Lightweight security accelerators for RISCV

Alberto Josue Ortiz, Brisbane Ovilla, Cuauhtemoc Mancillasi
CINVESTAV-IPN, Mexico

Abstract

Over the past years, the RISC-V (Reduced Instruction Set Computer - Five) ISA (instruction set architecture) has gained the attention of the academic and industrial sector as an open-source alternative to proprietary ISAs. Its modularity, simplicity, and custom instructions integration have made RISC-V an outstanding candidate for hardware and software development. The ISA has been implemented in numerous applications, from complex network on-chip or high-performance processors to embedded systems. The latter has raised significant concerns about their security, mainly because of the increase in connectivity.

To implement security solutions in embedded systems one has to overcome resource limitations, low power consumption, and real-time processing. These systems have to face various threats and vulnerabilities. One way to increase protection is to use cryptography.

We propose to integrate hardware modules. One of them is capable of performing the ASCON algorithm in its variations ASCON-128, ASCON-128a and ASCON-Hash. The other hardware modules will keep a safe generation, storage and management of the cryptographic keys. The toolset of Rocket chip, developed by the University of California, Berkeley provides the means to generate a custom Rocket core.

Finally, the designed core will be tested using the TEE MultiZone to show the increased performance in encryption/decryption and hashing data. It will be compared with the only software implementation. Our findings will contribute to the RISC-V lightweight security research.