UMR 6164
INSTITUT D'ELECTRONIQUE ET DE TELECOMMUNICATIONS DE RENNES
Département Microélectronique et Microcapteurs

Analyse et optimisation de l'injection de fautes par laser impulsionnel dans des composants MOSFET et études de sureté de fonctionnement

Contexte

Dans le cadre du CPER CYBER SSI (Sécurité des Systèmes d'Information), le Département Microélectronique et Microcapteurs de l'Institut d'Electronique et de Télécommunications de Rennes (IETR – UMR CNRS 6164) développe actuellement une plateforme de « Simulation de la détection de défaillances des systèmes physiques face aux attaques de sécurité » (plateforme CYBER-ELEC). Cette plateforme permettra d'étudier la défaillance des systèmes matériels sécurisés par injection de faute par irradiation laser, sur des mécanismes aussi divers que les sauts d'instruction, les altérations d'instructions, les modifications d'instructions, des inductions d'instructions ByPass, ou encore des mises en place de corruption de droits (mode ADMIN indu), ou encore en récupérant des clefs cryptographiques par attaque passive (écoutes sous laser).
L'étude de fautes simulées par l'injection laser est associée à la vulnérabilité de circuits ou systèmes électroniques sécurisés. Une attaque simulée par injection de faute a pour effet de perturber le fonctionnement d'un composant et/ou le contenu de la mémoire. Une fois l'attaque détectée, de nombreuses solutions existent selon les applications pour soit bloquer le composant/circuit, soit interdire l'accès à des données sensibles, soit réinitialiser le composant/circuit [Sarafianos 2013].

Projet

Le projet de thèse est associé à l'étude de l'injection de faute simulée par laser pulsé nanoseconde sur des transistors à effet de champ à grille isolée par un oxyde (*MOSFETs - Metal Oxide Semiconductor Field Effect Transistors*) qui pourront être élaborés et caractérisés au sein de l'IETR. Ces composants électroniques constituent les unités de bases de circuits mémoires et logiques. L'injection laser est responsable de la génération de porteurs (paires électrons/trous) susceptible de générer un transitoire de photo-courant dans les composants/circuits responsable du dysfonctionnement. Dans ce cas, le laser doit posséder des caractéristiques adaptées en termes de durée du pulse, longueur d'onde, énergie sur cible, taille du faisceau, et moment (synchronisation) d'injection des charges. Des preuves de concepts seront recherchées sur des architectures d'échantillons typiques élaborées directement à l'IETR.
Si l'origine physique de la faute par laser est assez bien connue, sa mise en œuvre, son analyse pour une attaque optimisée restent à ce jour un domaine d'étude à part entière dans le domaine de l'ingénierie du test de vulnérabilité (sureté de fonctionnement) et du vieillissement des dispositifs électroniques sécurisés. Les analyses proposées dans le projet de thèse se feront en fonction des caractéristiques du faisceau laser (durée du pulse, longueur d'onde, énergie reçue, taille du faisceau…). La mesure de transitoires de courant électrique en régime statique (*Single Event Upset*) ou dynamique (*Single Event Transient*) [Dutertre 2018] permettra l'analyse de scénario de fautes intentionnelles. Parallèlement, des études par simulation et modélisation de l'attaque sont aussi envisagées et seront confrontées aux mesures expérimentales réalisées sur les transistors *MOSFET*s en condition de fonctionnement.
L'objectif principal du projet de thèse est d'optimiser l'injection de faute par laser [Dutertre 2018] sur les circuits *MOSFET* typiques (détection et analyse), en vue d'améliorer la calibration pour les campagnes de tests et d'évaluation de la vulnérabilité des circuits électroniques sécurisés.
Des études de défaillance sous environnements sévères (exposition à des champs de température, …) pourront être menées. Des comparaisons entre une attaque par laser pulsé (*LFI : Laser Fault Injection*) et d'autres techniques (*EMFI : Electromagnetic Fault Injection*, attaque en charge (kV/ns), …) pourront être envisagées.

UNIVERSITÉ DE RENNES 1
CAMPUS DE BEAULIEU
(case 1103)
263 AV. DU GÉNÉRAL LECLERC
CS 74205
35042 RENNES CEDEX

TÉL. 33 (0)2 23 23 60 69
FAX 33 (0)2 23 23 56 57

...@univ-rennes1.fr

www.ietr.org

Références succinctes
[Dutertre 2018] J.M. Dutertre, *et al.*, IEEE Transactions on Device and Materials Reliability, 19(1), 6-15, 2018
[Sarafianos 2013] A. Sarafianos, *et al.*, IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), pp. 149-154, 2013

Lieu : Institut d'Electronique et de Télécommunications de Rennes, Campus de Beaulieu, 263 avenue du général Leclerc, 35042 Rennes

Financement : DGA (Pôle d'Excellence en Cybersécurité)

Profil souhaité

Le candidat devra posséder des connaissances en technologies microélectroniques et/ou en architectures de circuits électroniques intégrés, (mémoires, microprocesseurs...).
Des compétences en semi-conducteurs, optique, électronique et/ou une expérience en salle blanche/laboratoire de synthèse de matériaux seront aussi appréciées.
L'IETR faisant partie d'un périmétre ZRR, le candidat fera l'objet d'un agréement administratif d'accés par le Fonctionnaire de Défense et de Sécurité.

Modalités de candidature

Le dossier de candidature devra comprendre impérativement un CV détaillé, une lettre de motivation, et les relevés de notes de L3, M1 et M2, ainsi qu'un résumé succinct de votre projet scientifique de M2.
Une lettre de recommandation pourra le cas échéant être jointe au dossier.
L'ensemble des documents devra être adressé aux personnes mentionnées ci-dessous :

Laurent PICHON (lpichon@univ-rennes1.fr, tel : +332 23 23 56 65)
Philippe BABILOTTE (philippe.babilotte@univ-rennes1.fr, tel : +332 23 23 65 85)