

AVIS DE SOUTENANCE DE THESE DE DOCTORAT

Le **15-12-2017**
A **10:00** Amphi Amphi
Mines Saint-Étienne
880 Route de Mimet
13541 Gardanne

Soutiendra en vue de l'obtention du titre de Docteur de l'Ecole Nationale Supérieure des Mines de Saint-Etienne dans la spécialité : MICROELECTRONIQUE

David

EL-BAZE

Une thèse ayant pour sujet :

Conception et Évaluation d'un Détecteur Numérique d'Attaque par Injection de Fautes.

MEMBRES DU JURY :

Président

(Le président est désigné le jour de la soutenance)

Rapporteurs :

| | | | |
|----------|---------|------------|-------------------|
| Sicard | Etienne | Professeur | INSA Toulouse GEI |
| Leveugle | Régis | Professeur | Grenoble INP TIMA |

Examineurs :

| | | | |
|-----------|---------------|---------------------------|---------------------------|
| Rigaud | Jean-Baptiste | Maître assistant | Mines Saint-Étienne |
| Maurine | Philippe | Maître de Conférence | Université de Montpellier |
| Laurencin | Christophe | Head of Hardware security | STMicroelectronics |
| Renaudin | Marc | Professeur | Laboratoire TIMA |

Thèse préparée dans le centre CMP-GC à l'Ecole Nationale Supérieure des Mines de Saint-Etienne.

Travail co-encadré par : MAURINE Philippe
RIGAUD Jean-Baptiste

Destinataires : DRI, Accueil, SCIDEM, Centre,
D.CORTIAL « Le Progrès », 24 rue de la robotique – 42000 Saint-Etienne

Résumé :

Les circuits intégrés et les systèmes qui les utilisent sont sujets à diverses menaces, parmi lesquelles les attaques par injection de fautes. Cette dernière est une technique permettant la modification des données manipulées ou stockées par un circuit dans le but de le corrompre ou de permettre l'accès à des informations sensibles.

Les travaux réalisés au cours de cette thèse ont pour objectif de construire un capteur intégré pour la détection de tentatives d'injection de fautes pouvant être menées avec des Perturbations Electro-Magnétiques (PEM). Idéalement, la solution doit avoir une faible empreinte matérielle et son intégration doit être compatible avec le flot de conception de circuits utilisés dans l'industrie.

Un capteur numérique, c'est à dire qui n'exploite pas directement les variations de certains paramètres physiques comme les fluctuations des temps de propagations, est conçu et caractérisé. Il exploite la grande susceptibilité des bascules D aux PEM, comme souligné dans l'état de l'Art. Lors des différents tests réalisés, le capteur a montré qu'il est également sensible aux attaques par injection de fautes conduites avec d'autres moyens de perturbation que les PEM.

Le capteur développé donne de très bons résultats face aux injections de fautes par PEM et par perturbation de la polarisation de substrat, et des résultats plus mitigés face aux attaques par illuminations et par perturbation d'alimentation.

Ces résultats peuvent laisser penser qu'il existe des facteurs communs à ces attaques et laissent entrevoir la possibilité de créer un capteur généraliste d'attaques par injections de fautes.

David El-Baze

Le jury sera composé de :

| | | |
|----------------------|--------------------|--------------------|
| Etienne SICARD | INSA Toulouse | Rapporteur |
| Régis LEVEUGLE | Grenoble INP | Rapporteur |
| Marc RENAUDIN | Tiempo | Examineur |
| Christophe LAURENCIN | STMicroelectronics | Invité |
| Philippe MAURINE | LIRMM | Directeur de Thèse |
| Jean-Baptiste RIGAUD | EMSE | Encadrant |