PHotonic Augmented SEcurity via Physical Unclonable Functions

PHASEPUF

anr agence nationale de la recherche

Appel : AAPG CE 39

Année : 2020

Instrument : JCJC

Contact : fabio.pavanello@ec-lyon.fr

COORDINATEUR : Fabio Pavanello

PARTENAIRES : CNRS (INL)

Le projet PHASEPUF vise à développer une nouvelle classe de couches de sécurité via des fonctions physiques non clonables photoniques, exploitant les plateformes compatibles CMOS, et à démontrer leurs avantages en robustesse, fiabilité, consommation d'énergie et compacité par rapport aux approches électroniques PUFs

CONTEXTE ET OBJECTIFS

Récemment, des préoccupations majeures en matière de sécurité sont apparues en raison des avancées technologiques dans les techniques de rétro-ingénierie et de cyber-attaque portant atteinte à l'intégrité du matériel et à la sécurité des informations.

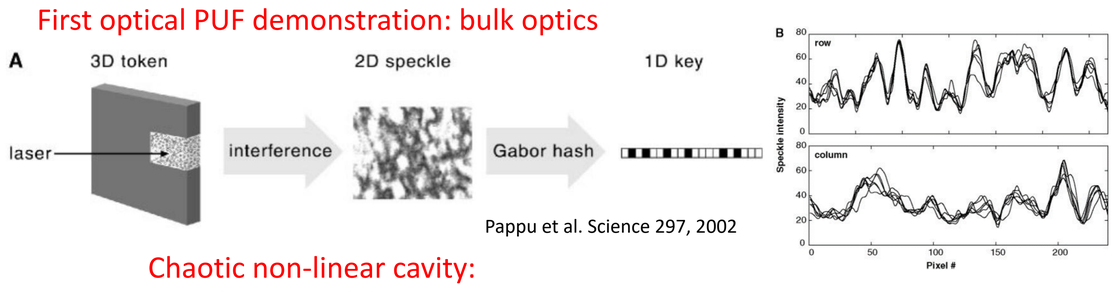
Les fonctions physiques non clonables sont des solutions permettant d'identifier du matériel (puce) contrefait ou de générer des clés cryptographiques, en évitant le stockage local dans la mémoire, grâce à leurs réponses complexes et imprévisibles.

L'objectif principal du projet PHASEPUF consiste à développer une nouvelle classe de primitives de sécurité basées sur des PUFs photoniques dans des plateformes compatibles CMOS. Les réponses des architectures PUF développées seront fortement affectées par les tolérances de fabrication de ces plateformes, contribuant à leur caractère aléatoire.

En particulier, le projet PHASEPUF contribuera à :

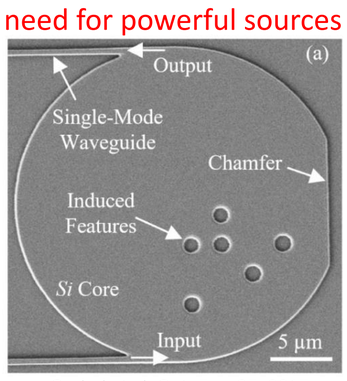
1. de nouvelles architectures PUF photoniques offrant un haut niveau de sécurité contre l'apprentissage automatique et les attaques par canal latéral
2. la réduction ou l'absence totale d'unités de correction d'erreurs pour le fonctionnement des PUF
3. un niveau plus élevé d'intégration sur puce des blocs de construction fondamentaux des PUF photoniques

First optical PUF demonstration: bulk optics

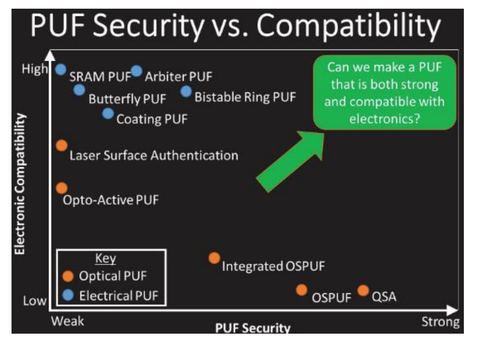


Pappu et al. Science 297, 2002

Chaotic non-linear cavity: need for powerful sources



Grubel et al. Opt. Exp. 25, 2017



Pavanello et al. ETS2021

MÉTHODOLOGIE ET RÉSULTATS

Le développement de PUFs photoniques sera basé sur les étapes suivantes :

1. conception et exploration de diverses architectures photoniques pour des PUF faibles et fortes au moyen de simulations au niveau des circuits- fabrication des architectures optimales en utilisant des fonderies compatibles CMOS
2. caractérisation des architectures à l'aide d'un banc d'essai électro-optique où différents scénarios seront envisagés pour évaluer leurs performances en cas de fluctuations, de vieillissement et d'attaques électriques
3. analyse des résultats expérimentaux et comparaison avec les simulations.

Couramment, des prototypes en SOI basés sur des architectures à réseau de résonateur à anneau sont en cours de fabrication. Un setup expérimentale à haute fréquence électro-optique est en cours de développement pour le testing des PUFs.

TECHNOLOGIES

Les technologies qui seront utilisées pour les différentes étapes sont :

1. des outils de simulation tels que lumerical interconnect et lumerical device pour simuler les différentes architectures qui sont proposées dans le projet PHASEPUF. Le traitement Python/matlab des résultats sera utilisé en conjonction avec les tests statistiques du NIST et la modélisation ML des résultats ainsi que d'autres métriques communes (fractional/weighted Hamming distance)
2. plates-formes compatibles CMOS, telles que la plate-forme photonique en silicium du CEA-LETI pour la fabrication, qui comporte une couche de dispositif de 300 nm d'épaisseur et plusieurs éléments
3. un banc d'essai électro-optique pour la caractérisation des puces photoniques, y compris le couplage optique (vertical) par le biais d'interfaces de coupleur de réseau et de sondes/emballages électriques sur la plaquette pour connecter la puce à la commande FPGA.
4. des serveurs haute performance seront utilisés pour l'analyse et la modélisation des données expérimentales

Pour évaluer la robustesse des PUFs photoniques, différents outils seront exploités :

1. un mandrin à température contrôlée permettant de modifier la température de l'échantillon pour émuler les fluctuations
2. injection de défauts électriques dans le système à l'aide d'un FPGA
3. des sondes RF en champ proche pour les attaques électriques
4. des sondes RF (on-wafer) pilotées par un générateur de formes d'onde arbitraires pour les tests au niveau du dispositif

cnrs inl ÉCOLE CENTRALELYON