



2023

Hélène Le Boudier, Ronan Lashermes et Fabien Autrel

Sécurité matérielle : les attaques physiques

Leçon 4 : *Attaques par observation*



IMT Atlantique

Bretagne-Pays de la Loire
École Mines-Télécom

Objectifs Pédagogiques :

- Comprendre ce qu'est une attaque par observation.
- Comprendre ce qu'est une fuite physique d'information.
- Connaître les différentes fuites physiques exploitables.
- Exploiter une fuite physique (le "personal identification number (PIN)" reste notre cas d'usage principal).
- Savoir se protéger des attaque par observation.

Table des matières

1	Introduction	3
2	Fuites physiques	3
2.1	Consommation de courant	3
2.2	Rayonnement électromagnétique	4
3	Différentes exploitations possibles	5
3.1	Analyse simple du courant	5
3.2	Attaques par caractérisation	6
3.3	Les attaques de type correlation power analysis (CPA)	6
4	Contre-mesures	7
4.1	Bruit et Désynchronisation	7
4.2	Masque	7
5	Conclusion	8

1 Introduction

Dans cette leçon, nous revenons sur les attaques par observations [1]. Elles ont été évoquées précédemment notamment dans la leçon numéro deux avec les attaques temporelles. Cette leçon porte essentiellement sur d'autres paramètres physiques exploitables que le temps. Aussi commençons par quelques rappels sur la définition.

Les **attaques par observation** appelées aussi parfois attaques par canaux auxiliaires¹ notées SCA se base sur l'observation du circuit pendant l'exécution des calculs.

Si un algorithme est théoriquement "sûr", le circuit dans lequel il est implémenté ne l'est pas forcément. C'est la frontière entre la théorie et la pratique. L'algorithme est théorique, le circuit lui est bien concret. Ainsi ce dernier a une consommation de courant, un temps de calcul, etc. Ce sont ces paramètres physiques qui peuvent nuire à la sécurité de notre algorithme. Ces paramètres ne sont pas faciles à anticiper d'un point de vue théorique, on parle de **fuite physique d'information** par un canal auxiliaire.

Ce type d'attaque est théoriquement non-invasive; en pratique, l'attaquant peut vouloir acquérir des mesures à un emplacement précis du circuit et finalement la réalisation implique une attaque semi-invasive voir invasive.

Attention, il ne faut pas confondre les attaques par canaux auxiliaires avec les attaques par canaux cachés. Les attaques par canaux cachés exfiltrent de l'information via un canal caché. Ce n'est pas le sujet de ce cours.

2 Fuites physiques

Les attaques par observation analysent une fuite physique d'un circuit. Il s'agit de mesures physiques comme le temps, la température, la consommation de courant, le rayonnement électromagnétique. Aussi comme dans toutes mesures expérimentales, il faut souvent prendre en compte un bruit environnant et des erreurs de mesure sont possibles.

2.1 Consommation de courant

L'idée est de se brancher directement sur le circuit pour mesurer sa consommation de courant. Un courant électrique est un déplacement de charges électriques. Chaque instruction réalisée par un circuit met en œuvre un certain nombre de transistors. À chaque instant, la mesure de l'intensité du courant électrique appelée **consommation de courant**, reflète l'activité du circuit.

Un circuit intégré est constitué d'un ensemble de portes logiques. La consommation de courant du circuit est la somme des consommations de courant de chacune de ses portes logiques. Une porte logique n'a pas une consommation de courant constante dans le temps.

Il existe deux modèles de consommation de courant des portes logiques.

- Un **modèle dynamique** où une porte logique consomme de l'énergie à chaque changement d'état
- Un **modèle statique** où une porte logique consomme de l'énergie même au repos.

Ces deux modèles sont couramment utilisés. On a donc la possibilité de distinguer une transition de 0 vers 1 d'une transition de 1 vers 0.

C'est pourquoi la consommation de courant d'une valeur présente dans le circuit, portée par un ensemble de portes logiques, est considérée comme proportionnelle :

- au **poids de Hamming (HW)**, qui est le nombre de bits à 1 ; ou
- à la **distance de Hamming (HD)** avec la dernière valeur calculée, qui est le nombre de variations de bit entre deux valeurs.

D'autre part, certaines opérations, plus coûteuses, augmentent la consommation électrique du circuit, notamment à cause de l'utilisation de plus de composants.

1. Attention la définition de ce terme peut varier d'une communauté scientifique à une autre.


2.2 Rayonnement électromagnétique

Les **émissions d'ondes électromagnétiques** d'un circuit sont causées par la circulation de courant en son sein. Cette circulation de charges dans le conducteur produit un champ électromagnétique composé d'un champ magnétique et d'un champ électrique, mathématiquement reliés par les équations de Maxwell [2]. Ces ondes électromagnétiques se propagent dans l'espace et ainsi peuvent être captées par une sonde. La sonde doit généralement être positionnée aussi près que possible de la surface active du circuit ; on parle de mesures en champ proche.

La FIGURE 1 représente une plateforme permettant d'acquérir le rayonnement électromagnétique d'un circuit. Cette plateforme est propriété de l'*Inria*.



FIGURE 1 – EMA, plateforme de side channel du Laboratoire Haute Sécurité (LHS) d'INRIA Rennes.

L'avantage majeur d'une analyse électromagnétique (EM) par rapport à une analyse par consommation de courant est le fait que les mesures sont prises localement. Un autre avantage est que ces attaques sont non-invasives. Mieux encore, puisque le circuit ne peut pas facilement détecter qu'il est observé car il n'y a pas de branchement ni même besoin d'un contact physique. Cependant, les mesures EM sont souvent plus sensibles au bruit et sont très dépendantes du positionnement de la sonde. La consommation de courant et l'EM sont étroitement liées, ainsi elles sont souvent modélisées et utilisées de manière très similaire. La FIGURE 2 présente des sondes de chez Langer EMV Technik .

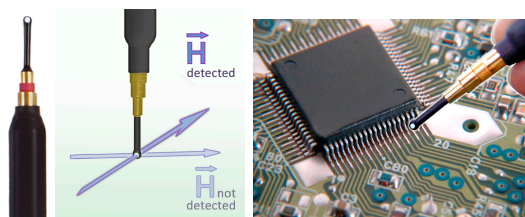


FIGURE 2 – Sonde de chez Langer EMV Technik [3]

3 Différentes exploitations possibles

3.1 Analyse simple du courant

L'**analyse simple** d'un paramètre physique [4], notée SPA, vise à déterminer directement, à partir d'une observation, par exemple de la consommation de courant, lors d'une exécution normale de l'algorithme, des informations sur le calcul effectué ou les données manipulées [5, 6, 7].

La simple power analysis (SPA) de Kocher vise l'algorithme **Square and Multiply** (voir FIGURE 3) très utilisé en cryptographie. Le but de cet algorithme est de calculer une exponentiation modulaire en réduisant au maximum le nombre de calculs possibles. Dans l'exemple suivant :

$$x^e \bmod n,$$

e est l'exposant et n le modulo.

```

1: procedure Square and Multiply( $x, e, n$ )
2:    $r = 1$ 
3:    $b = (e)_2$ 
4:   for  $i$  most significant bit to least significant bit do
5:     if  $b[i] = 1$  then
6:        $r = r^2 \cdot x \bmod n$ 
7:     else
8:        $r = r^2 \bmod n$ 
9:     end if
10:  end for
11:  return  $r$ 
12: end procedure

```

FIGURE 3 – Algorithme Square and Multiply

Pour cela l'exposant est écrit en binaire. Dans l'écriture si l'on a un 1 une multiplication et une élévation au carré sont calculées. Si l'on a un 0 seule une élévation au carré est calculée. Aussi cette suite de calculs est très caractéristique et peut s'observer directement sur une trace de consommation de courant comme l'illustre la FIGURE 4.

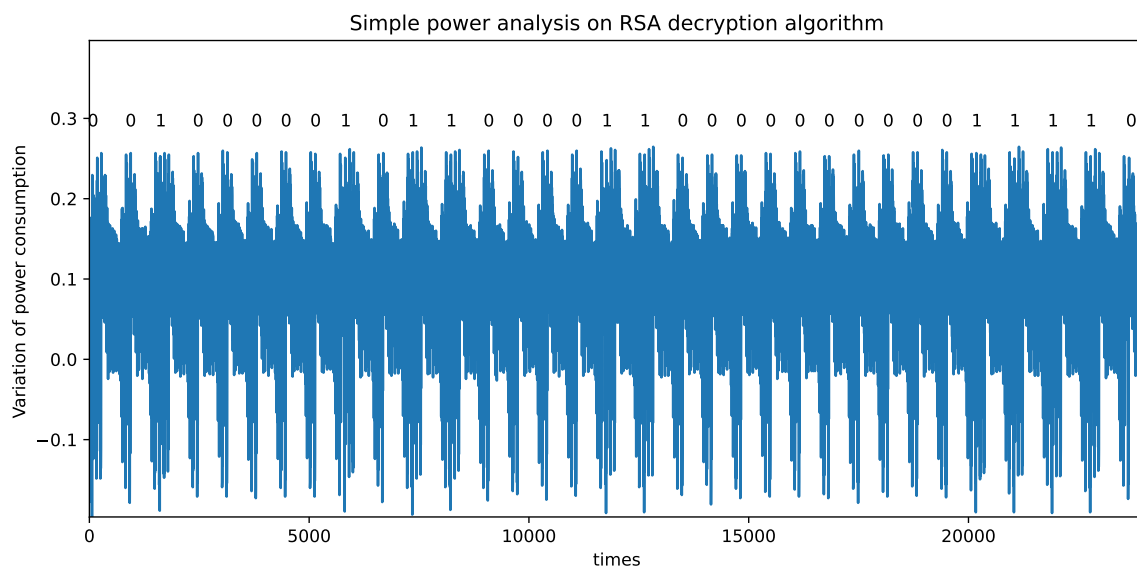


FIGURE 4 – SPA contre l'algorithme Square and Multiply utilisé dans algorithme RSA (illustration réalisée en projet par Jonathan Amatu, Maël Leproust, Salim Sama Mola et Alexis Prou étudiants à IMT-Atlantique, année 2024)

3.2 Attaques par caractérisation

Les **attaques par caractérisations**, appelées aussi profilées ou par apprentissage (Template attacks [8, 9, 10, 11, 12, 13]) sont les plus efficaces en termes d'information. En effet il n'y a pas de modèle mathématique mais un apprentissage de la fuite physique. Pour réaliser une telle attaque, on suppose que l'attaquant possède un circuit identique à celui qu'il souhaite attaquer ; dont il est l'utilisateur légitime.

Il y a donc deux circuits :

1. un circuit qui est la cible,
2. un circuit de référence sur lequel l'attaquant peut effectuer des modifications.

Il y a deux grandes étapes à une attaque par apprentissage.

1. **La caractérisation** ou phase d'apprentissage est la première étape. Il s'agit de caractériser le circuit de référence par rapport à une fuite d'information. Les mesures obtenues sont en fait une "signature" de l'exécution du programme au sein du circuit (instructions exécutées, données manipulées, ...). La caractérisation permet d'apprendre la fuite significative et les caractéristiques du bruit. Sans être capable d'identifier exactement une instruction ou des données manipulées, le biais statistique présent dans un signal peut être suffisant pour une exploitation. Beaucoup de mesures doivent être obtenues, le nombre dépendant du bruit présent dans le signal.
2. **L'attaque** en soit est la deuxième étape. L'attaquant réalise des mesures sur le circuit cible et va les confronter à sa caractérisation pour retrouver un secret. Selon les résultats expérimentaux, il est possible de distinguer l'exécution d'une instruction à la place d'une autre. Il est même possible de retrouver la valeur d'une donnée chargée dans un registre avec une probabilité non négligeable.

Les algorithmes cryptographiques sont très vulnérables à ce type d'attaque, mais ils ne sont pas les seuls. Une attaque d'une vérification de code PIN par caractérisation a été publiée [14].

3.3 Les attaques de type CPA

Les attaques les plus utilisées sont les attaques de type **correlation power analysis (CPA)** [15]. Les attaques regroupées dans cette famille ont les caractéristiques suivantes.

- Un modèle mathématique est proposé pour approcher la fuite physique.
- Des hypothèses sur le secret sont énumérées, aussi bien souvent ce sont des attaques de types diviser pour régner. C'est-à-dire que le secret est partitionné en morceaux retrouvés indépendamment les uns des autres.
- Un ou plusieurs outils statistiques sont utilisés pour faire ressortir les bonnes hypothèses.

La première attaque de cette famille était la "differential power analysis (DPA)" [16].

4 Contre-mesures

Dans ce cours nous vous présentons brièvement quelques exemples de contre-mesures. Il en existe d'autres dont certaines sont encore des sujets de recherche à part entière.

4.1 Bruit et Désynchronisation

L'**ajout d'instructions factices** permet de modifier le temps d'exécution ou la consommation de courant d'une portion de code embarqué. Cela ajoute du bruit et désynchronise les calculs [17, 18, 19]. Une désynchronisation est aussi possible si le programme n'exécute pas toujours les instructions dans le même ordre. Évidemment cette modification ne doit pas impacter la sémantique de l'algorithme.

4.2 Masque

Le **masquage** est l'une des contre-mesures les plus répandues face aux fuites d'information. Elle consiste à appliquer un masque aléatoire aux données que l'on souhaite protéger [20, 21, 22, 23, 24]. Cette solution nécessite d'adapter l'algorithme.

Le cas simple est le cas d'une fonction linéaire $f : \mathbb{F}_{2^m} \Rightarrow \mathbb{F}_{2^l}$. Soit $x \in \mathbb{F}_{2^m}$ la valeur intermédiaire à protéger et $m \in \mathbb{F}_{2^m}$ la valeur du masque aléatoire. Alors nous avons, par linéarité de f :

$$f(x) = f(x \oplus m) \oplus f(m) \quad .$$

Le calcul est fait en parallèle sur $x \oplus m$ et m et la valeur finale n'est reconstituée qu'au tout dernier moment. Aucune information n'a pu fuiter sur x car $f(x)$ n'est jamais évaluée. Pour obtenir de l'information sur x , il faut prendre en compte 2 fuites d'information (sur $x \oplus m$ et sur m) : on parle alors d'attaque d'ordre 2.

Plus généralement, on se protège d'une attaque d'ordre n par l'utilisation de n masques aléatoires. Mais ce schéma reste vulnérable à une attaque d'ordre $n + 1$.

Pour une fonction $f : \mathbb{F}_{2^m} \Rightarrow \mathbb{F}_{2^l}$ non linéaire (exemple les s-box d'un algorithme de chiffrement), la difficulté augmente. En général, on génère une fonction f_m tel que :

$$f_m(x \oplus m) = f(x) \oplus m \quad ;$$

ou de manière équivalente par changement de variable :

$$f_m(y) = f(y \oplus m) \oplus m \quad .$$

Il est important de s'assurer que, dans l'implémentation, $f(x)$ n'est jamais évaluée.

5 Conclusion

Les attaques par observation sont une réelle menace tout autant que les attaques par injections de fautes. Certaines fuites comme le rayonnement électromagnétique ne nécessitent aucun branchement. Aussi le circuit ne peut en aucun cas détecter l'attaque. De plus, certaines contre mesures comme la redondance de code pour lutter contre les injections de fautes sont des faiblesses supplémentaires d'un point de vue attaques par observations. En effet doubler un code est équivalent à doubler la fuite faute physique.

En conclusion, les attaques physiques sont une réelle vulnérabilité et doivent être prises en compte. N'implémentez pas votre sécurité uniquement en logiciel, si votre circuit est amené à sortir. Utiliser des circuits dédiés à la sécurité.

La leçon suivante et dernière leçon est consacrée à la certification des circuits.

Acronymes

PIN personal identification number. 2, 6

CPA correlation power analysis. 2, 6

DPA differential power analysis. 6

EM électromagnétique. 4

HD distance de Hamming. 3

HW poids de Hamming. 3

LHS Laboratoire Haute Sécurité. 4

SCA side channel analysis. 3

SPA simple power analysis. 5

Références

- [1] Jacques Fournier. Le circuit intégré, grande faiblesse des algorithmes cryptographiques? <http://www.industrie-techno.com/fic-2016-le-circuit-integre-grande-faiblesse-des-algorithmes-cryptographiques-42312>.
- [2] Timo Van Neerden. Les équations de maxwell expliquées simplement. <https://couleur-science.eu/?d=c7f412--les-equations-de-maxwell-expliquees-simplement>.
- [3] Langer. <https://www.langer-emv.com/en/index>.
- [4] Thomas S Messerges, Ezzy A Dabbish, and Robert H Sloan. Power analysis attacks of modular exponentiation in smartcards. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 144–157. Springer, 1999.
- [5] Thomas S Messerges, Ezzy A Dabbish, and Robert H Sloan. Power analysis attacks of modular exponentiation in smartcards. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 144–157. Springer, 1999.
- [6] Christophe Clavier and Marc Joye. Universal exponentiation algorithm a first step towards provable sparseness. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 300–308. Springer, 2001.
- [7] Stefan Mangard. A simple power-analysis (SPA) attack on implementations of the AES key expansion. In *ICISC 2002*. Springer.
- [8] Suresh Chari, Josyula R Rao, and Pankaj Rohatgi. Template attacks. In *Cryptographic Hardware and Embedded Systems-CHES 2002*. Springer, 2003.
- [9] Cédric Archambeau, Eric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater. Template attacks in principal subspaces. In *Cryptographic Hardware and Embedded Systems-CHES*, pages 1–14. Springer, 2006.
- [10] Christian Rechberger and Elisabeth Oswald. Practical template attacks. In *Information Security Applications*, pages 440–456. Springer, 2005.
- [11] M Abdelaziz Elaabid, Sylvain Guilley, and Philippe Hoogvorst. Template Attacks with a Power Model. *IACR Cryptology ePrint Archive*, 2007 :443, 2007.
- [12] Elisabeth Oswald and Stefan Mangard. Template attacks on maskingresistance is futile. In *Topics in Cryptology-CT-RSA 2007*, pages 243–256. Springer, 2006.
- [13] Omar Choudary and Markus G Kuhn. Efficient template attacks. In *International Conference on Smart Card Research and Advanced Applications*, pages 253–270. Springer, 2013.
- [14] Hélène Le Boudier, Thierno Barry, Damien Couroussé, Jean-Louis Lanet, and Ronan Lashermes. A template attack against verify pin algorithms. In *SECRYPT 2016*, pages 231–238, 2016.
- [15] Eric Brier, Christophe Clavier and Francis Olivier. Correlation Power Analysis with a Leakage Model. In *CHES*, pages 16–29, 2004.
- [16] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Annual International Cryptology Conference*, pages 388–397. Springer, 1999.
- [17] Matthieu Rivain, Emmanuel Prouff, and Julien Doget. Higher-order masking and shuffling for software implementations of block ciphers. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 171–188. Springer, 2009.
- [18] Marc Joye and Francis Olivier. Side-channel analysis., 2011.
- [19] Ryad Benadjila, Emmanuel Prouff, Rémi Strullu, Eleonora Cagli, and Cécile Dumas. Deep learning for side-channel analysis and introduction to ascad database. *Journal of Cryptographic Engineering*, 10(2) :163–188, 2020.
- [20] Alexandre Duc, Sebastian Faust, and François-Xavier Standaert. Making masking security proofs concrete. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 401–429. Springer, 2015.
- [21] Weize Yu and Selçuk Köse. A lightweight masked aes implementation for securing iot against cpa attacks. *IEEE Transactions on Circuits and Systems I : Regular Papers*, 64(11) :2934–2944, 2017.
- [22] Jovan D Golić and Christophe Tymen. Multiplicative masking and power analysis of aes. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 198–212. Springer, 2002.

- [23] Elisabeth Oswald, Stefan Mangard, Norbert Pramstaller, and Vincent Rijmen. A side-channel analysis resistant description of the aes s-box. In *International workshop on fast software encryption*, pages 413–423. Springer, 2005.
- [24] David Knichel, Amir Moradi, Nicolai Müller, and Pascal Sasdrich. Automated generation of masked hardware. *Cryptology ePrint Archive*, 2021.



IMT Atlantique Bretagne - Pays de la Loire - www.imt-atlantique.fr

Campus de Brest
Technopôle Brest-Iroise
CS 83818
29238 Brest Cedex 03
T +33 (0)2 29 00 11 11
F +33 (0)2 29 00 10 00

Campus de Nantes
4, rue Alfred Kastler - La Chantrerie
CS 20722
44307 Nantes Cedex 03
T +33 (0)2 51 85 81 00
F +33 (0)2 51 85 81 99

Campus de Rennes
2, rue de la Châtaigneraie
CS 17607
35576 Cesson Sévigné Cedex
T +33 (0)2 99 12 70 00
F +33 (0)2 99 12 70 08