LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

H2020 – 5 Septembre 2016

Equipe Systèmes Embarqués Sécurisés et Architectures Matérielles (SESAM)

Viktor Fischer, Lilian Bossuet

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

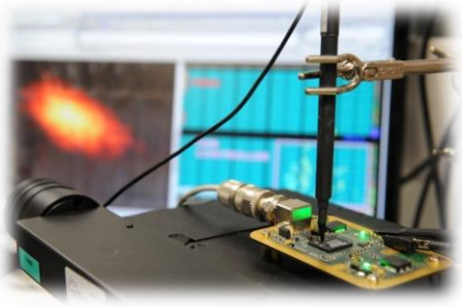
UNIVERSITÉ DE LYON

INSTITUT d'OPTIQUE GRADUATE SCHOOL ParisTech

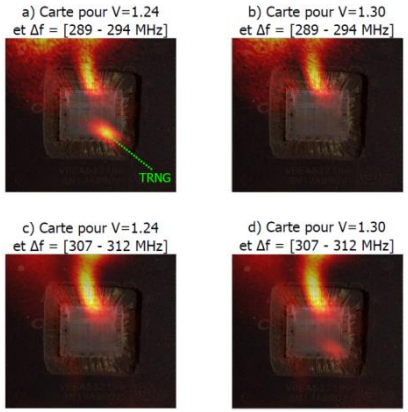
cnrs

Objectifs scientifiques

Conception de générateurs d'aléa (TRNG) et de fonctions physiques non clonables (PUF) pour la cryptographie



- Etude des sources d'aléa dans les circuits logiques (technologie CMOS)
- Méthodes, outils et modèles mathématiques utilisés pour caractériser l'aléa et son extraction
- Proposition de test embarqués permettant de tester les générateurs d'aléa en ligne
- Evaluation de la sécurité des générateurs d'aléa (attaques par injection de fautes et/ou analyse des canaux cachés)
- Application à la lutte contre la contrefaçon et le vol de circuits intégrés et d'IP



Architecture matérielles résistantes aux attaques cryptographiques passives et actives

- Architectures de crypto-processeurs incluant la gestion sécurisée des clés
- Architectures de systèmes cryptographiques post-quantiques résistantes aux attaques par analyse de canaux cachés

Equipe & collaborations européenes

Effectifs

- 2 Professeurs des Universités, 4 Maîtres de Conférences
- 1 Ingénieur de recherche du CNRS
- 6 Doctorants et 2 Post-doctorants

Projets collaboratifs européens

- EIT IAMIT - Identity and Access Management for the Internet of Things
  - SICS, UJM, TU Berlin, Ericsson, Deutsche Telekom

- H2020 HECTOR - Hardware Enable CrypTO and Randomness
  - KU Leuven, UJM, TU Graz, STMicroelectronics, Thales C & S, Brigtshight, Micronic, Technikon

- COST ACTION TRUDEVICE – Trustworthy Manufacturing and Utilization of Secure Devices