Avis de Soutenance

Monsieur Lucas RHETAT

Electronique, Micro et Nanoélectronique, optique et laser

Soutiendra publiquement ses travaux de thèse intitulés
nvSRAM Ferroélectriques pour la Sécurité Matérielle : Fiabilité, Flexibilité et Applications aux Fonctions Physiques Inclonables
Travaux dirigés par Monsieur Ian O'CONNOR

Soutenance prévue le ***lundi 30 novembre 2026*** à 14h00
Lieu : INP Phelma 3 Parv. Louis Néel, 38000 Grenoble
Salle : Amphithéâtre Z108

Composition du jury proposé

M. Ian O'CONNOR	Full professor	Ecole Centrale de Lyon	Directeur de thèse
Mme Ioana VATAJELU	Chargée de recherche HDR	TIMA	Rapporteure
M. Arnaud VIRAZEL	Maître de conférences	LIRMM	Rapporteur
M. Antoine FRAPPE	Professeur	JUNIA	Examinateur
M. Bastien GIRAUD	CEA Grenoble	Invité	
M. Jean-Philippe NOEL	CEA Grenoble	Invité	

Mots-clés : FeRAM, nvSRAM, Mémoire, Fonctions Physiques Inclonables (PUF), Sécurité matérielle, Ferroélectricité

Résumé :

Depuis la fin du XXème siècle, la numérisation croissante des activités humaines a progressivement fait de la donnée une ressource stratégique, indispensable au fonctionnement d'un nombre toujours plus important d'applications. En parallèle, les systèmes électroniques sont de plus en plus frugaux et intégrés à de très nombreux niveaux de la société. De nombreux efforts de recherche sont ainsi nécessaires pour concevoir des composants matériels capables d'assurer simultanément efficience, robustesse et sécurité. Dans ce contexte, les dispositifs ferroélectriques, offrant une combinaison rare de non-volatilité, faible consommation énergétique et compatibilité CMOS, apparaissent comme des candidats particulièrement prometteurs. Cette thèse étudie l'exploitation des propriétés physiques de ces dispositifs ferroélectriques pour la conception de nouveaux mécanismes de sécurité matérielle. Nous y adressons deux problématiques techniques particulièrement importantes : (i) la sécurité des données et (ii) l'authenticité matérielle. Concernant le premier point, nous explorons les mémoires hybrides nvSRAM ferroélectriques, co-intégrant finement une mémoire SRAM, performante mais volatile, et des capacités ferroélectriques (FeCAP), assurant la persistance des données. Cette forte proximité permet d'effectuer des transferts très efficaces entre mémoire volatile et mémoire non volatile et de limiter les échanges de données inter-composants, en particulier dans le cadre de systèmes intermittents frugaux et/ou critiques. Nous proposons une amélioration de la fiabilité de ces circuits, élargissant leurs applications par rapport à l'état de l'art. Concernant le second point, nous explorons dans quelle mesure ces mêmes circuits peuvent servir à implémenter des fonctions physiques inclonables (PUF) dont la fiabilité est intrinsèquement assurée au niveau matériel grâce à l'interaction FeCAP-SRAM, simplifiant ainsi leur caractérisation, leur intégration et réduisant leur surface d'attaque.

Summary:

Since the end of the 20th century, the increasing digitization of human activities has gradually turned data into a strategic resource, essential to the operation of an ever-growing number of applications. At the same time, electronic systems are becoming increasingly energy-efficient and integrated into numerous aspects of society. Consequently, significant research efforts are needed to design hardware components capable of simultaneously ensuring efficiency, robustness, and security. In this context, ferroelectric devices, which offer a rare combination of non-volatility, low power consumption, and CMOS compatibility, appear to be particularly promising candidates. This thesis investigates the use of the physical properties of these ferroelectric devices to design new hardware security mechanisms. We address two particularly important technical issues: (i) data security and (ii) hardware authenticity. Regarding the first point, we explore ferroelectric nvSRAM hybrid memories, which finely integrate high-performance but volatile SRAM with ferroelectric capacitors (FeCAP), ensuring data persistence. This close proximity enables highly efficient transfers between volatile and non-volatile memory and limits data exchanges between components, particularly in the context of frugal and/or critical intermittent systems. We propose an improvement in the reliability of these circuits, broadening their applications beyond the state of the art. Regarding the second point, we explore the capabilities of these same circuits to be used as implementation of unclonable physical functions (PUFs) whose reliability is intrinsically guaranteed at the hardware level thanks to the FeCAP-SRAM interaction, thereby simplifying their characterization and integration and reducing their attack surface.