Sécurité des Systèmes Electroniques Intégrés

Florent Bruguier, Pascal Benoit, Lionel Torres

Sécurité des Systèmes Electroniques Intégrés

Florent Bruguier, Pascal Benoit et Lionel Torres

LIRMM - Pôle CNFM de Montpellier (PCM)

Polytech Montpellier, Université de Montpellier, France

161 rue Ada, 34095 Montpellier Cedex 5

prénom.nom@lirmm.fr

Résumé : Les systèmes sécurisés sont maintenant omniprésents dans notre environnement quotidien, il est donc tout naturel de s'intéresser aux menaces que peuvent subir de tels systèmes. Cet article présente les différentes attaques auxquelles peut être soumis un circuit sécurisé en se focalisant plus particulièrement sur les plus faciles à mettre en œuvre : les attaques par canaux cachés. Ces attaques permettent très facilement de retrouver la clé de chiffrement utilisée dans un système intégré en mesurant, par exemple, sa consommation ou ses émissions électromagnétiques.

Mots clés : Cryptographie, Cryptanalyse, Attaques par canaux cachés, Consommation, Emissions électromagnétiques

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 et ceux que nous utilisons sont plus nombreux chaque jour. De nos jours, les «objets connectés » sont omniprésents et vont forcément nécessiter une attention tout particulière quant à la protection des données privatives. Ceux-ci transportent essentiellement de l'information dont il est important de garantir la sécurité. Cette problématique entraine un intérêt grandissant pour le domaine de la cryptologie, notamment autour de la conception des systèmes électroniques.

Rappelons que 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 (premières traces au IV siècle avant JC), 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 récepteur 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/observateur potentiel puisse connaitre le contenu du message même s'il venait à l'intercepter. Ces algorithmes fonctionnent selon le principe 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 afin de retrouver le texte clair.

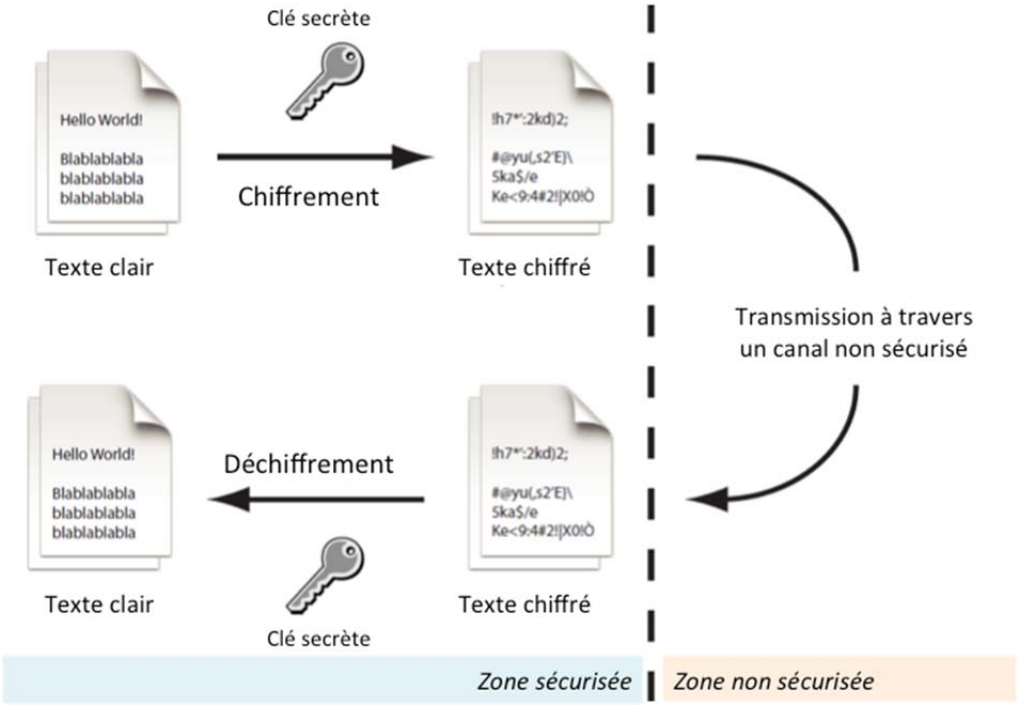

Figure 1: Principe de fonctionnement d'un algorithme de chiffrement

Comme énoncé par Auguste Kerckhoffs en 1883 dans "La cryptographie militaire", les algorithmes cryptographiques doivent demeurer publiques et seules les clés doivent rester secrètes [1]. 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.

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

2. Les attaques

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

- les attaques statistiques 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 dites par canaux cachés qui seront présentées plus en détails par la suite ;

Les attaques matérielles ou attaques physiques ciblent directement le support physique de l'algorithme cryptographique : la puce électronique. La puce électronique, aussi appelée circuit intégré, est un composant électronique permettant de reproduire une ou plusieurs fonctions électroniques plus ou moins complexes dans un seul composant. Dans notre cas, il s'agit de fonctions électroniques permettant de réaliser des opérations cryptographiques comme des chiffrements ou de déchiffrements

Les attaques matérielles 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 (Figure **2**). 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 seront ensuite analysées et exploitées afin de retrouver la clé secrète. Ces attaques nécessitent du temps, des moyens et des informations sur les systèmes attaqués.

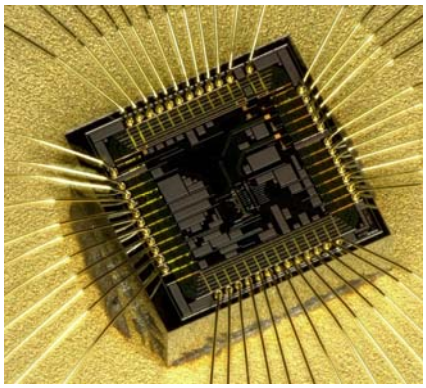

Figure 2 : Image microscope d'une puce électronique décapsulée

Les attaques passives ou attaques par canaux cachés utilisent des informations physiques du circuit en fonctionnement normal. Il peut s'agir du temps nécessaire au circuit pour effectuer un chiffrement, de sa consommation électrique ou encore de ses émissions électromagnétiques, ou en encore le nombre de photons émis. L'exploitation de ces informations physiques, que l'on appelle communément « fuites », permet de récolter les éléments nécessaire pour constituer une attaque (Figure **3**). Par ailleurs ces attaques peu couteuses, sont relativement efficaces.

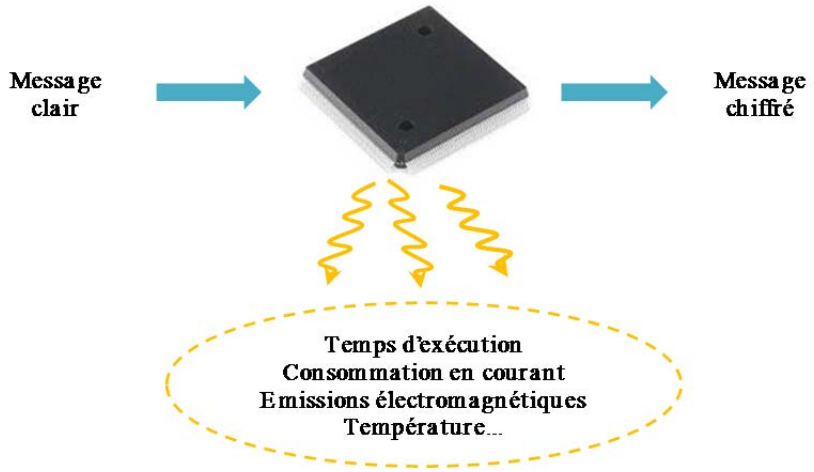

Figure 3 : Différents types de fuites exploitables sur un crypto-système

3. Mise en place d'une attaque par canaux cachés

Afin de réaliser une attaque par canaux cachés, il est nécessaire de s'intéresser dans un premier temps aux modèles de fuites qui seront ensuite utilisés pour lancer l'attaque et retrouver la clé secrète.

3.1. Modèles de fuites

Les circuits intégrés modernes sont réalisés en technologie CMOS (Complementary Metal Oxide Semiconductor). Un circuit CMOS est composé d'une multitude de cellules standards réalisant des fonctions élémentaires. Ces fonctions misent bout à bout permettent de réaliser les 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.

C'est ce modèle de fuites basé sur les émissions électromagnétiques qui sera utilisé pour illustrer le principe des attaques par canaux cachés.

3.2. Algorithme de chiffrement

Afin d'illustrer notre exemple, nous nous appuierons sur l'utilisation de l'AES (Advanced Encryption Standard) [3]. Cet algorithme symétrique est notamment utilisé dans les transactions bancaires mais aussi lors du chiffrement de certaines communications sur internet.

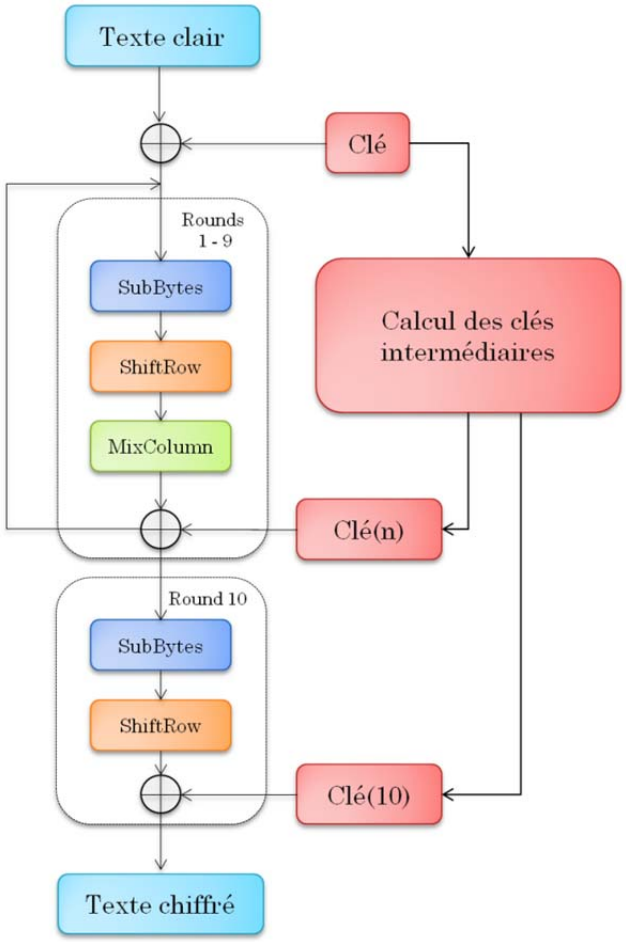

Figure 4 : Fonctionnement de l'algorithme AES

Il permet de chiffrer un message clair par paquets de 128 bits à l'aide d'une clé secrète de 128 bits. Le message clair est soumis à quatre opérations successives réalisées plusieurs fois en suivant un schéma défini à l'avance (Figure 4). Ces opérations ont pour noms : AddRoundKey, SubBytes, ShiftRow et MixColumn.

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).

L'objectif n'est pas ici de détailler précisément le fonctionnement de l'algorithme mais d'en présenter les grandes lignes. On se réfèrera donc à la littérature pour plus de détails. Rappelons cependant que l'AES , repose sur un principe de permutation et substitutions de caractères permettant de réaliser le chiffrement.

3.3. Banc de mesure

Cet exemple s'appuie sur l'utilisation du banc de mesure électromagnétique de la plateforme SECNUM implantée au LIRMM (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier) [6]. Ce banc de mesure, présenté sur la **Erreur ! Source du renvoi introuvable.**, permet de mesurer les émissions électromagnétiques d'un circuit de chiffrement.

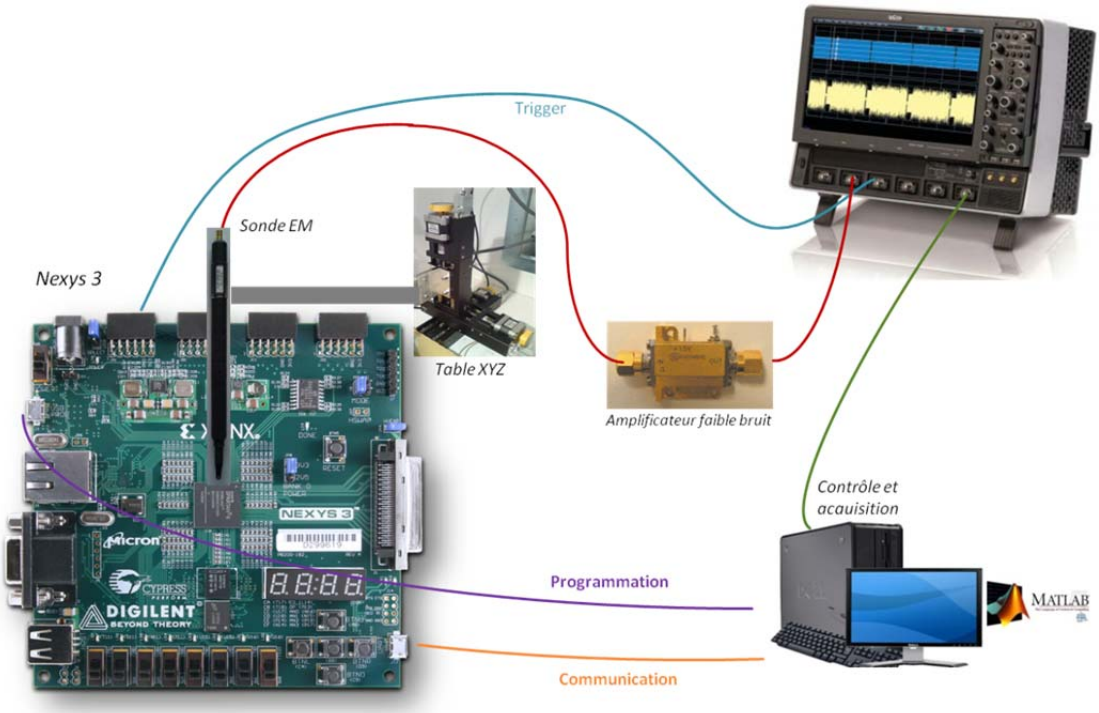

Figure 5 : Banc de mesure électromagnétique

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 à la surface du circuit et ainsi trouver le meilleur point pour réaliser l'attaque.

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 l'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.

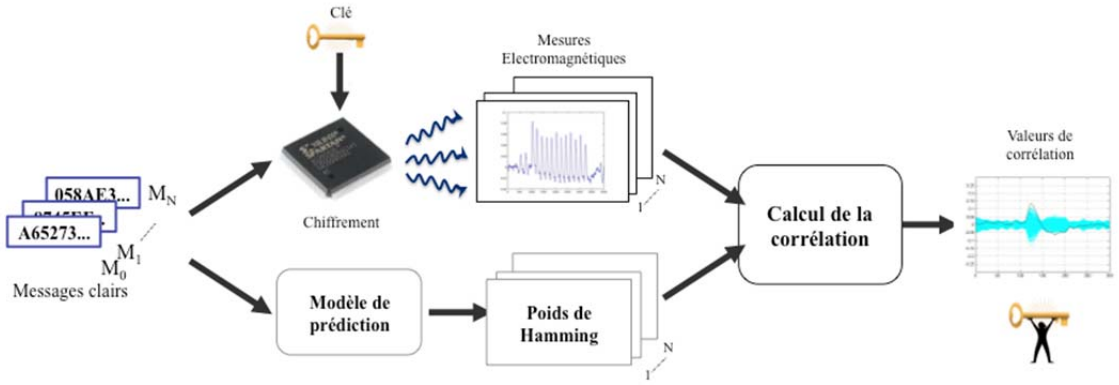

Figure 6: Déroulement de l'attaque

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 réalisés à l'aide du circuit à attaquer. Lors de chacun de ces chiffrements, les émissions électromagnétiques de l'algorithme ainsi que le texte clair envoyé au circuit sont enregistrés (Figure **7**).
- 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. On en déduit le nombre de transitors qui commutent lors de cette dernière opération. Ce nombre est appelé distance de Hamming.
- Il ne reste plus qu'à calculer la corrélation de Pearson entre les différents poids de Hamming et les consommations associées [5]. Expliqué grossièrement, la corrélation de Pearson est une opération mathématique permettant de démontrer si deux grandeurs évoluent ou non dans le même sens. Le résultat de plus forte amplitude correspond à la valeur de la meilleure sous-clé (Figure **8**).

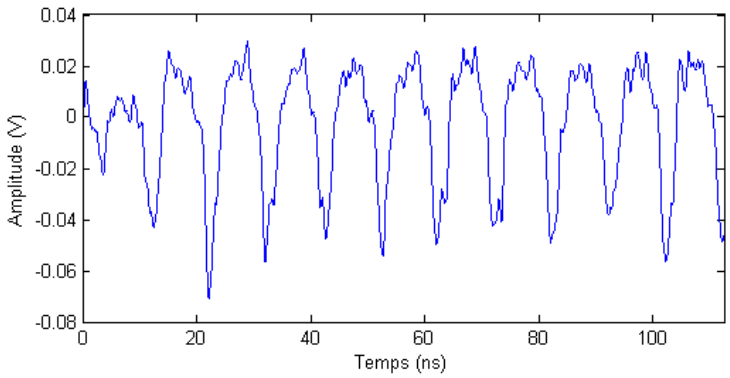

Figure 7 : Amplitude des émissions électromagnétiques relevées lors d'un chiffrement

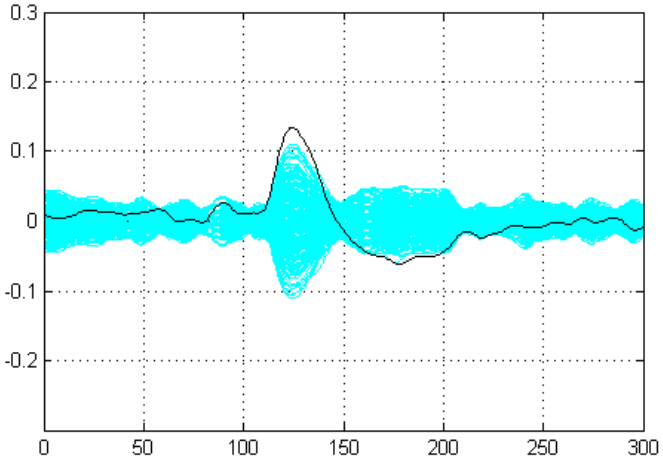

Figure 8 : Résultat du calcul de corrélation. En bleu, les valeurs de corrélation pour toutes les sous-clé. En noir, la courbe de plus forte amplitude correspond à la meilleure hypothèse de sous clé.

4. Conclusion

Dans un contexte où les objets connectés sont de plus en plus présents dans notre environnement, il est important de s'intéresser à la sécurité des données qui transitent par de tels objets. Nous venons de montrer que ceux-ci sont vulnérables aux attaques et en particulier aux attaques par canaux cachés. En effet, il est très facile de retrouver une clé de chiffrement en mesurant la consommation d'un circuit.

Afin de se prémunir de tels attaques, il est possible lors de la conception d'insérer des contremesures. Celles-ci permettent notamment d'équilibrer la consommation ou encore de masquer la clé de chiffrement. Néanmoins, ces contremesures ne constituent pas un solution idéale. Elles permettent juste de retarder les attaquants. La sécurité des objets connectés passe donc aussi par une vigilance des utilisateurs lors de l'utilisation de tels objets. En effet, la sécurité est l'affaire de tous.

5. 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.