Étude de la sensibilité des System-on-Chip aux attaques par illumination laser

Sujet de Thèse

Description

L'objectif de cette thèse sera d'étudier le potentiel des attaques par illumination laser pour extraire des secrets cryptographiques ou contourner un mécanisme de sécurité. En effet, les photocourants induits par l'illumination laser du silicium d'un circuit peut mener à la perturbation de celui-ci. Les cibles étudiées seront des System-on-Chip (SoC) du type de ceux utilisés dans des téléphones mobiles.

Des travaux de l'équipe SAS ont permis de montrer que d'autres types d'attaques comme l'injection de fautes par perturbation électromagnétique permettent de contourner des mécanismes de sécurité sur un System-on-Chip [1]. Pour les attaques par illumination laser, il a été démontré dans la littérature que, dans certaines situations, elles peuvent permettre de contourner des mécanismes de sécurité sur ces cibles [2]. Néanmoins, les phénomènes mis en jeu et la complexité de la micro-architecture de ce type de cibles rend le contrôle de la faute injectée par l'attaquant difficile [3].

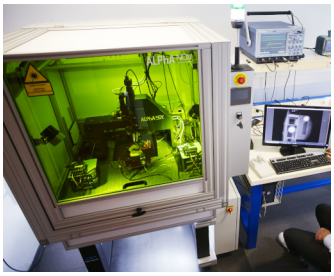

Figure 1: Banc laser bi-spot permettant d'illuminer deux zones d'un circuit

Dans un premier temps, le doctorant ou la doctorante explorera de nouvelles méthodes pour optimiser l'injection de fautes par illumination laser sur System-On-Chip (ex: conception d'un code sous attaque maximisant l'observabilité d'apparition d'erreurs dans

l'exécution de celui-ci, imagerie, photo-émission, défocalisation, exploration exploitant deux spots lasers...). Dans un second temps, les travaux de thèse viseront à étudier l'impact de la technologie et du noeud technologiquedu circuit cible sur la faisabilité de ce type d'attaque. Dans un troisième temps, les travaux se concentreront sur le developpement de nouvelles méthodes pour contourner des verrous spécifiques à l'injection de fautes par illumination laser dans un System-on-Chip.

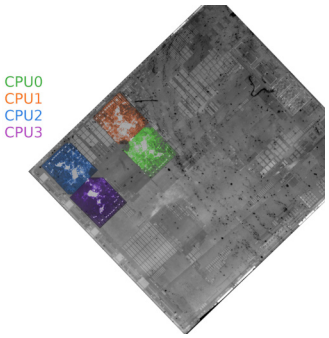

Figure 2: Identification des 4 coeurs de CPU d'un Système-on-Chip par photoémission. (Clément Gaine)

Les laboratoires LSCO (Laboratoire de Sécurité des COmposants) et LTSO (Laboratoire de Tests de Sécurité & Outils) accueilleront le/la doctorante sur son site de Gardanne au sein de l'équipe de recherche commune entre le CEA et l'MSE: SAS "Systèmes et Architectures Sécurisés". Cette équipe dispose d'équipements de pointe avec des bancs d'attaque physique au niveau de l'état de l'art international. Elle est située entre Aix-En-Povence et Marseille à Gardanne sur le campus Aix-Marseille Provence. La thèse sera co-dirigée par Jean-Max Dutertre (MSE) et Jessy Clédière (CESTI-Leti) et co-encadrée par Simon Pontié (CEA) et Driss Aboulkassimi (CEA).

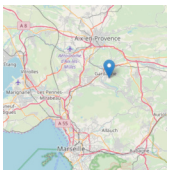

Figure 3: Campus Georges Charpak Provence: (lien)

Plus d'informations:

- https://www.simon.pontie.fr/sujet-these/laser-soc/index.html
- https://www.simon.pontie.fr/
- https://www.emse.fr/~dutertre/
- https://www.leti-cea.fr/cea-tech/leti/Pages/innovation-industrielle/innover-avec-le-Leti/CESTI.aspx
- https://www.leti-cea.fr/

- https://instn.cea.fr/these/etude-de-la-sensibilite-des-system-on-chip-aux-attaques-par-illumination-laser/
- https://www.abg.asso.fr/fr/candidatOffres/show/id_offre/119067/job/etude-de-la-sensibilite-des-system-on-chip-aux-attaques-par-illumination-laser-laser-fault-injection-exploration-on-system-on-chip

Profil recherché

Le candidat/La candidate pourra avoir suivi un cursus Mathématique, Informatique, Électronique ou micro-électronique. Une expérience en lien avec l'analyse de vulnérabilités matérielles n'étant pas obligatoire, mais appréciable.

La thèse démarrera début octobre 2024.

Candidature

Les candidatures sont fermées.

Bibliographie

[1] C. Fanjas, D. Aboulkassimi, S. Pontie, et J. Clédière, « Exploration of System-on-Chip Secure-Boot Vulnerability to Fault-Injection by Side-Channel Analysis », in *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 2023, p. 1-6. https://doi.org/10.1109/DFT59622.2023.10313346 https://hal.archives-ouvertes.fr/cea-04521287.

[2] A. Vasselle, H. Thiebeauld, Q. Maouhoub, A. Morisset, et S. Ermeneux, « Laser-induced fault injection on smartphone bypassing the secure boot », in *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2017, p. 41-48.

[3] T. Trouchkine, « SoC physical security evaluation », Theses, Université Grenoble Alpes [2020-....], 2021.