31 0x30
13  0x39 0x38 0x37 0xFFFFEE6B5ACA 0x35 0x34 0x33 0x32 0x31 0
   x30
11  0x39 0x434EFD 0x37 0x36 0x35 0x34 0x33 0x32 0x31 0x30
11  0x39 0x38 0x37 0x36 0x35 FFFFFFFFFFFFFFF4 0x33 0x32 0x31
    0x30
10  0x39 0x434EC5 0x37 0x36 0x35 0x34 0x33 0x32 0x31 0x30
```

FIGURE 3.6 – Valeurs des 10 registres de X19 à X28 dont un registre a été modifié par l'injection.

La première colonne, en vert, correspond au nombre d'occurrences de la faute. Sur 757 fautes monoregistres, 143 sont obtenues en réalisant un saut d'instruction sur une instruction manipulant le registre X24. La seconde faute est obtenue durant la manipulation du registre X26. Sur les 9 résultats présentés, représentant 56 % des fautes monoregistres, les registres dont les valeurs ont été corrompues sont les X20, X22, X24, X26 et X28. En analysant l'ensemble des fautes obtenues, nous observons que seuls les registres pairs sont corrompus. Cette analyse sera approfondie en partie 3.4 avec l'étude des mécanismes provoquant les fautes.

### 3.2.3 Modèle de fautes au niveau du jeu d'instructions

Les différentes expériences présentées jusqu'ici ont permis de mettre en évidence un premier modèle de faute. Afin de le confirmer, un nouveau code, présenté dans le code source 3.4 est utilisé. Ce code manipule 28 registres contrairement aux précédents qui n'en manipulaient que 10 afin de maximiser l'observabilité des fautes. L'idéal aurait été de manipuler et relire les 32 registres disponibles, cependant il est nécessaire d'en utiliser certains afin de stocker l'adresse de sauvegarde du contexte et différents paramètres de campagne. Ce code manipule aussi des données sur la partie des demi-mots de poids fort des registres, contrairement aux codes précédents. Chaque instruction est unique ce qui permet de mieux analyser les effets des perturbations.

```
//Sauvegarde du contexte
//Initialisation des registres
mov x0, #0xFFFFFFFFFFFFFFFF      //r0 = 0xFFFFFFFFFFFFFFFF
mov x1, #0xEFFFFFFFFFFFFFFF      //r1 = 0xEFFFFFFFFFFFFFFF
...
mov x8, #0x7FFFFFFFFFFFFFFF      //r8 = 0x7FFFFFFFFFFFFFFF
mov x13, #0x2FFFFFFFFFFFFFFF     //r13 = 0x2FFFFFFFFFFFFFFF
...
mov x30, #0x00FFFFFFFFFFFFFF     //r30 = 0x00FFFFFFFFFFFFFF
//Boucle de NOP
mov x9, #0xc0       //Initialisation du compteur de boucle r9=192
.beforecuanop       //Début de boucle beforecuanop
nop
nop
nop
nop
nop
nop
sub x9, x9, #0x1    //Décrémentation du compteur
cmp c9, #0x0        //Comparaison
b.ne .beforecuanop //Fin de boucle ou boucle beforecuanop
//Code sous test
sub x0, x0, #0x1 //r0 = r0 - 1
...
sub x10, x10, #0x1 //r10 = r10 - 1
sub x13, x13, #0x1 //r13 = r13 - 1
...
sub x30, x30, #0x1 //r30 = r30 - 1
sub x0, x0, #0x10 //r0 = r0 - 10
```

```
...
sub x10, x10, #0x10 //r10 = r10 - 10
sub x13, x13, #0x10 //r13 = r13 - 10
...
sub x30, x30, #0x10 //r30 = r30 - 10
sub x0, x0, #0x100 //r0 = r0 - 100
...
sub x10, x10, #0x100 //r10 = r10 - 100
sub x13, x13, #0x100 //r13 = r13 - 100
...
sub x30, x30, #0x100 //r30 = r30 - 100
sub x0, x0, #0x1000 //r0 = r0 - 1000
...
sub x10, x10, #0x1000 //r10 = r10 - 1000
sub x13, x13, #0x1000 //r13 = r13 - 1000
...
sub x30, x30, #0x1000 //r30 = r30 - 1000
sub x0, x0, #0x10000 //r0 = r0 - 10000
...
sub x10, x10, #0x10000 //r10 = r10 - 10000
sub x13, x13, #0x10000 //r13 = r13 - 10000
...
sub x30, x30, #0x100000 //r30 = r30 - 10000
sub x0, x0, #0x100000 //r0 = r0 - 100000
...
sub x10, x10, #0x100000 //r10 = r10 - 100000
sub x13, x13, #0x100000 //r13 = r13 - 100000
...
sub x30, x30, #0x100000 //r30 = r30 - 100000
//Boucle de NOP (similaire à celle avant le code sous test)
//Sauvegarde des registres
//Restauration du contexte
```

Code 3.4 – Code assembleur utilisé pour caractériser le modèle de fautes.

Nous déterminons un modèle de fautes qui classe la majorité des fautes en 4 catégories. Certaines fautes sont obtenues en réalisant une combinaison de ces 4 catégories. Un programme triant les résultats des campagnes a été implémenté. Sur 845 487 injections, les statistiques de fautes obtenues sont les suivantes :

- **Saut d'une instruction** 159 269, ce qui correspond à 55 % des fautes. Le contenu d'une instruction n'est pas exécuté.
- **Modification de l'opérande destination des instructions** 65 276, ce qui correspond à 22.6 % des fautes. Le numéro du registre de destination est modifié et l'écriture est effectuée dans un autre registre

- **Reset du demi-mot de poids fort** 10 818, ce qui correspond à 3.7 % des fautes. Les poids forts des registres sont remis à zéro.
- **Rejeu d'instruction** 5 371, ce qui correspond à 1.9 % des fautes. Une instruction est exécutée une seconde fois au lieu de l'instruction suivante.

Ces 4 catégories couvrent 83 % des fautes obtenues. Les 17 % restants, soit 48 732 fautes, n'ont pas pu être classés dans l'une ou plusieurs de ces 4 catégories.

### Saut d'une instruction

L'effet d'un saut d'instruction correspond à la non-exécution d'une instruction.

Par exemple, il est possible d'obtenir la valeur **1FFFFFFFFFEEEFEE** sur le registre 14 au lieu de **1FFFFFFFFFEEEEEE**. L'ensemble des autres registres ont les valeurs attendues. Cela correspond à l'effet de la suppression de l'instruction SUB %14,%14,#0X1.

Un saut d'instruction peut être obtenu par l'exécution d'une instruction hors contexte, c'est-à-dire qui a un effet qui n'est pas observable. La suite de l'exécution du programme n'est pas impactée. Ce type de fautes est celui qui est majoritairement observé. Il a été présenté à de nombreuses reprises à la fois lors d'attaques utilisant les ondes électromagnétiques [82, 38] ou laser [33].

### Modification de l'opérande destination des instructions

L'effet d'une modification de l'opérande de destination des instructions correspond à l'écriture du résultat dans un autre registre.

Par exemple, il est possible d'obtenir la valeur **1FFFFFFFFFEEEDEE** sur le registre 15 au lieu de **1FFFFFFFFFEEEEEE**. Le registre 14 est aussi impacté par cette faute, nous constatons un saut d'instruction avec la présence du résultat **1FFFFFFFFFEEEFEE**. Cela correspond à la transformation de l'instruction SUB %14,%14,#0X100 en SUB %14,%15,#0X100. L'opération SUB %15,%15,#0X100 est ensuite correctement exécutée. Dans notre exemple, seule l'instruction manipulant le registre 14 a été corrompue, entraînant la modification des valeurs de deux registres. Cette faute a été obtenue par la mise à l'état 1 d'un seul bit (*bitset*) de l'instruction.

Dans la figure 3.6, des adresses sont inscrites dans les valeurs de certains registres, mais cela n'a pas été le cas pour ce dernier test. Ces valeurs ont pu provenir de lectures d'informations stockées dans les registres. Le mécanisme de modification de l'opérande destination des instructions peut expliquer ce type de résultats.

### Reset du demi-mot de poids fort

Certaines valeurs de registres ont été modifiées et la partie de poids fort a été mise à zéro.

Par exemple, il est possible d'obtenir la valeur **00000000FFEEEEEE** sur le registre 5 au lieu de **AFFFFFFFFEEEEEE**.

Ce type de fautes peut être obtenu avec l'utilisation de l'instruction UXTH (Zero extend Halfword). Ce type de fautes a déjà été présenté sur des cibles de types SoC [79].

### Rejeu d'instruction

Le rejeu d'instructions correspond à l'exécution de deux fois la même instruction. Ce type de fautes est généralement obtenu simultanément avec un saut d'instruction.

Par exemple, il est possible d'obtenir la valeur **AFFFFFFFFEEEDEE** sur le registre 5 au lieu de **AFFFFFFFFEEEEEE**. La valeur du registre 8 vaut **7FFFFFFFFFEEEFEE** au lieu de **7FFFFFFFFFEEEEEE**. Ce type de fautes peut être obtenu par le rejeu de l'instruction SUB %5,%5,#0X100 au lieu de l'exécution de l'instruction SUB %8,%8,#0X100.

Dans certains cas, nous obtenons une combinaison d'une remise à zéro d'un demi-mot de poids fort, d'un saut d'instruction et d'un rejeu ou une modification de l'opérande destination d'une instruction. Cela peut s'observer avec la valeur **00000000FFEEEDEE** sur le registre 1 et **AFFFFFFFFEEEFEE** sur le registre 5. Une instruction manipulant le registre 1 a été rejouée à la place d'une instruction manipulant le registre 5, et une mise à zéro du demi-mot de poids fort du registre 1 effectuée.

### Autres fautes obtenues

Il a été observé quelques résultats qui s'obtiennent avec d'autres codes stockés en mémoire. Cela peut être la conséquence de la modification du pointeur de pile.

Nous en concluons donc que les perturbations électromagnétiques peuvent provoquer des corruptions d'instructions, que ce soit au niveau de l'opcode ou des opérandes. Le saut d'instruction est bien souvent l'exécution d'une instruction « hors contexte » plutôt que d'une instruction NOP.

## 3.3 Exploitation judiciaire sur une fonction de sécurité

La partie précédente a permis d'étudier les conséquences d'une perturbation électromagnétique au niveau du jeu d'instructions. Il a été choisi d'exploiter ces injections sur une cible en changeant le comportement d'une fonction de sécurité.

Ces travaux sont réalisés dans l'objectif de proposer de nouveaux outils aux force de l'ordre en termes de fouille légale de données (forensic). Par exemple, dans le cadre d'enquêtes judiciaires, les téléphones portables peuvent contenir des informations sensibles et fournir des preuves. Afin d'analyser leur contenu, il peut être nécessaire de réaliser une élévation de privilèges. Nous choisissons d'évoluer du profil de l'utilisateur classique vers l'utilisateur root, possédant tous les droits d'administration du système. La cible mobile visée fonctionne sur un système d'exploitation Linux dont la commande SU ouvre une session avec un identifiant d'un autre utilisateur. Nous pouvons, par exemple, nous authentifier comme utilisateur privilégié, mais cela peut nécessiter un mot de passe. L'objectif est donc d'identifier une vulnérabilité dans ce programme afin de réaliser l'authentification sans mot de passe.

### 3.3.1 Préambule : le programme SU

Le programme SU est lancé avec une permission SETUID permettant son exécution par un autre utilisateur. Dans notre cas, cela signifie qu'il est lancé avec les droits d'administrateur dès son démarrage. Si l'authentification réussie, alors nous obtenons une interface permettant d'exécuter des programmes en tant qu'utilisateur root, sinon les droits d'utilisateur sont rendus.

Dans le cadre de l'injection de fautes, la première idée est de modifier le retour de la comparaison du mot de passe entré et de celui stocké. Cependant, une protection est implantée contre les attaques par brute-force, c'est-à-dire essayant toutes les combinaisons de mots de passe possible. Cette protection rajoute un délai aléatoire entre 2.25 et 3.75 secondes après la vérification du mot de passe si celui-ci n'est pas correct. C'est donc une difficulté supplémentaire à gérer pour réussir la synchronisation de l'attaque. Nous cherchons à perturber le déroulement d'une instruction assembleur dont la durée d'exécution est de l'ordre d'une nanoseconde. La gigue sur l'instant d'exécution de l'instruction est d'une seconde, ainsi cela demande $10^9$ tentatives pour espérer perturber cette instruction dans le cas d'un taux de succès de l'injection de 100 %. Cela signifie qu'il faudrait 92jours avec 10 essais par seconde. Nous sommes donc dans l'obligation d'effectuer un saut d'instruction avant l'introduction de ce délai aléatoire, nous ne pouvons pas réaliser l'injection de fautes sur le retour de la fonction UNIX_VERIFY_PASSWORD.

Une étude du code SU montre que la bibliothèque LIBPAM est appelée pour authentifier l'utilisateur. Celle-ci transmet la requête au module PAM_UNIX, comme présenté dans la figure 3.7.

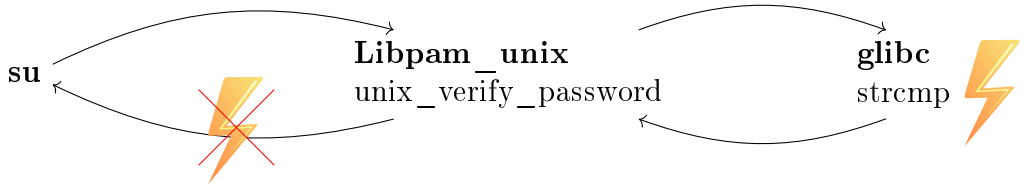



FIGURE 3.7 – Schéma des appels à des fonctions depuis la commande SU.

Le module PAM_UNIX appelle la fonction STRCMP de la bibliothèque GLIBC afin de comparer le hash du mot de passe mémorisé et le hash du mot de passe tapé. Ce ne sont donc pas les mots de passe qui sont directement comparés, mais le résultat de leur conversion par une fonction de hashage. Cela évite de stocker en clair le mot de passe.

La comparaison est réalisée en analysant les chaînes de caractères par bloc de 8 caractères de la gauche vers la droite. Si deux blocs sont différents alors la comparaison est stoppée et les deux chaînes sont identifiées comme différentes. Le mot de passe permettant de s'authentifier comme utilisateur root est *root*. Celui utilisé pour les tentatives de connexions est *fail*. Les hash de ces deux chaînes sont présentés dans la figure 3.8.

— $6$wWxFc|tJdeOI05|KNO$lAAh|w8Th... -> Hash de *root*
— $6$wWxFc|tJdeOI05|KNO$Uung|4U7s... -> Hash de *fail*
mot 1 | mot 2 | mot 3 | mot ...

FIGURE 3.8 – Retour du hachage des chaînes de caractères *root* et *fail*.

Nous observons que pour les deux chaînes de caractères, les deux premiers mots sont identiques. Le hash est composé de différents éléments séparés par le signe $, le premier élément indique que la méthode de hachage utilisée est SHA512CRYPT. Le second élément est associé au sel, c'est-à-dire une donnée supplémentaire luttant contre d'autres types d'attaques. Il faut noter que, quelle que soit la chaîne en entrée de la fonction de hachage, les débuts des chaînes hashées sont toujours identiques. Ainsi les 2 premières comparaisons sont toujours vraies.

Une sortie prématurée de la boucle pendant la première ou seconde comparaison interprétera un mot de passe comme valide. Cependant, une injection lors de la 3ème comparaison va aussi causer une sortie de boucle, mais le mot de passe sera considéré comme erroné, car les chaînes comparées seront différentes. Cela ne réalisera pas d'élévation de privilège.

Le schéma d'attaque est de forcer la sortie de la boucle pendant les 2 premières exécutions. Ainsi, toute la chaîne hachée n'est pas vérifiée et le résultat de la comparaison est vrai. Afin de valider ces scénarios, le code assembleur de la fonction

```
L(loop_misaligned):
  ...
  ldr data1, [src1], #8
  ldr data2, [src2], #8
  sub tmp1, data1, zeroones
  orr tmp2, data1, #REP8_7f
  eor diff, data1, data2  //Non-zero if differences found
  bic has_nul, tmp1, tmp2 //Non-zero if NUL terminator
  orr syndrome, diff, has_nul
  cbz syndrome, L(loop_misaligned)
  b L(end)
```

Code 3.5 – Code assembleur de la fonction `strcmp`.

`strcmp` est présenté dans le code source 3.5.

Ce code charge deux mots, effectue la comparaison et cherche une différence (ou la fin de la chaîne), puis continue la comparaison ou s'arrête. L'instruction Compare and Branch on Zero (CBZ) est en charge du branchement au début de la fonction pour réaliser la comparaison du mot suivant, ou de l'arrêt de la comparaison.

La validation du schéma d'attaque a d'abord été réalisée en simulation, par l'utilisation du debugger GDB. Cela consiste à exécuter la fonction STRCMP sur notre cible et à émuler les effets du saut de l'instruction CBZ. Les simulations effectuées montrent qu'un saut de la première ou seconde exécution de l'instruction CBZ termine effectivement la boucle sans détection de différence dans les mots de passe. Cela valide la preuve de concept de la vulnérabilité, le *control flow* peut être théoriquement modifié. Des tests d'injection ont d'abord été réalisés sur le code STRCMP intégré dans un programme de test pour en réaliser la preuve de concept. L'attaque a ensuite été mise en place sur la commande SU afin de se rapprocher d'un cas d'exploitation réel.

### 3.3.2 Préparation de l'attaque sur la commande SU

Afin de conserver les conditions expérimentales des résultats précédents, nous réalisons l'injection lorsque le programme est exécuté sur le CPU 3. Pour ce faire, l'outil SUCRACK [57], conçu par Leidecker afin de réaliser des attaques par brute-force est modifié pour réaliser des attaques par fautes. Dans un premier temps, l'ensemble des programmes fonctionnant sur la carte de développement sont déplacés du CPU 3 vers les trois autres. Lorsqu'une commande SU est démarrée, l'exécution de son processus est déplacée vers le CPU 3. Cette modification de l'emplacement d'exécution du processus est optionnelle, mais améliore l'efficacité de l'attaque.

Certaines fonctionnalités de SUCRACK ont été désactivées et la gestion d'une communication UART a été ajoutée. Celle-ci informe le PC de commande de la réussite de

| Délai (en ns) | Échec | Succès | Erreurs | Total |
|---|---|---|---|---|
| 220 | 5805 | 12 | 183 | 6000 |
| 240 | 5787 | 21 | 192 | 6000 |
| 260 | 5785 | 20 | 195 | 6000 |
| 280 | 5731 | 19 | 250 | 6000 |

TABLEAU 3.2 – Résultats de l'injection de fautes sur la commande SU.

l'authentification, c'est-à-dire du succès de l'attaque. Cette communication UART relance aussi une exécution du code cible sans attendre la fin de la précédente. Ainsi, plusieurs instances de la commande SU sont exécutées en parallèle, ce qui accélère le déroulement de la campagne. Cependant, il est possible de réaliser des injections de fautes sans cette communication même si cela diminue la fréquence des tentatives d'injections de fautes.

Le signal de synchronisation (ou trigger) présente un front montant avant l'exécution de la fonction STRCMP et descendant juste après. Cependant la durée entre la commutation du trigger et l'attaque est d'environ 100 ns, alors que le temps de préparation d'une impulsion par le générateur Avtech est de 350 ns. Pour cela, un autre trigger et des instructions NOP sont insérés avant la commutation du premier trigger.

La carte de développement comprend deux utilisateurs : user et root. Le programme préparant l'attaque est démarré en tant que root. Il attend ensuite le démarrage des commandes SU afin d'en déplacer l'exécution sur le CPU 3.

### 3.3.3 Réalisation de l'attaque sur la commande SU

L'exploitation est réalisée avec un CPU choisi et en activant le DVFS, c'est-à-dire sans contrôler la fréquence de fonctionnement. Des programmes de stress, tel que celui présenté sur le code source 3.2, sont exécutés. L'amplitude de l'impulsion de tension est de 360 V et le délai entre la réception du signal de synchronisation et l'impulsion est varié de 220 à 280 ns. Les résultats de l'injection de fautes sont inscrits dans le tableau 3.2.

Nous obtenons un taux maximum d'environ 20 succès sur 6000 injections pour des délais compris entre 240 et 280 ns. Cela correspond à 1 succès toutes les 300 injections, soit toutes les 15 minutes. Environ 3 % des résultats sont des pertes de communications avec la carte suite à son redémarrage.

Après chaque succès de l'attaque, la carte exécute un redémarrage automatique. Une situation de panique du noyau (kernel panic) est signalée : *Unable to handle kernel paging request at virtual address XXXX*. Cette erreur au niveau du noyau provient d'un accès à une zone mémoire inexistante. Le noyau informe qu'il entame

un redémarrage de la carte à la suite de cette erreur. L'exploitation n'est donc pas utilisable directement, mais nous pouvons imaginer exécuter une commande, avant le redémarrage, qui rend l'élévation de privilège persistante.

### 3.3.4 Modification des droits d'accès aux ressources sur la carte

Nous cherchons désormais à montrer que l'exploitation nous authentifie avec la fonction SU sans connaître le mot de passe et qu'il est possible de lancer une commande d'élévation de privilège persistante. L'expérience est similaire à celle de la partie 3.3.3, cependant nous ajoutons la commande "&& CHMOD +S /BIN/BASH" à celle envoyée. Cela modifie les permissions de la commande BASH et donc de donner les droits root à tous les utilisateurs.

Nous vérifions avant de lancer la commande que l'état de /BIN/BASH est :

```
-rwxr-xr-x 1 root root 892K Feb 5 2019 /bin/bash.bash
```

Après le premier succès de l'attaque et le redémarrage de la carte, le résultat est :

```
-rwsr-sr-x 1 root root 892K Feb 5 2019 /bin/bash.bash
```

Nous constatons que le droit **s**, signifiant SETUID, a été ajouté à la commande bash et que cela est fait de manière persistante. La commande BASH est celle de l'interpréteur du langage Bash exécutant des scripts. Grâce à la présence de cette permission, tous les utilisateurs de la carte, y compris user, ont la possibilité d'exécuter la commande BASH en tant qu'utilisateur root. Tous les utilisateurs ont donc accès à des fonctions privilégiées.

Cette expérience prouve qu'il est possible de réaliser une élévation de privilège en utilisation l'injection de fautes par perturbations électromagnétiques sur un SoC. Quelques contraintes ont été imposées. L'utilisation du CPU 3 par la fonction ciblée a été forcée, ce qui augmente le taux de succès. Une liaison série UART est ouverte afin de faciliter la mise en place du banc de test et de lancer plusieurs exécutions de la commande SU en parallèle pour accélérer la fréquence d'injection. Ces deux modifications ne sont pas accessibles dans un contexte d'enquête judiciaire, mais elles n'invalident pas la preuve de concept.

La synchronisation de l'attaque a été réalisée en utilisant une broche d'entrée/-sortie numérique GPIO activée via une librairie dans la fonction STRCMP. Afin de rendre plus utilisable en pratique cette attaque, nous cherchons par la suite à ne pas utiliser de GPIO pour la déclencher.

| Gigue | Temps moyen pour 1 faute | Faisabilité |
|---|---|---|
| 30 ns | 15 secondes | Excellente |
| 300 ns | 3 minutes | Excellente |
| 3 µs | 25 minutes | Correcte |
| 30 µs | 4 heures | Correcte |
| 300 µs | 2 jours | Moyenne |
| 1 ms | 6 jours | Difficile |
| 5 ms | 30 jours | Impossible |
| 10 ms | 60 jours | Impossible |

TABLEAU 3.3 – Temps moyen pour réussir une injection de fautes en fonction de la gigue.

### 3.3.5 Possibilité d'une synchronisation sur saisie du mot de passe

Le déclenchement de l'attaque doit être synchrone avec la saisie du mot de passe. Nous le vérifions en mesurant la gigue entre l'envoi du mot de passe et l'appel à la fonction STRCMP dans la commande SU.

L'expérience est réalisée avec le mode DVFS activé ainsi que les CPUs 0, 1 et 2 désactivés. L'histogramme des délais est présenté sur la figure 3.9.

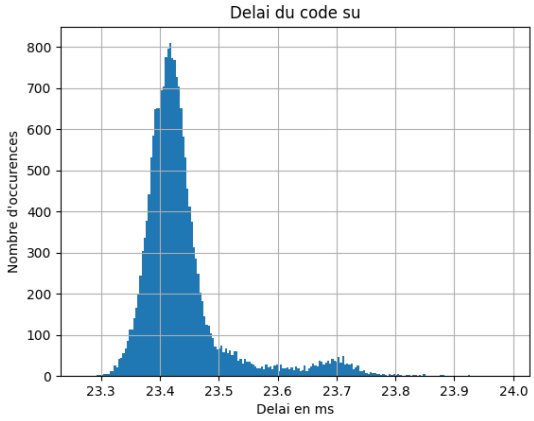



FIGURE 3.9 – Délai entre la réception du mot de passe et l'appel à la fonction STRCMP.

Le délai moyen est d'environ $\mu = 23.43$ ms et l'écart type de $\sigma = 77$ µs. Une gigue d'environ 200 µs est observée. A la cadence d'attaque maximale, nous obtenons 1 faute toutes 15 secondes pour une gigue de 30 ns. Si la gigue augmente cela accroît d'autant le délai. Nous en déduisons le tableau 3.3 en considérant une répartition uniforme.

Ainsi, si la gigue est d'environ 200 µs, avec les mêmes considérations, il serait possible de réussir une injection tous les deux jours. Pour réduire cette gigue, nous pouvons améliorer la synchronisation temporelle en déclenchant via d'autres moyens tels que la surveillance des connexions avec la flash/RAM, les consommations électriques ou encore les émissions électromagnétiques. Nous pouvons aussi chercher une nouvelle vulnérabilité plus proche de la réception du mot de passe.

J'ai développé un outil de synchronisation sur l'apparition d'une signature fréquentielle avant mes travaux de thèse. Son utilisation a été validée lors d'injections de fautes sur un SoC [4]. Cet outil permettrait ici de se synchroniser sans GPIO. Néanmoins, nous n'avons pas poussé cette attaque jusqu'à une exploitation complète étant donné que l'objectif était uniquement de présenter l'EMFI comme outil potentiel de la police scientifique sur des cibles complexes de type SoC.

### 3.3.6 Scénario d'utilisation dans le cas judiciaire

L'un des points problématiques du contexte judiciaire est de contourner le démarrage sécurisé ou d'obtenir un accès root. Les solutions commerciales telles que celles proposées par Cellebrite ou MSAB fonctionnent en utilisant les codes de déverrouillage pour accéder à un appareil [29]. L'EMFI est une alternative car elle cible le matériel. Les résultats montrent que l'EMFI, de manière similaire aux attaques logicielles, peut être utilisée pour accéder aux données d'un smartphone, exécuter ou planifier l'exécution d'un code. L'EMFI peut également être utilisée comme une première étape afin d'augmenter la potentialité des outils logiciels d'analyse légale habituels. En effet, l'EMFI pourrait fournir de nouveaux contenus à analyser. Nous pouvons imaginer utiliser l'EMFI pour contourner les mécanismes de sécurité afin d'extraire un boot-ROM. Le code extrait peut être analysé, afin d'identifier une faille logicielle et d'être exploité en utilisant des outils conventionnels. Ainsi, l'utilisation conjointe de ces deux techniques peut repousser les limites des outils de police scientifique.

Alternativement, la figure 3.10 illustre un scénario pour utiliser l'EMFI afin d'accéder aux données d'un système sécurisé par un chiffrement de type LUKS. Le chiffrement Linux Unified Key Setup (LUKS) est le standard de chiffrement utilisé avec les noyaux Linux permettant de chiffrer l'intégralité d'un disque. Ce type de chiffrement procure une robustesse face aux attaques par brute-force et analyses forensiques [43].

En écoutant la communication entre le système et le disque dur, il n'est pas possible de récupérer les données [43]. Cependant, une version déchiffrée est accessible par l'utilisateur root. Nous pourrions utiliser l'EMFI pour faire une escalade de privilèges et avoir accès aux données chiffrées.

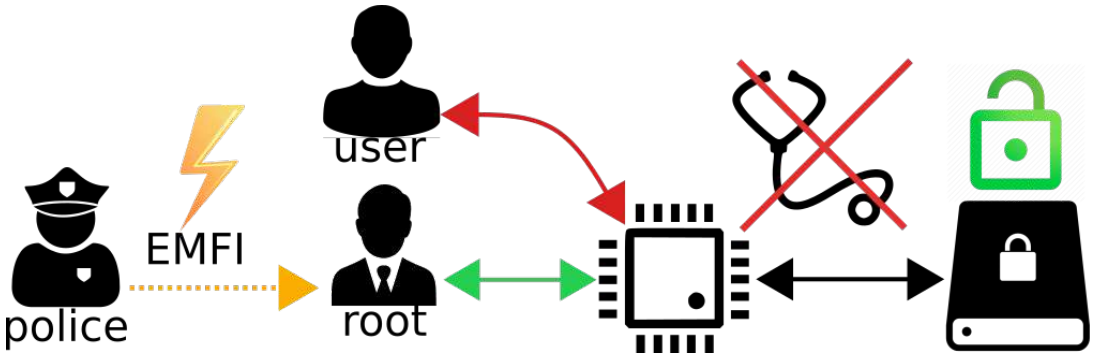



FIGURE 3.10 – Scénario d'utilisation de l'injection de fautes par perturbations électromagnétiques dans un contexte de police judiciaire pour accéder à un disque chiffré avec LUKS.

## 3.4 Étude des fautes au niveau microarchitectural

Les résultats de la partie 3.2 ont abouti à la définition d'un modèle de fautes mettant en avant 4 mécanismes. Cependant, la compréhension de certains phénomènes nécessite une étude plus fine au niveau microarchitectural.

### 3.4.1 Parité des registres fautés en fonction de la position

Les résultats de la partie 3.2.2 ont montré que seuls des registres pairs ont été impactés par l'injection. Une cartographie spatiale a donc été réalisée sur le code 3.3, manipulant des registres sans dépendance entre eux. Les paramètres d'injections (délai et tension) sont restés inchangés. Les résultats sont présentés sur la figure 3.11.

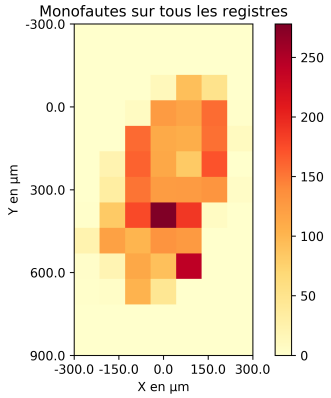



FIGURE 3.11 – Cartographie spatiale avec le code assembleur sans dépendance.

La zone spatiale sensible à l'injection mesure environ 700 µm*400 µm. Si nous décomposons les résultats sur les registres pairs et impairs, nous obtenons la figure 3.12.

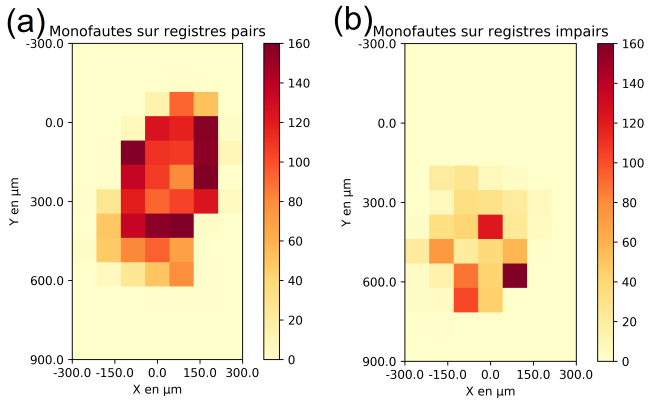



FIGURE 3.12 – Cartographie spatiale de la figure 3.11 pour les registres pairs **(a)** et impairs **(b)**.

Ces résultats montrent que la corruption des registres pairs (uniquement) a été obtenue pour une position donnée de la sonde d'injection. Ici, différentes positions ont été testées permettant des fautes des registres pairs et impairs. La position influe donc sur la parité des registres fautés. Nous constatons deux zones distinctes en fonction de la parité des registres. Environ 3 000 fautes sur les registres pairs sont obtenues contre 1 000 sur les impairs.

Cela peut être du à la manière dont sont chargées les instructions ou à la façon d'écrire dans les registres par exemple. Un code de test avec 9 instructions au lieu de 10 est alors utilisé afin de vérifier si cette parité provient d'une sensibilité des registres ou du flot d'instructions.

Les résultats de l'exploration spatiale montrent que la position influe toujours sur le type de registres fautés. Les valeurs donnent 5 300 registres pairs contre 100 impairs fautés. L'expérience a été refaite avec un code légèrement différent, les valeurs d'initialisation ont été modifiées. Les instructions visées sont donc restées inchangées, mais les valeurs de répartition sont ici de 100 registres pairs contre 2 435 impairs.

La position de la sonde d'injection influe donc sur la parité des registres perturbés. Pour une même position, il est possible de modifier un registre pair ou impair en fonction du code utilisé. Cela signifie que l'injection ne vise pas directement les registres mais le code les manipulant. Nous aurions pu nous attendre à ce que le nombre de registres pairs et impairs fautés soit identique, cependant la cible est complexe et ne semble pas exécuter les instructions ainsi. Cela met en évidence que ce ne sont pas les registres qui sont sensibles, mais une partie de l'architecture qui manipule les instructions. Une hypothèse serait que les instructions à exécuter sont chargées par 2 dans le pipeline, une pouvant être plus sensible que l'autre.

Afin que les instructions soient exécutées par le CPU, elles sont chargées en mémoire flash dans un premier temps. Ensuite, elles transitent par la cache de niveau

2 (cache L2). Elles sont par la suite transférées en cache de niveau 1 pour les instructions (cache L1I) pour arriver au CPU, comme présenté en figure 3.13.

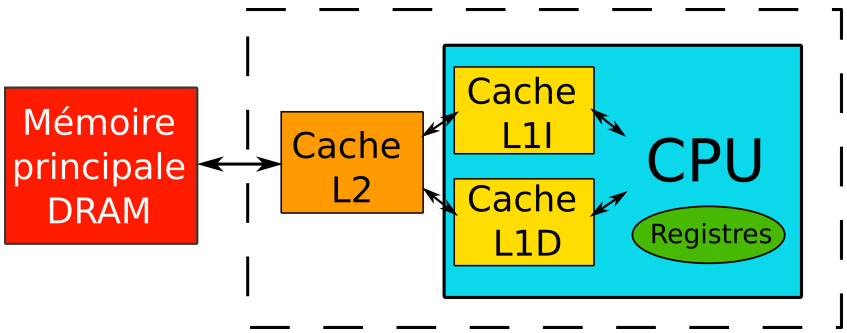



FIGURE 3.13 – Les différents niveaux de mémoire du microprocesseur.

L'ensemble des fautes observées l'ont été uniquement sur des instructions et non des données. Nous en déduisons que les perturbations peuvent survenir de la sortie du cache L2 jusqu'à l'exécution, en passant par le cache L1I. Nous nous intéressons donc aux effets sur les caches.

### 3.4.2 Influence du chargement en mémoire du code

La modification des instructions est possible lors de leurs transferts de la Flash vers le CPU. L'influence du chargement en cache ou non des instructions doit donc être étudiée. Afin de forcer la mise en cache du code, il est possible d'exécuter plusieurs fois un code de taille réduite et de réaliser l'injection sur sa dernière exécution. Pour cela, un code est exécuté de nombreuses fois puis un trigger est levé au niveau de la dernière itération du code, comme décrit sur la figure 3.14.

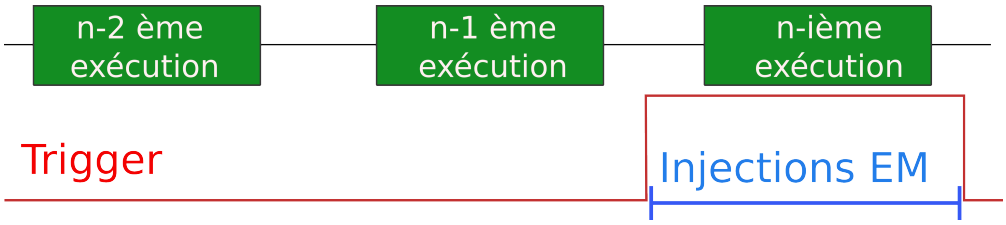



FIGURE 3.14 – Manipulation permettant de réaliser une injection sur un code dont la mise en cache est forcée.

Pour effectuer cette expérimentation, nous utilisons le code assembleur manipulant des données sans dépendance (code source 3.4). Nous réalisons jusqu'à 30 itérations de ce code avant de lever le trigger et de réaliser l'injection de fautes sur l'exécution suivante. L'impulsion de tension est engendrée par un générateur de marque Avtech, d'amplitude 360 V et de durée 6 ns. Le délai entre la réception du signal de synchronisation et le déclenchement de l'impulsion est varié entre 100 et 7000 ns avec un pas de 20 ns. Le nombre de fautes pour différents nombres d'itérations exécutées avant celle ciblée est présenté sur la figure 3.15.

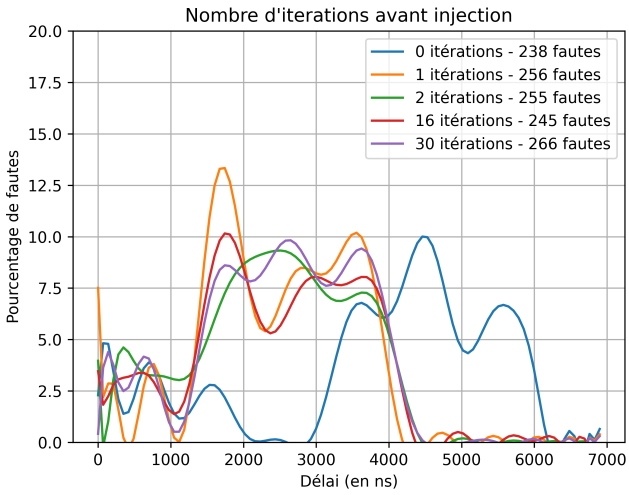



FIGURE 3.15 – Influence du nombre d'itérations sur le nombre de fautes obtenues.

Les résultats sont similaires lorsqu'il y a eu entre 1 et 30 itérations du code avant l'injection, nous obtenons majoritairement les fautes pour des délais entre 1500 et 4000 ns, avec un nombre de fautes compris entre 245 et 266. Par contre, le comportement est différent lorsqu'il n'y a pas eu de mise en cache. En effet, sans aucune itération du code avant l'injection, les fautes apparaissent pour un délai plus important, entre 3000 et 6000 ns. La durée pendant laquelle des fautes sont obtenues est augmentée de 2500 ns à 3000 ns, mais le nombre de fautes reste cependant proche avec 238 fautes. Cela montre qu'une itération suffit à charger le code cible en cache. Alors, afin de mieux mettre en avant les différences entre 0 et 1 itération, la manipulation est répétée 100 fois. Le nombre de fautes associé à chaque itération est présenté sur la figure 3.16.

Les fautes correspondant au code exécuté pour la première fois apparaissent majoritairement 2000 ns après celles pour lesquelles une exécution a déjà eu lieu. Le nombre de fautes est proche pour les 2 cas, entre 1392 et 1589. Nous en concluons qu'il est possible de fauter un code qu'il ait été mis en cache ou pas.

Lors de la première exécution, le code est récupéré en mémoire flash puis transféré en cache L2, et en cache L1I avant d'être chargée dans le pipeline. La figure 3.13 représente les différents niveaux de mémoire du microprocesseur. La taille du code exécuté étant relativement faible, il peut être stocké en cache L1I d'une taille de 32 Ko, ainsi lors de la seconde exécution, il peut être cherché en cache L1I. Cela explique l'apparition plus rapide des fautes lors de la seconde exécution.

### 3.4.3 Persistance des fautes

Les fautes sont produites et propagées jusqu'à leur exécution par le CPU. Afin de les exploiter au mieux, il est intéressant de savoir si nous pouvons créer des fautes

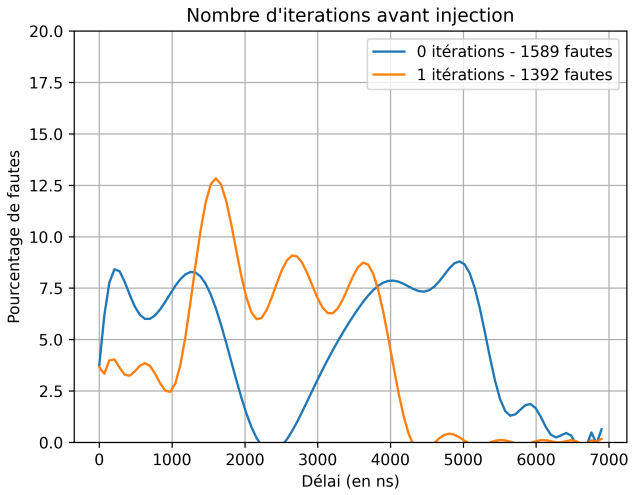



FIGURE 3.16 – Nombre de fautes obtenu pour 0 et 1 itération du code avant celui ciblé.

persistantes. Pour cela, un trigger est levé au niveau de l'avant-dernière itération d'un code et des injections sont effectuées pendant 2 fois la durée du code de test, comme décrit sur la figure 3.17. Cette manipulation compare les effets des injections électromagnétiques sur l'avant-dernière et la dernière itération du code, tandis que la lecture des valeurs contenues dans les registres se fait toujours sur la dernière instruction.

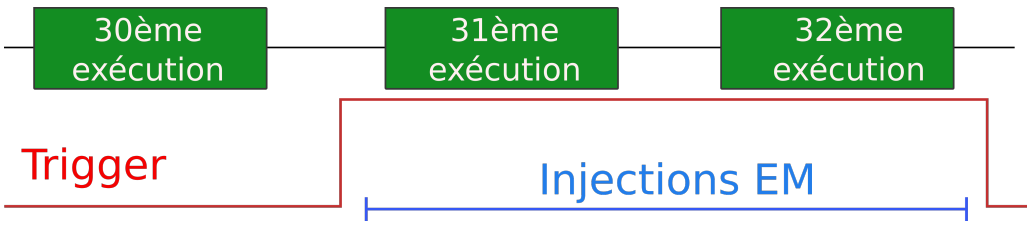



FIGURE 3.17 – Manipulation évaluant la persistance des fautes.

Le code exécuté est celui utilisé dans la partie précédente. Nous réalisons 30 exécutions du code sous attaque avant de lever le signal de synchronisation sur la $31^{\text{ème}}$ et $32^{\text{ème}}$ itération. La relecture des valeurs contenues dans les registres est exécutée après la descente du signal de synchronisation. D'après une analyse des émissions électromagnétiques du processeur, le premier code est exécuté de 0 à 4000 ns, avant l'exécution du second code. Le nombre de fautes lors de l'exécution du code test est présenté sur la figure 3.18.

Nous remarquons une première zone avec peu de fautes, jusqu'à 3000 ns, et une seconde avec environ 10 fois plus de fautes, entre 3500 et 9000 ns. Les types de fautes obtenus pendant la première partie de la cartographie temporelle (c'est-à-dire avant 3000 ns) sont similaires à celles sur la seconde partie (entre 3500 et 9000 ns). Cela

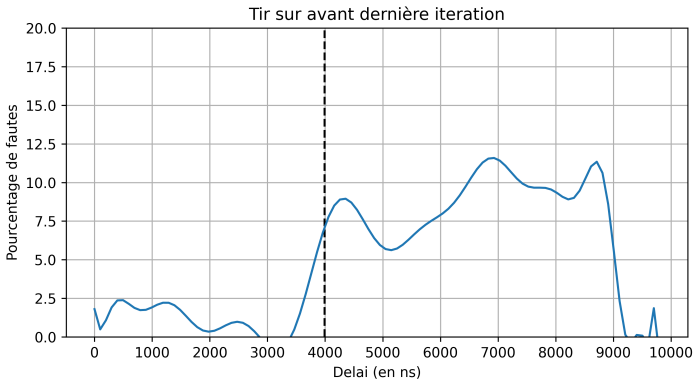



FIGURE 3.18 – Tir sur 2 exécutions successives du code test.

signifie que les fautes obtenues durant l'injection sur l'avant-dernière et la dernière exécution sont similaires.

Nous en concluons qu'il est possible de réaliser des injections de fautes persistantes, bien qu'elles soient très minoritaires. Si on fait l'hypothèse d'une injection de fautes lors du transfert entre la cache L2 et la cache L1I, le nombre de fautes devrait être similaire lors des injections sur l'avant-dernière ou la dernière itération car le code est stocké en cache L1I après la première exécution. Or, ce n'est pas ce que nous observons. Dans le paragraphe 3.4.1, il a été montré que l'injection de fautes était réalisée après la sortie du cache L2. Cela signifie que l'injection de fautes peut être réalisée principalement lors du transfert entre la cache L1I et le CPU (partie droite de la figure 3.18) mais aussi dans le contenu des instructions de la cache L1I (partie gauche de la figure 3.18). La figure 3.19 représente les différents niveaux de mémoire du microprocesseur avec les zones de corruptions possibles.

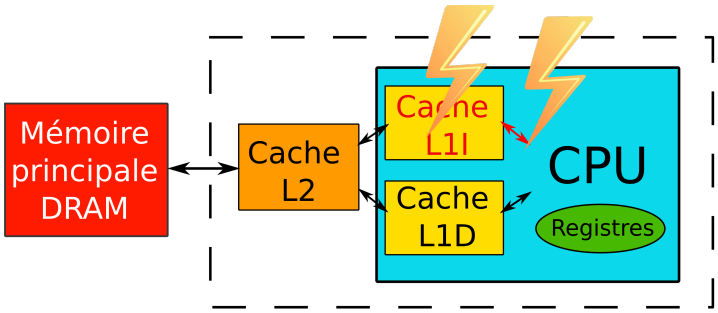



FIGURE 3.19 – Les différents niveaux de mémoire du microprocesseur, avec les zones de corruption possibles par perturbations électromagnétiques.

### 3.4.4 Position de l'instruction dans le pipeline

Il a été montré que les instructions étaient fautées lors de leur transfert de la cache L1I vers le CPU. Afin de vérifier que toutes les instructions peuvent être modifiées, il faut vérifier qu'une instruction peut être perturbée quelle que soit sa position dans le pipeline.

Pour ce faire, nous utilisons le simulateur de processeur GEM5 [60]. Ce logiciel open-source émule et visualise le chargement et l'exécution des instructions. Son étude a permis d'observer que les instructions sont récupérées en cache L1I par paquets de 16 (la largeur du bus est de 64 octets et chaque instruction fait 32 bits). Elles sont ensuite récupérées par un second *fetch* puis stockées par 4 et traitées par 2 dans l'étape *decode* du pipeline. Ensuite, dans le cas d'instructions manipulant des entiers, c'est-à-dire le cas de nos codes de tests, deux voies séparées amènent les instructions à deux unités arithmétiques et logiques (ALU) différentes. Cela suppose que nous pourrons avoir des comportements similaires par multiple de 2, 4, 8 ou 16 en fonction du niveau où est créée la faute.

Nous réalisons donc des injections en faisant varier le nombre de NOP entre la boucle d'attente et le code sous attaque. L'instruction assembleur ALIGN est une directive alignant l'emplacement d'une instruction sur une zone spécifiée en complétant si nécessaire avec des instructions NOP. Nous l'utilisons afin de faire varier la position d'une instruction dans le pipeline. En effet, nous réalisons un premier alignement, puis nous ajoutons des instructions NOP qui décaleront la position de l'instruction dans le pipeline. Étant donné que les instructions sont chargées par le *fetch* par paquets de 16, nous introduisons un nombre de NOP entre 0 à 15. Le code est constitué d'une seule opération de soustraction sur chacun des registres sans dépendance. Des injections de fautes sont réalisées en utilisant le générateur Avtech avec une amplitude de tension de 360 V, et le nombre de fautes sur quelques registres est présenté sur la figure 3.20.

Ces registres ont été choisis arbitrairement, mais l'ensemble des résultats sont similaires sur les 28 registres examinés. Certains registres sont plus sensibles aux perturbations quelle que soit la position des instructions les manipulant dans le pipeline. Nous remarquons que le nombre de fautes évolue de manière analogue sur les registres en fonction du nombre de NOP. Cependant leur position dans le pipeline est différente, ce qui signifie que cette variation du nombre de fautes n'est pas liée aux modifications du code assembleur. Deux hypothèses pourraient justifier ces résultats : une variation des conditions expérimentales (position de la sonde par exemple), ou une origine des injections de fautes avant le chargement dans le pipeline.

Une modification significative de la position de la sonde aurait inversé la parité des registres fautés. L'évolution de nombre de fautes par registre étant relativement similaire, une variation de la position de la sonde n'est pas à l'origine de ces résultats. Cela confirme que l'injection de faute est réalisée lors du transfert entre le

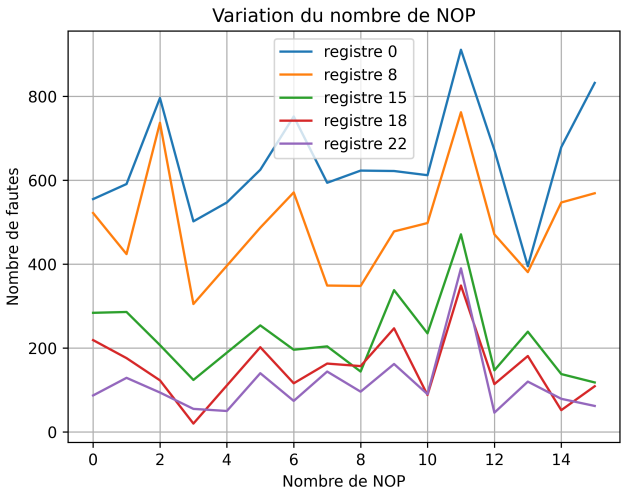



FIGURE 3.20 – Influence du nombre de NOP sur le nombre de fautes.

cache L1I et le CPU.

## 3.5 Modification des conditions expérimentales

Les fautes ont majoritairement été obtenues sur des codes test dans des conditions choisies favorablement pour maximiser le nombre et la variété des fautes. Lors d'une exploitation de l'injection de fautes par des forces de l'ordre, l'environnement est incontrôlable. Ainsi, ces conditions peuvent ne pas être réunies, nous étudions alors l'effet de ces choix.

### 3.5.1 Influence du choix du CPU

Les expériences ont été réalisées en ciblant uniquement le CPU 3, les premières expériences n'ayant pas permis de perturber les autres CPUs. Le code source 3.4 met en évidence les effets de l'injection de fautes. Les cartographies spatiales sur toute la surface de la puce en ciblant à chaque fois un CPU différent sont présentées sur la figure 3.21. Les zones permettant de faire des fautes sont différentes sur chacun des CPUs, une superposition est effectuée afin de mieux visualiser leur répartition. La couleur verte est associée aux fautes réalisées sur le CPU 0, la orange sur le CPU 1, la bleue sur le CPU 2 et la violette sur le CPU 3. L'impulsion de tension est réalisée avec le générateur de marque Avtech, avec une amplitude de 360 V et une durée d'impulsion de 6 ns. La durée du retard interne au générateur d'impulsions de tension est fixée à 150 ns.

Dans cette expérience, le CPU 3 a été ciblé en position centrale (X=0 et Y=0). Le taux maximum de succès sur le CPU 3 est d'environ 60 %. Le CPU 0 et le CPU 1 sont également sensibles aux perturbations mais le taux de succès maximum est de 30 %. A noter que la zone de sensibilité du CPU 1 est beaucoup plus restreinte.

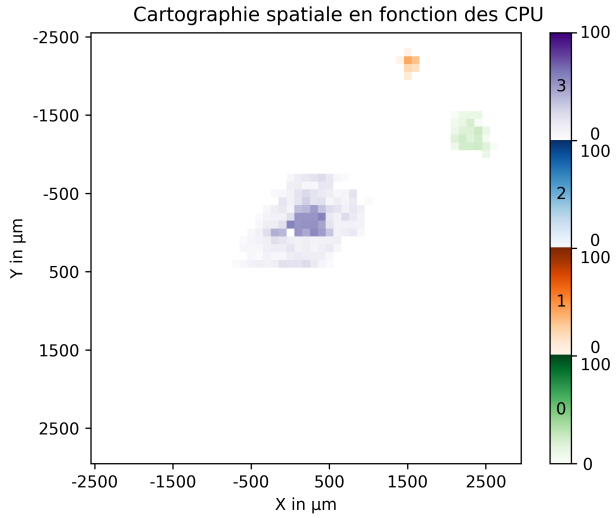



FIGURE 3.21 – Influence de la position d'injection sur le nombre de fautes pour chaque CPU.

Il est donc possible de fauter 3 des 4 CPUs avec le banc d'injection de fautes disponible avec d'importantes différences de sensibilité. Cependant, il est possible qu'avec un banc d'injection plus puissant le CPU 2 puisse aussi être perturbé. Le fait de pouvoir perturber le fonctionnement du CPU 0 ouvre de nouvelles possibilités, car c'est le CPU exécutant les fonctions de sécurité lors du démarrage de la carte.

Une cartographie par photoémission a été réalisée afin d'identifier la position de chacun des CPUs. Lors de son fonctionnement, un circuit intégré produit des photons avec un rayonnement infrarouge au niveau de sa face arrière. La caméra infrarouge AlphaNov [10], disponible au laboratoire Micro-Packs [11, 28], qui a été utilisée pour capturer et analyser ces émissions est présentée sur la figure 3.22.

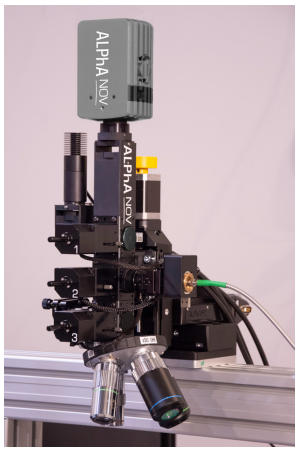



FIGURE 3.22 – Banc laser d'AlphaNov de la plateforme Micro-Packs [11, 28].

Un code est exécuté en boucle sur un CPU afin d'identifier plus facilement chacun des CPUs. Les résultats sont présentés sur la figure 3.23

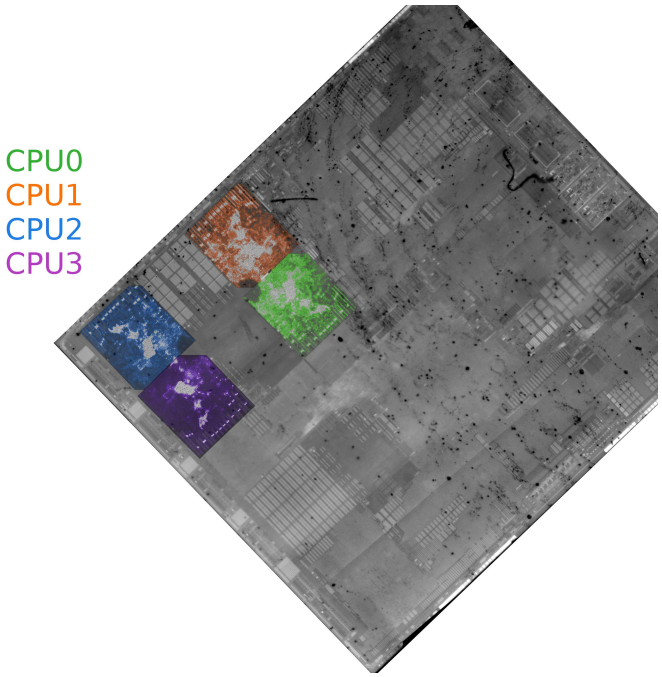



FIGURE 3.23 – Résultats des captures de photoémission pour identifier les différents CPUs.

Nous retrouvons le même arrangement des CPUs entre la photoémission et les positions sensibles en injection électromagnétique. Cela montre que les zones sensibles sont proches des CPUs.

### 3.5.2 Influence de la fréquence

Pour la majorité des expériences, la fréquence de fonctionnement de la cible était fixée à 1.2 GHz. La gigue temporelle étant dépendante du nombre d'instructions, cela permettait de la minimiser. Nous cherchons à évaluer si la fréquence de fonctionnement de la cible influe sur la sensibilité de la puce. Pour cela, le nombre de fautes produit pour différentes fréquences de fonctionnement est représenté sur la figure 3.24. L'impulsion de tension est réalisée avec le générateur Avtech, avec une amplitude de 360 V et une durée d'impulsion de 6 ns. Le durée du retard interne au générateur d'impulsions de tension est variée entre 0 et 1000 ns, par pas de 5 ns. 300 injections sont réalisées avec les mêmes caractéristiques d'impulsions (amplitude, durée et retard).

Il est donc possible de fauter le CPU 3 à des fréquences de fonctionnement de 1.2 GHz, 1.152 GHz, 1.094 GHz, 998 MHz et 800 MHz. Nous obtenons environ 60 fautes au maximum, pour des délais de 140 ns pour la fréquence de 1200 MHz, 145 ns pour 1152 MHz, 220 ns pour 1094 MHz, 350 ns pour 998 MHz. Pour une fréquence de

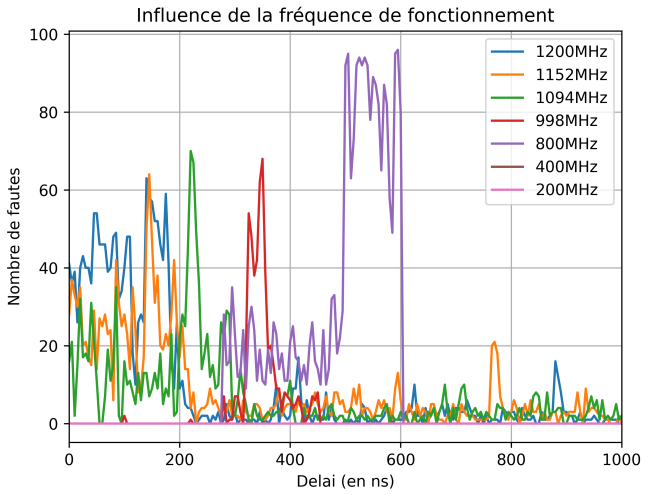



FIGURE 3.24 – Nombre de fautes pour différentes fréquences de fonctionnement.

fonctionnement de 800 MHz, la durée de la zone sensible est de 100 ns, et le nombre de fautes maximal est de 90. En revanche, il n'a pas été possible de réussir des injections de fautes pour des fréquences de fonctionnement de 200 et 400 MHz. La tension d'alimentation du CPU est de 1.05 V pour les fréquences de 200 et 400 MHz, 1.15 V à 800 MHz et 1.35 V au-dessus. Bien que la carte propose théoriquement une vitesse de fonctionnement à 533 MHz, son implémentation n'a pas fonctionné.

Si nous considérons uniquement les résultats présentés sur la figure 3.24 dont le modèle de faute correspond à un saut d'instruction, nous obtenons la figure 3.25.

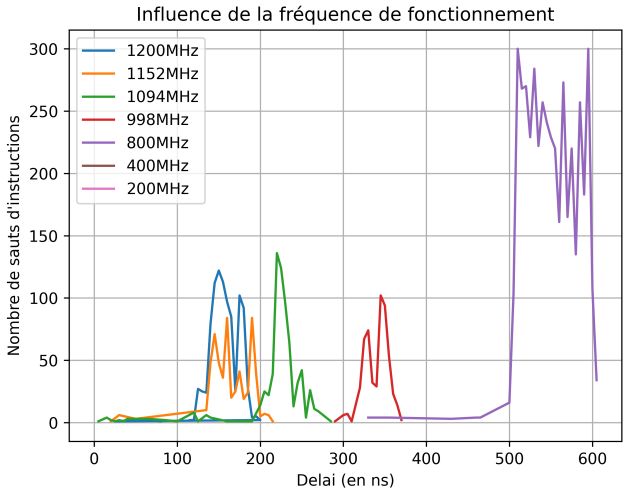



FIGURE 3.25 – Nombre de sauts d'instructions pour différentes fréquences de fonctionnement.

Le nombre de sauts d'instructions, et donc de fautes facilement exploitables, est d'environ 100 fautes pour les fréquences de fonctionnement comprises entre 998 MHz et 1.2 GHz. Pour la fréquence de 800 MHz, le nombre maximal de sauts d'instructions obtenus est de 300. Le nombre de sauts d'instructions correspond au nombre d'instructions qui ont été modifiées, ainsi une faute peut produire plusieurs sauts d'instructions. Dans le cas de la fréquence de 800 MHz, nous obtenons en moyenne 3.3 sauts d'instructions par résultats fautés. Nous observons que malgré un nombre de fautes similaire pour les différentes fréquences d'horloge, le nombre de sauts d'instructions à 800 MHz est plus important. À cette fréquence, l'apparition de plusieurs sauts d'instructions pour une même impulsion est quasi-systématique, ce qui signifie qu'une faute engendre plusieurs sauts d'instruction. La proportion de fautes obtenue est alors plus importante qu'aux autres fréquences.

Le modèle de fautes obtenues lorsque la carte fonctionne à 800 MHz est comparé avec ce que nous avons à 1.2 Ghz au le tableau 3.4.

| Type de faute | Occurrence à 1.2 GHz | Occurrence à 800 MHz |
|---|---|---|
| Sauts d'instructions | 55 % | 48.7 % |
| Modification de l'opérande destination des instructions | 22.6 % | 2.2 % |
| Reset du demi-mot de poids fort | 3.7 % | 0.6 % |
| Rejeu | 1.9 % | 38.9 % |
| Autres | 16.8 % | 9.6 % |

TABLEAU 3.4 – Comparaison des fautes obtenues entre 800 MHz et 1.2 Ghz.

Nous constatons que le nombre de sauts d'instructions reste relativement similaire entre les deux fréquences de fonctionnement. En revanche, le nombre de modifications d'opérande destination des instructions est diminué, contrairement au nombre de rejeu qui est très nettement augmenté. Un fonctionnement forcé de la cible à 800 MHz est donc relativement intéressant, car cela permet d'obtenir un nombre de fautes important et facilement interprétable.

### 3.5.3 Influence de la forme de l'impulsion de la perturbation

#### Polarité de l'impulsion

Il a été vu au chapitre 2 que la polarité de l'injection influait sur les caractéristiques des champs engendrés, nous étudions désormais l'effet sur un SoC. Les injections ont été réalisées avec une impulsion de tension positive et négative, produite depuis un générateur de marque Avtech, avec une amplitude de 360 V et une durée d'impulsion de 6 ns. Les cartographies spatiales des zones sensibles sont tracées sur la figure 3.26. Le seuil de la tension négative permettant d'injecter des fautes

est de -300 V, et les résultats sont présentés pour des tensions de +380 et -380 V. Le code source 3.4, manipulant 58 registres sans dépendance de données a été utilisé.

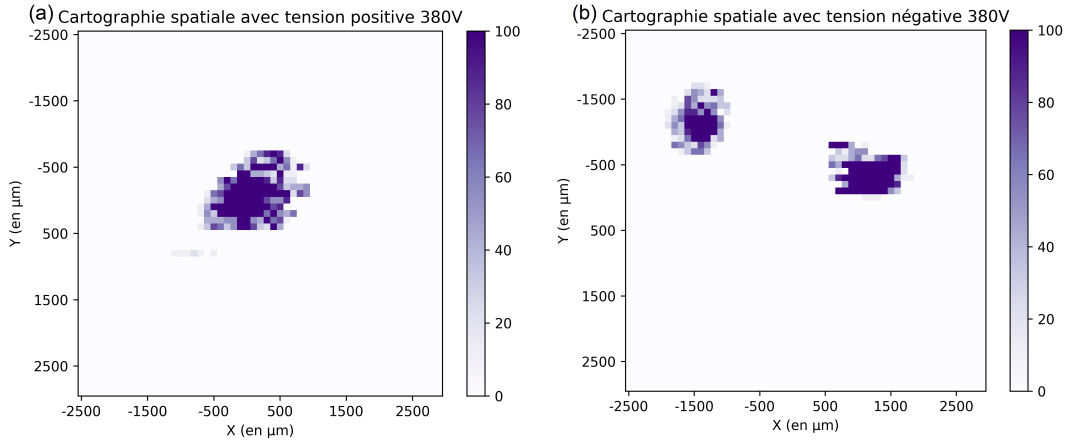



FIGURE 3.26 – Cartographies spatiales des fautes pour une impulsion de 380 V **(a)** et de -380 V **(b)**.

Nous observons que la zone sensible à l'injection de fautes avec la tension négative est différente de celle avec la même tension positive. Le nombre de fautes maximal obtenu par position est similaire à celui avec des tensions positives. En revanche, le résultat des injections de faute varie. Par exemple, le taux de sauts d'instructions diminue à 19 %, celui de rejeu à 6.7 %, le taux de reset du demi-mot de poids fort à 5.1 % et les modifications d'opérandes destination à 3.3 %. Environ 65 % des fautes ne sont pas explicables par le modèle présenté.

Nous constatons donc que la modification de la polarité de l'impulsion modifie la zone sensible ainsi que le modèle de fautes. Un dispositif de suppression des rebonds a été présenté au paragraphe 2.5.5, il est intéressant de voir comment il modifie les fautes produites.

### Impulsion de tension monopolaire

Une diode est insérée au niveau de la sonde afin de supprimer les rebonds et de générer une impulsion de tension monopolaire positive aux bornes de la sonde. Cette méthode a été présentée par Toulemont et al. [100] et étudiée dans la section 2.5.5. Le signal impulsionnel est produit depuis un générateur de marque Avtech, avec une amplitude de 360 V et une durée d'impulsion de 6 ns. Le code 3.4, manipulant 58 registres sans dépendance de données a été utilisé. Sur environ 200 000 injections, 8329 fautes sont obtenues. Nous ne comptons qu'un seul saut d'instruction et 34 reset du demi mot de poids fort. En revanche, plus de 95 % des fautes concernent uniquement le registre 4, elles sont représentées dans le tableau 3.5.

Le premier résultat correspond à celui qui est attendu lorsqu'il n'y a pas d'injection de fautes. Les résultats présentés dans les lignes suivantes ne peuvent pas s'expliquer par le modèle de faute présenté dans la section 3.2.3. Ces résultats sont

| Registre 4 | Occurrences (%) |
|---|---|
| BFFFFFFFFFEEEEEE | 198 031 (96.0 %) |
| BFFFE7FFFDEEEEEE | 4 819 (2.3 %) |
| BFFFF7FFFDEEEEEE | 874 (0.4 %) |
| BFF9A7FDFDEEEEEE | 738 (0.4 %) |
| BFFBA7FFFDEEEEEE | 573 (0.2 %) |
| BFFBE7FFFDEEEEEE | 561 (0.2 %) |
| BFFFF7FFFFEEEEEE | 347 (0.2 %) |
| BFF9A3FDFDEEEEEE | 80 (<0.1 %) |
| ... | ... |

TABLEAU 3.5 – Résultats obtenus sur le registre 4 avec une impulsion monopolaire.

difficiles à interpréter étant donné que les fautes sont présentes sur un seul registre. La génération de ce type d'impulsion étant relativement récente, l'étude des effets des fautes n'a pas été réalisée.
Nous en concluons cependant que la modification de l'impulsion perturbe différemment la puce ce qui crée des effets différents. Ainsi, il pourrait être possible de faire varier la forme du signal d'excitation pour varier les fautes générées.

## 3.6 Conclusion

Dans ce chapitre, une méthode pour réaliser des injections de fautes sur une cible complexe a été présentée. Elle consiste dans un premier temps à utiliser un code avec une plage temporelle suffisamment longue pour faciliter la synchronisation entre la perturbation électromagnétique et son exécution. Dans un second temps, des cartographies spatiales à haute tension et avec une sonde à large diamètre sont effectuées pour déterminer des zones sensibles aux perturbations électromagnétiques, c'est-à-dire produisant des crash et redémarrages de la cible. Enfin, les cartographies sont affinées en tension et spatialement avec une sonde de diamètre plus fin. Cette méthode a été appliquée à un processeur présent sur des smartphones, avec un système d'exploitation basée sur Linux et a permis la réalisation d'injections de fautes par perturbations électromagnétiques.

Le fonctionnement de la commande SU, utilisée dans l'ensemble des systèmes Linux, a été corrompu permettant une élévation de privilège. La mise en place de cette attaque demande l'utilisation d'un signal de synchronisation basé sur un GPIO.

Un modèle de faute au niveau du jeu d'instruction justifiant la majorité des effets a été présenté. Les effets majoritaires sont des sauts d'instructions, mais la modification de l'opérande destination des instructions, le reset du demi-mot de poids fort et le rejeu d'instructions sont aussi présents. Différentes études ont été menées

au niveau microarchitectural. Les perturbations provoquent des effets assimilables à un saut d'instruction, lors du transfert des instructions entre la cache L1I et le CPU.

Une injection de fautes par perturbations électromagnétiques sur cible complexe avec un système d'exploitation a été réalisée ainsi que son exploitation. Des tests permettant le relâchement des contraintes expérimentales ont été réalisés. 3 des 4 CPUs ont pu être perturbés par des perturbations électromagnétiques, et des injections de fautes ont été réussies pour des fréquences de fonctionnement du processeur entre 800 MHz et 1.2 GHz. Le changement de fréquence modifie le modèle de fautes. Enfin, les effets des impulsions de tension avec une polarité positive et négative ont été comparés, ainsi qu'avec des impulsions de tension monopolaires. Ces derniers types d'impulsions produisent des effets différents de ceux avec l'impulsion de tension de l'état de l'art, ouvrant la possibilité à de nouvelles attaques.

L'ensemble de ces résultats montrent que les injections de fautes par perturbations électromagnétiques peuvent être appliquées avec succès sur des plateformes mobiles. Ainsi, face à ces menaces, une contre-mesure sera proposée au chapitre 4.

# Chapitre 4 : Mitigation des attaques par injection de fautes par perturbations électromagnétiques

Dans la science-fiction, notamment les X-Men issus de l'univers Marvel des comics books [92], l'ennemi Magnéto maîtrise le magnétisme tandis que le Professeur Charles-Xavier cherche à le contrer afin de protéger l'humanité. Charles-Xavier est aussi capable de détecter la présence et les intentions des autres mutants et de les contrer de façon surhumaine. Un clin d'œil à cet univers est fait dans ce chapitre, en appelant ChaXa le nouveau dispositif de contre-mesure, breveté en janvier 2021.

## Sommaire du chapitre

Les contre-mesures aux attaques matérielles consistent à protéger les circuits intégrés pour garantir leurs sécurité, confidentialité et intégrité. Il existe plusieurs dispositifs proposant la protection des circuits intégrés, mais aucune n'est connue pour assurer la sécurité de la cible contre tous les types d'attaques matérielles. Il est donc actuellement nécessaire de prévoir différentes solutions complémentaires et compatibles entre elles. Dans ce contexte, nous proposons un dispositif unique fournissant simultanément :

- **Un blindage passif** atténuant les fuites électromagnétiques et l'effet des perturbations électromagnétiques ou lasers
- **Une détection des attaques par écoute électromagnétique** lors de l'approche d'une sonde d'écoute
- **Un brouillage actif contre les attaques par écoute électromagnétique**
- **Une détection des attaques par injection de fautes par perturbations électromagnétiques** lors de l'approche d'une sonde d'attaque et d'une impulsion électromagnétique
- **Une détection d'intrusion et protection contre la rétro-ingénierie** en assurant sa propre supervision, c'est-à-dire en détectant un endommagement du blindage. Le sondage ou la modification du circuit lors de son fonctionnement n'est pas réalisable.

Les attaques physiques par observation des canaux cachés ou par injection de fautes peuvent être réalisées en ciblant les faces avant ou arrière des composants. Ainsi, afin de réaliser une protection efficace, il est nécessaire de proposer un système protégeant toutes les faces vulnérables du circuit.

## 4.1 Description du dispositif ChaXa

### 4.1.1 Principe de fonctionnement

L'architecture générale de principe du dispositif de protection et de supervision contre les attaques physiques est illustré dans la figure 4.1. Il consiste à déposer un polymère chargé de particules de ferrites sur la surface cible. Aux deux extrémités du blindage en ferrite ainsi constitué, des sondes d'émission et de réception sont positionnées, que nous appellerons successivement SEC pour Sonde d'Émission ChaXa et SRC pour Sonde de Réception ChaXa. Cela permet de concevoir un système d'émission/réception de faible épaisseur. La sonde d'émission (SEC) produit un signal électromagnétique qui est ensuite transmis de proche en proche par flux magnétique transitoire grâce aux particules de ferrite recouvrant le circuit cible jusqu'à la sonde de réception (SRC).

Nous observons sur l'illustration un boîtier au format DIP, décapsulé, avec la ferrite positionnée au centre. Les deux spires, à gauche, constituent la SEC et les trois spires, à droite, la SRC.

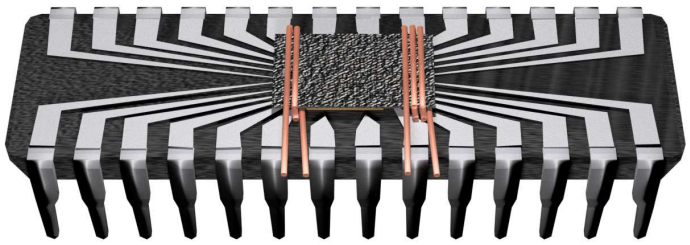


FIGURE 4.1 – Illustration de l'architecture du dispositif de contre-mesure ChaXa.

Le polymère chargé par les particules de ferrite agit comme un blindage atténuant les ondes électromagnétiques le traversant. Ce blindage permet lors d'une attaque par écoute électromagnétique de diminuer l'intensité du rayonnement électromagnétique issu du circuit cible, rendant la conduite de l'attaque plus difficile. Il permet aussi, dans le cas d'une injection de faute électromagnétique, d'atténuer la perturbation électromagnétique afin de rendre inefficace l'injection de fautes. La SEC associée au dispositif engendre un flux électromagnétique périodique qui est capté par la SRC. Cette partie active du dispositif détecte l'approche d'une sonde d'attaque ou d'écoute comportant un noyau de ferrite et également toute détérioration du dispositif effectué dans le but de lui faire perdre ses propriétés.

Nous distinguons sur la figure 4.2 le dispositif situé au-dessus du circuit cible, un ATmega328P embarqué sur une plateforme Arduino Uno. Nous pouvons y retrouver la ferrite avec ses deux bobines ainsi qu'une sonde d'écoute électromagnétique.

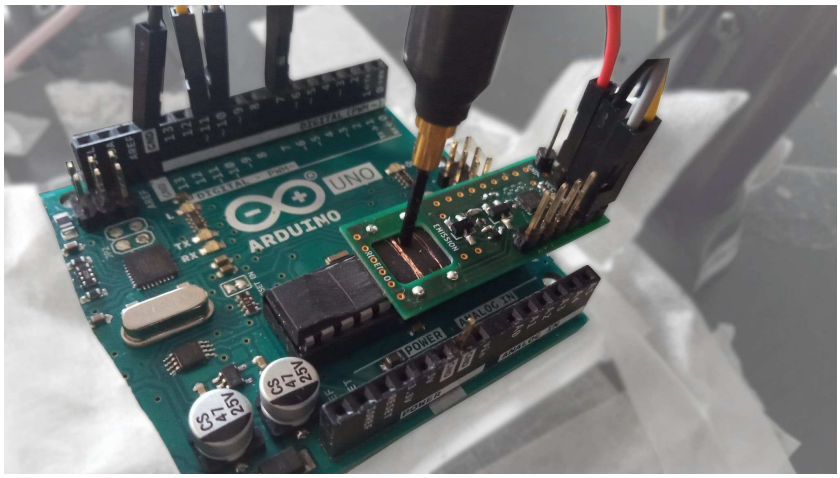



FIGURE 4.2 – Dispositif de protection ChaXa disposé au-dessus d'un microcontrôleur lors d'une attaque par écoute électromagnétique.

La communication entre l'ATmega328P et le dispositif ChaXa est réalisée via un protocole UART. La SEC et la SRC comprennent un nombre de spires compris entre 1 et 10. Cependant, pour une meilleure sensibilité de détection, il est recommandé de composer la SEC de 2 à 3 spires et la SRC de 2 à 5 spires.

### 4.1.2 Schéma électrique de principe du dispositif

Le dispositif est composé :

— d'au moins une feuille ou couche de ferrite en alliage d'oxyde de fer, Nickel-Zinc ou Manganèse-Zinc.

— d'un étage d'émission, noté E sur la figure 4.3, relié à la SEC et adapté pour émettre des impulsions de courant électrique dans la bobine d'émission.

— d'un étage de réception, noté R sur la figure 4.3, relié à la SRC et adapté à la détection de l'amplitude crête de la tension électrique engendrée par le flux magnétique transitoire aux bornes de la bobine de réception.

— d'un convertisseur analogique/numérique, relié à l'étage de réception pour informer le système électronique et/ou autre microcontrôleur via un bus, des variations de l'amplitude crête aux bornes de la bobine de réception.

— d'une électronique de gestion basée sur un microcontrôleur. Il est noté µC sur la figure 4.3.

La représentation schématique 4.3 illustre le dispositif de protection et supervision d'un circuit intégré face aux attaques par injection et écoute électromagnétiques.

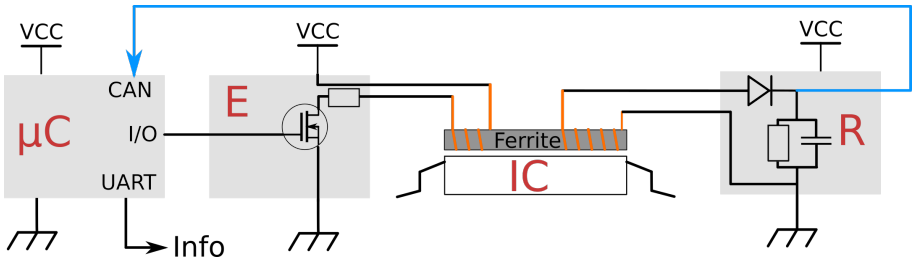



FIGURE 4.3 – Représentation schématique du dispositif de protection et de supervision.

L'étage d'émission est principalement composé d'un transistor déclenchant la génération des impulsions via la SEC. Un port GPIO contrôle la fermeture du transistor afin de générer une variation de courant ($\frac{di}{dt}$) qui engendre un flux magnétique ($\frac{dB}{dt}$) au niveau de la SEC.

L'étage de réception est principalement composé d'une résistance de 100 kΩ et d'un condensateur 1 nF. La SRC récolte le flux magnétique et produit une force électromotrice. Cette force est redressée à l'aide d'une diode et charge une capacité réservoir. La mesure la tension aux bornes de la résistance et du condensateur permet de déterminer le flux magnétique reçu au niveau de la SRC. Cette valeur est relative à l'amplitude des signaux reçus. Enfin, des diodes, non représentées sur le schéma, limitent l'effet des pics de tensions aux bornes de la SRC, dans le cas où un attaquant réalise une injection électromagnétique à proximité de la sonde.

Nous retrouvons sur la figure 4.4 le dispositif ChaXa sur lequel nous pouvons observer les bus de commande (UART) et d'alimentation (VCC et GND).


FIGURE 4.4 – Illustration de l'architecture du dispositif de contre-mesure ChaXa.

Le microcontrôleur de gestion est un ATtiny416, dont la dimension est de 3 mm*3 mm. La consommation électrique du dispositif est de 7 mA lors d'une alimentation avec une tension de 5 V. Cette consommation est principalement due à celle du microcontrôleur ATtiny416. Il serait cependant possible de basculer le microcontrôleur en mode *sleep* durant les temps d'attente afin de diviser la consommation par un facteur 3 [68].

## 4.2 Preuve de concept

La preuve de concept du dispositif est effectuée en vérifiant qu'il est capable de détecter une atteinte de l'intégrité de la cible et qu'il protège contre les attaques par perturbation et observation.

### 4.2.1 Vérification de l'intégrité de la cible

Afin de contrôler de l'intégrité de la cible, nous vérifions l'intégrité du dispositif de protection. Nous cherchons aussi à détecter des menaces passives proches de la cible, telle que l'approche d'une sonde.

#### Contrôle de l'intégrité de ChaXa

Une des fonctions premières du dispositif est de vérifier l'intégrité du circuit cible, c'est-à-dire de vérifier que les signaux internes au circuit intégré ne sont pas modifiés. Pour cela, il faut s'assurer que le boîtier n'est pas endommagé, ce qui revient à vérifier l'intégrité du dispositif ChaXa. Pour ce faire, la continuité électromagnétique entre les deux sondes est vérifiée régulièrement afin de détecter toute altération. Ces vérifications sont exécutées à des instants aléatoires afin de limiter le risque qui est lié à l'identification de l'instant de la vérification permettant à un attaquant de fausser

les mesures en fournissant à la SRC un signal équivalent au fonctionnement nominal. Le montage présenté sur la figure 4.5.a est réalisé afin de contrôler le fonctionnement de l'intégrité.

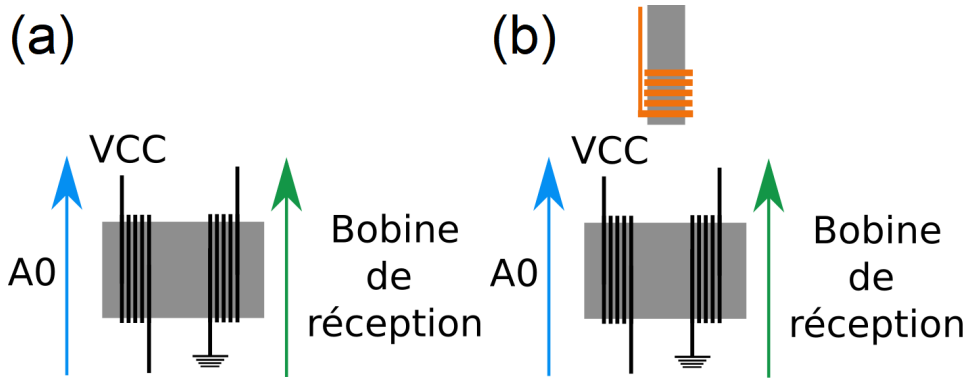



FIGURE 4.5 – Montage pour la vérification de l'intégrité : sans **(a)** et en présence à proximité d'une sonde d'injection ou d'écoute dotée d'une ferrite **(b)**.

La tension A0, en orange, est celle aux bornes du port GPIO contrôlant la génération des impulsions de courant. Sur la figure 4.6, nous pouvons observer la tension A0, celle aux bornes de la bobine de réception et celle aux bornes de la capacité de charge (A1).

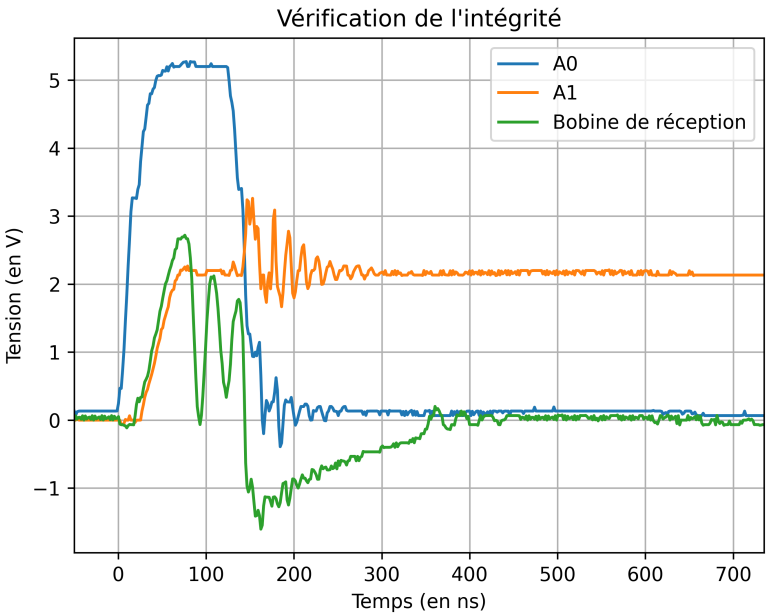



FIGURE 4.6 – Vérification de l'intégrité (état normal).

La tension du port A0 augmente jusqu'à 5.2 V, déclenchant ainsi une impulsion de tension dans la SEC. La tension aux bornes de la SRC augmente alors jusqu'à 2.7 V,

puis la tension aux bornes de la capacité (A1) augmente jusqu'à 2.2 V. Lorsque la tension du port A0 redescend à 0 V, après 150 ns environ, nous observons une variation parasitant l'ensemble des mesures. Ces oscillations s'atténuent en 100 ns. La tension aux bornes de la capacité diminue lentement et elle est égale à 2.1 V 700 ns après le début de l'impulsion. Nous pouvons donc confirmer la création d'une force électromotrice qui charge la capacité du circuit de réception. Un flux magnétique circule donc entre la SEC et la SRC.

Un attaquant pourrait penser à détériorer la feuille de ferrite pour approcher sa sonde et éliminer l'effet de blindage. Cela a donc pour effet d'endommager le blindage. Afin de s'assurer qu'il n'est pas possible d'altérer l'état de la protection sans détection, l'effet de divers degrés des dégradations de la feuille de ferrite sur la tension aux bornes de la capacité est représenté sur la figure 4.7.

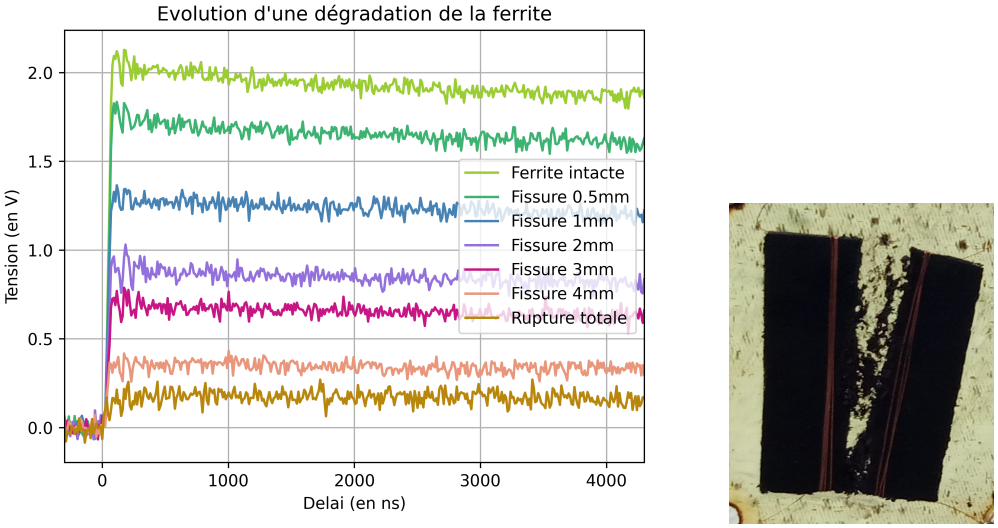



FIGURE 4.7 – Évolution d'une dégradation de la feuille de ferrite.

En l'absence de dégradation de la ferrite, la tension maximale mesurée est égale à 2.0 V. La mesure de la tension par l'ADC est réalisée 700 ns après la génération de l'impulsion, la valeur mesurée correspond donc à une tension de 1.9 V. Lorsqu'une fissure de taille 0.5 mm*1 mm est réalisée, la tension à l'instant de la mesure par l'ADC est de 1.7 V. La tension diminue ensuite avec l'évolution de la dégradation. Il est donc possible de fixer une valeur de tension de référence à 1.8 V qui correspond à une ferrite intacte pour une valeur supérieure et à une ferrite dégradée pour une valeur inférieure. Dans cette preuve de concept, une fissure d'une taille inférieure à 0.5 mm est décelable par le microcontrôleur de supervision qui en informe le microcontrôleur cible, via une communication UART. Le dispositif est donc capable de détecter une altération de sa propre intégrité.

Un attaquant pourrait imaginer leurrer le solénoïde récepteur par un simple pont ré-

sistif. Afin de contrer cette attaque, il est possible de varier la durée et la tension des perturbations. Ainsi, la tension aux bornes de la SRC ne sera pas proportionnelle à la perturbation et l'attaque sera contrée. Il est aussi envisageable de réaliser plusieurs mesures successives de la tension aux bornes de la capacité réservoir afin de limiter ce type d'attaques. Avec ces deux variantes, il sera nécessaire de réaliser une phase de calibration supplémentaire pour prendre en compte les différentes perturbations produites ou la décroissance de la tension aux bornes de la capacité réservoir.

### Détection de menace passive proche de la cible : sonde composée de ferrite

Afin de protéger le circuit contre les analyses par écoutes électromagnétiques (EMA) et l'injection de fautes par perturbations électromagnétiques (EMFI), le processus de contrôle de l'intégrité vise également à détecter la présence d'une sonde espionne composée de ferrite.

La puissance du flux électromagnétique transmise entre la SEC et la SRC est diminuée en raison d'une mutuelle inductance qui s'établit avec la sonde (d'injection ou d'écoute) et qui perturbe le flux incident. En cas de présence d'une sonde à base de ferrite, ce couplage est plus important permettant par conséquent de détecter la présence d'une sonde dans un champ proche à la cible.

De manière similaire à la figure 4.6 et tel que présenté dans le montage 4.5.b, nous retrouvons sur la figure 4.8 la tension en sortie du port GPIO (A0), et aux bornes de la capacité (A1) et de la SRC. Cependant, cette figure a été obtenue suite aux tests de rapprochement d'une sonde composée d'une ferrite de diamètre 1 mm à la surface de la protection ChaXa. La figure 4.8 montre que le dispositif est capable de détecter la tentative d'attaque par cette sonde, en écoute ou injection.

En effet, la tension du port A0 augmente jusqu'à 5 V, déclenchant ainsi une impulsion de tension dans la SEC. La tension aux bornes de la SRC augmente alors jusqu'à 1 V, puis la tension aux bornes de la capacité (A1) augmente elle aussi jusqu'à 1 V. Nous observons des oscillations sur la tension de la SRC, après la diminution à 0 V de la tension du pin A0. Ces oscillations ne modifient pas la tension aux bornes de la capacité qui, diminue lentement, et dont la valeur nominale est de 1.0 V 700 ns après le début de l'impulsion. Nous pouvons remarquer que la tension mesurée aux bornes du condensateur (A1) est très inférieure à celle dans le cas d'un fonctionnement nominal. La valeur de la tension mesurée 700 ns après le début de l'impulsion diminue de 2.1 V à 1.0 V. Le dispositif décele l'approche d'une sonde de ferrite de diamètre 1 mm à une distance maximale de 1 mm.

### Évolution de la détection d'une menace passive en fonction de la température

Le dispositif est fourni pour fonctionner dans une plage de température située de 25°C à 70°C. La mesure de la tension aux bornes du condensateur est effectuée directement depuis le microcontrôleur en utilisant son ADC. Les valeurs mesurées par l'ADC sur une plage de température allant de 25°C à 70°C sont présentées sur la

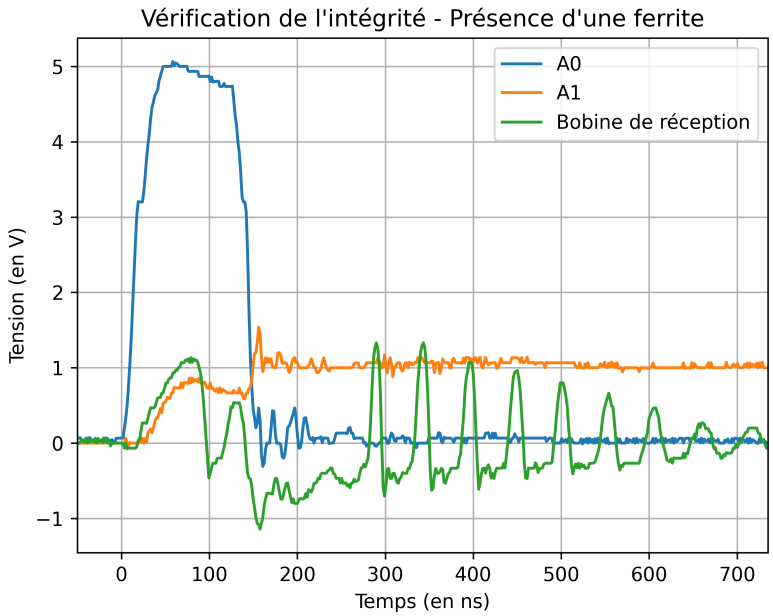



FIGURE 4.8 – Vérification de l'intégrité (présence d'une ferrite).

figure 4.9. Pour cela, l'ensemble du dispositif est placé dans une enceinte thermique dont la température est contrôlée. Une centaine de mesures ont été réalisées avec un pas de 5°C.

La courbe grise correspond aux mesures effectuées en fonctionnement nominal et celle en rouge à celles réalisées avec la présence sonde d'attaque composée de ferrite au-dessus du dispositif. Nous constatons la présence d'une certaine dérive des mesures en fonction de la température. Sans présence d'une sonde d'attaque, la valeur moyenne retournée par l'ADC fluctue entre 610 et 645, en fonction de la température et avec la présence d'une sonde d'attaque, entre 550 et 590. Les valeurs obtenues dans les deux conditions, avec et sans présence d'une sonde d'attaque, sont différentes pour une température donnée. Ainsi, il est possible de définir un seuil, sur les valeurs retournées par l'ADC, permettant de repérer la présence d'une sonde d'attaque ou d'écoute.

Il peut être choisi d'avoir un seuil d'alerte fixe, par exemple à la valeur 600, mais certaines alertes de détection de modification de l'intégrité du dispositif lors de températures supérieures à 65°C peuvent être des faux positifs. Une reconfiguration est possible pour avoir un seuil d'alerte variable en fonction de la température de l'environnement. Le microcontrôleur ATmega328P possédant un capteur de température interne, la mise en place de ce système est relativement aisée. Le dispositif est donc capable de déceler la présence d'une sonde d'écoute ou d'injection à base de ferrite ferromagnétique pour des températures de circuit allant de 25 à 70°C.

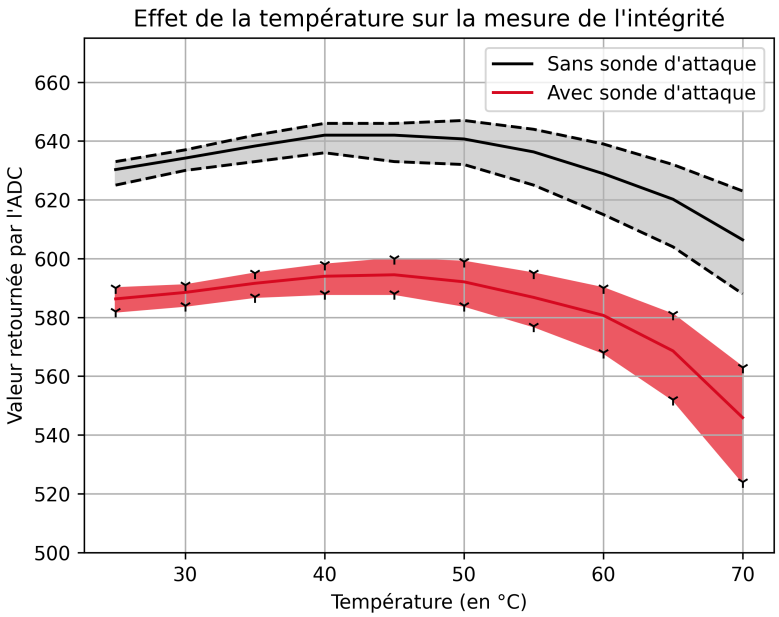



FIGURE 4.9 – Tension aux bornes du condensateur, mesurée par un ADC, en fonction de la température.

### 4.2.2 Protection contre les attaques par perturbation

Les attaques par injection de fautes perturbent le fonctionnement d'un circuit. L'objectif de ChaXa est de protéger les composants contre ces attaques qu'elles soient de type électromagnétique ou laser.

#### Injection de fautes par perturbations électromagnétiques

**Blindage électromagnétique** Le blindage ferromagnétique est à la fois l'élément de base du dispositif ChaXa, et le premier niveau de protection proposé par ce dispositif. Pour mettre en évidence l'efficacité de ce blindage, une expérience a été réalisée sur un microcontrôleur ATmega328P décapsulé. Ce microcontrôleur exécute un code manipulant les registres comme présenté dans le code 2.1. L'exécution de ce code est susceptible d'être mise en défaut dès que la tension de consigne du générateur d'impulsion de tension est supérieure à 90V. Un générateur d'impulsion de tension Avtech AVRK-4-B est utilisé afin de produire des impulsions d'une durée de 6 ns. Une sonde d'injection, dite de référence, composée d'une ferrite conique d'un diamètre de base 1500 µm et de 10 spires est utilisée. Nous retrouvons sur la figure 4.10 le dispositif de blindage fixé au-dessus même du microcontrôleur ATmega328P.

Quand la surface du microcontrôleur cible est couverte par une feuille de ferrite, il n'est pas possible de fauter l'ATmega pour des tensions délivrées allant jusqu'à 550 V. Nous en concluons que le blindage introduit une protection contre les injections électromagnétiques d'au moins un facteur 550/90=6 (ou 15.7dB) sur l'ampli-

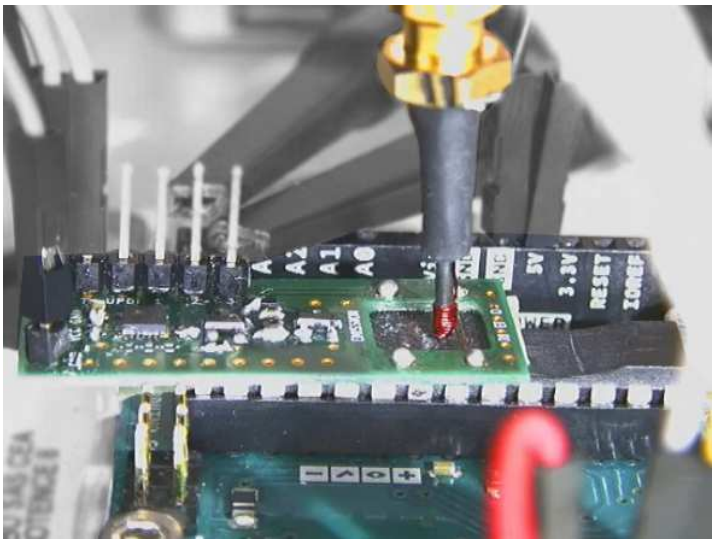



FIGURE 4.10 – Dispositif protégeant un microcontrôleur durant une attaque par injection de faute basé sur les perturbations électromagnétiques.

tude de l'impulsion de tension à l'origine de la perturbation.

**Détection d'injection électromagnétique** La détection d'une attaque par injection électromagnétique peut être réalisée à 2 niveaux :

- **Lors de l'approche d'une sonde** par la vérification de la transmission entre les deux sondes du dispositif
- **Lors de l'impulsion électromagnétique engendrée par la sonde d'attaque** par la détection d'une surtension dans le circuit de réception

Dans le second cas, lors de la génération de la perturbation électromagnétique, un champ magnétique est émis au niveau de la sonde d'attaque et se propage jusqu'à la feuille de ferrite. Celle-ci transmet cette perturbation par guidage inductif à la SRC. Ces signaux induits aux bornes de la SRC ont pour effet de charger la capacité réservoir de surveillance et de modifier la tension nominale seuil normalement mesurée à ses bornes. La vérification expérimentale est réalisée en approchant une sonde d'injection, dite de référence, composée d'une ferrite conique de diamètre de base 1500 µm et de 10 spires de fil de diamètre 200 µm. Une impulsion de tension est générée en utilisant un générateur de marque Avtech. Nous pouvons voir sur la figure 4.11 le montage réalisant l'injection.

La tension aux bornes du condensateur du circuit de réception est mesurée durant l'impulsion, et est représentée sur la figure 4.12. L'effet de l'injection de fautes est mesuré pour des tensions de consignes du générateur Avtech de 100 et 400 V.

Nous mesurons une tension de 3 V pour une tension de consigne de 100 V, 5 V pour tension de consigne de 400 V. L'augmentation de l'amplitude de l'impulsion de tension accentue la variation de tension aux bornes du condensateur. La perturbation est donc détectable en surveillant les variations de tensions aux bornes du

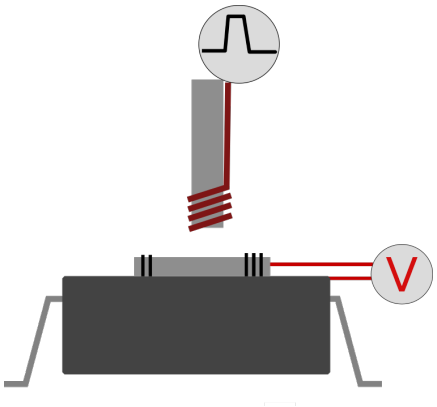



FIGURE 4.11 – Montage pour la vérification de la détection d'injection de fautes par perturbations électromagnétiques.

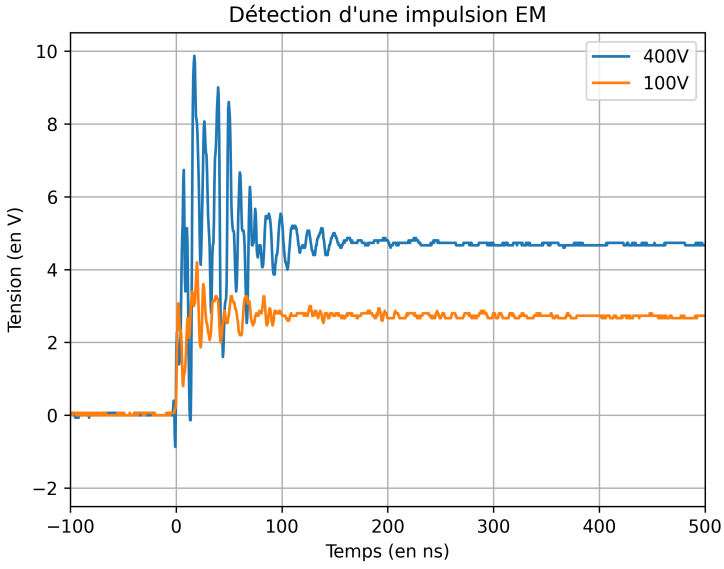



FIGURE 4.12 – Effet d'impulsions électromagnétiques, produites avec des tensions de consigne de 100 V et 400 V, sur la tension du condensateur du circuit de réception.

condensateur.

Un signal engendré par un générateur d'impulsions d'amplitude de tension de 80 V dans une sonde d'injection est détecté par le bloc de réception et peut déclencher une alerte. Nous pourrons donc détecter toutes les perturbations supérieures à cette valeur. Il a été montré en 4.2.2 que le seuil de fautes était de 550 V sur le microcontrôleur cible protégé avec la feuille de ferrite. Le dispositif détecte les tentatives d'injections électromagnétiques à des tensions bien inférieures au seuil minimum requis pour corrompre le fonctionnement du circuit.

Cette protection contre les attaques par injection de fautes électromagnétiques a donc un double effet. D'une part le blindage oblige l'attaquant à augmenter les niveaux de tensions de perturbation appliqués et d'autre part la perturbation sera détectée.

#### Injection de fautes par perturbation laser

**Blindage laser** La réalisation d'injection de fautes par perturbation laser nécessite une préparation de l'échantillon, notamment un amincissement du substrat. La présence d'une feuille de ferrite opaque empêche les signaux produits par un laser de la traverser. Un attaquant devra donc enlever le dispositif afin d'exposer la puce de silicium pour réaliser une injection de faute laser. Cependant, il a été montré en 4.2.1 que le dispositif est capable de détecter toute modification de son intégrité. Le dispositif protège donc contre les attaques par injection de fautes par perturbation laser.

### 4.2.3 Protection contre les attaques par observation

L'idée principale ici est de protéger les composants contre les attaques par observation qui permettent de retrouver les clés d'un algorithme de chiffrement. La présence d'une couche de ferrite constitue un premier niveau de protection par blindage passif, comme représenté sur la figure 4.13.b. En parallèle, nous pouvons aussi utiliser la SEC afin de générer un brouillage actif contre l'écoute side-channel, comme représenté sur la figure 4.13.c.

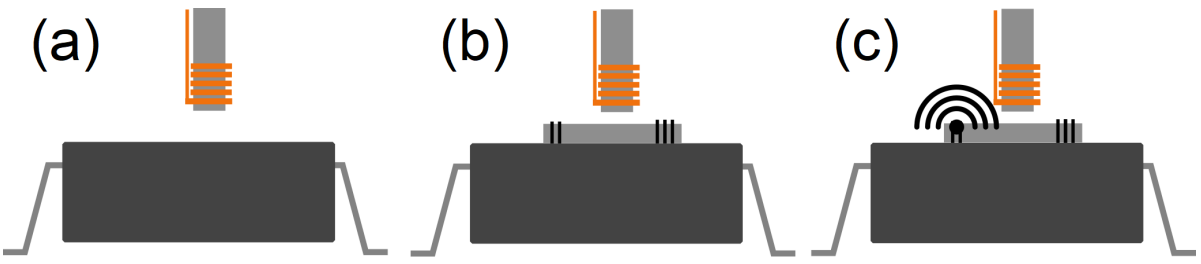



FIGURE 4.13 – Montage pour les acquisitions side-channel sans protection **(a)**, avec un blindage passif **(b)** et actif **(c)**.

Dans l'ensemble des expérimentations, la distance entre la puce et la sonde est constante. Cela signifie qu'une distance égale à l'épaisseur du dispositif ChaXa est présente lors de l'acquisition sur circuit sans protection.

### Cible de test sans protection

L'efficacité de ces mesures contre les écoutes side-channel est testée sur un AES logiciel [32] exécuté sur un ATmega328P ayant une fréquence d'horloge de 16 MHz. L'acquisition est réalisée à l'aide d'une sonde Langer RF-U 5-2 [91] et d'un amplificateur Langer PA306 [12]. Un port de sortie du microcontrôleur déclenche l'acquisition de façon synchronisée avec l'AES.

Le signal mesuré en sortie d'amplificateur est représenté sur la figure 4.14.

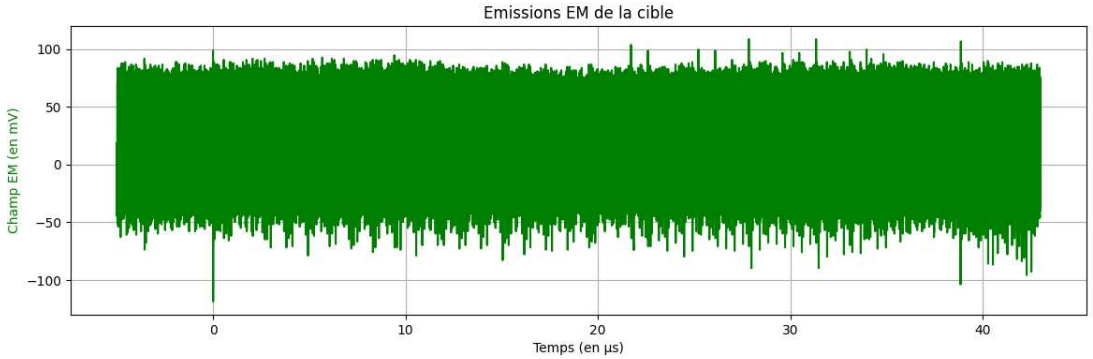



FIGURE 4.14 – Trace électromagnétique des émissions sur le circuit sans protection.

L'amplitude du signal est d'environ 150 mV. Une attaque Correlation Power Analysis (CPA) [27] est menée sur ces traces électromagnétiques afin d'en déduire la clé secrète.

Des hypothèses sur les valeurs manipulées sont effectuées afin de calculer leurs émissions de courant. Le coefficient de corrélation de Pearson entre le modèle de fuite et les données mesurées a été calculé afin d'estimer la valeur la plus probablement manipulée. En corrélant les hypothèses de fuites supposées avec un ensemble d'acquisitions expérimentales. Nous réalisons ici, l'analyse sur le 1er tour de l'AES et nous ciblons la sortie de la fonction SubBytes.

Un ensemble de 100 acquisitions a été réalisé. La figure 4.15 montre les résultats de corrélation de chaque candidat de clé en fonction du nombre d'acquisitions analysées. Chaque courbe représente l'évolution de la corrélation d'un octet avec les données expérimentales. Initialement, chaque octet a une corrélation de 1, cependant celle-ci doit diminuer pour l'ensemble des clés candidates sauf pour la clé correcte. Les résultats de l'attaque CPA sont présentés pour deux octets de la clé. Il a été choisi de représenter la meilleure et la moins bonne évolution de la corrélation (octets 2 et 15).

L'ensemble des positions de chacune des clés octets pour les 3 types d'acquisitions est présenté dans le tableau 4.1 page 174.

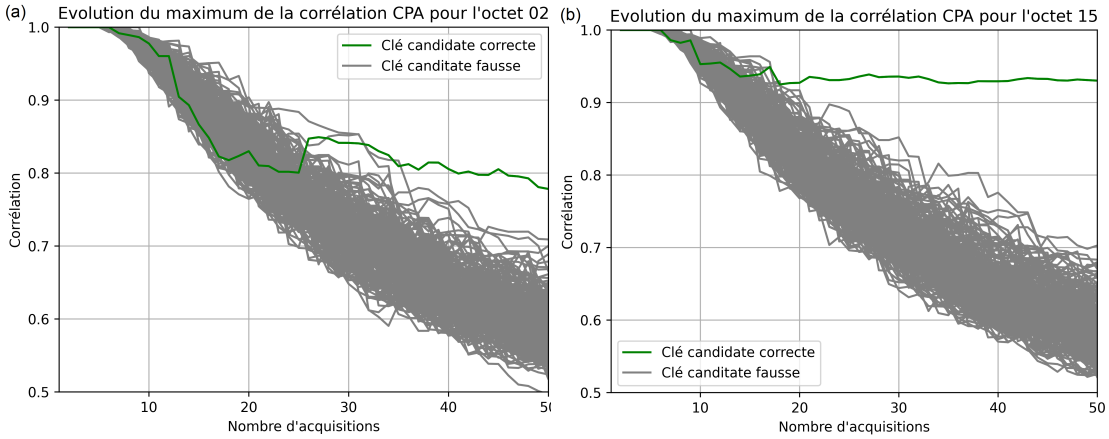



FIGURE 4.15 – Résultats de l'attaque CPA pour l'octet 0x02 **(a)** et 0x15 **(b)** sur une cible sans protection.

L'évolution de la corrélation est représentée pour 50 acquisitions. Les coefficients de corrélations obtenus pour chaque clé octet correcte, représentée en vert, varient de 0.78 à 0.93. L'attaque CPA permet de trouver l'ensemble des octets de la clé de chiffrement à l'aide d'environ 30 acquisitions. L'attaque est réussie après une durée de manipulation inférieure à 1 minute (35 secondes).

### Cible de test avec un blindage passif

Afin de tester le blindage passif, une feuille de ferrite est intercalée entre le microcontrôleur et la sonde d'écoute, comme sur la figure 4.13.b.
Le signal mesuré en sortie d'amplificateur est représenté sur la figure 4.16.

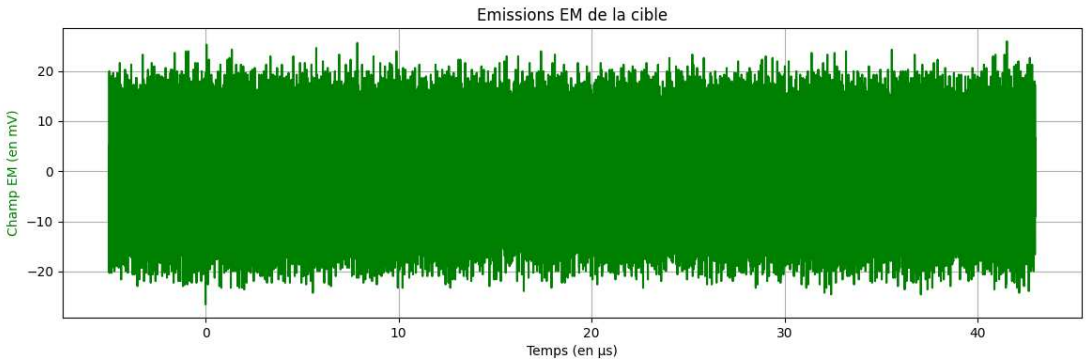



FIGURE 4.16 – Trace électromagnétique des émissions sur le circuit avec un blindage passif.

Nous constatons une atténuation de l'amplitude du signal reçu (de 150 mV à 40 mV). Une attaque CPA est réalisée en utilisant 3500 acquisitions. La figure 4.17

montre la corrélation de chaque candidat de clé en fonction du nombre d'acquisitions analysées pour deux octets de la clé (2 et 15). L'ensemble des positions de chacune des clés octets est présenté dans le tableau 4.1.

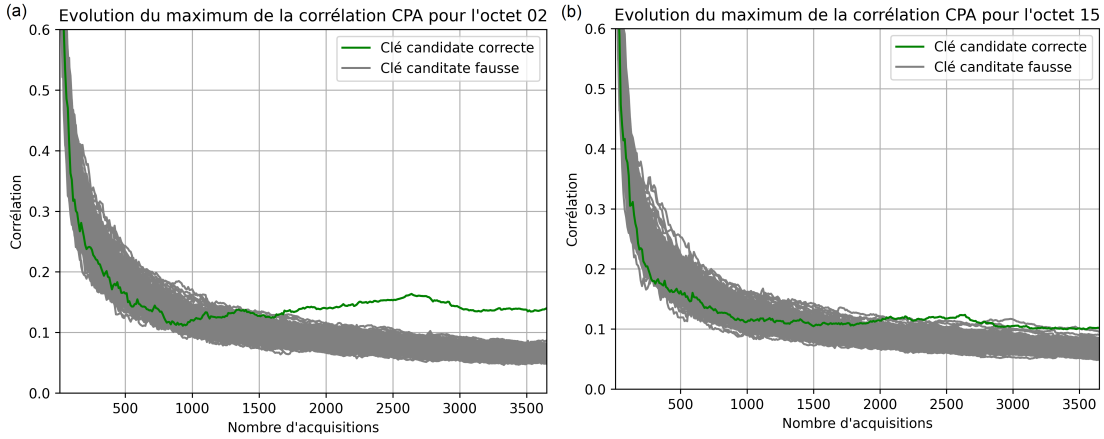



FIGURE 4.17 – Résultats de l'attaque CPA pour l'octet 0x02 **(a)** et 0x15 **(b)** sur une cible avec blindage passif.

Les coefficients de corrélations obtenus varient de 0.09 à 0.14 alors qu'ils étaient 7 fois plus élevés sans protection. Mais, en étudiant la progression du coefficient de corrélation, nous pouvons trouver la clé de chiffrement à l'aide d'environ 2500 acquisitions. L'attaque est donc réussie après une durée de manipulation de 35 minutes, soit 80 fois plus que sans protection. L'effet passif du blindage augmente donc le niveau de difficulté des attaques par écoute side-channel, mais celles-ci restent possibles. Il est donc être nécessaire de renforcer la protection.

### Cible de test avec un blindage actif

Afin de générer un blindage actif, un pin GPIO du microcontrôleur de supervision est connecté à la SEC et est alterné entre les niveaux haut et bas de façon à générer un fort champ électromagnétique. Ce bruit électromagnétique est réalisé durant l'exécution d'un code critique afin de perturber les acquisitions par écoute side-channel, comme sur la figure 4.13.c. Durant cette phase, la consommation de courant est de 70 mA tandis qu'elle est de 7 mA en fonctionnement classique. Afin de diminuer la consommation électrique, il est possible de diminuer l'intensité du brouillage, bien que cela nécessite un compromis entre consommation électrique et protection. Dans notre cas, il a été choisi de limiter la durée de la phase de brouillage au 1er tour de l'AES.

Le signal mesuré en sortie d'amplificateur est représenté sur la figure 4.18.

Nous observons des signaux d'une amplitude de 2.5 V, contre 40 mV dans le cas du blindage passif. La génération du brouillage est désynchronisée de l'exécution de l'algorithme AES, ce qui empêche de donner l'information du début de l'exécution du code AES à un attaquant.

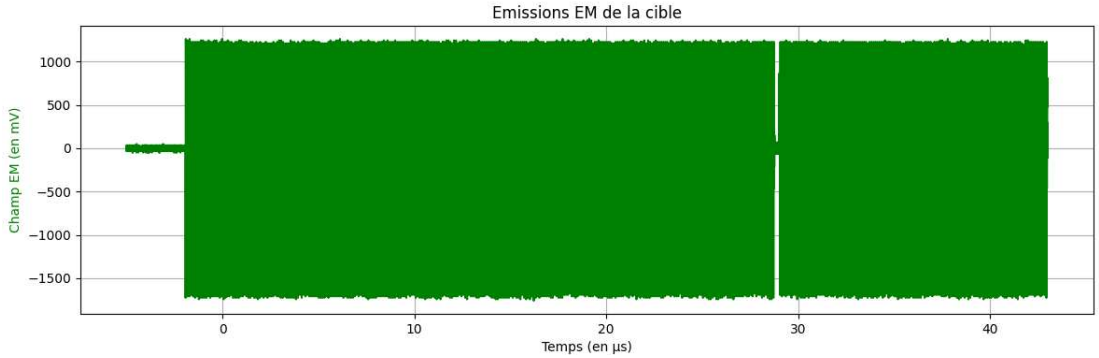



FIGURE 4.18 – Trace électromagnétique des émissions sur le circuit avec un brouillage actif.

Une attaque CPA a été réalisée en utilisant 135 000 acquisitions, ce qui correspond à une durée d'acquisitions de 24 heures. La figure 4.17 montre la corrélation de chaque candidat de clé en fonction du nombre d'acquisitions analysées pour deux octets de la clé (2 et 15). L'ensemble des positions de chacune des clés octets est présenté dans le tableau 4.1.

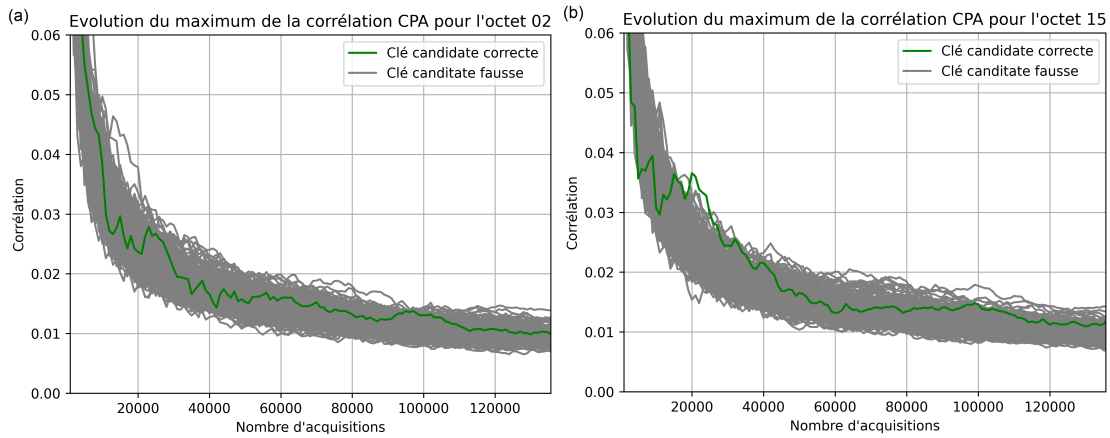



FIGURE 4.19 – Résultats de l'attaque CPA pour l'octet 0x02 **(a)** et 0x15 **(b)** sur une cible avec blindage actif.

Les coefficients de corrélations obtenus varient de 0.008 à 0.012, et la progression du coefficient de corrélation est confondue entre toutes les clés candidates. L'attaque CPA ne permet pas de trouver un octet de la clé de chiffrement. La durée de manipulation est d'environ 40 heures. La réalisation de l'attaque demande donc un temps supérieur à celle sur la cible sans blindage par au moins un facteur 4000 et au blindage passif par un facteur 40. L'amplitude des signaux mesurés impose d'effectuer un changement d'échelle verticale des acquisitions, cependant il a été vérifié que l'introduction de ce bruit de quantification n'apportait pas de changement du nombre d'acquisitions nécessaire pour retrouver la clé secrète. Ainsi, la protection est assurée par le dispositif ChaXa. Le brouillage est donc efficace contre les attaques

| Octet | Référence<br>50 acquisitions | Passif<br>3 500 acquisitions | Actif<br>135 000 acquisitions |
|---|---|---|---|
| 0 | 1 | 1 | 145 |
| 1 | 1 | 1 | 130 |
| 2 | 1 | 1 | 83 |
| 3 | 1 | 1 | 169 |
| 4 | 1 | 1 | 37 |
| 5 | 1 | 1 | 242 |
| 6 | 1 | 1 | 130 |
| 7 | 1 | 1 | 38 |
| 8 | 1 | 1 | 134 |
| 9 | 1 | 1 | 102 |
| 10 | 1 | 1 | 107 |
| 11 | 1 | 1 | 119 |
| 12 | 1 | 1 | 222 |
| 13 | 1 | 1 | 251 |
| 14 | 1 | 1 | 155 |
| 15 | 1 | 1 | 10 |

TABLEAU 4.1 – Récapitulatif des positions des octets de la clé suite à une attaque CPA.

side-channel électromagnétiques simples.

En résumé, la clé secrète de l'AES est trouvée à l'aide de 50 acquisitions sur un circuit sans protection et avec 3 500 sur le circuit protégé passivement avec une feuille de ferrite. Le tableau 4.1 montre aussi que sur le circuit protégé avec un brouillage actif, la position des octets de la clé secrète avec 135 000 acquisitions est comprise entre 10 et 251. Cela signifie que l'attaque CPA ne permettra pas d'extraire la clé secrète.

**Attaques CPA approfondies** L'attaque CPA réalisée précédemment ne permet plus de trouver la clé de chiffrement avec la protection par génération de bruit électromagnétique aléatoire. Une analyse approfondie a été effectuée afin de vérifier l'efficacité du blindage. La transformation de Fourier rapide (FFT) des signaux avec le blindage actif et sans blindage est tracée sur la figure 4.20.

Sur les deux figures, nous pouvons observer un pic à 16 MHz correspondant à la fréquence de fonctionnement de l'ATmega. Sur la figure avec le brouillage, nous observons bien les émissions dues au blindage à une fréquence de 10 MHz et ses harmoniques. Cela correspondant à la fréquence de basculement de l'état de la sortie du microcontrôleur générant le brouillage.
Nous pouvons envisager deux solutions pour limiter l'effet du brouillage et conserver les fuites de l'AES. D'une part, réaliser un filtrage passe-bande entre 10 et 20 MHz, ce qui conserve les fuites si leur fréquence est proche de celle de fonctionnement du

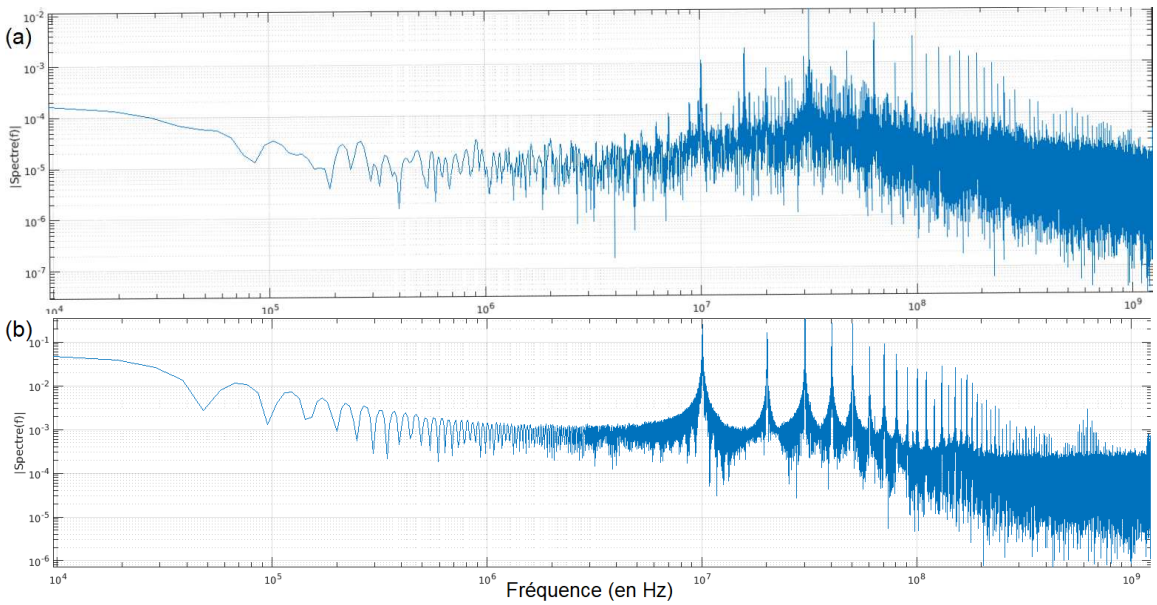



FIGURE 4.20 – Comparaison du module de la FFT du signal sans blindage **(a)** et avec le blindage actif **(b)**.

circuit. D'autre part, effectuer un filtrage passe-bas avec une fréquence de coupure de 17 MHz si la fréquence des fuites est inférieure à celle du circuit. Les résultats de ces traitements sont représentés sur la figure 4.21.

Nous pouvons constater que la partie brouillage du signal est bien atténuée dans les deux cas. Une attaque CPA est alors effectuée sur ces 135 000 traces filtrées. Malgré ces traitements, il n'a pas été possible d'extraire la clé de chiffrement.

La combinaison d'un blindage passif et d'un brouillage actif est donc efficace contre des attaques side-channel électromagnétiques plus complexes.

## 4.3 Protection de cibles complexes

Des essais ont permis de valider le fonctionnement du dispositif ChaXa sur des microcontrôleurs, mais les cibles SoC doivent aussi être protégées. Pour cela, il est aussi nécessaire de vérifier que le fonctionnement de ChaXa ne perturbe pas celui du processeur.

### 4.3.1 Dimensions de la protection à base de ferrite

Pour des composants de type SoC, la surface de la puce peut être assez importante, de l'ordre de plusieurs centaines de $mm^2$ (9.2 mm*19.6 mm pour un Intel i9-9900K par exemple). La protection contre les injections électromagnétiques pourra être assurée par la présence de la feuille de ferrite. Cependant, il est nécessaire de s'assurer que l'intégrité de la ferrite peut être vérifiée sur des surfaces aussi grandes.

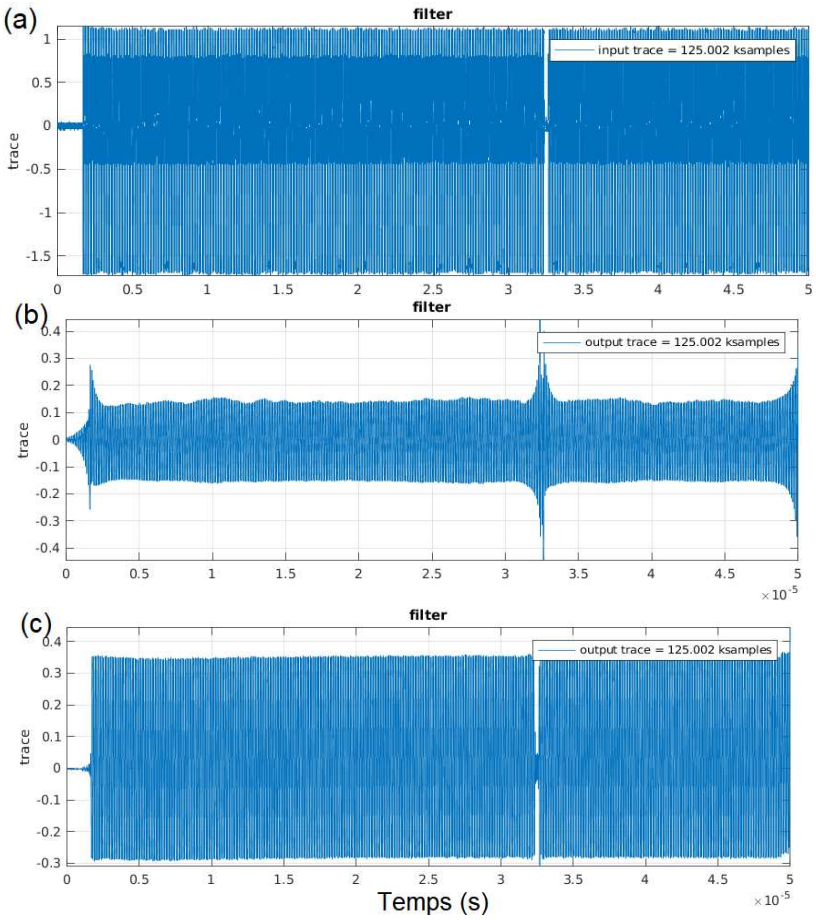



FIGURE 4.21 – Acquisitions électromagnétiques réalisées avec un brouillage actif **(a)**, et après un filtrage passe-bande entre 10 et 20 MHz **(b)** ou un filtrage passe-bas à 17 MHz **(c)**.

Il a été choisi de protéger la cible utilisée dans le chapitre 3, c'est-à-dire une carte de développement pour cibles mobiles comportant un SoC embarquant 4 Cortex-A53 et fonctionnant à une fréquence de 1.2 GHz. La surface du silicium est d'environ 7*8 $mm^2$ et la zone maximale sensible aux perturbations électromagnétiques mesure 3*3 $mm^2$. Un dispositif de protection composée d'une ferrite de 7*8 $mm^2$ et de deux sondes séparées d'une distance de 6 mm a été réalisé.

Une analyse similaire aux paragraphes 4.2.1 a été menée. La conclusion est que le dispositif détecte l'approche d'une sonde avec ferrite d'un diamètre 1 mm. La vérification de l'intégrité du dispositif est fonctionnelle, le détecteur protège des surfaces compatibles avec celles des cibles mobiles.

Afin d'utiliser le dispositif ChaXa sur la plateforme de développement, il est nécessaire de réaliser des changements de niveaux de tension sur la communication UART, étant donné que le dispositif ChaXa utilise un niveau 0-5 V tandis que la carte de développement entre 0 et 1.8 V. Pour cela, nous utilisons un LevelShifter de la marque Digilent. L'alimentation du dispositif ChaXa est directement réalisée depuis la carte de développement, comme présenté sur la figure 4.22.

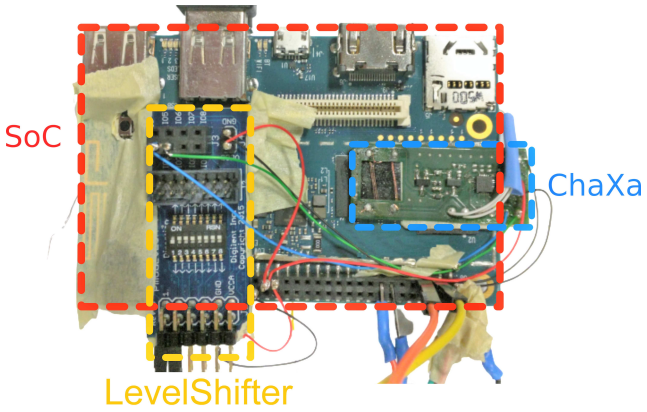



FIGURE 4.22 – Photographie du dispositif ChaXa sur une plateforme mobile.

Le dispositif est visible sur la partie droite de la photographie. L'alimentation (VCC + GND) est reliée à la carte de développement. Le bus de communication UART est relié au LevelShifter, convertissant des signaux à 1.8 V du SoC vers 5 V pour ChaXa et inversement. Ce LevelShifter est aussi relié à la carte de développement.

Dans le cas où il est nécessaire de couvrir des surfaces plus importantes, il est possible d'ajouter une seconde ferrite pour accroître la transmission du champ $\vec{B}$ entre les SEC/SRC. Afin de protéger des surfaces encore plus grandes, il peut être nécessaire d'ajouter une SRC et un second circuit de traitement pour doubler la distance à protéger.

Alternativement, pour la protection de dispositifs de petites dimensions, telles que des cartes à puces, il est possible de ne pas utiliser de ferrite mais de conserver les parties d'émission et de réception. Sur des distances de l'ordre de 1 mm, le couplage entre la SEC et la SRC peut être réalisé sans la présence de feuille de ferrite. Les sondes peuvent être réalisées avec des pistes de métaux, et donc directement ajoutées lors de l'étape de conception. Le blindage contre les attaques par injections de fautes devra être assuré en ajoutant une feuille de ferrite au-dessus du circuit, dans le boîtier par exemple. Cette solution a l'avantage d'être plus facilement intégrable dans un processus de fabrication.

### 4.3.2 Compatibilité électromagnétique du brouillage avec le fonctionnement du SoC

Il est important de s'assurer que le fonctionnement du dispositif de brouillage ne perturbe pas celui de la cible en particulier dans le cas de la génération d'un bruit électromagnétique. Pour vérifier cela, un algorithme AES128 a été implémenté sur la carte de développement et un brouillage est déclenché pendant son exécution afin de le protéger. La figure 4.23 présente les résultats des acquisitions où nous pouvons constater la présence d'un brouillage.

Le déclenchement du brouillage est réalisé via la communication UART entre la cible et le dispositif. Un délai aléatoire est volontairement introduit avant le déclenchement du brouillage. Ainsi, la durée entre le début du brouillage et de l'AES est variable empêchant une synchronisation des attaques par ce biais. Nous constatons sur la figure un décalage entre les deux brouillages, d'environ 40 µs.

Les résultats des chiffrements AES correspondent à ceux attendus. Un watchdog, protection vérifiant que le circuit n'est pas bloqué à une étape, n'émet aucun avertissement, ainsi le fonctionnement de la carte n'est pas altéré par le brouillage. Nous pouvons donc envisager l'utilisation du dispositif ChaXa sur cibles mobiles.

### 4.3.3 Protection contre les attaques par perturbations

La vérification de l'efficacité du blindage contre les injections de fautes par perturbations électromagnétiques n'a pas été réalisée. Le banc d'injection utilisé dans le chapitre 3 pour réaliser les injections sur cette cible était à sa limite maximale de fonctionnement. C'est-à-dire que la tension de consigne du générateur d'impulsion de tension était proche de sa limite maximale. Ainsi il est probable que l'augmentation de la distance avec la cible à cause de l'épaisseur du dispositif ne permette plus de réaliser des fautes. Cependant, l'efficacité du blindage électromagnétique a déjà été prouvée sur microcontrôleur, ainsi nous pouvons admettre son fonctionnement sur SoC, plus complexe à perturber.

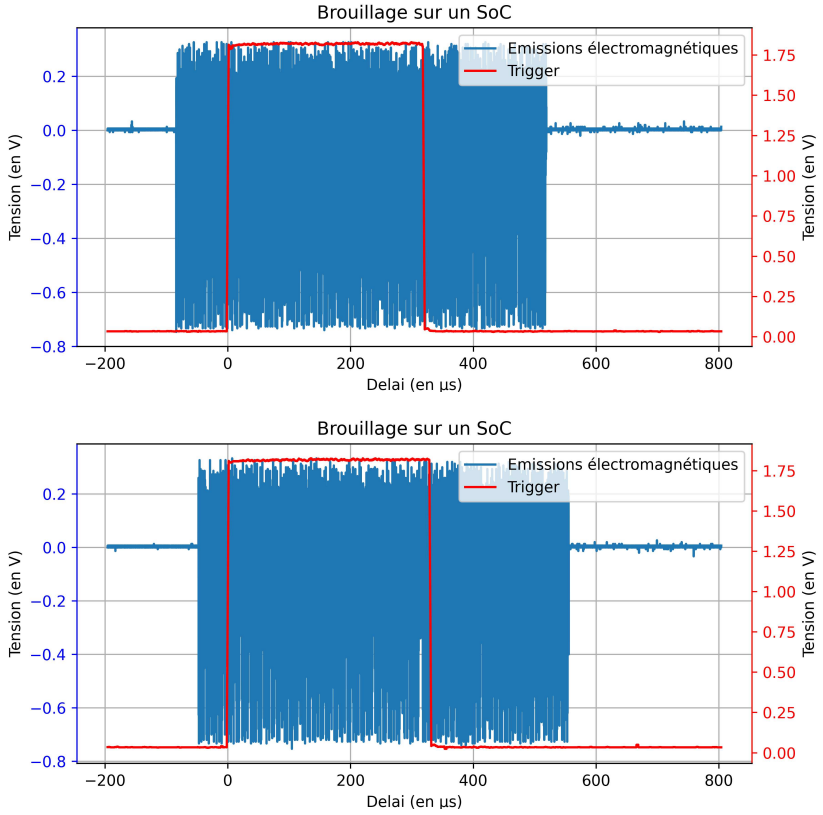



FIGURE 4.23 – Émissions électromagnétiques du processeur pendant son fonctionnement.

### 4.3.4 Protection contre les attaques par observation

Pour montrer l'efficacité de la protection par blindage passif et brouillage actif sur les cibles de type SoC. Le protocole présenté en partie 4.2.3 a été utilisé. La fréquence de fonctionnement du microprocesseur est de 1.2 GHz. Une attaque CPA est menée afin de déterminer la clé secrète d'un algorithme de chiffrement AES. Dans un premier temps, l'analyse est effectuée sur une puce sans protection, puis sur une puce avec un blindage passif, composée d'une couche de ferrite, et enfin d'un brouillage actif. L'évolution de la corrélation de chaque clé candidate en fonction du nombre d'acquisitions est présentée sur la figure 4.24.

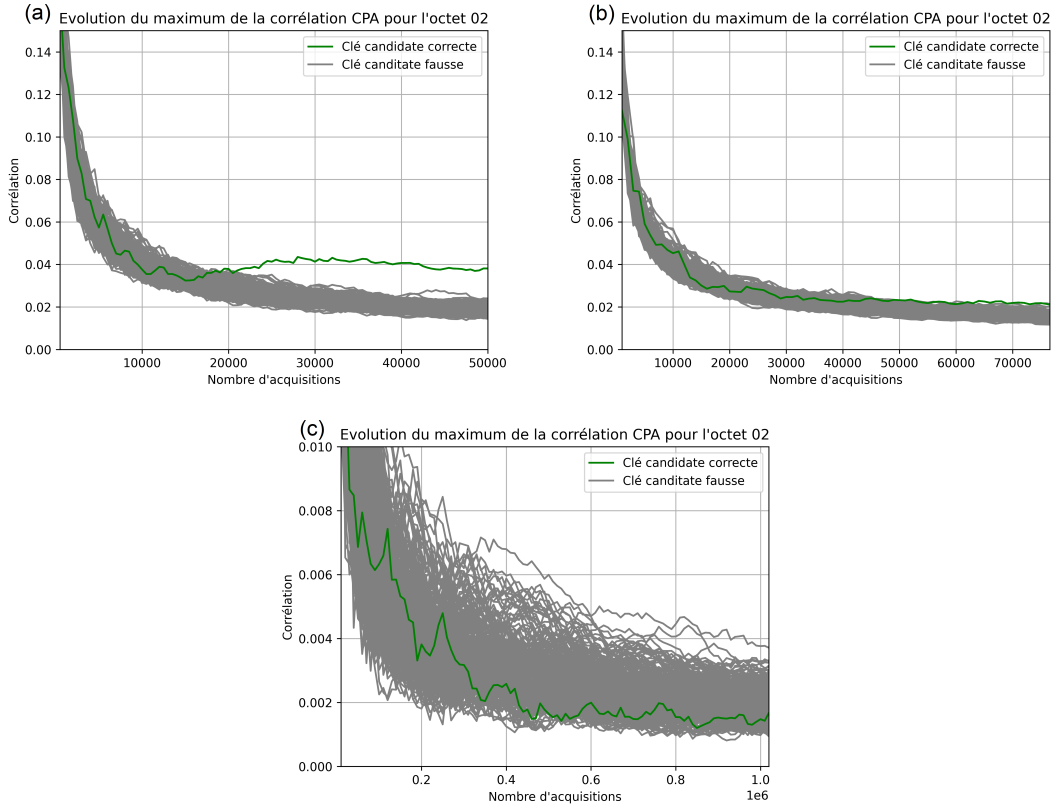



FIGURE 4.24 – Résultats de l'attaque CPA pour l'octet 02 sur une cible sans protection **(a)**, un blindage passif **(b)** et actif **(c)**.

Il a été choisi de ne représenter l'évolution que de l'octet 2 de la clé secrète, cependant les résultats sont similaires sur l'ensemble des octets de la clé secrète. L'ensemble des positions de chacune des clés octets est présenté dans le tableau 4.2.

Nous constatons que sur la cible sans protection, représentée sur la figure 4.24.a,

| Octet | Référence<br>50 000 acquisitions | Passif<br>76 550 acquisitions | Actif<br>1 019 600 acquisitions |
|---|---|---|---|
| 0 | 1 | 9 | 203 |
| 1 | 1 | 1 | 202 |
| 2 | 1 | 2 | 171 |
| 3 | 1 | 1 | 44 |
| 4 | 1 | 4 | 89 |
| 5 | 1 | 4 | 157 |
| 6 | 1 | 1 | 163 |
| 7 | 1 | 6 | 62 |
| 8 | 1 | 1 | 2 |
| 9 | 1 | 2 | 180 |
| 10 | 1 | 7 | 125 |
| 11 | 1 | 11 | 131 |
| 12 | 1 | 3 | 25 |
| 13 | 1 | 4 | 146 |
| 14 | 1 | 3 | 178 |
| 15 | 1 | 9 | 12 |

TABLEAU 4.2 – Récapitulatif des positions des octets de la clé suite à une attaque CPA.

la clé candidate correcte se différencie des autres candidates avec 20 000 acquisitions.

Sur la cible protégée avec un blindage passif, représentée sur la figure 4.24.b, avec 76 550 acquisitions, il est possible de différencier la clé correcte des autres candidates. Sur l'ensemble des octets de la clé secrète, il peut être nécessaire d'augmenter le nombre d'acquisitions ou de réaliser une attaque par brute-force pour tester quelques combinaisons d'octets candidats. Nous pouvons considérer qu'une attaque de ce type réussira.

Avec la cible protégée par ChaXa, représentée sur la figure 4.24.c, il n'est pas possible de différencier la clé secrète des autres candidates pour plus d'un million d'acquisitions. Sur l'ensemble des octets de la clé secrète, l'analyse ne permet pas de trouver un seul octet de chiffrement, ou information sur celui-ci.

Dans le tableau 4.2, nous constatons que la position des clés candidates pour l'attaque sur dispositif protégé est comprise entre 2 et 203. Ainsi, une attaque par CPA ne permet pas d'obtenir la clé secrète.

Des optimisations d'attaques consistant à réaliser un filtrage du brouillage, c'est-à-dire en utilisant un filtre stop-bande entre 10 et 20 MHz, ont été menées et n'ont pas permis d'améliorer les résultats de l'attaque CPA. Nous en concluons que le brouillage est efficace sur des cibles fonctionnant à des vitesses élevées.

Nous pouvons noter que sur ces trois campagnes, la gigue temporelle entre la levée de trigger et l'exécution de l'AES a été minimisée. Plusieurs exécutions de l'algorithme ont précédé celle sur lequel a eu lieu la mesure afin que les instructions soient mises en cache, ce qui limite la gigue et facilite l'attaque. Il aurait aussi pu être choisi de réaliser une synchronisation post-acquisition sur les traces de référence et avec un blindage passif afin d'améliorer les résultats de l'attaque. Cependant, étant donné qu'il est impossible de réaliser de resynchronisation sur les traces avec un blindage actif, cela n'a pas été réalisé. Dans une application réelle, la désynchronisation entre le code et le déclenchement de l'acquisition complexifierait d'autant plus l'attaque.

## 4.4 Conclusion

Dans ce chapitre, le fonctionnement d'un nouveau système de protection dénommé « ChaXa » a été décrit, et sa preuve de concept fournie. Ce dispositif de supervision d'un circuit intégré, breveté par le CEA en janvier 2021, a pour objectif de répondre à la problématique de sécurité des circuits sensibles contre les attaques par injection de fautes électromagnétiques. L'efficacité du dispositif ChaXa a été démontrée par la conception d'un prototype compact implémentant le schéma électronique de principe. Bien que cette protection puisse être intégrée à la phase de packaging, le prototype est proposé comme un système additionnel, autonome, que l'on place par collage à la surface de la cible à protéger : un microcontrôleur ou un microprocesseur. Nous avons implémenté le système de test et de supervision avec un protocole de communication entre la cible et ChaXa basé sur une communication UART, et un logiciel de supervision de la protection exécuté par le microcontrôleur de supervision. Enfin, la preuve de fonctionnement du dispositif a été réalisée en protégeant un microcontrôleur ATmega328P et un microprocesseur. ChaXa assure également son autoprotection par le contrôle de son intégrité physique. La liste exhaustive des protections contre les attaques physiques apportée par ChaXa est synthétisée ci-dessous :

- Contre les attaques par injections de fautes basées sur les perturbations électromagnétiques :
  - Blindage passif basé sur la couche ferromagnétique, apportant une atténuation supérieure à 15dB
  - Détection de la présence d'une sonde à base de ferrite
  - Détection des impulsions électromagnétiques
- Contre les attaques par observation :
  - Blindage passif atténuant le champ électromagnétique en provenance de la cible
  - Détection de la présence d'une sonde d'écoute passive à base de ferrite
  - Générateur de bruit électromagnétique pour perturber les mesures du champ électromagnétique effectuées par l'attaquant

- Contre les attaques par injections de fautes par perturbations laser :
  - Blindage passif basé sur la couche ferromagnétique
- Protection de la contre-mesure :
  - Vérification dynamique de l'intégrité de la couche ferromagnétique
  - Détection d'intrusions

# Conclusion et perspectives

La caractérisation et la modélisation des attaques par injections de fautes par perturbations électromagnétiques sont susceptibles d'aboutir à contourner les mécanismes de sécurité sur des cibles de type SoC. Dans le domaine de la fouille légale de données (forensic), l'exploitation des attaques physiques sur les systèmes embarqués peut être un élément clé dans les affaires judiciaires. En revanche, l'exploitation des attaques à mauvais escient risque de compromettre la sécurité des utilisateurs. Dans le cadre des travaux présentés dans cette thèse, la compréhension des mécanismes d'injection a permis de faire progresser l'efficacité des mécanismes de défense.

Le premier objectif atteint au cours de cette thèse a été l'amélioration des sondes et générateurs d'impulsions dans le but d'optimiser les caractéristiques spatio-temporelles et l'intensité des perturbations électromagnétiques. Le second objectif achevé avec succès consistait à introduire des fautes sur une cible complexe et à les exploiter dans une procédure d'élévation de privilège. Enfin, le troisième objectif était de proposer et de valider une technique de protection des circuits microprocesseurs contre les injections de fautes par perturbations électromagnétiques.

Dans un premier temps, nous avons présenté les attaques physiques ainsi qu'un état de l'art détaillé des techniques d'injection de fautes par perturbations électromagnétiques du point de vue des bancs d'injections et des modèles de fautes et méthodes d'exploitations. Différents dispositifs de protection contre les attaques matérielles ont été passés en revue, notamment pour le blindage et la détection des attaques.

Le second chapitre a montré qu'une modélisation du champ électromagnétique émis par des sondes d'injections à partir de la loi de Biot et Savart pouvait conduire à la conception de nouvelles sondes plus efficaces. L'influence de nombreux paramètres a été évaluée, de façon statique et dynamique. De nouvelles géométries de sondes ont été proposées, améliorant ainsi l'intensité du champ magnétique produit et permettant d'affiner leur localité spatiale. Le fonctionnement des générateurs d'impulsions a également été modélisé et analysé afin de comprendre le fonctionnement de l'ensemble de la chaîne d'acquisition et d'aboutir à des impulsions monopolaires. Ces travaux permettent désormais d'adapter la taille des sondes en fonction de la distance avec la cible, d'optimiser leur résolution spatiale, temporelle et l'intensité des perturbations créées.

Le troisième chapitre a exposé une méthodologie pour réussir des injections de fautes sur une cible complexe de type SoC. Un modèle de faute expliquant plus de 80% des fautes obtenues a été détaillé. Une exploitation en réalisant une élévation de privilèges sur un processeur présent dans des smartphones avec un système d'exploitation de type Linux a été réalisée. Différentes études des mécanismes de génération de fautes mettent en évidence que la corruption des instructions est réalisée durant leur transfert entre la cache L1I et le CPU. Les contraintes expérimentales ont enfin pu être relâchées conduisant à la perturbation de plusieurs CPUs, ayant des vitesses de fonctionnement entre 800 MHz et 1.2 GHz, et des impulsions de tension bipolaires avec une polarité positive ou négative ainsi que monopolaires.

Pour contrer ces menaces, le chapitre 4 propose un dispositif servant à empêcher les attaques par perturbations électromagnétiques sur cibles mobiles. ChaXa assure à la fois une protection passive et active permettant le blindage d'un circuit contre des attaques physiques utilisant des perturbations électromagnétiques, mais aussi de détecter toute tentative d'attaque, tant sur des microcontrôleurs que microprocesseurs. Son efficacité est aussi démontrée contre les attaques par écoutes électromagnétiques et injections laser.

L'amélioration des bancs d'injection de fautes doit également faire face à la complexité grandissante des cibles (technologies de 4 nm avec des fréquences de fonctionnement à 3 GHz pour le Samsung S22 par exemple). La poursuite de ces travaux conduirait à une première piste de recherche sur l'amélioration continue de la localité spatio-temporelle des sondes en étudiant de nouvelles géométries de sondes ou matériaux ferromagnétiques. Une seconde voie pourra viser la mise au point de nouveaux générateurs d'impulsions ayant une dérivée du courant en fonction du temps $\frac{di}{dt}$ bien plus importante que celle dont nous disposons actuellement.

Nous terminerons ce propos en affirmant que la recherche sur l'amélioration des attaques et le développement de contre-mesures, telles que celles effectuées dans cette thèse est nécessaire au développement de nouveaux produits, car l'efficacité et la complexité des attaques iront toujours de façon croissante durant les prochaines années. En outre, de plus en plus d'outils rendent désormais les attaques accessibles à des non-experts et à des budgets plus réduits. Les fabricants doivent prendre en compte ces menaces déjà présentes dans les listes de vulnérabilités CWE [1] [2] [3] car les attaquants auront toujours l'avantage sur les concepteurs de produits de ne pas être contraints par les questions de délais ou coûts.

1. http ://capec.mitre.org/data/definitions/624.html
2. http ://capec.mitre.org/data/definitions/625.html
3. https ://cwe.mitre.org/data/definitions/1319.html

# PUBLICATIONS [1, 2, 3, 4, 5, 6, 7]

## Journaux

- Carlton SHEPHERD, Konstantinos MARKANTONAKIS, Nico VAN HEIJNINGEN, Driss ABOULKASSIMI, Clément GAINE, Thibaut HECKMANN et David NACCACHE. "Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis". In : *Computers and Security* 111 (2021), p. 102471.

## Conférences

- Clément GAINE, Driss ABOULKASSIMI, Simon PONTIÉ, Jean-Pierre NIKOLOVSKI et Jean-max DUTERTRE. "Electromagnetic Fault Injection as a New Forensic Approach for SoCs". In : *IEEE International Workshop on Information Forensics and Security (WIFS)* (2020).
- Clément GAINE, Jean-Pierre NIKOLOVSKI, Driss ABOULKASSIMI et Jean-Max DUTERTRE. "New Probe Design for Hardware Characterization by ElectroMagnetic Fault Injection". In : *2022 International Symposium on Electromagnetic Compatibility - EMC EUROPE* (2022).
- Clément FANJAS, Clément GAINE, Driss ABOULKASSIMI, Simon PONTIÉ et Olivier POTIN. "Real-Time Frequence Detection to Synchronize Fault Injection on System-on-Chip". In : *eprint* (2022).

## Communications

- Clément GAINE, Driss ABOULKASSIMI, Jean-Pierre NIKOLOVSKI et Jean-Max DUTERTRE. *Active shielding against physical attacks by observation and fault injections: ChaXa*. Workshop on Practical Hardware Innovation in Security and Characterization (PHISIC) 2022. 2022.
- Clément GAINE, Driss ABOULKASSIMI, Simon PONTIÉ, Jean-Pierre NIKOLOVSKI et Jean-Max DUTERTRE. *Injection de fautes par perturbations électromagnétiques sur System-on-Chip*. Journées d'Attaques par Injections de Fautes (JAIF). 2021.

## Brevets

- Clément GAINE, Driss ABOULKASSIMI et Jean-Pierre NIKOLOVSKI. "FR2100695 - Dispositif de protection et de supervision d'un système électronique comprenant au moins un composant électronique, notamment contre les attaques électromagnétiques". 2021.

# Annexes

## Tableau récapitulatif des sondes

| | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| A |  |  |  |  | | |
| B |  |  |  |  |  |  |
| C |  |  |  |  |  | |
| D |  |  |  |  | | |
| E |  |  |  |  |  |  |
| F |  |  |  |  |  |  |

| Identifiant de la sonde | Diamètre de la sonde (en µm) | Diamètre du fil (en µm) | Nombre de spires | Matériau |
|---|---|---|---|---|
| A1 - Référence - cylindrique | 1500 | 200 | 10 | référence |
| A2 - Référence - conique | 1500 | 200 | 10 | référence |
| A3 - Capacitive | - | - | - | - |
| A4 - 250µm | 250 | 40 | 2 | Polymère |
| B1 - 67_0.75mm | 750 | 40 | 5 | 78 |
| B2 - 67_1mm | 1000 | 200 | 5 | 78 |
| B3 - 67_1.5mm | 1500 | 200 | 5 | 78 |
| B4 - 67_2mm | 2000 | 200 | 5 | 78 |
| B5 - 67_3mm | 3000 | 200 | 5 | 78 |
| B6 - 67_3mm_1t | 3000 | 200 | 1 | 78 |
| C1 - 78_0.75mm | 750 | 40 | 5 | 78 |
| C2 - 78_1mm | 1000 | 200 | 5 | 78 |
| C3 - 78_1.5mm | 1500 | 200 | 5 | 78 |
| C4 - 78_2mm | 2000 | 200 | 5 | 78 |
| C5 - 78_2mm_9t | 2000 | 200 | 9 | 78 |
| D1 - Sansferrite_1mm | 1000 | 200 | 5 | Plastique - PLA |
| D2 - Sansferrite_1.5mm | 1500 | 200 | 5 | Plastique - PLA |
| D3 - Sansferrite_2mm | 2000 | 200 | 5 | Plastique - PLA |
| D4 - Sansferrite_3mm | 3000 | 200 | 5 | Plastique - PLA |
| E1 - 78_cuivre | 1500 | 200 | 5 | 78 + cuivre |
| E2 - 78_cuivre+ferrite | 1500 | 200 | 5 | 78 + cuivre + ferrite |
| E3 - 78_chapeau | 1500 | 200 | 5 | 78 + chapeau |
| E4 - 78_radiale | 1500 | 200 | 9 tours radiaux | 78 + cuivre |
| E5 - 78_2mm_9t _1superposition | 2000 | 200 | 9 (5 + 4) | 78 |
| E5 - 78_2mm_9t _2superpositions | 2000 | 200 | 9 (4 + 3 + 2) | 78 |

| Identifiant de la sonde | Diamètre de la sonde (en µm) | Diamètre du fil (en µm) | Nombre de spires | Matériau |
|---|---|---|---|---|
| F1 - 78_1.5mm_250um | 1500 | 200 | 5 | 78 |
| F2 - 78_1.5mm_150um | 1500 | 150 | 5 | 78 |
| F3 - 78_1.5mm_100um | 1500 | 100 | 5 | 78 |
| F4 - 78_ruban_1t | 1500 | 100 | 1 tour ruban | 78 |
| F5 - 78_ruban_5t | 1500 | 100 | 5 tours ruban | 78 |
| F6 - 78_ruban_9t | 1500 | 100 | 9 tours ruban | 78 |

La référence du fil d'un diamètre 200 µm est Multicomp ECW0.2, d'un diamètre 150 µm est CUL100/0.15 et d'un diamètre 100 µm est CUL100/0.10. Le fil de diamètre 40 µm est de marque Spiram.

# Liste des figures

# Liste des tableaux

# Liste des codes

# Bibliographie


[8] Karim Abdellatif et Olivier Hériveaux. "SiliconToaster : A Cheap and Programmable EM Injector for Extracting Secrets". In : *FDTC 2020* (2020).

[9] Driss Aboulkassimi, Michel Agoyan, Laurent Freund, Jacques Fournier, Bruno Robisson et Assia Tria. "ElectroMagnetic analysis (EMA) of software AES on Java mobile phones". In : *2011 IEEE International Workshop on Information Forensics and Security* (2011), p. 1-6. DOI : 10.1109/WIFS.2011.6123131.

[10] *Alphanov - Banc optique de Photoémission*. URL : https://www.alphanov.com/produits-services/banc-optique-photoemission.

[11] *ALPhANOV livre un banc laser d'injection de fautes à la plateforme MicroPackS*. URL : https://www.alphanov.com/actualites/alphanov-livre-banc-laser-injection-de-fautes.

[12] *Amplificateur PA306 de Langer*. URL : https://www.langer-emv.de/en/product/preamplifier/37/pa-306-sma-set-preamplifier-100-khz-to-6-ghz/817.

[13] Ross Anderson, Mike Bond, Jolyon Clulow et Sergei Skorobogatov. "Cryptographic Processors-A Survey". In : *Proceedings of the IEEE* 94 (mars 2006), p. 357-369. DOI : 10.1109/JPROC.2005.862423.

[14] Apple, Alvin T Chang et Anna-Katrina Shedletsky. "US20150351292A1 - Wireless Electronic Device with Magnetic Shielding layer". 2015.

[15] AvTech. *Datasheet AVIR-3-B*. URL : http://www.avtechpulse.com/options/vxi.

[16] AvTech. *Datasheet AVL-5-B*. URL : http://www.avtechpulse.com/options/vxi.

[17] Josep Balasch, Daniel Arumí et Salvador Manich. "Design and validation of a platform for electromagnetic fault injection". In : *2017 32nd Conference on Design of Circuits and Integrated Systems, DCIS 2017 - Proceedings* 2017-Novem (2018), p. 1-6. DOI : 10.1109/DCIS.2017.8311630.

[18] Josep Balasch, Benedikt Gierlichs, Oscar Reparaz et Ingrid Verbauwhede. "DPA, bitslicing and masking at 1 GHZ". In : *IACR Cryptol. ePrint Arch.* 9293 (sept. 2015), p. 599-619. DOI : 10.1007/978-3-662-48324-4_30.

[19] Alessandro Barenghi, Guido Bertoni, Emanuele Parrinello et Gerardo Pelosi. "Low Voltage Fault Attacks on the RSA Cryptosystem". In : *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)* (2009), p. 23-31. doi : 10.1109/FDTC.2009.30.

[20] Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Mauro Pellicioli et Gerardo Pelosi. "Low voltage fault attacks to AES". In : *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)* (2010), p. 7-12. doi : 10.1109/HST.2010.5513121.

[21] Alessandro Barenghi, Luca Breveglieri, Israel Koren, Gerardo Pelosi et Francesco Regazzoni. "Countermeasures against fault attacks on software implemented AES". In : *WESS '10* (jan. 2010), p. 7. doi : 10.1145/1873548.1873555.

[22] David El-Baze, Jean-Baptiste Rigaud et Philippe Maurine. "A Fully-Digital EM Pulse Detector". In : *2016 Design, Automation Test in Europe Conference Exhibition (DATE)* (2016), p. 439-444.

[23] Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, Saki Osuka, Masahiro Kinugawa, Daisuke Fujimoto et Yu Ichi Hayashi. "Characterization of EM faults on ATmega328p". In : *International Symposium on Electromagnetic Compatibility, IEEE* (2019), p. 4. url : https://www.esat.kuleuven.be/cosic/publications/article-3006.pdf.

[24] Arthur Beckers, Masahiro Kinugawa, Yu Ichi Hayashi, Daisuke Fujimoto, Josep Balasch, Benedikt Gierlichs et Ingrid Verbauwhede. "Design Considerations for EM Pulse Fault Injection". In : *Smart Card Research and Advanced Aplications- CARDIS 2019* (2019), p. 1-16.

[25] Arthur Beckers, Masahiro Kinugawa, Yuichi Hayashi, Daisuke Fujimoto, Josep Balasch, Benedikt Gierlichs et Ingrid Verbauwhede. "Design Considerations for EM Pulse Fault Injection". In : *CARDIS 2019* (2020). url : https://www.esat.kuleuven.be/cosic/publications/article-3086.pdf.

[26] Jakub Breier, Shivam Bhasin et Wei He. "An electromagnetic fault injection sensor using Hogge phase-detector". In : *2017 18th International Symposium on Quality Electronic Design (ISQED)* (2017), p. 307-312. issn : 1948-3287. doi : 10.1109/ISQED.2017.7918333.

[27] Eric Brier, Christophe Clavier et Francis Olivier. "Correlation Power Analysis with a Leakage Model". In : *Proc of Cryptographic Hardware and Embedded Systems* 3156 (août 2004), p. 16-29.

[28] *Caractérisation sécurité - Micro-PackS*. url : https://www.pf-micropacks.org/fr/micro-packs/offres-et-services/caracterisation-securitaire/.

[29] *Cellebrite - UFED Premium*. url : https://cellebrite.com/en/premium/.

[30] Clément Champeix, Nicolas Borrel, Jean-Max Dutertre, Bruno Robisson, Mathieu Lisart et Alexandre Sarafianos. "Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induced currents". In : *2015 IEEE 21st International On-Line Testing Symposium (IOLTS)* (2015), p. 150-155. DOI : 10.1109/IOLTS.2015.7229849. URL : https://hal-emse.ccsd.cnrs.fr/emse-01227307.

[31] Laurent Chusseau, Rachid Omarouayache, Jeremy Raoult, Sylvie Jarrix, Philippe Maurine, Karim Tobich et al. "Electromagnetic analysis, deciphering and reverse engineering of integrated circuits (E-MATA HARI)". In : *IEEE/IFIP International Conference on VLSI and System-on-Chip, VLSI-SoC* 2015-Janua (January 2015). ISSN : 23248440. DOI : 10.1109/VLSI-SoC.2014.7004189.

[32] *Code Arduino exécutant un AES logiciel.* URL : https://gitlab.emse.fr/c.gaine/article%5C_blindage%5C_chaxa/-/blob/master/annexes/extrait%5C_code%5C_aes.ino.

[33] Brice Colombier, Alexandre Menu, Jean-Max Dutertre, Pierre-Alain Moëllic, Jean-Baptiste Rigaud et Jean-Luc Danger. "Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller". In : *Cryptology ePrint Archive: article 2018/1042* (2018). URL : https://eprint.iacr.org/2018/1042.pdf.

[34] Ang Cui et Rick Housley. "{BADFET}: Defeating Modern Secure Boot Using Second-Order Pulsed Electromagnetic Fault Injection". In : *11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17)* (2017). URL : https://www.usenix.org/conference/woot17/workshop-program/presentation/cui.

[35] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson et Assia Tria. "Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES". In : *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium, September 9, 2012* (2012), p. 7-15. DOI : 10.1109/FDTC.2012.15.

[36] Amine Dehbaoui, Amir-Pasha Mirbaha, Nicolas Moro, Jean-Max Dutertre et Assia Tria. "Electromagnetic Glitch on the AES Round Counter". In : *Constructive Side-Channel Analysis and Secure Design - 4th International Workshop, COSADE 2013* 7864 LNCS (2013), p. 17-31. ISSN : 03029743. DOI : 10.1007/978-3-642-40026-1-2.

[37] Mathieu Dumont, Mathieu Lisart et Philippe Maurine. "Modeling and Simulating Electromagnetic Fault Injection". In : *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 40.4 (2021), p. 680-693. DOI : 10.1109/TCAD.2020.3003287.

[38] Jean-max DUTERTRE, Alexandre MENU, Olivier POTIN et Jean-baptiste RIGAUD. "Microelectronics Reliability Experimental analysis of the electromagnetic instruction skip fault model and consequences for software countermeasures". In : *Microelectronics Reliability* 121 (March 2021), p. 114133. ISSN : 0026-2714. DOI : 10.1016/j.microrel.2021.114133. URL : https://doi.org/10.1016/j.microrel.2021.114133.

[39] Mahmoud ELMOHR, Haohao LIAO et Catherine GEBOTYS. "EM Fault Injection on ARM and RISC-V". In : *Proceedings - International Symposium on Quality Electronic Design, ISQED* 2020-March (2020), p. 206-212. ISSN : 19483295. DOI : 10.1109/ISQED48828.2020.9137051.

[40] FAIR-RITE. *67 Material Data Sheet - Fair Rite*. URL : https://www.fair-rite.com/67-material-data-sheet/.

[41] FAIR-RITE. *78 Material Data Sheet - Fair Rite*. URL : https://www.fair-rite.com/78-material-data-sheet/.

[4] Clément FANJAS, Clément GAINE, Driss ABOULKASSIMI, Simon PONTIÉ et Olivier POTIN. "Real-Time Frequence Detection to Synchronize Fault Injection on System-on-Chip". In : *eprint* (2022).

[42] Colin O FLYNN. *NewAE NAEAN0011 : Electromagnetic Fault Injection (EMFI) for Automotive Safety & Security Testing with ChipSHOUTER*.

[43] Clemens FRUHWIRTH. *TKS1-An anti-forensic, two level, and iterated key setup scheme*. 2004.

[7] Clément GAINE, Driss ABOULKASSIMI et Jean-Pierre NIKOLOVSKI. "FR2100695 - Dispositif de protection et de supervision d'un système électronique comprenant au moins un composant électronique, notamment contre les attaques électromagnétiques". 2021.

[5] Clément GAINE, Driss ABOULKASSIMI, Jean-Pierre NIKOLOVSKI et Jean-Max DUTERTRE. *Active shielding against physical attacks by observation and fault injections: ChaXa*. Workshop on Practical Hardware Innovation in Security and Characterization (PHISIC) 2022. 2022.

[6] Clément GAINE, Driss ABOULKASSIMI, Simon PONTIÉ, Jean-Pierre NIKOLOVSKI et Jean-Max DUTERTRE. *Injection de fautes par perturbations électromagnétiques sur System-on-Chip*. Journées d'Attaques par Injections de Fautes (JAIF). 2021.

[2] Clément GAINE, Driss ABOULKASSIMI, Simon PONTIÉ, Jean-Pierre NIKOLOVSKI et Jean-max DUTERTRE. "Electromagnetic Fault Injection as a New Forensic Approach for SoCs". In : *IEEE International Workshop on Information Forensics and Security (WIFS)* (2020).

[3] Clément GAINE, Jean-Pierre NIKOLOVSKI, Driss ABOULKASSIMI et Jean-Max DUTERTRE. "New Probe Design for Hardware Characterization by ElectroMagnetic Fault Injection". In : *2022 International Symposium on Electromagnetic Compatibility - EMC EUROPE* (2022).

[44] Karine GANDOLFI, Christophe MOURTEL et Francis OLIVIER. "Electromagnetic Analysis: Concrete Results". In : *Cryptographic Hardware and Embedded Systems - CHES 2001* (2001).

[45] GEMPLUS. "FR2893183 - Procede de protection d'un composant électronique contre les attaques par injection de faute". 2007.

[46] Daniel GENKIN, Adi SHAMIR et Eran TROMER. "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis". In : *CRYPTO* (2013).

[47] Joseph GRAVELLIER, Jean-Max DUTERTRE, Yannick TEGLIA, Philippe LOUBET-MOUNDI, Philippe LOUBET et Moundi HIGH. "High-Speed Ring Oscillator based Sensors for Remote Side-Channel Attacks on FPGAs". In : *2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig)* (2019), p. 1-8. DOI : 10.1109/ReConFig48160.2019.8994789. URL : https://hal.archives-ouvertes.fr/hal-02481050.

[48] Ludovic GUILLAUME-SAGE, Karim TOBICH, Assia TRIA, Jean-Max DUTERTRE, Philippe MAURINE, Loic ZUSSA et al. "Efficiency of a Glitch Detector against Electromagnetic Fault Injection". In : *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014* (2014), p. 1-6. DOI : 10.7873/DATE.2014.216.

[49] Wei HE, Jakub BREIER, Shivam BHASIN, Noriyuki MIURA et Makoto NAGATA. "Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection". In : *Proceedings - 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016* (2016), p. 102-113. DOI : 10.1109/FDTC.2016.13.

[50] Naofumi HOMMA, Yu Ichi HAYASHI, Noriyuki MIURA, Daisuke FUJIMOTO, Daichi TANAKA, Makoto NAGATA et Takafumi AOKI. "EM attack is non-invasive? - Design methodology and validity verification of EM attack sensor". In : *Lecture Notes in Computer Science* 8731 (2014). ISSN : 16113349.

[51] Michael HUTTER et Jörn-Marc SCHMIDT. "The Temperature Side Channel and Heating Fault Attacks". In : *IACR Cryptol. ePrint Arch.* 2014 (2013), p. 190.

[52] Sylvie JARRIX, Tristan DUBOIS, Ronan ADAM, Philippe NOUVEL, Bruno AZAIS et Daniel GASQUET. "Probe characterization for electromagnetic near-field studies". In : *IEEE Transactions on Instrumentation and Measurement* 59 (2 2010), p. 292-300. ISSN : 00189456. DOI : 10.1109/TIM.2009.2023148.

[53] Sunghyun JIN, Suhri KIM, HeeSeok KIM et Seokhie HONG. "Recent advances in deep learning-based side-channel analysis". In : *ETRI Journal* 42 (2019), p. 292-304. ISSN : 1225-6463. DOI : 10.4218/etrij.2019-0163.

[54] Evgueni KAVERINE, Sebastien PALUD, Franck COLOMBEL et Mohamed HIMDI. "Investigation on an Effective Magnetic Permeability of the Rod-Shaped Ferrites". In : *Progress In Electromagnetics Research Letters* 65 (2017), p. 43-48.

[55] Paul KOCHER, Joshua JAFFE et Benjamin JUN. "Differential Power Analysis". In : *Advances in Cryptology — CRYPTO' 99* (1999), p. 388-397. URL : http://www.cryptography.com.

[56] Thomas KORAK et Michael HOEFLER. "On the effects of clock and power supply tampering on two microcontroller platforms". In : *Proceedings - 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2014* (2014), p. 8-17. DOI : 10.1109/FDTC.2014.11.

[57] LEIDECKER. *Sucrack*. URL : https://www.leidecker.info/projects/sucrack.shtml.

[58] Naiwei LIU, Wanyu ZANG, Songqing CHEN, Meng YU et Ravi SANDHU. "Adaptive Noise Injection against Side-Channel Attacks on ARM Platform". In : *ICST Transactions on Security and Safety* 6 (19 2019), p. 159346. ISSN : 2032-9393. DOI : 10.4108/eai.25-1-2019.159346.

[59] J. LONGO, E. De MULDER et Michael TUNSTALL. "SoC it to EM: Electromagnetic side-channel attacks on a complex system-on-chip". In : *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9293 (2015), p. 620-640. ISSN : 16113349.

[60] Jason LOWE-POWER, Abdul Mutaal AHMAD, Ayaz AKRAM, Mohammad ALIAN, Rico AMSLINGER, Matteo ANDREOZZI et al. *The gem5 Simulator: Version 20.0+*. Juill. 2020. URL : http://arxiv.org/abs/2007.03152.

[61] Houssem MAGHREBI, Thibault PORTIGLIATTI et Emmanuel PROUFF. "Breaking Cryptographic Implementations Using Deep Learning Techniques". In : *IACR Cryptol. ePrint Arch.* (2016).

[62] Fabien MAJÉRIC, Eric BOURBAO et Lilian BOSSUET. "Electromagnetic security tests for SoC". In : *2016 IEEE International Conference on Electronics, Circuits and Systems, ICECS 2016* (2016), p. 265-268. DOI : 10.1109/ICECS.2016.7841183.

[63] Philippe MAURINE. "Techniques for EM fault injection: Equipments and experimental results". In : *Proceedings - 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2012* (2012). DOI : 10.1109/FDTC.2012.21.

[64] Philippe MAURINE, Jean-Max DUTERTRE, Sébastien ORDAS, Ludovic GUILLAUME-SAGE, Karim TOBICH et Philippe MAURINE. "Evidence of a new EM-induced fault model". In : *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2015), p. 50-51. ISSN : 16113349.

[65] Nourdin Ait el MEHDI. "Analyzing the Resilience of Modern Smartphones Against Fault Injection Attacks". DELF, 2019.

[66] Alexandre MENU, Shivam BHASIN, Jean-Max DUTERTRE, Jean-Baptiste RIGAUD et Jean-Luc DANGER. "Precise spatio-temporal electromagnetic fault injections on data transfers". In : *Proceedings - 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2019* (2019), p. 1-8. DOI : 10.1109/FDTC.2019.00009.

[67] Alexandre MENU, Jean-Max DUTERTRE, Olivier POTIN, Jean-Baptiste RIGAUD et Jean-Luc DANGER. "Experimental analysis of the Electromagnetic instruction Skip Fault Model". In : *15th Design and Technology of Integrated Systems in Nanoscale Era (DTIS)* (2020). DOI : 10.1109/DTIS48698.2020.9081261.

[68] MICROCHIP. *Datasheet ATtiny212/214/412/414/416*. 2020.

[69] Amir-pasha MIRBAHA, David NACCACHE, Anne-Lise RIBOTTA, Michel AGOYAN, Jean-max DUTERTRE et Assia TRIA. "How to Flip a Bit ?" In : *2010 IEEE 16th International On-Line Testing Symposium* (2010), p. 235-239. DOI : 10.1109/IOLTS.2010.5560194.

[70] Noriyuki MIURA, Zakaria NAJM, Wei HE, Shivam BHASIN, X T NGO, Makoto NAGATA et Jean-Luc DANGER. "PLL to the rescue: A novel EM fault countermeasure". In : *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (2016), p. 1-6. DOI : 10.1145/2897937.2898065.

[71] David P. MONTMINY, Rusty O. BALDWIN, Michael A. TEMPLE et Mark E. OXLEY. "Differential electromagnetic attacks on a 32-Bit microprocessor using software defined radios". In : *IEEE Transactions on Information Forensics and Security* 8 (12 2013), p. 2101-2114. ISSN : 15566013. DOI : 10.1109/TIFS.2013.2287600.

[72] Nicolas MORO, Amine DEHBAOUI, Karine HEYDEMANN, Bruno ROBISSON et Emmanuelle ENCRENAZ. "Electromagnetic Fault Injection: Towards a Fault Model on a 32-bit Microcontroller". In : (2013), p. 77-88. DOI : 10.1109/FDTC.2013.9.

[73] Colin O'FLYNN. *ChipSHOUTER-PicoEMP*. 2021. URL : https://github.com/newaetech/chipshouter-picoemp.

[74] Colin O'FLYNN et Jasper van WOUDENBERG. *The Hardware Hacking Handbook - Breaking Embedded Security with Hardware Attacks*. Sous la dir. de No Starch PRESS. 2021.

[75] Rachid OMAROUAYACHE, Jere RAOULT, Sylvie JARRIX, Laurent CHUSSEAU et Philippe MAURINE. "Magnetic Microprobe Design for EM Fault Attack". In : *2013 International Symposium on Electromagnetic Compatibility* (2013), p. 949-954. ISSN : 2325-0364. DOI : 978-1-4673-4980-2/13/$31.00.

[76] Sébastien ORDAS, Ludovic GUILLAUME-SAGE et Philippe MAURINE. "EM injection: Fault model and locality". In : *Proceedings - 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2015* (2015). DOI : 10.1109/FDTC.2015.9.

[77] Gilles PIRET et Jean-Jacques QUISQUATER. "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad". In : *Workshop on Crypto-graphic Hardware and Embedded Systems (CHES 2003)* (2003). DOI : 10.1007/978-3-540-45238-6.

[78] François POUCHERET, Karim TOBICH, Mathieu LISART, Laurent CHUSSEAU, Bruno ROBISSON et Philippe MAURINE. "Local and direct EM injection of power into CMOS integrated circuits". In : *Proceedings - 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2011* (2011). DOI : 10.1109/FDTC.2011.18.

[79] Julien PROY, Karine HEYDEMANN, Alexandre BERZATI, Fabien MAJÉRIC et Albert COHEN. "Studying EM Pulse Effects on Superscalar Microarchitectures at ISA Level". In : *ACM International Conference Proceeding Series* (2019). DOI : 10.1145/3339252.3339253. URL : http://arxiv.org/abs/1903.02623.

[80] Pengfei QIU, Dongsheng WANG, Yongqiang LYU et Gang QU. "VoltJockey: Breaking SGX by Software-Controlled Voltage-Induced Hardware Faults". In : *2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)* (2019), p. 1-6. DOI : 10.1109/AsianHOST47458.2019.9006701.

[81] Jeremy RAOULT, Pierre PAYET, Rachid OMAROUAYACHE et Laurent CHUSSEAU. "Electromagnetic coupling circuit model of a magnetic near-field probe to a microstrip line". In : *EMC Compo 2015 - 2015 10th International Workshop on the Electromagnetic Compatibility of Integrated Circuits* (978 2015), p. 29-33. DOI : 10.1109/EMCCompo.2015.7358325.

[82] Lionel RIVIERE, Zakaria NAJM, Pablo RAUZY, Jean-Luc DANGER, Julien BRINGER et Laurent SAUVAGE. "High precision fault injections on the instruction cache of ARMv7-M architectures". In : *Proceedings of the 2015 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2015* (2015), p. 62-67. DOI : 10.1109/HST.2015.7140238.

[83] Laurent SAUVAGE. "Electric probes for fault injection attack". In : *2013 Asia-Pacific Symposium on Electromagnetic Compatibility, APEMC 2013* (2015), p. 1-4. DOI : 10.1109/APEMC.2013.7360655.

[84] Jörn-Marc SCHMIDT et Michael HUTTER. "Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results". In : *Proceedings of the Austrochip (2007)* (2007).

[85] SEPI'88. *Primo simposio nazionale su sicurezza elettromagnetica nella protezione dell'informazione.* 1998.

[86] SEPI'91. *Symposium on electromagnetic security for information protection.* 1991.

[87] Davood Shahrjerdi, Jeyavijayan Rajendran, Siddharth Garg, Farinaz Koushanfar et Ramesh Karri. "Shielding and securing integrated circuits with sensors". In : *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD* 2015-Janua (January 2015), p. 170-174. ISSN : 10923152. DOI : 10.1109/ICCAD.2014.7001348.

[88] Claude Shannon. "Communication in the Presence of Noise". In : *Proceedings of the I.R.E* (1949).

[1] Carlton Shepherd, Konstantinos Markantonakis, Nico van Heijningen, Driss Aboulkassimi, Clément Gaine, Thibaut Heckmann et David Naccache. "Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis". In : *Computers and Security* 111 (2021), p. 102471.

[89] Sergei P. Skorobogatov. "Local heating attacks on flash memory devices". In : *2009 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2009* (2009), p. 1-6. DOI : 10.1109/HST.2009.5225028.

[90] Sergei P. Skorobogatov et Ross J. Anderson. "Optical Fault Induction Attacks". In : Lecture No (2003), p. 2-12.

[91] *Sonde RF-U 5-2 de Langer*. URL : https://www.langer-emv.de/en/product/rf-passive-30-mhz-up-to-3-ghz/35/rf2-set-near-field-probes-30-mhz-up-to-3-ghz/272/rf-u-5-2-h-field-probe-30-mhz-up-to-3-ghz/16.

[92] Lee Stan, Kirby Jack et Brodsky Sol. *X-Men*. 1963.

[93] National Institute of Standards et Technology. *Advanced Encryption Standard (AES) FIPS197*. 2001. URL : http://csrc.nist.gov/csor/.

[94] National Institute of Standards et Technology. *Digital Signature Standard (DSS) FIPS186*. National Institute of Standards et Technology, juill. 2013. DOI : 10.6028/NIST.FIPS.186-4. URL : https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[95] Adrian Tang, Simha Sethumadhavan et Salvatore Stolfo. "CLKSCREW: Exposing the perils of security-oblivious energy management". In : *26th USENIX Security Symposium (USENIX Security 17)* (2017), p. 1057-1074. URL : https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/tang.

[96] Niek Timmers et Cristofaro Mune. "Escalating Privileges in Linux Using Voltage Fault Injection". In : *Proceedings - 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2017* 2017-Janua (2017), p. 1-8. DOI : 10.1109/FDTC.2017.16.

[97] Niek Timmers, Albert Spruyt et Marc Witteman. "Controlling PC on ARM Using Fault Injection". In : *Proceedings - 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016* (2016), p. 25-35. DOI : 10.1109/FDTC.2016.18.

[98] Randy Torrance et Dick James. "The State-of-the-Art in IC Reverse Engineering". In : *CHES* (2009).

[99] J Toulemont, J M Galliere, P Nouet, Eric Bourbao et Philippe Maurine. "A Simple Protocol to Compare EMFI platforms". In : *IACR Cryptol. ePrint Arch.* (2020), p. 1-9.

[100] J. Toulemont, G. Chancel, J. M. Galliere, F. Mailly, P. Nouet et P. Maurine. "On the scaling of EMFI probes". In : *2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)* (sept. 2021), p. 67-73. doi : 10.1109/FDTC53659.2021.00019. url : https://ieeexplore.ieee.org/document/9565575/.

[101] Oualid Trabelsi, Laurent Sauvage et Jean-Luc Danger. "Characterization at logical level of magnetic injection probes". In : *2019 Joint International Symposium on Electromagnetic Compatibility, Sapporo and Asia-Pacific International Symposium on Electromagnetic Compatibility, EMC Sapporo/APEMC 2019* (2019), p. 625-628. doi : 10.23919/EMCTokyo.2019.8893692.

[102] Thomas Trouchkine, Guillaume Bouffard et Jessy Clédière. "Fault Injection Characterization on modern CPUs : From the ISA to the Micro-Architecture". In : *Proceedings of the 13th WISTP International COonference on Information Security Theory and Practice* (2019).

[103] Thomas Trouchkine, Sébanjila Kevin Bukasa, Mathieu Escouteloup, Ronan Lashermes et Guillaume Bouffard. "Electromagnetic fault injection against a System-on-Chip, toward new micro-architectural fault models". In : *Working paper or preprint* (2019). url : http://arxiv.org/abs/1910.11566.

[104] Aurelien Vasselle, Hugues Thiebeauld, Quentin Maouhoub, Adele Morisset et Sebastien Ermeneux. "Laser-Induced Fault Injection on Smartphone Bypassing the Secure Boot". In : *Proceedings - 2017 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2017* 2017-Janua (2017), p. 41-48. doi : 10.1109/FDTC.2017.18. url : https://ieeexplore.ieee.org/document/8167709.

[105] Aurélien Vasselle, Philippe Maurine et Maxime Cozzi. "Breaking mobile firmware encryption through near-field side-channel analysis". In : *Proceedings of the ACM Conference on Computer and Communications Security* (nov. 2019), p. 23-32. issn : 15437221. doi : 10.1145/3338508.3359571.

[106] Harold A. Wheeler. "Simple inductance formulas for radio coils". In : *Proceedings of the Institute of Radio Engineers* 16 (10 1928), p. 1398-1400. issn : 07315996. doi : 10.1109/JRPROC.1928.221309.

[107] *Yocto Project*. url : https://www.yoctoproject.org/.

École Nationale Supérieure des Mines de Saint-Étienne

NNT : 2022LYSEM013

Clément GAINE

# EVALUATION AND MITIGATION OF THE RISK OF FAULT INJECTION ATTACKS BY ELECTROMAGNETIC PERTURBATIONS ON MOBILE PLATFORMS

Speciality : Microelectronics

Keywords : Security, Physical attacks, Fault injection attacks, Electromagnetic pulse, Countermeasures

Abstract :

Physical attacks by injection of faults by electromagnetic perturbations have the particularity of inducing voltage variations in a circuit to corrupt its operation. Commonly performed on microcontrollers, they are being extended to complex circuits such as multicore processors. Used in mobile systems, these circuits contain a lot of personal data which must be secured.

This thesis aims at improving fault injection techniques by electromagnetic perturbations on mobile targets in order to identify their level of vulnerability and to propose adapted protections.

A modeling of the magnetic field generated by injection probes was carried out from the Biot and Savart law. It was completed by a dynamic study of the injector-probe couple. Through simulations and experiments, the properties of the probes were optimized to improve the concentration of the magnetic flux, to control the polarity of the impulse response and to maximize the intensity of the induced perturbations. This work has led to the improvement of the probes used in the state of the art.

In addition, a methodology has been implemented to introduce faults on a processor present on smartphones. It has led to an exploitation of the EMFI to obtain an elevation of privilege on a Linux OS.

Finally, a new protection device based on an active shielding principle has been proposed. Its ability to detect EMFI attempts and to jam attacks by electromagnetic analysis has been experimentally validated.

École Nationale Supérieure des Mines de Saint-Étienne

NNT : 2022LYSEM013

Clément GAINE

# EVALUATION ET MITIGATION DU RISQUE D'ATTAQUE PAR INJECTION DE FAUTES PAR PERTURBATIONS ELECTROMAGNETIQUES SUR PLATE-FORMES MOBILES

Spécialité : Microélectronique

Mots clefs : Sécurité, Attaques physiques, Attaques par injection de fautes, Impulsion électromagnétique, Contre-mesures

Résumé :

Les attaques physiques par injection de fautes par perturbations électromagnétiques ont la particularité d'induire des variations de tension dans un circuit afin de corrompre son fonctionnement. Couramment réalisées sur des microcontrôleurs, elles sont en cours d'extension sur des circuits complexes de type processeurs multicœur. Utilisés dans les systèmes mobiles, ces circuits abritent de nombreuses données personnelles dont il faut garantir la sécurité.

Cette thèse a pour objectif d'améliorer les techniques d'injection de fautes par perturbations électromagnétiques sur les cibles mobiles dans le but d'identifier leur niveau de vulnérabilité et de proposer des protections adaptées.

Une modélisation du champ magnétique engendré par des sondes d'injection a été réalisée à partir de la loi de Biot et Savart. Elle a été complétée par une étude dynamique du couple injecteur-sonde. Par des simulations et des expériences, les propriétés des sondes ont été optimisées, afin d'améliorer la concentration du flux magnétique, maîtriser la polarité de la réponse impulsionnelle et maximiser l'intensité des perturbations induites. Ces travaux ont abouti à l'amélioration des sondes utilisées dans l'état de l'art.

Par ailleurs, une méthodologie a été mise en place permettant d'introduire des fautes sur un processeur présent sur des smartphones. Elle a donné lieu à une exploitation de l'EMFI pour obtenir une élévation de privilège sur un OS Linux.

Enfin, un nouveau dispositif de protection basé sur un principe de blindage actif a été proposé. Sa capacité à détecter les tentatives d'EMFI et à brouiller les attaques par analyse électromagnétiques a été validée expérimentalement.