Formation en Sécurité Numérique : Théorie et Mise en Pratique sous la Forme d'un Stage Technologique

Florent Bruguier, Pascal Benoit, Lionel Torres

Formation en Sécurité Numérique : Théorie et Mise en Pratique sous la Forme d'un Stage Technologique

Florent Bruguier, Pascal Benoit et Lionel Torres

LIRMM / Polytech Montpellier, Université de Montpellier, France
Pôle CNFM de Montpellier (PCM)
161 rue Ada, 34095 Montpellier Cedex 5
prénom.nom@lirmm.fr

Résumé : Cet article présente une formation sur le thème de la sécurité numérique des circuits intégrés proposée par le Pôle CNFM de Montpellier (PCM). Les systèmes sécurisés sont maintenant omniprésents dans notre environnement quotidien et il est donc tout naturel de s'intéresser aux attaques que peuvent subir de tels systèmes. Cette formation de trois jours permet de sensibiliser les étudiants/professionnels aux problématiques des attaques dites par canaux cachés. Ces attaques permettent de retrouver la clé de chiffrement utilisée dans un système intégré en mesurant, par exemple des informations comme la consommation en courant.

Mots clés : Attaques par canaux cachés, consommation, émissions électromagnétiques, contremesures, banc de mesure, formation initiale, formation continue.

1. Introduction

Nous sommes amenés quotidiennement à utiliser des systèmes numériques. Les cartes à puces, les cartes vitales ou encore les passeports biométriques constituent quelques exemples de systèmes numériques sécurisés. Ceux-ci sont plus nombreux chaque jour, notamment avec l'avènement de l'internet des objets. Ils servent essentiellement à transporter de l'information dont il est important de garantir la sécurité (authentification, confidentialité, intégrité...). Cette problématique entraine un intérêt grandissant pour le domaine de la cryptologie, mais aussi une approche parfois différente pour la conception des systèmes électroniques intégrés.

L'implantation matérielle et logicielle de tels systèmes est devenue leur principal point faible. En effet, l'analyse de paramètres physiques du circuit tels que, par exemple, l'analyse de la consommation électrique (DPA, CPA...), des émissions électromagnétiques (CEMA, DEMA...) ou encore le temps de traitement (Timing Attack...) constituent autant d'aides aux attaques de ces circuits. Ces attaques permettent en un minimum de temps et avec peu d'efforts de découvrir les clés de chiffrement utilisées par les algorithmes symétriques ou asymétriques. Il est donc important de sensibiliser les futurs concepteurs de ces systèmes aux failles qu'ils peuvent contenir mais aussi aux méthodes pour les minimiser afin de réaliser les systèmes les plus fiables possibles.

Article publié par EDP Sciences et disponible sur le site http://www.j3ea.org ou http://dx.doi.org/10.1051/j3ea/2015028

Au sein du Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM), la plateforme régionale SECNUM (SECurité NUMérique) permet d'étudier, d'évaluer et d'accompagner les académiques et industriels vers la conception de circuits et systèmes embarqués robustes vis-à-vis de contraintes sécuritaires, et notamment les attaques par canaux cachés. Grâce au projet d'Initiatives D'Excellence en Formations Innovantes (IDEFI), projet FINMINA porté par le GIP CNFM, un banc d'analyses électromagnétiques est proposé afin de permettre la formation d'étudiants et de professionnels (formation initiale et continue).

La formation présentée ici est dispensée à des étudiants de fin de cycle Master/Ingénieur sous forme d'un stage technologique de 3 jours. Elle a pour objectif de comprendre et mettre en pratique les attaques par canaux cachés mais aussi de sensibiliser les stagiaires aux problématiques de sécurité des systèmes intégrés.

Après une présentation du contexte, le principe des attaques par canaux cachés sera brièvement explicité. Enfin, le déroulement des 3 jours de formation sera détaillé.

2. La cryptographie moderne

La cryptologie, étymologiquement "science du secret", englobe la cryptographie et la cryptanalyse. La cryptographie s'attache à protéger les messages à travers l'écriture secrète de ceux-ci tandis que la cryptanalyse consiste à tenter de déchiffrer un message sans en connaitre la clé de chiffrement utilisée. Même si la cryptologie est un art ancien, celle-ci n'est considérée comme une science que depuis le milieu du XX° siècle avec l'apparition des algorithmes de chiffrement modernes.

Ces algorithmes permettent d'assurer :

- la confidentialité, qui garantit que l'information est lisible uniquement par les personnes autorisées.
- l'intégrité, qui permet de vérifier que le message n'a pas été manipulé sans autorisation ou par erreur.
- l'authentification, qui permet au destinataire du message d'en vérifier l'origine et/ou l'identité de l'expéditeur.

L'intérêt de tout algorithme cryptographique est de transmettre un message entre un expéditeur et un destinataire sans qu'un attaquant potentiel puisse connaître (ou corrompre) le contenu du message même s'il venait à l'intercepter. Le principal général d'un chiffrement est présenté sur la Figure 1. Le message à chiffrer, appelé texte clair, est chiffré à l'aide d'une clé de chiffrement aussi appelée clé secrète. Cette opération permet d'obtenir le texte chiffré. Celui-ci est ensuite déchiffré par le destinataire à l'aide d'une clé de déchiffrement pour retrouver le texte clair.

Comme énoncé par Auguste Kerckhoffs en 1883 dans "La cryptographie militaire" [1], les algorithmes cryptographiques doivent demeurer publics et seules les clés doivent rester secrètes. Pour garantir la fiabilité sécuritaire d'un algorithme, il faut également que celui-ci soit au préalable vérifié par des experts. Autrement dit, la sécurité d'un message chiffré réside uniquement dans le secret de la clé et non pas dans celle de l'algorithme utilisé qui pourra être connu de tous.

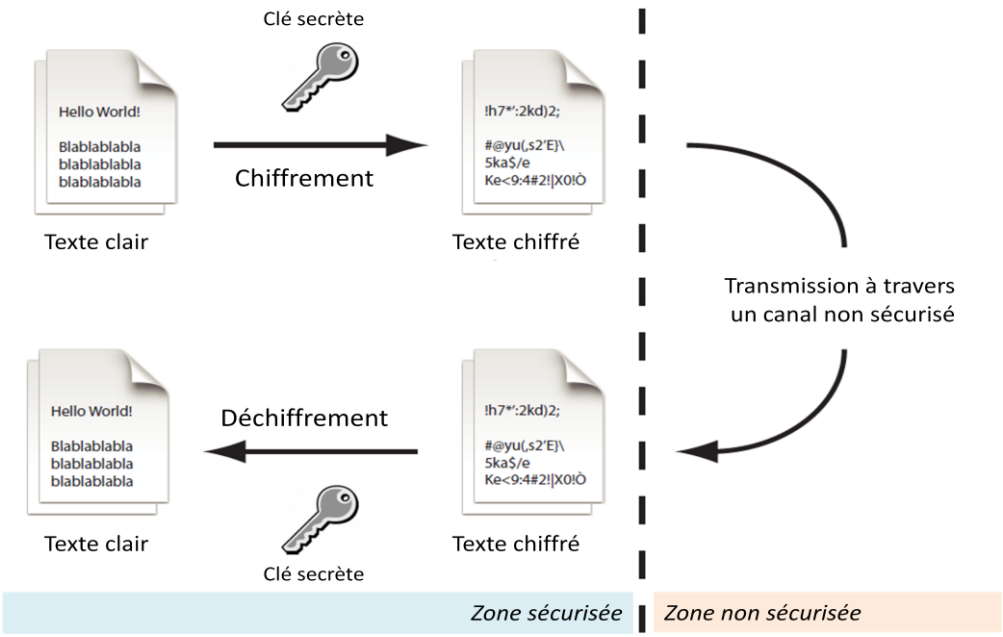

Figure 1 : Principe de fonctionnement d'un algorithme de chiffrement

Lors des opérations de chiffrement et déchiffrement, si la clé utilisée est identique, l'algorithme est dit symétrique. Lorsque deux clés différentes sont utilisées, celui-ci est dit asymétrique.

3. Les attaques par canaux cachés

3.1. Les différents types d'attaques

Les méthodes de cryptanalyse qui sont les processus par lesquels la clé secrète est retrouvée sont appelés attaques. Il existe trois grandes familles d'attaques :

- les attaques mathématiques qui permettent grâce à des méthodes mathématiques de retrouver la clé,
- les attaques logicielles qui tentent de déchiffrer les programmes contenus dans les crypto-systèmes en utilisant des failles logicielles,
- les attaques matérielles et plus particulièrement les attaques par canaux cachés qui sont à la base de la formation présentée ici.

Les attaques matérielles ou attaques physiques ciblent directement le support physique de l'algorithme cryptographique : la puce électronique dans notre cas. Ces attaques peuvent être classées en deux groupes distincts : les attaques actives et les attaques passives.

Les attaques actives consistent à manipuler la puce, ses entrées ou son environnement pour en extraire la clé secrète. Par exemple, pour obtenir des informations sur la conception d'un circuit, un attaquant peut le décapsuler grâce à une abrasion chimique ou encore une découpe laser afin d'obtenir des informations sur la conception du circuit. Dans la même catégorie sont rangées les attaques en faute. Ces attaques consistent à créer des fautes dans le circuit à l'aide d'injection laser, d'injection électromagnétique ou encore en faisant varier sa tension d'alimentation. Les fautes ainsi obtenues permettent de créer des erreurs dans le

circuit. Ces erreurs sont ensuite analysées et exploitées afin de retrouver la clé secrète. Ces attaques nécessitent du temps, des moyens et des informations sur les systèmes attaqués.

Les attaques passives ou attaques par canaux cachés utilisent des informations « fuitant » du circuit en fonctionnement normal (Figure 2). Il peut s'agir du temps nécessaire au circuit pour effectuer un chiffrement, de sa consommation électrique ou encore de ses émissions électromagnétiques. Ces attaques ont l'avantage, par rapport aux autres types d'attaques physiques, de ne pas laisser de traces mais aussi d'être peu coûteuses tout en étant relativement efficaces.

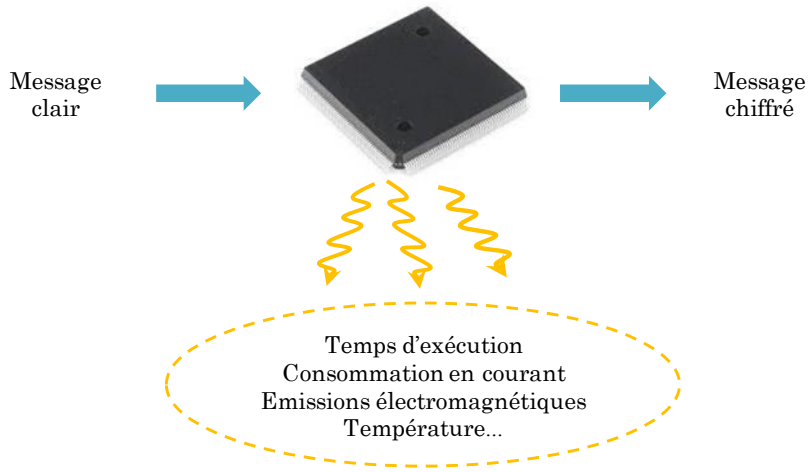

Figure 2 : Différents types de fuites exploitables sur un crypto-système

3.2. Modèles de fuites

Les circuits intégrés modernes sont réalisés en technologie CMOS (Complementary Metal Oxide Semiconductor). Chaque circuit CMOS est composé d'une multitude de cellules standards réalisant des fonctions élémentaires. Ces fonctions mises bout à bout permettent de réaliser différentes fonctionnalités d'un circuit et la consommation d'un tel circuit correspond à la somme de la consommation de chacune de ces portes logiques. Cette dernière peut être décomposée en deux parties :

- la consommation statique qui correspond aux fuites de chacun des transistors,
- la consommation dynamique qui correspond à la consommation des transistors lors de leurs commutations.

La consommation dynamique dépend de l'activité du circuit. Cette activité est directement liée à la commutation des transistors : plus de transistors commutent et plus cette consommation est élevée. Il est donc possible d'établir une relation entre le nombre de transistors qui commutent et la consommation du circuit. C'est cette relation qui est utilisée comme modèle de fuites pour attaquer le circuit et trouver la clé de chiffrement.

De plus, lorsque un courant traverse un conducteur, un rayonnement électromagnétique est créé. En effet, lors des changements d'état des transistors, un appel de courant a lieu générant une variation du champ électromagnétique [2]. L'analyse de ces émissions présente deux avantages par rapport à la mesure du courant :

- les émissions électromagnétiques dépendent uniquement des variations de consommation et donc de la consommation dynamique du circuit,
- ces émissions sont localisées et il est possible de venir les mesurer en un point précis du circuit.

Au final, la mesure du champ électromagnétique revient à mesurer la consommation dynamique locale du circuit.

Ce sont ces deux modèles de fuites (consommation et émissions électromagnétiques) qui sont utilisés au cours de la formation présentée ici pour illustrer le principe des attaques par canaux cachés.

3.3. Algorithme de chiffrement

Même si nous aborderons le fonctionnement de plusieurs algorithmes de chiffrement lors de cette formation (DES, AES, RSA...), la plupart des exemples pédagogiques sont basés sur l'utilisation de l'AES (Advanced Encryption Standard). La référence [3] présente d'une manière détaillée le fonctionnement de cet algorithme, nous attacherons ici à ne donner que les grands principes. Cet algorithme symétrique est notamment utilisé dans les transactions bancaires mais aussi lors du chiffrement de certaines communications sur internet.

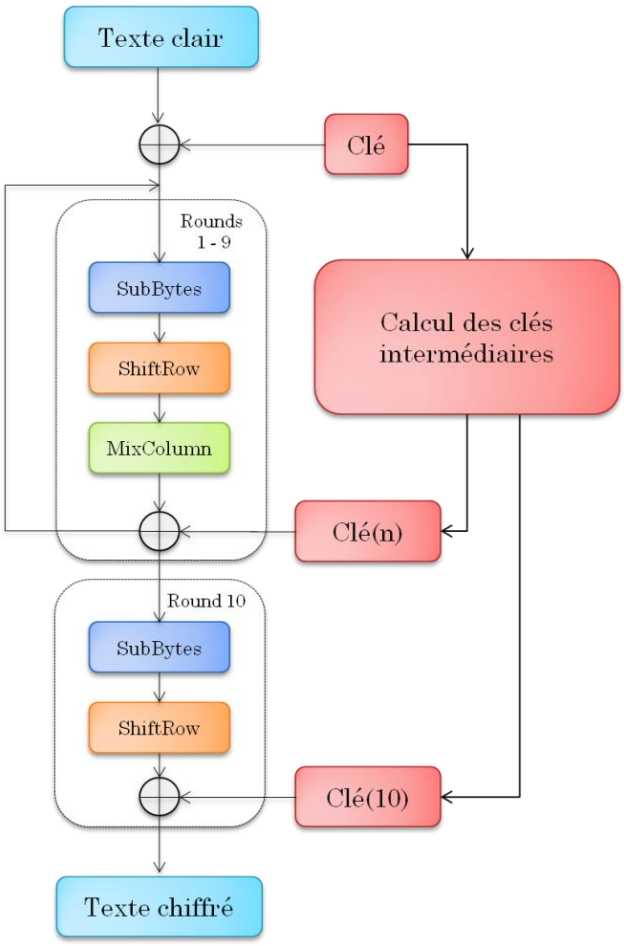

Figure 3 : Fonctionnement de l'algorithme AES

Il permet de chiffrer un message clair par paquets de 128 bits à l'aide d'une clé secrète de 128, 192, 256 bits. Ces paquets sont représentés sous la forme d'une matrice de 4 x 4 octets. Ces octets sont soumis à quatre opérations successives réalisées plusieurs fois en suivant un schéma défini à l'avance (Figure 3). Ces opérations ont pour noms : *AddRoundKey, SubBytes, ShiftRow et MixColumn.*

La première opération, *AddRoundKey*, consiste à effectuer une opération *OUexclusif* bit à bit entre le texte clair et la clé secrète. Le résultat de cette opération est ensuite utilisé comme entrée de l'étape suivante. Celle-ci, *SubBytes*, consiste elle à remplacer chaque octet de la donnée par l'octet correspondant dans une table de substitution. Ensuite, lors de l'opération *ShiftRow*, les octets de la donnée sont transposés. Pour cela, les octets sont traités ligne par ligne. La première ligne reste inchangée tandis que les octets sont décalés d'un vers la droite pour la seconde ligne, de deux vers la droite pour la troisième et de trois vers la droite pour la dernière. L'opération suivante, *MixColumn*, est une multiplication dans le corps de Galois de la matrice obtenue précédemment avec une matrice définie dans l'algorithme. Enfin, l'opération *AddRoundKey* est à nouveau réalisée. Cette fois, au lieu d'utiliser la clé, une sous-clé est générée à partir de la clé initiale.

Ces quatre opérations sont répétées dix fois. Chacune de ces itérations est appelée Round. Les neuf premiers Rounds sont identiques tandis que le dernier est plus court (absence de l'opération *MixColumn*).

3.4. Déroulement de l'attaque

La première attaque basée sur l'analyse de la consommation a été proposée par P. Kocher en 1999 [4]. L'objectif de cette attaque est d'utiliser la corrélation entre la puissance consommée par le circuit de chiffrement et la clé secrète utilisée. Pour cela, il est nécessaire de choisir un point d'attaque où la consommation du circuit est dépendante de la clé utilisée. Il est mathématiquement démontré que c'est le cas à la sortie des opérations non-linéaires [3]. Dans le cas de l'AES, l'opération non linéaire à la sortie de laquelle est lancée l'attaque est l'opération *SubBytes*.

Une fois le point d'attaque identifié, l'attaque se déroule de la manière suivante :

- Des chiffrements de textes clairs de 128 bits générés aléatoirement sont chiffrés à l'aide du circuit contenant la clé secrète à retrouver. Lors de chacun de ces chiffrements, les émissions électromagnétiques de l'algorithme (ou sa consommation) ainsi que le texte clair envoyé au circuit sont enregistrés.
- Dans un second temps, l'analyse de ces résultats peut commencer. Pour cela, la clé secrète de 128 bits est découpée en une matrice de 4 x 4 sous-clés d'un octet chacune. La recherche de la clé s'effectue ensuite en traitant séparément chacune de ces sous-clés.
- La valeur à la sortie de la première opération *SubBytes* est ensuite calculée pour chacune des 256 valeurs possibles de la sous-clé recherchée et cela pour chacun des textes clairs chiffrés pendant notre expérimentation.
- Le poids de Hamming (nombre de bits à 1) de chacune des valeurs obtenues est calculé.
- Il ne reste plus qu'à calculer la corrélation de Pearson (corrélation entre variables aléatoires) entre les différents poids de Hamming et les consommations associées [5]. Pour chaque hypothèse de sous-clé, on obtient à chaque instant une valeur de corrélation. Une comparaison est effectuée entre les corrélations obtenues

pour la totalité des hypothèses de sous-clés et la corrélation ayant la plus forte amplitude correspond à la valeur de la meilleure sous-clé.

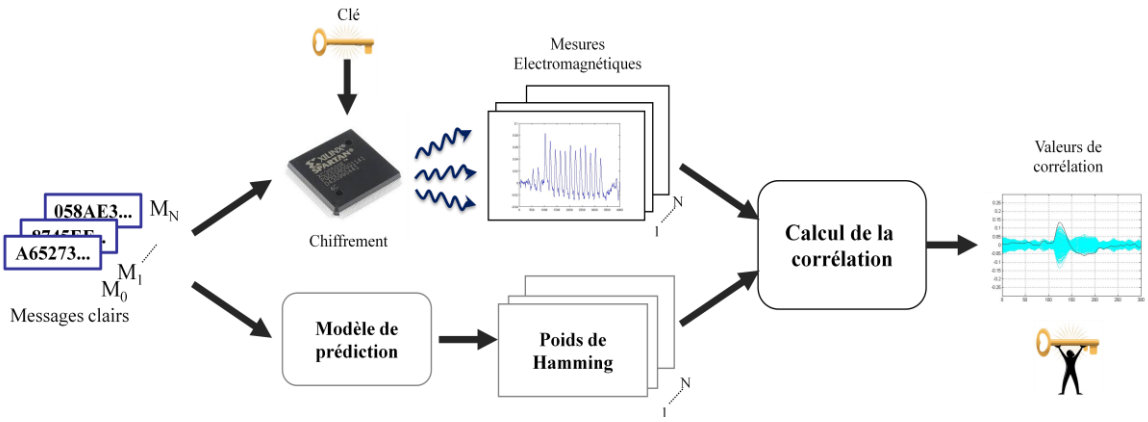

Figure 4 : Déroulement de l'attaque

3.5. Banc de mesure

La formation présentée ici s'appuie, entre autre, sur l'utilisation du banc de mesure électromagnétique de la plateforme SECNUM du pôle CNFM de Montpellier [6]. Ce banc de mesure, présenté sur la Figure 5, permet de mesurer les émissions électromagnétiques d'un circuit lorsque celui-ci effectue des chiffrements.

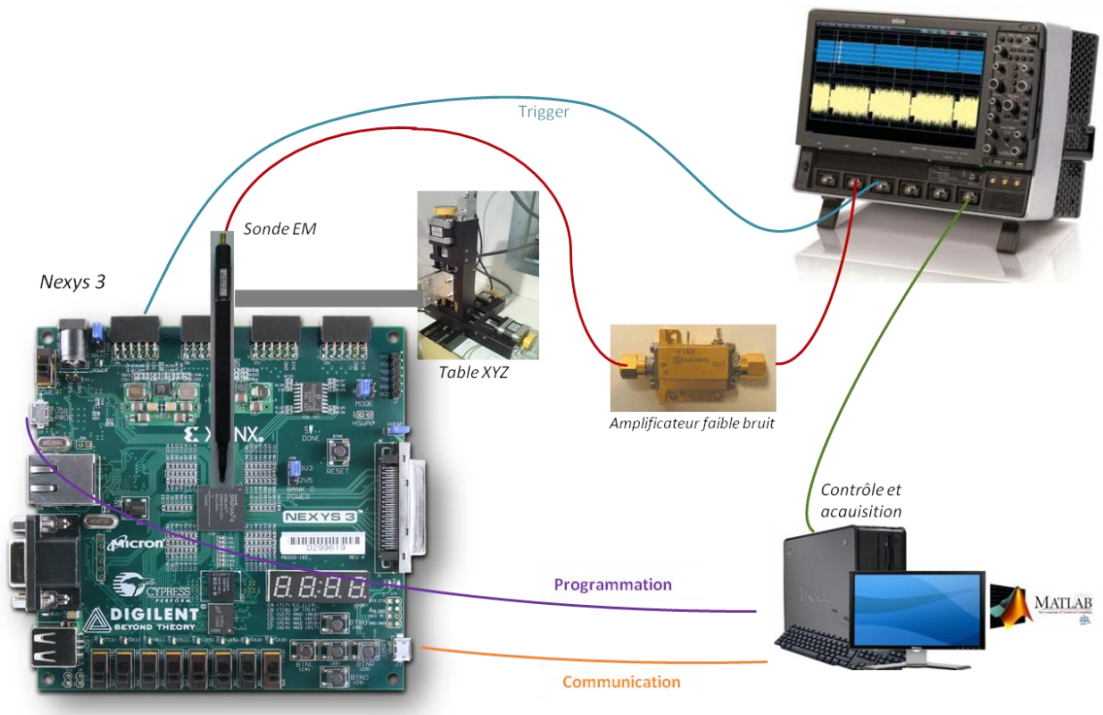

Figure 5 : Banc de mesure électromagnétique

La mesure des émissions électromagnétiques s'appuie sur l'utilisation d'une sonde électromagnétique qui capture le signal émis par le circuit de chiffrement. Celui-ci est ensuite amplifié à l'aide d'un amplificateur faible bruit connecté à un oscilloscope. L'oscilloscope, piloté par un ordinateur de contrôle, permet d'enregistrer ce signal pour le traiter ultérieurement. L'ordinateur permet également, par exemple, de programmer le FPGA contenant un cryptoprocesseur AES mais aussi de communiquer avec le circuit afin de lancer les chiffrements. Une table XYZ vient compléter ce système de mesure en permettant de déplacer la sonde électromagnétique à la surface du circuit et ainsi trouver le meilleur point pour réaliser l'attaque.

4. Contenu de la formation

La formation sur la sécurité des circuits intégrés est dispensée à des étudiants de fin de cycle Master/Ingénieur sous forme d'un stage technologique de 3 jours. Elle peut également être mise en place pour des professionnels (ingénieurs, techniciens, chefs d'entreprise...) dans le cadre d'une formation continue.

Elle a pour objectif de comprendre et mettre en pratique les attaques par canaux cachés en s'appuyant sur différents exemples pratiques. Pour cela, différentes versions de l'algorithme AES sont utilisées (AES exécuté sur un processeur classique, AES implémenté sur FPGA avec ou sans contre-mesures...).

Afin de suivre cette formation, il est nécessaire que les stagiaires aient des notions d'électronique, de traitement du signal et de conception de systèmes intégrés.

Cette formation est décomposée en plusieurs parties au cours desquels les stagiaires se familiarisent avec différents aspects des attaques par canaux cachés. Les "wokshops" servent à introduire les concepts et présenter la théorie tandis que les labs permettent de mettre en application ces concepts au travers de manipulations et d'expérimentations.

4.1. Partie 1 : Contexte et introduction

Une partie importante de la formation même si ce n'est pas le cœur de celle-ci est de permettre aux stagiaires de se forger un début de culture en sécurité des systèmes intégrés. Pour cela, une partie de la formation est dédiée à présenter les grands principes de la cryptographie ainsi que les enjeux associés. Les principaux algorithmes cryptographiques symétriques et asymétriques ainsi que leur fonctionnement sont également explicités. Un tour d'horizon des différents types d'attaques matérielles est proposé. Cet aspect contextuel prend de l’ordre de une heure et demie.

4.2. Partie 2 : Attaques par canaux cachés

Le principe des attaques par canaux cachés est présenté dans cette partie. L'objectif est de décrire en détails le fonctionnement de ce type d'attaques. Pour cela, un exemple didactique est proposé. Celui-ci est basé sur un exemple simple. Il s'agit d'une attaque en consommation d'un cryptoprocesseur DES. Les différentes étapes de l'attaque sont explicitées. Le principe des fuites émises lors de l'exécution de l'algorithme cryptographique est décrit à la fois dans le cas de la mesure de consommation mais aussi de la mesure des émissions électromagnétiques. On en déduit les modèles de fuites classiques que sont le poids de Hamming et la distance de Hamming. Puis, un point est fait sur le protocole expérimental et notamment les techniques d'acquisition des courbes. Afin d'être exhaustif,

l'accent est ensuite mis sur les différents distingueurs. Pour cela, les attaques différentielles sont d'abord introduites à travers un exemple simple. S'en suit, la présentation du principe de fonctionnement de la corrélation de Pearson ainsi qu'une généralisation à tout type de « distingueurs ». Cet aspect qui est essentiel à la compréhension des phénomènes physiques mis en jeu est généralement enseigné sur 3 heures.

4.3. Partie 3 : Acquisition de courbes d'attaque

L'objectif est que les participants mettent en place les différents éléments de l'expérimentation. Cela se déroule généralement sur 2 heures.

Durant les différentes expérimentations, les cryptosystèmes sont implémentés sur FPGA. Ceci permet de maîtriser un maximum le design et son implémentation. Avant de commencer toute expérimentation, le FPGA utilisé (Spartan 6) ainsi que sa carte d'accueil (Nexys 2) sont présentés aux participants. Le principe de fonctionnement de ce type de composants reconfigurables est rapidement évoqué et l'implémentation du composant cryptographique attaqué est présentée. Il s'agit, dans un premier temps, d'un processeur généraliste exécutant un algorithme AES. Cette implémentation est volontairement très peu sécurisée et donc permet de réduire les temps de calcul nécessaires à l'attaque.

Avant de passer à l'expérimentation, les stagiaires sont amenés à programmer le composant et configurer la communication entre le PC de commande et la carte à l'aide d'un premier script de commande Matlab.

Ensuite, une description du banc de mesure utilisé est réalisée. Les différents éléments sont présentés. Dans le cas d'une attaque en consommation, le montage est relativement simple et ne nécessite pas de réglages ou d'ajustements particuliers.

Dans le cas de l'utilisation des émissions électromagnétiques, la carte est positionnée au centre du système. Une fois tous les éléments connectés, des chiffrements sont réalisés et la position de la sonde est ajustée. Ceci permet de trouver la position optimale pour lancer l'attaque. Une fois cette position trouvée, il ne reste plus qu'à lancer les acquisitions. Toutes ces acquisitions sont réalisées à l'aide d'un script Matlab configuré par les participants. Ce script permet de configurer l'oscilloscope, d'envoyer le texte clair au FPGA puis de recevoir le texte chiffré pour vérification mais aussi de récupérer les courbes de consommation ou d'émissions électromagnétiques et de les stocker en vue de lancer l'attaque.

4.4. Partie 4 : Codage d'une attaque

Les courbes étant acquises, il ne reste plus qu'à mettre en place la partie "calculatoire" de l'attaque. Cette partie est réalisée à l'aide du logiciel Matlab. Ce langage de programmation a été choisi car il permet très facilement de visualiser des données (courbes, graphiques...) tout en permettant de faire du calcul statistique (différence des moyennes, corrélation...). Même si certaines parties de ce lab peuvent paraître complexes, les participants sont suffisamment guidés pour arriver à un résultat positif et des fichiers avec tout ou partie des solutions sont également disponibles en cas de besoin.

La première étape consiste à ouvrir les mesures et les afficher. Ceci permet une première prise en main de Matlab mais aussi il est possible de vérifier que les mesures sont correctes. A partir de cet affichage, il est également possible de visualiser les différents Rounds de l'algorithme de chiffrement et donc de choisir la partie de la courbe sur laquelle est lancée l'attaque.

La seconde étape consiste à calculer en fonction des hypothèses de sous-clé et des textes clairs, la valeur associée au modèle de fuite choisi. Le plus facile à implémenter étant le modèle du poids de Hamming, nous avons choisi de travailler avec celui-là. Ce modèle est appliqué au premier Round de l'algorithme de chiffrement. Les stagiaires sont donc amenés à calculer le poids de Hamming associé à chacune des hypothèses de sous-clés à la sortie de l'opération *SubBytes.* Cette opération donne pour chacune des sous-clés et chacun des textes clairs une valeur comprise entre 0 et 8.

La matrice de valeur ainsi obtenue est ensuite corrélée aux différentes mesures réalisées précédemment. Une fonction permettant de réaliser cette opération de corrélation est fournie aux stagiaires afin d'éviter qu'ils ne perdent trop de temps sur ce point.

Le codage de l'attaque est terminé, il ne reste plus qu'à observer le résultat en traçant les valeurs de corrélation pour chacune des hypothèses et à analyser le résultat. La bonne sous-clé est celle de plus forte amplitude.

4.5. Partie 5 : Etude d'un cryptoprocesseur

Le processeur attaqué dans la première partie est remplacé ici par un cryptoprocesseur AES. L'objectif est de mieux saisir le fonctionnement d'une attaque sur ce type de composants. Les participants sont à nouveau amenés à effectuer des mesures en vue d'attaquer le circuit. L'attaque codée dans la partie précédente est réutilisée et améliorée.

Lors de la mesure des émissions électromagnétiques de ce circuit, les courbes présentent un nombre de pics égal au nombre de rounds de l'algorithme utilisé, puisque il s'agit d'une implémentation matérielle de l'algorithme. Les variations d'amplitudes induites par l'envoi de différents messages en clairs sont également faciles à observer (l'attaque en elle même nécessite juste un plus grand nombre de courbes).

4.6. Partie 6 : Contremesures

L'objectif de la dernière journée est d'étudier les contremesures. Dans un premier temps, une présentation des principaux types de contremesures pouvant contribuer à l'amélioration de la sécurité des circuits vis-à-vis des attaques par canaux cachés est effectuée. S'en suit l'étude détaillée de deux contremesures implémentées sur un processeur généraliste : une contremesure de type dissimulation et une contremesure de masquage. Ces deux contremesures sont par la suite évaluées à l'aide du banc de mesure et de nouvelles attaques sont lancées.

5. Conclusion

Dans un contexte où la sécurité des systèmes est au cœur des préoccupations des concepteurs, cette formation permet aux stagiaires de faire un tour d'horizon des attaques matérielles que peuvent subir les circuits cryptographiques. C'est l'occasion pour les étudiants de prendre conscience de l'importance de la sécurité lors de la conception de tels systèmes. En plus d'acquérir des compétences sur les algorithmes cryptographiques et les attaques par canaux cachés, les participants sont amenés à mettre en œuvre ce type d'attaque sur différents supports matériels. Ils sont également amenés à réfléchir à des solutions de protection concrètes à travers la présentation de contremesures et leur étude.

6. Références

[1] Kerckhoffs, A. « La cryptographie militaire », Journal des sciences militaires, vol. IX, pp. 5–38, Janvier 1883, pp. 161–191, Février 1883.

[2] Ordas, T., Lisart, M., Sicard, E., Maurine, P., & Torres, L. (2009). Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits. In Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation (pp. 229-236). Springer Berlin Heidelberg.

[3] National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, November 2001.

[4] Kocher, P. C., Jaffe, J., & Jun, B. (1999). Differential Power Analysis. In Advances in Cryptology (pp. 388–397).

[5] Brier, E., Clavier, C., and Olivier, F. Correlation Power Analysis with a LeakageModel. In CHES, volume 3156 of LNCS, pages 16–29. Springer, August 11–13 2004. Cambridge, MA, USA

[6] Bourrée, M., Bruguier, F., Barthe, L., Benoit, P., Maurine, P., & Torres, L. (2012). SECNUM: an Open Characterizing Platform for Integrated Circuits. In European Workshop on Microelectronics Education (EWME) (pp. 88 – 91). Grenoble: EDA Publishing Association.

7. Liste des sites internet intéressants

Plateforme SECNUM :
http://www.lirmm.fr/Secnum/

Plaquette de la formation :
http://www.cnfm.fr/VersionFrancaise/animations/images/doc_telechargements/actualites/actus2014/Plaquette_SECNUM_Formations.pdf

Action IDEFI-FINMINA :
http://www.cnfm.fr/VersionFrancaise/actualites/actualites_manifestations.htm

8. Biographies

Florent BRUGUIER est ingénieur de recherche au sein du Pôle CNFM de Montpellier (PCM) et de l'Université de Montpellier. Il est en charge de la formation et de l'animation scientifique autour de la plateforme de sécurité numérique SECNUM. Il a obtenu son Master en 2009 et son doctorat en 2012 à l'Université de Montpellier II. Ses travaux de recherche portent sur la caractérisation de procédé de fabrication et de vieillissement sur FPGA ainsi que sur la sécurité des systèmes intégrés. Il est l'auteur ou le coauteur d'une vingtaine de publications.

Pascal BENOIT est Maître de Conférences à l'Université de Montpellier, à l'Ecole Polytechnique Universitaire de Montpellier. Il effectue ses recherches au Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM). Il a été

recruté comme enseignant-chercheur après l'obtention d'un doctorat en 2004 et une année de post-doctorat en Allemagne. Ses travaux se focalisent sur les problématiques de consommation, de fiabilité et de sécurité des systèmes intégrés; ils ont donné lieu à plusieurs brevets et une centaine de publications dans des revues et des conférences internationales. Il est impliqué dans l'animation et l'organisation d'évènements scientifiques majeurs, par exemple en tant que président de comité des programmes de RAW 2011. Il est actuellement directeur adjoint des Services Nationaux du CNFM.

Lionel TORRES, 44 ans, Professeur des Universités, Directeur Adjoint de Polytech Montpellier et Directeur Adjoint du pôle CNFM de Montpellier, après un doctorat en Electronique, un passage dans la société ATMEL, il est revenu dans le giron de l'enseignement et de la recherche en 1996 à l'Université Montpellier et au sein de Polytech Montpellier et au laboratoire LIRMM (Laboratoire d'Informatique, Robotique et Microélectronique de Montpellier), dont il a dirigé le département Microélectronique pendant 4 ans (2007-2011). Ses travaux s'intéressent à la conception de circuits et systèmes intégrés sécurisés et l'utilisation de technologies émergentes. Ils ont donné lieu à plus d'une trentaine de revues internationales et plus de 150 conférences internationales, et une dizaine de brevets.