**Avis de Soutenance**

Monsieur Paul JIMENEZ

Soutiendra publiquement ses travaux de thèse intitulés

*Sécurité augmentée par la photonique via des fonctions physiques non clonables*

dirigés par Monsieur Xavier LETARTRE

Soutenance prévue le ***lundi 29 septembre 2025*** à 10h00
Lieu :   Ecole Centrale de Lyon 36 Avenue Guy de Collongue, Bâtiment W1, 69130 Écully
Salle : Amphithéâtre 203

**Composition du jury proposé**

|  |  |  |
| --- | --- | --- |
| M. Xavier LETARTRE  | Ecole Centrale de Lyon  | Directeur de thèse  |
| M. Jean-Pierre SEIFERT  | Technische Universität Berlin  | Rapporteur  |
| Mme Delphine MARRIS-MORINI  | Université Paris-Saclay  | Rapporteure  |
| M. Lilian BOSSUET  | Université Jean-Monnet  | Examinateur  |
| Mme Elena-Ioana VATAJELU  | Laboratoire TIMA, Techniques of Informatics and Microelectronics for integrated systems Architecture, CNRS  | Examinatrice  |
| M. Fabio PAVANELLO  | Laboratoire CROMA, Centre de Radiofréquences, Optique et Micro-nanoélectronique des Alpes, CNRS  | Co-encadrant de thèse  |
| M. Cédric MARCHAND  | Ecole Centrale de Lyon  | Co-encadrant de thèse  |
| **Mots-clés :**  | Photonique,Securité,Fonction physique non clonable,, |

|  |
| --- |
| **Résumé :**   |
| Dans un contexte où la multiplication des objets connectés est de plus en plus importante et où la protection des données est critique, certaines nouvelles technologies et certains outils peuvent être utilisés afin de compromettent la sécurité des dispositifs matériels. Pour lutter contre les attaques sur les dispositifs, les fonctions physiques non-clonables (Physical Unclonable Functions, PUFs) constituent une solution prometteuse. Cette classe de primitive de sécurité tire profit des variations des procédés de fabrication pour créer des circuits uniques. Lorsque soumis à certains stimuli, ils génèrent une ou plusieurs réponses qui peuvent être utilisées dans des protocoles d’authentification ou pour générer des clés cryptographiques uniques. Sachant que les variations de fabrications sont imprédictibles et aléatoires, les PUFs peuvent servir d’empreintes digitales idéalement non-clonable. On retrouve à la genèse des PUFs un système optique utilisant un laser et un échantillon comportant des centres de diffusion diélectriques, ce système n’étant pas intégrable dans nos appareils, on a vu l’émergence de PUFs électroniques facilement intégrables. Cependant, beaucoup d’entre eux ont montré leurs limites, on a alors vu l’émergence de nouveaux PUFs photoniques, s’appuyant sur le développement des technologies en photonique intégrée ces dernières années et sur les nombreux degrés de liberté que l’utilisation de la lumière apporte. Comme évoqué, les PUFs ayant étés principalement électroniques, on s’est beaucoup concentré sur les réponses binaires de PUFs dont on essaie de quantifier les propriétés aléatoires dans le domaine binaire. Dans cette thèse, nous nous sommes intéressés à la manière dont nous pouvons quantifier les propriétés aléatoires des réponses de PUFs ou des générateurs de nombre aléatoires opérant dans le domaine analogique, comme ce peut être le cas avec les PUFs photoniques. Nous nous sommes alors penchés sur trois métriques l’approximate entropy (ApEn), la fuzzy entropy (FuzEn) et la disentropie de l’autocorrélation. Nous avons voulu comparer cette dernière à l’ApEn utilisée en sécurité et la FuzEn étant une version améliorée de l’ApEn. Nous avons alors vu que la disentropie de l’autocorrélation pouvait détecter des patterns discrets présents dans une séquence analogique. Cette dernière pouvant être une réponse de générateur de nombre aléatoire ou de PUF opérant dans le domaine analogique. Nous avons cependant noté certaines de ses limites. Il existe de multiples similarités entre le premier PUF optique fonctionnant avec un laser et des centres de diffusion diélectriques et les systèmes de résonateurs en anneau photoniques fonctionnant dans le domaine temporel. En nous appuyant sur la littérature, nous avons voulu tout d’abord travailler sur des systèmes composés de résonateurs en anneau. Nous avons alors fait fabriquer ces structures sur une plateforme SiN, nous permettant de quantifier les tolérances de fabrication de la plateforme et l’impact des tolérances de fabrication sur les structures. Les mesures ont été effectuées dans le domaine spectral et ont permis de montrer qu’il était possible de fabriquer des circuits uniques. Cette unicité a été vérifiée même lorsque les circuits sont placés les uns à côté des autres, là où les corrélations devraient être les plus grandes. Nous avons également montré qu’en utilisant des algorithmes appropriés, ces signatures spectrales sont robustes aux changements de température. Grâce à ces résultats, nous avons effectué des premières simulations en utilisant la TCMT des les propriétés temporelles de ces structures lorsqu’on les soumet à de la lumière modulée comme challenge et obtenu des résultats encourageants. Enfin, cette thèse s’ouvre sur une humble réflexion autour de diverses questions et conséquences sociales, éthiques ou philosophiques des technologies d’identification hardware comme les PUFs.  |
|   |