General Information

Lab-STICC: *Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance*

CNRS UMR 6285, UBS, UBO, ENSTA-Bretagne, IMT Atlantique, ENIB

Locations: Lorient and Brest

Hardware/software security&crypto group:
8 faculties, $\approx$ 12 PhD students, postdocs, ATER, engineers

Contact: Arnaud TISSERAND
`arnaud.tisserand@univ-ubs.fr` +33 (0)2 97 87 46 49

Area of interest	Y or N
CIP-01-2016-2017: Telecom	Y
CIP-01-2016-2017: Health	Y
CIP-01-2016-2017: Finance	Y
SEC-10-FCT-2017	Y

Competencies

Lab-STICC

- Skills:
  - Hardware security for embedded systems:
    - memory and communication protection
    - secure OS with HW blocks, DIFT
    - multicore / manycore security
  - Crypto implementations in hardware & embedded software:
    - asymmetric (ECC, HECC, RSA, PQC)
    - arithmetic aspects (operators, libraries)
    - homomorphic encryption
  - Secure hardware implementation:
    - side channel and fault injection attacks and protections
    - targets: FPGA and ASIC (reconfigurable, CGRA, ASIP)
    - high-level synthesis (HLS) for security
- Organisation: partner in several projects (e.g. AEther 06–09), WP leader, leader for hardware demonstrator, help from dedicated staff in EU projects application (UBS/CNRS)

Project Interest

- Hardware crypto implementations & protection against physical attacks
- Hardware security of compiled embedded software
- Optimized implementations (speed, energy) implementations for homomorphic (or other advanced) encryption schemes
- Hardware & software resources for TEEs