L'émission Rayonnée des Cartes à Puce: une Vue d'Ensemble

Jean-Jacques Quisquater, Michael Neve,
Eric Peeters, François-Xavier Standaert.

Résumé Depuis bientôt dix ans, la recherche cryptographique s'intéresse aux attaques par canal caché. Il a notemment été démontré que le comportement de tout dispositif peut être déduit de paramètres secondaires comme sa consommation ou son temps d'execution. Les émissions électromagnétiques rayonnées par une carte à puce ou un microprocesseur peuvent ainsi réveler des secrets manipulés en cours de fonctionnement. L'objet de cet article est de montrer la portée de ces attaques et d'exposer les contre-mesures pour les prévenir.

1 Introduction

L'histoire des attaques par mesure des fuites involontaires de cryptosystèmes est loin d'être un phénomène nouveau. A la fin du XIXème siècle déjà, on avait découvert que certains problèmes de couplage électrique (crosstalk) pouvaient permettre d'espionner les lignes téléphoniques. Plus récemment (années 50), le mot de code TEMPEST fut associé à toute la méthodologie des réception, amplification et traitement de radiations électromagnétiques. Les exemples d'utilisation de tels procédés ne manquent pas. Certains d'entre eux sont décrits dans [3].

Avec l'avènement de la cryptographie moderne (1980), les algorithmes furent implémenté dans des cartes à puce, considérées alors comme inviolables. On supposait à l'époque que "casser" de tels systèmes était impossible, vu le temps de calcul prohibitif d'une attaque exhaustive. Ce raisonnement fur largement remis en cause dè les premières publications relatives aux attaques par canaux caché (1996). L'objectif de ce type d'attaque est de déduire des informations sur les données manipulées par un dispositif à partir de mesures physiques. Des analyses par mesure du temps de calcul (*Timing Attack* [5]), par mesure de la consommation (*Simple/Differential Power Analysis* [6]) et plus récemment des analyses par mesure du rayonnement électromagnétique (*Simple/Differential ElectroMagnetic Analysis* [1,2,4]) furent ainsi appliquées à la carte à puce, avec un succè surprenant, grandement facilité par la technologie CMOS (Complementary Metal-Oxide-Semiconductor) en vogue à l'époque. Ces attaques visent en général un ou plusieurs bits d'un résultat intermédiaire lors de l'exécution d'un algorithme crypptographique. Le but est d'essayer d'établir une corrélation entre leurs transitions prévues de manière théorique (en fonction d'une clé prédite) et les traces de courant et/ou de rayonnement électromagnétique. Dans le cas où la clé prédite est effectivement la bonne, la corrélation entre la prédiction et la

mesure sera évidente. Tout cela demande évidemment d'obtenir des traces de "bonnes" qualités et un grand soin doit être apporté au banc de mesure.

La plupart des circuits intégrés actuels sont encore construits en technologie CMOS. Les portes logiques implémentées nécessitent plus de place mais, en contrepartie, permettent une consommation statique nulle ce qui est un critère très important dans de nombreuses applications portables. En prenant l'exemple d'un inverseur CMOS, qui est un des éléments standards de nombreux circuits, on observe qu'une transition d'état d'un bit (de 0 à 1 ou inversément), produit une impulsion de courant sur des lignes ou des interconnexions. Il en résulte un rayonnement électromagnétique expliqué par les équations de Maxwell. Les circuits intégrés étant pour la plupart des circuits synchrones, c'est au moment du flanc montant de l'horloge que le nombre de portes qui changent d'état est le plus important et donc que le rayonnement mesuré est aussi le plus important. Une horloge étant un signal de forme carré (plutôt trapézoïdal en réalité), on s'attend donc à avoir un contenu fréquentiel réparti en un pic important à la fréquence de base ainsi que plusieurs autres pics aux harmoniques. Ces phénomènes sont à l'origine des attaques par canaux caché.

Ce document résume un certain nombre de réultats obtenus récemment dans le domaine. L'origine du rayonnement d'un processeur est expliquée en Section 2. Le Section 3 décrit certains instruments de mesure utiles pour mener les attaques. Le Section 4 rappelle quelques expériences significatives publiées récemment et nous discutons les contremesures aux attaques par rayonnement en Section 5. Finalement, les conclusions sont en Section 6.

2 Les différents types de rayonnement électromagnétique des circuits intégrés

Deux grandes catégories d'émanations électromagnétiques sont généralement recensées dans la littérature [2] :

1. **Les émanations directes :** Ces émanations résultent des flux de courant parcourant un circuit. Dans le cas de circuits CMOS, il s'agit principalement d'impulsions de courant dont le rayonnement s'étale sur un spectre fréquentiel assez large (la fréquence de base et ses harmoniques).
2. **Les émanations non intentionelles :** Elles sont liées au problème de couplage électrique et électromagnétique entre composants proches. De nombreux centres de recherche essayent actuellement de modéliser ce phénomène pour parvenir à en diminuer les effets. En pratique, les émanations observées peuvent être compromettantes, car elles réultent de la modulation de signaux de couplage avec certaines porteuses (aux fréquences harmoniques du signal d'horloge principalement). Il peut s'agir de modulation AM (entre une porteuse et un signal de données) ou une modulation FM.

Souvent, il se révèle plus utile de travailler avec les émanations non intentionnelles. En effet, certaines porteuses modulées peuvent avoir une propagation

nettement supérieure que les émanations directes. Ceci peut permettre des attaques sans ouverture de l'envelloppe protectrice du dispositif (depackaging) jusqu'à plusieurs mètres de distance.

Néanmoins, nous avons recensé dans cet article des expériences menées en champ proche (nécessitant un depackaging du chip et un positionnement précis) ainsi que des expériences en champ plus lointain nécessitant l'utilisation d'antennes log-périodique, Yagi, ...

3 Instruments et sondes

Le types de sondes et d'instruments utilisés pour mener une attaque par mesure de rayonnement dépend fortement du champ considéré : champ proche ou champ lointain.

3.1 Mesures en champ proche

Il est possible d'utiliser différents types de sondes pour mesurer les composantes électriques $\overrightarrow{E}$ et magnétiques $\overrightarrow{H}$ du champ électromagnétique. On considère en général que la composante magnétique est la plus importante. Dans ce contexte, de petites boucles inductives de 3mm de diamètre, faites à la main [1], consituent la solution la plus simple. Des sondes plus évoluées de quelques micromètres [4] permettent néanmoins d'obtenir de meilleurs réultats, notamment en positionnant la microsonde juste au-dessus (quelques microns) de la zone d'intérêt (le processeur, le driver de bus,...).

3.2 Mesures en champ lointain

Il a également été proposé dans [2] d'utiliser des antennes biconiques et log-périodiques large bande mais aussi des antennes faible bande, haut gain tel que les antennes Yagi. Dans ce contexte, on s'attache aux émanations non intentionnelles et un récepteur/démodulateur devra être utilisé dans la chaîne d'acquisition.

4 Expérimentation, résultats et observations

Les différentes expériences relatées dans les différents articles [2,1] furent réalisées sur différentes cartes à puce dans lequel un algorithme cryptographique est implémenté tel que le DES, RSA et COMP128, ou encore sur des dispostifs cryptographiques ou des accélérateurs SSL. Pour chacune de ces expériences certaines dépendances furent mises en évidence et cela malgré certaines contremesures activées.

Dans [2], les auteurs expliquent qu'ils ont programmé une carte à puce avec une boucle infinie de 13 cycles. L'horloge externe fournie était de 3.68 MHz.

En utilisant une sonde en champ proche (une simple boucle), une amplification large bande et un oscilloscope 8-bit, 500 MHz, ils ne purent pas dans le domaine temporel voir une indication de l'exécution de la boucle. Par contre, en effectuant une FFT et en passant donc dans le dommaine temporel, plusieurs pics se démarquant des autres furent remarqués : l'horloge et ses nombreuses harmoniques mais aussi un pic à 283 KHz qui correspond à 3.68MHz/13, c'est à dire la fréquence d'exécution de la boucle. En fait on peut généraliser ces observations en disant que lors du traitement des traces électromagnétiques, il peut s'avérer parfois très utile de travailler dans le domaine fréquentiel plutôt que dans le domaine temporel. Certaines instructions/données peuvent présenter des dépendances différentes dans les deux dommaines et parfois une différence sur un bit visé sera beaucoup plus visible dans un des deux domaines.

Dans une autre expérience, toujours expliquée en détail dans [2], la sonde en champ proche est, cette fois, connectée à un récepteur AM, réglé sur la 41ème harmonique à 150.88 MHz. Cette fois autant dans le domaine temporel que fréquentiel, l'effet de la boucle fut visible. Ce qui tend à montrer que parfois certaines harmoniques peuvent avoir un contenu très riche. Mais également les auteurs trouvèrent aussi bien en champ proche qu'en champ lointain des différences de la fréquence de boucle en fonction de certains bits calculés.

En champ lointain cette fois les auteurs de [2] s'intéressèrent à un accélérateur SSL. Et grâce à une antenne log-périodique situé à environ 15 pieds du serveur, ils purent obtenir des courbes suffisamment précises pour mener à bien un type d'attaque appelé "template attacks" [9]. Ils se focalisèrent sur des harmoniques intermédiaires comme porteuse. En effet, les harmoniques les plus basses souffrent en général de beaucoup de bruit et interférences et les hautes harmoniques ont une puissance de signal bien moindre (ce qui est normal en pratique puisque les signaux d'horloge ne sont pas tout à fait carrés).

Tous semblent s'accorder pour dire que la rapport signal à bruit (SNR) des traces électromagnétiques est de plusieurs magnitudes supérieur à celui des traces de consommation. [4] avance le chiffre de 30 dB de différence.

En fait un soin important doit être apporté à l'implémentation hardware, car une bonne partie des attaques se font en identifiant des instructions qui émettent plus que les autres. [2] explique qu'il existe de "mauvaises" instructions. Et malgré le générateur de bruit enclenché, ils furent capable de classer avec une bonne probabilité la valeur du bit attaqué et cela avec peu d'échantillons (20-30).

On peut conclure cette section en disant que les expériences ménées ont démontré la puissance d'une attaque menée par analyse du rayonnement émis par un processeur. Elle peut parfois réussir là où une attaque par mesure de courant échoue, par exemple à cause d'un générateur de bruit aléatoire est actvivé. Et cela, non seulement en champ proche qui nécessite en général un depackaging de la puce, mais aussi en champ lointain. On imagine évidemment la portée pour les industriels de telles menaces. Mais la communauté scientifique de plus en plus active dans ce domaine commence à apporter son lot de contre-mesures,

que ce soit au niveau software, hardware ou encore de la technologie utilisée. Le détail des explications données ici étant certainement insuffisant, nous invitons le lecteur à consulter les différents articles sus cités.

5 Contre-mesures

Les émissions électromagnétiques étant intrinsèquement liées aux caractéristiques physiques du dispositif étudié, les nombreuses contre-mesures envisageables ne sont pas adéquates ou directement applicables pour tous les produits. On ne peut donc pas parler de contre-mesure ultime qui élimenerait tout risque de fuite par voie électromagnétique. C'est pourquoi il convient mieux de mentionner les différents principes de défense, qui devront être adaptés pour chaque utilisation particulière.

L'état de l'art rapporte trois axes d'action : réduire les émissions ou empêcher leur propagation ; décorréler les radiations de l'application qui les génèrent et finalement modifier l'architecture physique de manière à compliquer l'acquisition des mesures. Ces contre-mesures peuvent se situer au niveau matériel (hardware) ou au niveau de la programmation (software). Une protection acceptable contre les attaques EM résident souvent en d'astucieuses combinaisons de contre-mesures.

Depuis le XIXème siècle, les cages de Faraday sont utilisées fréquemment comme boucliers électromagnétiques. Si le métal composant la cage est parfaitement conducteur et ne comporte aucune ouverture, la cage est complètement hermétique aux champs électriques et constitue ainsi un bouclier électromagnétique parfait. Cependant, la cage de Faraday reste une idéalisation théorique pour différentes raisons. La première est due aux imperfections des matériaux qui les rendent résistifs : la profondeur de pénétration n'est dès lors plus nulle. Par ailleurs, les connections physiques qui transmettent l'énergie et les signaux d'entrée-sortie aux composants requièrent la présence d'ouvertures. Bien que des solutions existent, elles ne sont pas facilement compatibles avec les procédés de fabrication actuels ou avec les normes (particulièrement dans le cas des cartes à puce où l'épaisseur est standardisée à 0.76mm - ISO 7816).

La réduction de la consommation est une voie de recherche en microélectronique pour des raisons autres que cryptograpiques ; et qui va de paire avec le perfectionnement de procédé de fabrication. Une faible consommation pourrait être une contre-mesure intéressante pour réduire les fuites par analyse de puissance et d'émission EM. Par exemple, les techniques de SOI (Silicon On Insulator - la masse d'un transistor CMOS est remplacé par un matériau isolant) permettent de réduire le courant consommé [8], ce qui a pour effet de limiter le champ électromagnétique émis. Par ailleurs, les fréquences de travail peuvent être plus grandes.

Dans certains cas très spécifiques, il est possible de sécuriser le composant à protéger en l'isolant et en contrôlant les accès (physiques et informatiques). La distance due au périmètre de sécurité suffit alors à rendre inexploitables

les radiations, a fortiori en combinaison avec une cage de Faraday. Cependant, l'exemple des cartes à puce montre que cette sécurité n'est pas applicable de façon générale.

Un autre axe de recherche tend à rendre les fuites EM inexploitables parce que décorrélées du secret de la carte. Dans les processeurs synchrones, chaque registre est cadencé à la fréquence de l'horloge, dont le signal en créneau est très riche en harmoniques. La signature spectrale de tels processeurs, comportant principalement des composantes à la fréquence fondamentale ainsi qu'à ses multiples, rend les attaques électromagnétiques plus faciles à mettre en œuvre. Une solution élégante consiste à éliminer le signal d'horloge et rendre l'architecture asynchrone. Ce procédé permet de limiter les fuites EM en concentrant le spectre en bandes.

Une autre contre-mesure se base sur le principe suivant : puisque ce sont les transitions entre les niveaux logiques qui fuient, pourquoi ne pas harmoniser les émissions EM en accompagnant chaque transition par sa contraposée [10] ? Pour ce faire, chaque signal est accompagné de son contraire, sur une piste très proche. Cette redondance d'information permet de mieux équilibrer les transitions au niveau électromagnétique. En outre, cette technique permet d'inclure des procédures de détection d'erreur et d'intrusion.

Parallèlement à ces contre-mesures physiques, des stratégies de protection se basent au niveau software. Des astuces de programmations peuvent par exemple camoufler des opérations conditionnelles par de fausses opérations. D'un autre côté, un masque peut être appliqué aux données sensibles de manière rendre toute prédiction par canal caché plus difficile. Calculer $y = \{(x + r_1 n)^{d+r_2\varphi(n)} \bmod r_3 n\} \bmod n$ donnera le même résultat que $y = x^d \bmod n$ (si r_i sont de naturels choisis aléatoirement). Des combinaisons d'hardware et de software sont mises en œuvre telles que les chiffrements à la volée des bus de communication.

Finalement l'architecture même du cryptoprocesseur peut être repensée pour que, malgré les fuites, les attaques électromagnétiques soient nettement plus difficiles à monter. Les techniques de combinaisons demandent déjà de sérieuses modifications de l'architecture du composant à sécuriser. Une idée basée sur le Projet RAW (du MIT Laboratory for Computer Science) est de répartir le calcul cryptographique et les données secrètes sur l'ensemble de la puce. La parallèlisation du chiffrement sur un réseau de micro-unités indépendantes, combinée à d'autres contre-mesures, rendent les attaques par canal caché extrêmement difficiles à mettre en place.

Les fondeurs de cartes à puce détiennent assurément des brevets concernant d'autres contre-mesures. Schlumberger a ainsi une solution qui consiste à disposer face à face deux demies puces : bien que ce procédé assure une meilleure défense contre les attaques intrusives et réduise les radiations, son coût semble prohibitif par rapport aux faibles moyens nécessaires pour acquérir les mesures.

6 Conclusion

Les fuites par émissions életromagnétiques sont particulièrement difficiles à éradiquer car leur présence est une conséquence physique immédiate du comportement microélectronique du dispositif. Les attaques basées sur ce canal caché sont donc susceptibles d'être applicables à tout circuit et la communauté scientifique s'active non seulement à mieux comprendre ces attaques et leur portée mais encore à en établir des contre-mesures fiables. Bien qu'il ne soit pas pratiquement possible de rendre un microprocesseur imperméable à ces fuites, des contre-mesures existent pour les réduire, pour les rendre inintelligibles ou encore pour compliquer les mesures à un point tel que les attaques deviennent théoriquement infaisables avec les moyens actuels.

Références

1. Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic analysis : Concrete results. In Ç.K. Koç, D. Naccache, and C. Paar, Ed., *Cryptographic Hardware and Embedded Systems (CHES 2001)*, volume 2162 of *Lecture Notes in Computer Science*, pp. 251–261. Springer, 2001.
2. Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao and Pankaj Rohatgi The EM side-channel(s). In B.S. Kaliski Jr. and Ç.K. Koç, Ed., *Cryptographic Hardware and Embedded Systems (CHES 2002)*, volume 2523 of *Lecture Notes in Computer Science*, pp. 29–45. Springer, 2002.
3. Jean-Jacques Quisquater & David Samyde Cryptanalyse par side channel Dans *Sécurité des communications sur Internet - SECI02*
4. Jean-Jacques Quisquater and David Samyde. Electromagnetic analysis (EMA) : Measures and counter-measures for smart cards. In I. Attali and T.P. Jensen, Ed., *Smart Card Programming and Security (E-smart 2001)*, volume 2140 of *Lecture Notes in Computer Science*, pp. 200–210. Springer, 2001.
5. Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, Ed., *Advances in Cryptology - CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pp. 104–113. Springer, 1996.
6. Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In M. Wiener, Ed., *Advances in Cryptology - CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pp. 388–397. Springer, 1999.
7. Marc Joye and Francis Olivier. Side-Channel Analysis `http ://www.win.tue.nl/ henkvt/side-channel.pdf`
8. A. Nève de Mevergnies, D. Flandre, J.-J. Quisquater Feasibility of Smart Cards in Silicon-On-Insulator (SOI) Technology. Proc. of the *USENIX workshop on Smartcard Technology*, Chicago (USA), May 10-11, 1999, 7 pp..
9. S. Chari, J.R. Rao and P. Rohatgi. Template Attacks. In B.S. Kaliski Jr. and Ç.K. Koç, Ed., *Cryptographic Hardware and Embedded Systems (CHES 2002)*, volume 2523 of *Lecture Notes in Computer Science*, pp. 13–28. Springer, 2002.

10. S. Moore, R. Anderson, P. Cunningham, Mullins R., & Taylor G. Improving Smart Card Security using Self-timed Ciruits. Proceedings of *Eighth International Symposium on Asynchronous Circuits and Systems (Async'02)*, pp.193-200, 2002.