



General information

CEA List

Belgacem BEN HEDIA

belgacem.ben-hedia@cea.fr
01 69 08 21 22

Targeted topics

SU-DS04-2018-2020	Electrical Power and Energy System	IA
SU-DS05-2018-2019	Critical sectors: Privacy Accountability	IA
SU-ICT-01-2018	Dynamic countering of cyber-attacks	IA

DATA PROTECTION

- *Lightweight cryptography*
 - **High performance cryptography for highly constrained things**
 - **8bit to 64bit CPU implementations of lightweight stream ciphers, with counters-measures against power/fault-injection attacks**
- *Homomorphic encryption*
 - **Computing with encrypted data, without decrypting it: enables processing of confidential data on untrusted servers.**
 - **CEA compiler transforms C++ algorithm into equivalent, privacy-preserving code, with minimal computational overhead.**
 - **Millisecond bootstrapping scheme to reduce cryptographic noise**
- *Detection of cyber-attacks in IoT*
 - **Physical and logical attacks**
 - **Monitoring and light-weight machine learning techniques**

CODE PROTECTION

- *Compilation of software countermeasures*
 - **Countermeasures against side-channel attacks**
 - **Code polymorphism: behavioral variability to thwart side-channel attacks.**
 - **Suitable for computing & memory constrained embedded processors (IoT, mobile applications)**
- *Countermeasures against fault-injection attacks*
 - **Fault tolerance, including against multiple fault injections**
 - **Fault detection & Control-Flow Integrity**
 - **Fine-grain integrity of program execution: detection of integrity violations at the granularity of a single machine instruction**

HW PROTECTION

- *Secure hypervision with ARM trustzone*
 - **Data protection & error isolation through memory partitioning and protection.**
 - **« Blind » hypervision protects from attacks from other domains, and from hypervisor itself**
 - **Minimal Trusted Computing Base implemented in ARM/TrustZone, security formally verified with static code analysis**
 - **Experiences of Intel/SGX secure environment**
- *Many-core systems safety*
 - **Deterministic execution and interference-free cohabitation of mixed critical applications**