CLONER UNE FONCTION PHYSIQUE NON CLONABLE PAR L'ANALYSE DE SON RAYONNEMENT ELECTROMAGNETIQUE

L. Bossuet, B. Colombier, N. Bochard, V. Fischer

Université de Lyon, CNRS, Laboratoire Hubert Curien UMR 5516,
F-42023, SAINT-ETIENNE, France, lilian.bossuet@univ-st-etienne.fr

Résumé. Les fonctions physiques non clonables sur silicium (ou en anglais les silicium PUF pour *physical unclonable functions*) sont des dispositifs physiques permettant l'identification unique de circuits intégrés. De plus en plus prisées par l'industrie, elles comportent toutefois quelques failles de sécurité importantes. Comme nous le montrons dans cet article, lorsque les PUF exploitent des cellules oscillantes, il est possible de les cloner grâce à une analyse spectrale dédiée de leur rayonnement électromagnétique. Cet article présente deux méthodologies d'analyse dédiées aux cellules qui oscillent de façon permanente ou de façon transitoire.

I. INTRODUCTION

Les fonctions physiques non clonables (ou en anglais les PUF pour *physical unclonable functions*) sont des dispositifs physiques permettant l'identification unique de systèmes matériels (optiques, électroniques ou autres). Leur réponse à un challenge d'entrée (un stimuli) doit être imprévisible, stable et unique. Il ne doit pas être possible physiquement de reconstituer (ou de simuler) un dispositif équivalent (un clone) à une PUF ayant la même réponse pour tous les challenges possibles. C'est la garantie de ne pas pouvoir « cloner » une PUF qui apporte la sécurité au processus d'identification physique. Cependant, dans le cas des PUF réalisées directement sur le même silicium qu'une puce microélectronique, des possibilités de clonage existent.

Dans cet article, nous nous intéressons aux PUF sur silicium exploitant des cellules oscillantes en anneaux à oscillation permanente (*ring-oscillators* ou RO) et à oscillation transitoire (*transient-effect-ring-oscillator*s ou TERO). Cet article présente nos travaux pionniers sur l'analyse du rayonnement électromagnétique des cellules oscillantes, RO et TERO, et son exploitation pour cloner des PUF basées sur ces cellules. L'utilisation du canal électromagnétique est très pertinente lorsque la réponse de la PUF ne sort jamais du circuit intégré ce qui est le cas d'utilisation le plus courant. Nous considérons dans ces travaux que l'attaquant a la possibilité de modifier le challenge de la PUF ciblée mais n'a pas connaissance de sa réponse qu'il cherche donc à reconstituer et modéliser.

La suite de cet article est constituée de la façon suivante : la section II présente les prérequis nécessaires à la compréhension des PUF sur silicium exploitant des cellules oscillantes, les sections III et IV présentent les résultats expérimentaux de nos travaux. La section V conclut cet article.

II. LES PUF SUR SILICIUM EXPLOITANT LES CELLULES OSCILLANTES

Une PUF sur silicium est un système d'extraction de l'entropie issue des variations du procédé de fabrication CMOS [1] (c'est principalement la fluctuation dans la densité de dopants qui implique des variations très locales des caractéristiques des transistors qui est exploitée), dite entropie intrinsèque du circuit intégré. Les PUF peuvent être considérées comme des empreintes digitales des circuits intégrés. Elles sont étudiées depuis plus de quinze ans, la première proposition de PUF sur silicium date de 2002, elle est due à des chercheurs du MIT [1].

Le dispositif d'identification se base sur une paire de "challenge / réponse" qui est l'association entre un ensemble de défis et les réponses retournées par la PUF. La figure 1 illustre ce principe.

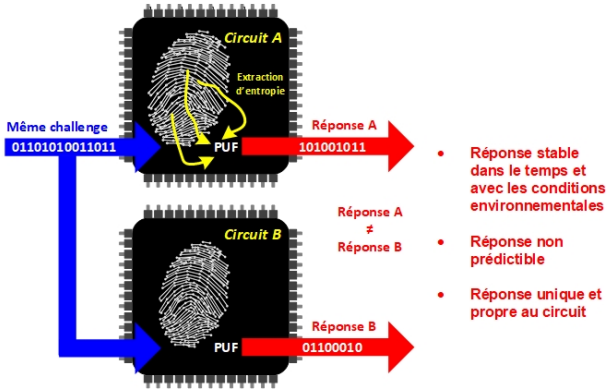

Fig. 1. Illustration du fonctionnement d'une PUF insérée dans deux circuits intégrés, A, et B identiques.

Cette figure présente deux circuits identiques (dont les puces ont été fabriquées par exemple dans la même usine, le même jour sur le même wafer), le circuit A et le circuit B. Chacun des deux circuits embarque exactement la même PUF. Si un même challenge est envoyé à la PUF du circuit A et à celle du circuit B, les deux réponses obtenues doivent être différentes (avec en moyenne la moitié des bits des deux réponses qui sont différents) tout comme les empreintes digitales de deux individus humains conçu en même temps (des jumeaux/jumelles donc) sont différentes. Poursuivons l'analogie avec les empreintes digitales humaines : les réponses des PUF doivent être stables dans le temps et même lorsque les conditions environnementales changent (ici les variations de la température et de la tension d'alimentation des circuits intégrés sont le plus souvent considérées), les réponses ne sont pas prédictibles du fait du caractère aléatoire des variations du procédé de fabrication des

circuits intégrés, il n'est pas possible de prédire à l'avance quelle sera la réponse d'une PUF à un challenge encore non testé.

Le principe très général du fonctionnement d'une PUF est le suivant : deux cellules électroniques très simples sont conçues dans le circuit de façon strictement identique. Une fois conçues, la PUF mesure de façon intrinsèque une différence de caractéristique entre les deux cellules. Si celles-ci sont effectivement conçues de la même façon, alors le résultat de cette mesure dépend uniquement de la variation du procédé de fabrication qui est aléatoire.

Il existe plusieurs solutions pour construire des PUF sur silicium. À partir des années 2010, de nombreuses équipes académiques ont étudié ces constructions en cherchant quel type de PUF est le plus adapté pour une réalisation dans des circuits de type FPGA et ASIC. Toutes ces études ont conclu que les PUF basées sur des cellules oscillantes offraient le meilleur compromis entre les performances (principalement définies par la qualité statistique des réponses de la PUF) et la difficulté de la réalisation [2].

Une première solution pour construire une PUF à base de structures oscillantes est d'utiliser des RO. On parle alors de RO-PUF. Dans ce cas, la caractéristique physique mesurée par la PUF est la fréquence d'oscillation de deux oscillateurs (choisis parmi un grand nombre) théoriquement identiques. La figure 2 illustre ce principe. Sur celle-ci, la RO-PUF est constituée de deux groupes distincts A et B de *m* oscillateurs en anneau (dans l'article original qui décrit la RO-PUF, les oscillateurs ne sont pas séparés en deux groupes distincts mais cela fait apparaitre des corrélations directes dans les couples (challenge, réponse) de la RO-PUF). Tous les oscillateurs sont identiques et sont constitués d'un nombre *N* impair d'inverseurs. La fréquence d'oscillation moyenne de chacun des oscillateurs dépend de *N* et des variations du procédé de fabrication CMOS. Sur la figure 2, nous voyons que le mot de challenge *Select cell* permet de sélectionner, en commandant les multiplexeurs et démultiplexeurs, le couple d'oscillateurs dont la fréquence d'oscillation est comparée.

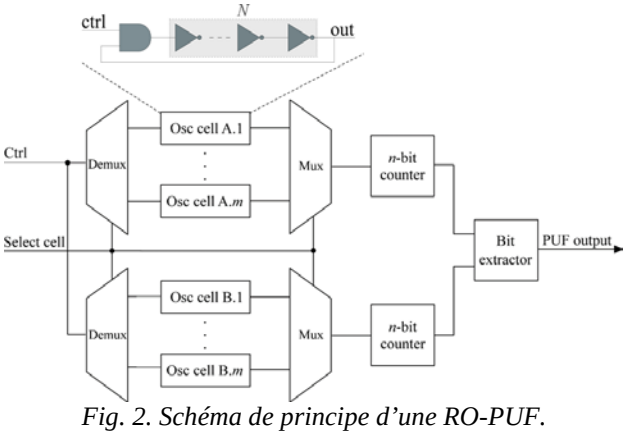

Fig. 2. Schéma de principe d'une RO-PUF.

Pour comparer la fréquence d'oscillation des deux oscillateurs sélectionnés, on utilise des compteurs qui comptent tant que le signal de contrôle (*Ctrl*) est actif. L'oscillateur en anneau qui produira le plus grand nombre en sortie du compteur a la fréquence la plus élevée. Suivant qu'il soit l'oscillateur sélectionné pour le groupe A ou pour le groupe B, la sortie de la RO-PUF sera placée à l'état logique bas ou haut.

Cloner une RO-PUF est possible dès lors que l'on connait la fréquence d'oscillation des différents RO utilisés. Au début des années 2010, nous avons montré que ce clonage était possible grâce à l'analyse du rayonnement électromagnétique des cellules RO [3] comme nous le présenterons dans la section III de cet article.

Pour tenter de régler ce problème tout en continuant à utiliser des cellules oscillantes, dont les caractéristiques sont très intéressantes pour la construction des PUF, nous avons proposé une nouvelle PUF, la TERO-PUF [2], exploitant des TERO et pour laquelle la fréquence d'oscillation n'est plus utilisée pour générer la réponse. La cellule TERO est une structure dans laquelle deux RO sont couplés, comme cela est présenté sur la figure 3. Ainsi, lorsque le signal *Ctrl* est activé, deux fronts (deux événements électriques) circulent dans la cellule qui oscille alors pendant un certain temps avant de se stabiliser à l'état logique '0' ou '1'. Comme nous l'avons montré [2], du fait des variations du procédé de fabrication CMOS, le rapport cyclique du signal de la TERO varie de 50 % à 0% (état logique final '0') ou de 50% à 100% (état logique final à '1') car un des deux événements électriques va rattraper l'autre (c'est la conséquence de ce que l'on appelle l'effet *drafting* [2]). La durée des oscillations est donc dépendante de la variation des procédés de fabrication. Ce n'est donc pas la fréquence d'oscillation mais le nombre de périodes d'oscillation avant l'arrêt qui est exploité pour générer la réponse de la PUF. L'architecture globale de la TERO-PUF est la même que celle de la RO-PUF (voir figure 2) en remplaçant les RO par des TERO.

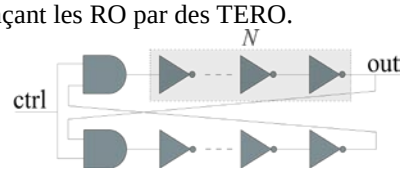

Fig. 3. La cellule TERO.

III. ANALYSE ELECTROMAGNÉTIQUE DES CELLULES RO

Les oscillateurs en anneaux, ou RO, sont connus pour être sensibles, du point de vue de leur fréquence d'oscillation, aux paramètres de fonctionnement du circuit (température, tension d'alimentation). Ils sont d'ailleurs couramment utilisés comme capteur de température dans les circuits intégrés. Pour cloner une RO-PUF il faut mesurer, depuis l'extérieur du circuit qui embarque la RO-PUF, la fréquence d'oscillation des RO. La méthode que nous proposons pour cela se base sur la sensibilité des RO aux conditions environnementales et l'analyse fréquentielle de leur rayonnement électromagnétique.

Pour deux conditions de fonctionnement différentes d'un RO, sa fréquence d'oscillation est différente. D'autres signaux périodiques peuvent parcourir le circuit intégré

embarquant le ou les RO dont on souhaite analyser le rayonnement électromagnétique, mais il s'agit principalement de signaux synchrones avec la source d'horloge générés par un système (générateur à base de quartz associé à une boucle à verrouillage de phase) bien moins sensibles aux variations environnementales du circuit. Donc, en soustrayant le spectre fréquentiel du rayonnement électromagnétique du circuit pour une condition de fonctionnement et pour une autre condition, les contributions des RO devraient être prépondérantes sur le spectre différentiel obtenu devant les autres contributions. La méthode que nous proposons est décrite sur la Figure 4.

Pour obtenir deux spectres du rayonnement électromagnétique à deux conditions différentes, nous avons choisi de modifier la tension d'alimentation du circuit, qui est très facilement et précisément contrôlable. La modification de la température extérieure est envisageable mais son contrôle est plus difficile.

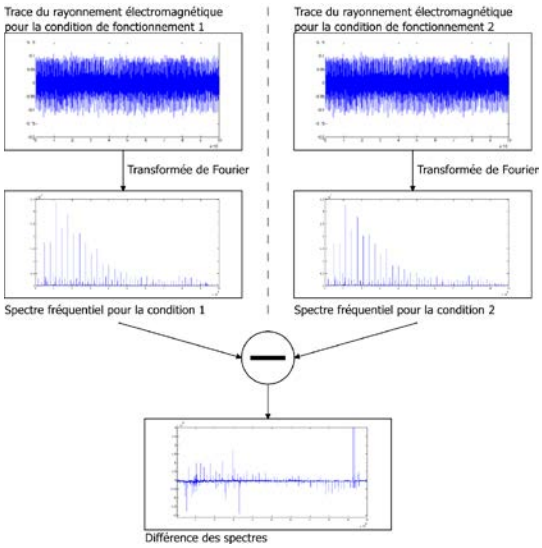

Fig. 4. Illustration de la méthode d'analyse spectrale différentielle du rayonnement électromagnétique.

Pour réaliser nos mesures, le banc de test utilisé est assez simple et se compose de :

- Une sonde électro-magnétique LANGER RF-U 2.5-2 ayant une bande passante de 30 MHz à 3000 MHz et une résolution spatiale de 500 µm,
- un amplificateur faible bruit MITEQ ayant une bande passante de 100 MHz à 1 GHz, un gain de 48 dB de gain et 0.7 dB de figure de bruit,
- un oscilloscope Lecroy WaveRunner 640 Zi avec une fréquence d'échantillonnage de 40 GS/s,
- une alimentation programmable,
- une table XYZ Prior H101A + FB204 de résolution XY 10 nm et une répétabilité de 1µm.

Avec ce banc, nous effectuons, point à point (90 points sur chacun des axes X et Y), une cartographie différentielle du rayonnement électromagnétique du circuit embarquant le ou les RO. Pour chaque point, dix mesures composées de 400 000 échantillons sont recueillies pour chacune des deux conditions de fonctionnement. Nous effectuons une moyenne sur les dix densités spectrales obtenues en chaque point pour chacune des conditions de fonctionnement.

La figure 5 donne le résultat de la méthode proposée lorsque le circuit ciblé est un FPGA Intel Cyclone III qui contient 50 RO à 3 inverseurs. La tâche jaune-rouge présente la position physique du rayonnement des RO sur la plage de fréquence de 289 MHz à 294 MHz (tous les détails techniques sont présentés dans [4]). Ainsi, nous sommes en capacité de localiser physiquement les RO et leur plage de fréquence d'oscillation. Des résultats similaires ont été confirmés avec un FPGA Microsemi Fusion. A partir de ces travaux, l'utilisation du signal de challenge d'une RO-PUF permet de sélectionner les RO deux par deux et de reproduire la réponse de la PUF comme cela a été montré dans [5].

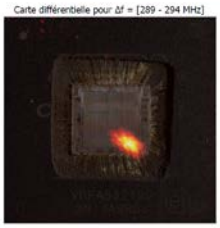

Fig. 4. Localisation spectrale et fréquentielle des RO par analyse spectrale du rayonnement électromagnétique.

IV. ANALYSE ELECTROMAGNÉTIQUE DES CELLULES TERO ET DE LA TERO-PUF

Comme nous l'avons indiqué dans la section II de cet article, la seule connaissance des fréquences d'oscillation des cellules TERO lors de l'état oscillant transitoire ne permet pas de reconstituer la réponse d'une TERO-PUF. Il faut pouvoir mesurer la durée de l'état oscillant et la fréquence d'oscillation pour déterminer le nombre de périodes d'oscillation des cellules TERO avant leur arrêt. Pour cela, nous avons utilisé le même banc d'analyse que celui décrit précédemment mais nous utilisons cette fois à la place de l'oscilloscope un analyseur de spectre temps réel Tektronix RSA607. Celui-ci nous permet de suivre l'évolution de l'amplitude d'une contribution spectrale à une fréquence donnée, ce qui est une information essentielle pour notre mesure.

Contrairement au cas des RO, nous souhaitons mesurer la variation d'amplitude spectrale dans le temps. Cette mesure est plus difficile car plus bruitée que la mesure de fréquence. Pour faciliter la mesure, nous avons dû procéder au décapsulage des deux cibles FPGA utilisées : un FPGA Xilinx Spartan 6 et un FPGA Intel Cyclone V. Pour ce faire nous avons procédé à l'application d'un mélange 5/1 d'acide nitrique (HNO3)/sulfurique (H2SO4) à une température de 44°C pendant 240 secondes avant un nettoyage à l'acétone. Le résultat de la décapsulation est présenté sur la figure 5.

Dans un premier temps, nous avons analysé le spectre du rayonnement électromagnétique de deux cellules TERO identiques, composées chacune de 14 inverseurs,

commandées par le même signal de contrôle et placées dans le même FPGA. La figure 6 donne le spectrogramme (qui représente la variation des amplitudes spectrales dans le temps sur une bande de fréquence) mesuré sur une bande de 7MHz autour de 174MHz avec la cible Xilinx Spartan 6 (nous obtenons les mêmes résultats avec la cible Intel Cyclone V).

(a) Intel Cyclone V (b) Xilinx Spartan 6

Fig. 5. Les deux modules comportant les FPGA Xilinx Spartan 6 et Intel Cyclone V décapsulés pour notre étude.

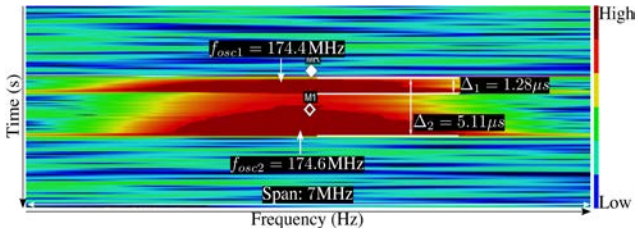

Fig. 6. Spectrogramme du rayonnement électromagnétique de deux cellules TERO identiques placées dans un FPGA Xilinx Spartan 6.

Sur la figure 6 nous pouvons constater que deux contributions spectrales démarrent à l'instant représenté par le curseur losange plein (*MR*). Une est centrée à la fréquence de 174.4 MHz et dure 1.28 µs et l'autre est centrée à la fréquence de 174.6 MHz et dure 5.11µs. Nous pouvons donc en conclure qu'une des deux cellules TERO oscille pendant 223 périodes avant l'arrêt et que l'autre oscille 892 périodes avant l'arrêt.

La TERO-PUF est composée d'un grand nombre de cellules TERO. C'est pourquoi nous avons, à partir de la première expérience, cherché à obtenir le spectrogramme d'une TERO-PUF complète composée de deux blocs de 128 cellules TERO à 14 inverseurs tel que présenté dans [6]. En modifiant le challenge et activant deux à deux les cellules TERO toutes les 10 µs nous obtenons le spectrogramme présenté sur la figure 7 (ici pour 4 challenges différents successifs).

Nous voyons sur la figure 7 l'équivalent de 4 fois le spectrogramme obtenu à la figure 6 pour deux cellules. Nous pouvons donc en tirer l'information du nombre de périodes d'oscillation avant l'arrêt des deux cellules TERO sélectionnées par le challenge de la TERO-PUF.

Obtenir à partir de ces mesures la valeur précise du nombre de périodes d'oscillations de chacune des deux fois 128 cellules TERO de la TERO-PUF est simple et de complexité linéaire. Effectivement, si nous avons la pleine maitrise du challenge de la TERO-PUF, nous pouvons sélectionner la cellule A1 du groupe A de 128 cellules TERO et sélectionner la cellule B1 du groupe B de 128 cellules TERO. L'analyse du spectrogramme nous donne alors les nombres N1 et N2 de périodes d'oscillation avant l'arrêt mais sans pouvoir déterminer lequel correspond à la cellule A1 ou à la cellule B1. En reproduisant la même mesure en sélectionnant toujours la cellule A1 mais une cellule différente du groupe B, la cellule B2, nous obtenons par comparaison avec la première mesure le nombre de périodes d'oscillation avant l'arrêt des cellules A1, B1 et B2. En procédant ainsi de suite nous pouvons cloner la TERO-PUF juste en rejouant la réponse aux challenges sans cloner sa structure interne elle-même.

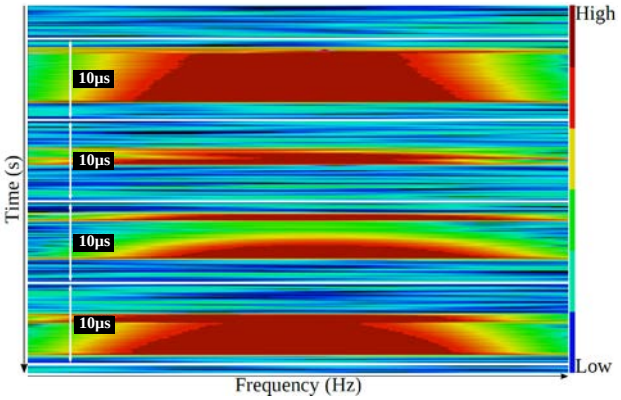

Fig. 7. Spectrogramme du rayonnement électromagnétique d'une TERO-PUF dans un FPGA Xilinx Spartan 6 pour 4 challenges différents.

V. CONCLUSION

Nous avons montré dans cet article que l'analyse spectrale du rayonnement électromagnétique des circuits intégrés comportant des PUF à base de cellules oscillantes RO ou TERO est un outil efficace et puissant pour cloner ces PUF. C'est un problème majeur de sécurité pour l'utilisation pratique et industrielle de ces PUF auquel il convient de répondre par des protections dédiées qui sont encore en cours d'étude.

REFERENCES

[1] C. Böhm, M. Hofer. *"Physical Unclonable Functions in Theory and Practice"*. Springer 2013

[2] A. Cherkaoui, L. Bossuet, C. Marchand. "Design, Evaluation and Optimization of Physical Unclonable Functions based on Transient Effect Ring Oscillators", IEEE Trans. on Inf. Forensics and Security, Vol. 11, No. 6, pp. 1291-1305, June 2016.

[3] P. Bayon, L. Bossuet, A. Aubert, V. Fischer. *"EM radiation analysis on true random number generators: Frequency and localization retrieval method"*. IEEE APEMC 2013

[4] P. Bayon. *"Attaques électromagnétique ciblant les générateurs d'aléa"*, thèse de doctorat, Université Jean Monnet, janvier 2014.

[5] D. Merli, D. Schuster, F. Stumpf, and G. Sigl, *"Semi-invasive EM attack on FPGA RO PUFs and countermeasures"*, ACM WESS 2011

[6] U. Mureddu, B. Colombier, N. Bochard, L. Bossuet, V. Fischer. *"Transient Effect Ring Oscillators Leak Too"*. In IEEE ISVLSI 2019.