Apport de la modélisation multi-physiques aux problématiques de sécurité des circuits intégrés face aux agressions laser

Thèse à l'École des Mines de Saint-Etienne (France)

Septembre ou octobre 2019

Key-words : Injection de fautes, laser, modélisation multi-physique, simulation analogique, sécurité des circuits intégrés.

Contexte : La sécurité des puces électroniques consiste à garantir l'intégrité des composants électroniques et le secret des données qu'elles contiennent (telles que des clefs de cryptographie, des logiciels, des blocs de propriété intellectuelle, des données en mémoires, etc.) vis-à-vis de manipulations frauduleuses appelées *attaques*. L'objectif de ce travail de thèse est de contribuer à la conception de protections (contre-mesures), d'en évaluer l'efficacité et de les intégrer dans les flots de conception des circuits intégrés.
L'agression par fautes laser est une technique dont la problématique physique est très proche de celle des évènements singuliers (SEE) induits par les particules dans les environnements radiatifs naturels [1, 2]. Dans le cas des radiations, les particules génèrent des paires électron-trou le long de leur parcours dans le semi-conducteur. Les mécanismes de transport et de collections de charges induisent l'apparition de courants transitoires qui perturbent électriquement l'état de certaines portes logiques du circuit considéré. Dans les mécanismes d'interaction laser- matière, l'interaction prédominante à l'origine de l'apparition de paires électron-trou est l'effet photoélectrique. Les autres interactions, comme l'effet Compton, ne sont significatives que lorsque les photons ont des énergies supérieures à 105 eV.
Une plateforme de simulation multi-physique des effets singuliers induits par les environnements radiatifs naturels, MUSCA SEP3 [3, 4], est développée au Département Physique Instrumentation Environnement Espace (DPHY) de l'ONERA depuis 2007. Les domaines d'applications concernent l'estimation des risques opérationnels, l'anticipation des risques pour les futures technologies et le durcissement par design dont le périmètre est comparable à celui relatif aux contre-mesures. La brique physique relative aux processus d'interaction dans le silicium concerne principalement les particules de types neutron, protons, ions etc. Cependant, dans le cadre du projet ANR LIESSE, un module laser a été développé et utilisé dans le cadre de comparaison d'injection laser sur des structures simples (diodes, transistors).

Sujet de thèse : Cette thèse a pour objectif d'étendre le domaine d'application de la plateforme MUSCA SEP3 à celui de la problématique *sécurité*. De par la proximité de ces deux sujets (phénomènes radiatifs naturels vs. attaques par illumination laser), l'effort concerne principalement la consolidation du modèle physique décrivant l'interaction laser-matière, ainsi que certains effets d'échelles liés aux caractéristiques spatiales du laser (taille de spot de un à plusieurs dizaines de micromètres) et aux durées d'impulsions utilisées par les attaquants (dans le domaine des nanosecondes).
Une phase expérimentale impliquera l'utilisation de véhicules de tests (existants) sous faisceau laser (campagnes réalisées sur le banc laser du Centre Microélectronique de Provence, Mines de Saint-Etienne) pour confronter les mesures à la modélisation. Des travaux similaires d'utilisation de mesures expérimentales sur circuits de test à des fins de modélisation électrique [5, 6] et d'intégration des modèles dans les outils de CAO [7, 8] ont déjà été menés dans notre équipe de recherche.

Une seconde étape consistera à proposer de nouvelles contre-mesures [9, 10], adaptées aux défis posés par les échelles nanométriques, et d'en vérifier l'efficacité par simulation. Ces travaux coupleront donc une étude expérimentale basée sur des injections de fautes réalisées sur banc laser, et une large partie de modélisation basée sur la plateforme MUSCA SEP3 (véhicule de tests de type transistors et circuits fonctionnels). La description physique sera couplée avec une plateforme d'injection de fautes au niveau circuit et fonctionnel.

Une collaboration étroite est prévue avec les équipes sécurité de la société ST Microélectronique qui porte un intérêt marqué vis-à-vis de ces travaux de recherche. Il est prévu d'échanger des résultats expérimentaux utiles aux travaux de modélisation et possiblement de faire fabriquer par ST des dispositifs intégrés de validation proposés dans le cadre des travaux de thèse.

Profil du candidat : master 2 ou ingénieur en électronique / microélectronique.

Candidature : la thèse est proposée pour financement à l'appel "Emplois Jeunes Doctorants" de la région PACA (https://www.maregionsud.fr/aides-et-appels-a-projets/detail/emplois-jeunes-doctorants). Le dossier de candidature doit être envoyé à la région pour le **24 mai 2019** date limite (réponse en juin 2019).

Aspects administratifs : la durée de la thèse est 36 mois. La date de début envisagé est le 1er octobre 2019 (souplesse possible). Salaire net : 1698 €/mois.

Directeur de thèse : Dr. Jean-Max Dutertre (Mines Saint-Etienne), dutertre@emse.fr
Co-directeur de thèse : Dr. Guillaume Hubert (ONERA), Guillaume.Hubert@onera.fr
Co-encadrant : Dr. Jean-Baptiste Rigaud (MSE), rigaud@emse.fr
Partenaire industriel : ST Microelectronics, site de Rousset
Laboratoire d'accueil des travaux de thèse :
Equipe commune Systèmes et Architectures Sécurisés
Centre Microélectronique de Provence
880, avenue de Mimet
13541 Gardanne

Contact - candidature :
- Dr. Jean-Max DUTERTRE – dutertre@emse.fr, +33 (0)4 42 61 67 36,

References

[1] J.-M. Dutertre and et al., "Laser fault injection at the cmos 28 nm technology node: an analysis of the fault model," in *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, ser. 14th Workshop on Fault Diagnosis and Tolerance in Cryptography, Sep. 2018, pp. 1–6.

[2] S. Buchner, F. Miller, V. Pouget, and D. McMorrow, "Pulsed-laser testing for single-event effects investigations," *Nuclear Science, IEEE Transactions on*, vol. 60, no. 3, pp. 1852–1875, June 2013.

[3] G. Hubert, S. Duzellier, C. Inguimbert, C. Boatella-Polo, F. Bezerra, and R. Ecoffet, "Operational ser calculations on the sac-c orbit using the multi-scales single event phenomena predictive platform (musca sep^3)," *IEEE Transactions on Nuclear Science*, vol. 56, no. 6, pp. 3032–3042, Dec 2009.

[4] G. Hubert and et al., "Set and seu analyses based on experiments and multi-physics modeling applied to the atmel cmos library in 180 and 90-nm technological nodes," *IEEE Transactions on Nuclear Science*, 2014.

[5] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, "Seu sensitivity and modeling using pico-second pulsed laser stimulation of a d flip-flop in 40 nm cmos technology," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), 2015 IEEE International Symposium on*, Oct 2015, pp. 177–182.

[6] M. Lacruche, N. Borrel, C. Champeix, C. Roscian, A. Sarafianos, J.-B. Rigaud, J.-M. Dutertre, and E. Kussener, "Laser fault injection into sram cells: Picosecond versus nanosecond pulses," in *On-Line Testing Symposium (IOLTS), 2015 IEEE 21st International*, July 2015, pp. 13–18.

[7] R. Viera, P. Maurine, J.-M. Dutertre, and R. Possamai Bastos, "Role of laser-induced ir drops in the occurrence of faults: Assessment and simulation," in *2017 Euromicro Conference on Digital System Design (DSD)*, Aug 2017, pp. 252–259.

[8] R. A. Viera, J.-M. Dutertre, P. Maurine, and R. P. Bastos, "Standard cad tool-based method for simulation of laser-induced faults in large-scale circuits," in *Proceedings of the 2018 International Symposium on Physical Design*, ser. ISPD '18. New York, NY, USA: ACM, 2018, pp. 160–167.

[9] A. Sarafianos, M. Lisart, O. Gagliano, V. Serradeil, C. Roscian, J.-M. Dutertre, and A. Tria, "Robustness improvement of an sram cell against laser-induced fault injection," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, DFT 2013*, 2013, pp. 149–154.

[10] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, "Experimental validation of a bulk built-in current sensor for detecting laser-induced currents," in *On-Line Testing Symposium (IOLTS), 2015 IEEE 21st International*, July 2015, pp. 150–155.