Newsletter

OPEN INITIATIVES IN HARDWARE SECURITY

OPEN COMPETITION FOR PQC

The technological advances are approaching quantum computers with enough computing power to threaten current cryptography. Current public-key cryptosystems based on the hardness of integer factorization and discrete logarithms will become vulnerable to attacks using a sufficiently large quantum computer. Post-Quantum Cryptography (PQC) has emerged to face it.

- Standardization is a key factor in the transition towards a quantum-safe era. The standards for PQC are fostered by NIST which launched a public competition to request, evaluate, and standardize one or more quantum-resistant public-key and signature algorithms.
- The development of efficient implementations of PQC on embedded systems compatible with tight constraints on power consumption and memory size, as well as limitations on time and processing power, is a challenging research topic.

OPEN-SOURCE HARDWARE FOR PQC

ATHENa: Automated Tools for Hardware EvaluatioN is a project started at George Mason University, aimed at fair, comprehensive, and automated evaluation of hardware cryptographic cores targeting FPGAs, All Programmable Systems on Chip, and ASICs. Click here to get open resources in Hardware and Embedded Systems available at ATHENa PQC.

Other open-source hardware PQC projects:

- Bit Flipping Key Encapsulation (BIKE) ➡ Scalable Hardware Implementation for Reconfigurable Devices
- Hamming Quasi-Cyclic (HQC) ➡ HW implementation
- Supersingular Isogeny Key Encapsulation (SIKE) ➡ HW implementation

OTHER OPEN HW CRYPTO REPOSITORIES AND IP CORES

- OpenTitan
- Chair for Security Engineering @ Ruhr-Universität Bochum
- CryptoHDL @ hadipourh
- OpenCores

TOOLS FOR FORMAL VERIFICATION

- ATHENa
- REBECCA

This GoIT project receives support from the European Union's Horizon Europe research and innovation programme and has received funding under grant agreement No 101070660. Funded by the European Union.

OPEN INITIATIVES IN HARDWARE SECURITY

OPEN COMPETITIONS FOR LIGHTWEIGHT CRYPTOGRAPHY

LightWeight Cryptography (LWC) provides symmetric encryption methods with a low computational complexity. This makes feasible the LWC can be integrated into constrained devices, protecting them against cyberattacks. LWC international standardization and guidelines compilation have been explored in several open competitions:

- NIST LWC: a process to solicit, evaluate, and standardize schemes providing authenticated encryption with associated data and optional hashing functionalities for constrained environments. NIST announced the selection of the Ascon family in February 2023.
- CAESAR: aims at finding authenticated encryption schemes in three categories (lightweight, high-performance and defense applications).

OPEN-SOURCE HARDWARE FOR LWC

- ATHENa LWC: include hardware implementations (evaluation and benchmarking) of finalists in the NIST LWC Standardization Process, as well as protected hardware implementations of LWC finalists.
- ATHENa CAESAR: include hardware implementations (evaluation and benchmarking) of CAESAR candidates.

Other open-source hardware LWC projects and repositories:

- Ascon Official HW implementation
- Ascon HW implementation
- RISC-V Ascon Accelerator
- Ascon, AES and Keccak Protected HW implementations
- Romulus HW implementation
- Grain-128AEAD HW implementation
- ISAP HW implementation

Info compiled by Pablo Navarro *navarro@imse-cnm.csic.es*
Instituto de Microelectrónica de Sevilla, CSIC/Universidad de Sevilla

This GoIT project receives support from the European Union's Horizon Europe research and innovation programme and has received funding under grant agreement No 101070660. Funded by the European Union.