SECURE PLATFORM FOR ICT SYSTEMS ROOTED AT THE SILICON MANUFACTURING PROCESS (SPIRS)

Blog 1: WP2 Outcomes

We start with a post dedicated to the results of Work Package 2 (WP2). WP2 tasks are devoted to design a hardware Root of Trust (RoT) for the system.

At the end of the first year of the project, the preliminary components of the RoT were delivered: a Physical Unclonable Function (PUF) based on ring-oscillators to generate the identifier of the device and an entropy source, a symmetric AES cipher, an implementation of the hash function SHA2-256, and an accelerator for RSA digital signatures.

At the end of WP2 active period, the final RoT has been unveiled. This final RoT comes with enhancements compared to the preliminary version. On one hand, the improvements align with the project's roadmap, which evaluated the initially proposed modules against Side-Channel Attacks (SCA) and Fault Injection Attacks (FIA). On the other hand, following the recommendations of the experts after during the midterm review of the SPIRS project, some of the existing modules have been improved, new modules have been included and also some modules have been replaced.

In comparison with the preliminary RoT, the final RoT introduces modifications in three modules: PUF, AES, and SHA-2. Additionally, three new modules have been designed during this second period of the WP2.

The final RoT components encompass a PUF, an AES symmetric cipher, SHA-2 and SHA-3 hash functions, a digital signature accelerator utilizing elliptic curves, and a System-Level Protection (SLP) block.

The PUF block has been improved by optimizing the resources of the chosen device for the resultant project platform. The PUF's performance has been assessed in terms of reliability, uniqueness, and uniformity for generating a device identifier. Various countermeasures have been explored to enhance its resilience against Electromagnetic (EM) attacks during the generation of PUF challenges, thereby avoiding potential correlations among the oscillators generating the response. Furthermore, the same PUF has been validated as a True Random Number Generator (TRNG).

The new version of AES block incorporates countermeasures, integrating a signature generator for FIA and Leakage-Resilient Masking Scheme (LEMS) for SCA. Both countermeasures are compatible and have undergone evaluation concerning resource consumption, fault coverage, and information leakage.

The RoT incorporates two hashing blocks: a new improved hardware implementation of all hash functions within the SHA-2 family, and a novel architecture for the Keccak function intended for use in the hash functions of the SHA-3 family. The results demonstrate high competitiveness when compared to other state-of-the-art proposals.

In the realm of digital signatures, a novel architecture, based on a 4-level Karatsuba modular multiplier, has been developed to accelerate the EdDSA25519 digital signature scheme instead of the RSA accelerator proposed in the preliminary version of the RoT.

Finally, the RoT incorporates a protective block at the system level (SLP) to prevent FIA attacks across the entire system. The implemented security measures include voltage, temperature, and pulse detectors. The SLP module detects when the circuit operates under abnormal conditions (temperature and power supply) and identifies fault injections in control and clock systems. The module activates an alarm signal, indicating a potential security risk to the system.

Furthermore, the team has advanced in implementing Post-Quantum Cryptography (PQC) algorithms on embedded systems. New safeguarded schemes against timing and power SCA have been proposed for the NTRU algorithm. Recently, the team has oriented efforts towards the CRYSTAL-Kyber algorithm.

Lead partner of WP2: CSIC

Author: M. C. Martínez- Rodríguez (CSIC; Instituto de Microelectrónica de Sevilla)

Submission date: 15/02/2024

This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 952622