Proposition d'une nouvelle approche de Strong PUF basée sur une couche mince multidimensionnelle

Benjamin Malthiery (0000-0002-4299-4467), Estelle Wagner (0000-0003-4837-483X), Philippe Elbaz-Vincent (0000-0002-8629-3021), Giacomo Benvenuti (0000-0002-8369-636X)

***Résumé*—Les Physical Unclonable Functions (PUF) constituent un axe de recherche important pour la lutte contre les contrefaçons et la sécurisation des systèmes embarqués. Elles ont le potentiel technique pour servir de méthode d'authentification ou pour générer des clés sans exposer le secret comme le ferait une mémoire non volatile, tout en respectant des exigences sur la consommation et le coût. De nombreuses constructions ont ainsi pu être proposées durant les deux dernières décennies. L'objet est ici de formuler un modèle conceptuel d'une PUF basée sur des couches minces d'oxydes micro-structurées et d'estimer sa capacité de diversification et donc justifier son intérêt dans le panorama de solutions actuelles. Cette étude permet également de contextualiser les contraintes qu'il s'agira de relever lors du passage à une phase d'industrialisation.**

***Mots clés*—Anti-contrefaçon, Couches minces d'oxydes multidimensionnelles, Physical Unclonable Function (PUF), Sécurité**

I. INTRODUCTION

Traditionnellement, la sécurité des solutions anti-contrefaçon est basée sur des éléments graphiques et optiques obtenus à partir de composants ou d'outils de production considérés comme trop difficiles et trop chers à acquérir pour un contrefacteur. Cependant, ils ne permettent pas l'identification de chaque unité et peuvent également nécessiter une phase de vérification impliquant des lecteurs externes coûteux. En complément, des solutions basées sur l'identification par radiofréquence (RFID) ont été développées afin de se conformer aux exigences de la logistique, telles que l'aide au suivi et à la traçabilité des marchandises, mais leurs architectures matérielles les rendent incompatibles avec la gestion des primitives cryptographiques recommandées. Un problème similaire existe sur la plupart des systèmes embarqués où les identifiants et les clés sont simplement stockés dans une mémoire non volatile (NVM) au lieu d'utiliser des éléments sécurisés pour réduire les coûts d'ingénierie et de matériel.

L'idée des Physical Unclonable Functions (PUF) a depuis émergé et gagné en intérêt, en partie pour limiter les attaques sur les puces NVM qui permettent de récupérer des clés secrètes. Elle consiste en une empreinte physique unique et infalsifiable fournissant une identité à un objet. Plus précisément, le concept repose sur les variations aléatoires mineures d'une propriété mesurable que deux instances d'un objet présenteront en raison de l'impossibilité de contrôler le processus de production à un niveau infinitésimal (cf. Fig. 1). Ainsi, une PUF peut être basée sur des éléments faisant déjà partie de la conception, ce qui permet des économies de surface et de consommation par rapport à des solutions coûteuses telles que les éléments sécurisés, tout en offrant une meilleure sécurité que les puces NVM puisque l'identité est extraite des mesures physiques uniquement lorsque l'information est nécessaire. En outre, il devient possible de les utiliser pour l'authentification ou la génération de clés si elles remplissent les propriétés statistiques d'unicité, de reproductibilité et d'imprévisibilité, suggérant ainsi une primitive cryptographique économique et efficace. Elles présentent donc un intérêt particulier dans les domaines de la lutte contre la contrefaçon et de la cybersécurité [1], [2].

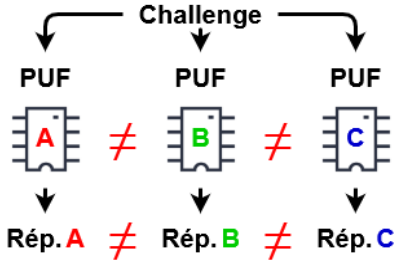

Fig. 1. Notion d'unicité associée à une PUF. Les 3 circuits proviennent d'un même environnement de production mais des variations mineures permettent de les distinguer. En appliquant la même évaluation, ou challenge, on obtient des réponses différentes.

Dans ce qui suit, nous abordons les solutions pratiques existantes (section II) et présentons une solution innovante basée sur une approche physico-chimique (section III).

II. CONTEXTE DES PUF

Les arguments évoqués en introduction ont encouragé

Date de soumission : 20 janvier 2023. L'auteur déclare que les travaux présentés sont en partie financés par le Grenoble Alpes Cybersecurity Institute.
Auteur correspondant : Benjamin Malthiery. Les auteurs ont travaillé conjointement à l'élaboration des travaux et à la relecture du manuscrit.

Benjamin Malthiery est doctorant Cifre chez 3D-Oxides, 41 rue Henri Fabre, F-01630 Saint-Genis-Pouilly, France, et à l'Univ. Grenoble Alpes, CNRS, IF, 38000 Grenoble, France, sous la direction respective du Dr. Giacomo Benvenuti, référent entreprise, et du Pr. Philippe Elbaz-Vincent, directeur de thèse (courriels : benjamin.malthiery@univ-grenoble-alpes.fr et benjamin.malthiery@3d-oxides.com).

Estelle Wagner est ingénieure R&D chez 3D-Oxides, 41 rue Henri Fabre, F-01630 Saint-Genis-Pouilly, France (courriel : estelle.wagner@3d-oxides.com).

Philippe Elbaz-Vincent est Professeur à l'Univ. Grenoble Alpes, CNRS, IF, 38000 Grenoble, France (philippe.elbaz-vincent@math.cnrs.fr).

Giacomo Benvenuti est directeur technique chez 3D-Oxides, 41 rue Henri Fabre, F-01630 Saint-Genis-Pouilly, France (courriel : giacomo.benvenuti@3d-oxides.com).

divers projets, chacun utilisant potentiellement une approche et un formalisme différents, jusqu'à ce qu'il devienne difficile de dresser une liste exhaustive de toutes les constructions et de leurs variantes. De même, il est compliqué de définir des indicateurs de performance tenant compte des critères de sélection hétérogènes (niveau de sécurité, consommation, dimensions physiques et coût). On retrouve donc généralement une catégorisation des PUF en fonction de la propriété physique évaluée pour faciliter les comparaisons. À ce sujet, les lecteurs sont invités à consulter les articles de McGrath *et al.* [3] ainsi que Ning *et al.* [4] qui dressent un panorama des constructions ; ces deux références reflètent la diversité des propositions que l'on peut actuellement trouver dans la littérature.

Dans un premier temps, la distinction repose sur la nature électronique ou non de la PUF. Le premier groupe formé comprend ensuite les sous-catégories de PUF basées sur les délais, les éléments mémoire et l'électronique analogique, tandis que le second groupe comporte notamment les propositions exploitant des propriétés optiques. La Table I fournit une liste succincte de quelques exemples [5]–[13].

TABLE I
EXTRAIT DE LA CLASSIFICATION PARAMETRIQUE PROPOSEE PAR MCGRATH *ET AL.* [3]

Nature	**Concept**	**Paramètres**	**Exemples**
Electro.	Domaine temporel	Délai	Arbiter PUF
		Oscillations	RO PUF
	Eléments mémoire	Etat binaire	SRAM PUF Memristor PUF
	Constantes	Courbes I-V	SHIC PUF
		Capacité	Coating PUF
Autres	Optique	Intensité	Optical PUF
		Fréquence	LCD PUF
	Magnétisme	Intensité	Magnetic PUF

En parallèle de la classification paramétrique, on peut aussi considérer d'autres propriétés du système. La source d'aléa peut être *implicite* si elle est liée au procédé de fabrication ou *explicite* si des étapes supplémentaires sont nécessaires lors de la production. La méthode d'évaluation peut être *intrinsèque* si la propriété évaluée est lue directement par le système ou *extrinsèque* si cette étape requiert un lecteur externe. Enfin, la terminologie regroupe sous le terme *Weak PUF* les constructions ne disposant que d'un faible nombre d'évaluations distinctes, et sous le terme *Strong PUF* les constructions pour lesquelles le dénombrement d'évaluations est exponentiel par rapport aux dimensions physiques de la PUF.

En plus de ces classifications qualitatives, il s'agit de proposer des outils de comparaison agnostiques. La communauté a donc établi au fil des ans un jeu de valeurs statistiques [14] pour comparer l'unicité, la reproductibilité et l'imprévisibilité des constructions proposées. Il faut toutefois noter que le niveau de sécurité d'une construction dépend également de la qualité de son intégration et que cela peut avoir un impact lors de l'élaboration des critères de sélection. Ainsi, chaque argument en faveur d'une solution doit être vérifié dans le contexte de l'application finale.

III. UN NOUVEAU MODELE DE PUF OPTIQUE

A. Description

Malgré l'intérêt porté aux PUF électroniques, on note que les PUF optiques ont attiré une attention particulière depuis les travaux de Pappu *et al.* [11] en 2002 en raison de la complexité des phénomènes physiques observés. La forte densité volumétrique d'information et le caractère stochastique du processus de production tendent à suggérer une solution plus sûre que les PUF basées sur des éléments mémoire pour lesquelles Helfmeier *et al.* [15] ont par exemple pu reproduire une PUF de type SRAM (Static Random Access Memory). Les propriétés optiques sont censées complexifier l'obtention d'une simulation mathématique ou d'un clone physique. Cependant, elles souffrent de plusieurs limites comme la capacité à être intégrées et miniaturisées sur un dispositif [16]. Notre objectif est donc double puisqu'il consiste à exploiter la complexité des phénomènes optiques observés sur les couches minces comme source d'aléa tout en proposant un système compatible avec les exigences de miniaturisation et d'intégration.

Dans notre cas, on considère une nouvelle PUF optique basée sur des couches minces d'oxydes micro-structurées. Les matériaux multifonctionnels qui les constituent sont équivalents à une matrice multidimensionnelle/multi-valeurs. C'est l'un de ses principaux avantages par rapport aux solutions concurrentes : la non-linéarité des réponses renforce l'imprédictibilité tandis que le nombre important d'évaluations distinctes empêche une recopie par énumération exhaustive.

Dans la pratique, ce modèle de PUF consiste en une couche mince d'oxydes complexes positionnée entre un module OLED qui l'illumine et un capteur d'image CMOS qui quantifie l'intensité lumineuse transmise (cf. Fig. 2).

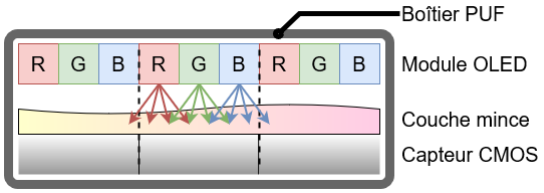

Fig. 2. Représentation schématique de la PUF proposée. Les réponses sont formées à partir de l'intensité transmise en différents points de la couche mince.

B. Capacité de diversification théorique

Afin d'estimer ce paramètre, on propose la notation suivante pour les dimensions du système :

- N représente le nombre de points de mesure ; la précision de l'ordre du micron (10^{-4} cm) sur le plan formé par la couche mince permet alors en théorie d'atteindre $(10^4)^2 = 10^8$ points par cm².
- L représente le nombre de valeurs disponibles sur un point de mesure et dépend de la profondeur de bits du capteur, ou autrement dit du pas de quantification du convertisseur Analogique-Numérique. Le capteur CMOS utilisé dispose d'une profondeur de 10 bits qui équivaut à environ 10^3 valeurs par point de mesure.

- Z représente le nombre de stimuli possibles par point de mesure. Les propriétés des couches minces varient en fonction de la longueur d'onde donc en fonction du spectre d'émission du module OLED. Pour un affichage RGB 8-bits, on estime Z de l'ordre de $(10^2)^3$.

La borne supérieure de la capacité de diversification du système atteint dans ce contexte $2^{10\wedge15}$ combinaisons par cm².

$$L^{Z*N} = 10^{3^{10^6*10^8}} \approx 2^{10^{15}}$$

Cela représente par exemple l'équivalent d'une mémoire de 125 To. Un attaquant doit ainsi gérer un espace de stockage non négligeable pour chaque PUF produite que l'on peut combiner à une limitation de la vitesse d'interrogation [17] ; il s'agira donc plutôt d'estimer la robustesse du système face à des solutions d'apprentissage machine qui stockent un modèle capable de prédire les réponses attendues.

IV. Conclusion

Bien que l'approche conceptuelle justifie l'étude de la PUF proposée, il reste pour le moment difficile de transposer cela à un modèle en raison de la complexité du système. Des séries d'acquisitions ont déjà permis d'analyser les performances statistiques selon différents niveaux de post-traitement mais cela ne suffit pas encore pour conclure quant à son niveau de sécurité.

Remerciements

Ce travail est rendu possible par le dispositif CIFRE établi entre l'entreprise 3D-Oxides et l'Institut Fourier de l'Université Grenoble Alpes. Le doctorant remercie les deux équipes qui l'encadrent dans ses recherches, en particulier le Dr. Giacomo Benvenuti, référent entreprise, et le Pr. Philippe Elbaz-Vincent, directeur de thèse.

Bibliographie

[1] "Panorama de la menace informatique 2021 – CERT-FR." https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-002/ (accessed Mar. 15, 2022).

[2] "Counterfeit and pirated goods get boost from pandemic, new report confirms," *Europol*. https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-and-pirated-goods-get-boost-pandemic-new-report-confirms (accessed Mar. 15, 2022).

[3] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, p. 011303, Mar. 2019, doi: 10.1063/1.5079407.

[4] H. Ning, F. Farha, A. Ullah, and L.-F. Mao, "Physical Unclonable Function: Architectures, Applications and Challenges for Dependable Security," *IET Circuits, Devices & Systems*, vol. 14, Feb. 2020, doi: 10.1049/iet-cds.2019.0175.

[5] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, Jun. 2004, pp. 176–179. doi: 10.1109/VLSIC.2004.1346548.

[6] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon Physical Random Functions," p. 13.

[7] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, Berlin, Heidelberg, 2007, pp. 63–80. doi: 10.1007/978-3-540-74735-2_5.

[8] P. Koeberl, Ü. Kocabaş, and A.-R. Sadeghi, "Memristor PUFs: A new generation of memory-based Physically Unclonable Functions," in *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 2013, pp. 428–431. doi: 10.7873/DATE.2013.096.

[9] U. Rührmair, C. Jaeger, C. Hilgers, M. Algasinger, G. Csaba, and M. Stutzmann, "Security Applications of Diodes with Unique Current-Voltage Characteristics," in *Financial Cryptography and Data Security*, Berlin, Heidelberg, 2010, pp. 328–335. doi: 10.1007/978-3-642-14577-3_26.

[10] P. Tuyls, G.-J. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-Proof Hardware from Protective Coatings," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, Berlin, Heidelberg, 2006, pp. 369–383. doi: 10.1007/11894063_29.

[11] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002, doi: 10.1126/science.1074376.

[12] G. Lenzini *et al.*, "Security in the shell: An optical physical unclonable function made of shells of cholesteric liquid crystals," in *2017 IEEE Workshop on Information Forensics and Security (WIFS)*, Dec. 2017, pp. 1–6. doi: 10.1109/WIFS.2017.8267644.

[13] R. S. Indeck and M. W. Muller, "Method and apparatus for fingerprinting magnetic media," US5365586A, Nov. 15, 1994 Accessed: Nov. 17, 2022. [Online]. Available: https://patents.google.com/patent/US5365586A/en

[14] A. Maiti, V. Gunreddy, and P. Schaumont, "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions," in *Embedded Systems Design with FPGAs*, P. Athanas, D. Pnevmatikatos, and N. Sklavos, Eds. New York, NY: Springer, 2013, pp. 245–267. doi: 10.1007/978-1-4614-1362-2_11.

[15] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, "Cloning Physically Unclonable Functions," in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Jun. 2013, pp. 1–6. doi: 10.1109/HST.2013.6581556.

[16] U. Rührmair *et al.*, "Optical PUFs Reloaded," 215, 2013. Accessed: Mar. 10, 2022. [Online]. Available: https://eprint.iacr.org/2013/215

[17] U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, and G. Csaba, "Applications of High-Capacity Crossbar Memories in Cryptography," *IEEE Transactions on Nanotechnology*, vol. 10, no. 3, pp. 489–498, May 2011, doi: 10.1109/TNANO.2010.2049367.