Équipe de recherche commune CEA/EMSE.

Soutenance de thèse de Mounia KHARBOUCHE-HARRARI, CMP

"Hybridation CMOS/STT-MRAM des circuits intégrés pour la sécurité matérielle de l'Internet des Objets".

Lundi 9 décembre à 13h30, en amphithéâtre HS02

Campus Georges Charpak Provence – 880 route de Mimet, Gardanne.

Le jury sera composé de :

- Bruno Rouzeyre Professeur des Universités, LIRMM Président
- Jacques-Olivier Klein Professeur des Universités, Paris Sud Rapporteur
- Lorena Anghel Professeur à l'INP, Grenoble Rapporteure
- Jean-Luc Danger Directeur d'études, Telecom ParisTech Examinateur
- Jean-Michel Portal Professeur des Universités, IM2NP Directeur de thèse
- Gregory Di Pendina Ingénieur de recherche CNRS, Spintec Encadrant
- Romain Wacquez Ingénieur-chercheur, CEA-Tech Encadrant
- Jérémy Postel-Pellerin Maître de conférences, IM2NP Encadrant
- Driss Aboulkassimi Ingénieur-chercheur, CEA-Tech Encadrant

Résumé

Cette dernière décennie a été le théâtre du développement rapide de l'Internet des Objets. Cette expansion s'accompagne du renforcement des besoins et contraintes des circuits intégrés : une consommation faible et une surface silicium maîtrisée. Toutefois, cet engouement récent pour les objets connectés pousse souvent les fabricants à précipiter la mise sur le marché de leurs produits, parfois au détriment de la sécurité.

Dans le cadre des travaux entrepris lors de cette thèse, nous nous sommes particulièrement intéressés aux atouts et inconvénients que peut apporter l'hybridation de la technologie CMOS avec la technologie mémoire non-volatile émergente STT-MRAM. Ces architectures innovantes doivent permettre le développement d'applications faible consommation visant la sécurité des objets connectés. Pour cela, la conception d'un algorithme de cryptographie légère hybride CMOS/STT-MRAM basé sur le chiffrement PRESENT a été réalisée.

Ainsi, la première étude menée a consisté à étudier la robustesse de jonctions mémoires STT-MRAMs unitaires face aux attaques physiques de type perturbation, avant leur intégration dans le chiffrement. Pour ce faire, des injections de fautes Laser ont été effectuées afin d'évaluer l'intégrité des données stockées.

Suite aux observations des expérimentations réalisées sur ces mémoires de type STT-MRAM perpendiculaires, un nouveau capteur d'attaques physiques basé sur cette technologie mémoire a été proposé, le DDHP. Ce détecteur permet la détection simultanée d'attaques photoélectriques et d'attaques thermiques qui peuvent viser les circuits intégrés.

Abstract

In the last decade, the Internet of Things deployment highlighted new needs and constraints in terms of consumption and area for integrated circuits. However, the recent craze for connected objects and due to the extremely pressing time-to-market demand, the manufacturers commercialize their products, sometimes at the expense of their security.

The main focus of the work undertook during this thesis consists in the hybridization of the CMOS technology with the emerging non-volatile memory technology STT-MRAM. This study aims to determine the assets and drawbacks of this hybridization. These innovating architectures must allow the development of low power applications and support the growth of secured connected objects. Thus, the design of a hybrid CMOS/STT-MRAM lightweight cryptographic algorithm based on the PRESENT cipher is realised.

This is how the first study carried out consisted in investigating the robustness of STT-MRAM junctions facing physical attacks, before their integration in the cryptographic algorithm. To do this, laser fault injections were performed in order to evaluate the integrity of the sensitive data stored in the cells.

Following the experiments carried out on perpendicular STT-MRAM memories, a new physical attack detector based on this memory technology is proposed, designated by DDHP. This sensor allows simultaneous detection of photoelectrical and thermal attacks that can target integrated circuits.

Mounia KHARBOUCHE-HARRARI, CMP