EUROPEAN PROCESSOR INITIATIVE

FRAMEWORK PARTNERSHIP AGREEMENT IN EUROPEAN LOW-POWER MICROPROCESSOR TECHNOLOGIES

Crypto-Accelerators for EPI Security

In the framework of strategic EU markets (e.g. HPC for automotive, aerospace, AI, industry4.0, robotics, biomedical), robustness and safety issues play a major role, requiring layered and itemized architecture with specific HW and dedicated private resources for security responsibility. For this reason, in close collaboration between University of Pisa (I) and Provenrun (F), the General Purpose Processor (GPP) ecosystem integrates a Security Subsystem (Fig. 1), that relies on an isolated blocks architecture, with specific HW and dedicated private resources. Each isolated block (Security Domain) guarantees security service availability and full independence of each security scheme that is accelerated in HW by an embedded cryptographic co-processor (Crypto-Tile).

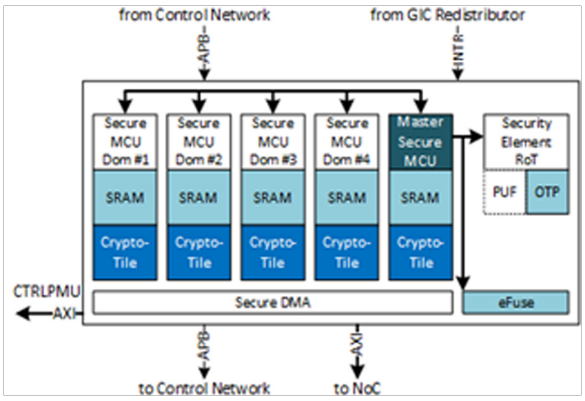

Fig. 1. GPP Security Subsystem

Crypto-Tile co-processor features:

- Implementation of Security Recommendations addressing threats, vulnerabilities and errors
- Secure MCU interface for installation and management of cryptographic keys and configuration, control and status of cryptographic operations
- Secure DMA interface for high-bandwidth data transfer
- HW acceleration of symmetric-key cryptographic algorithms (AES and AES modes of operation: ECB, CBC, CFB, OFB, CTR, CMAC, CCM, GCM, XTS), for 128b and 256b keys
- HW acceleration of public-key cryptography arithmetic on 256b and 521b elliptic curves (ECC)
- Supporting SW aided ECC schemes (ECDSA, ECDH, ECIES, ECMQV)
- HW acceleration of hash functions SHA2 and SHA-3 for computation of digests on 224, 256, 384 and 512 bits and supporting SW aided high-level hash schemes (HMAC)
- HW acceleration for random numbers generation, supporting both external seeds and internal seeds (by means of an embedded fully digital entropy generator)
- Evolution towards Post-Quantum Cryptography
- Support to security protocols and security standards such as TLS, SSH, MACsec, IPsec, WAVE, ESI, ITS

The Crypto-Tile architecture (Figure 2) consists in global registers for management of internal keys slots dedicated to each engine, and for secure configuration and handling of the tile and 4 crypto-processors (CP) for symmetric-key algorithms (AES), elliptic curve cryptography operations (ECC), hash functions (SHA) and random numbers generation (RNG). Each CP integrates a digital engine and dedicated registers for controlling and handling cryptographic operations and transferring data. Any registers of the Crypto-Tile can be accessed by the Secure MCU (Master Control Unit, e.g. a low-power RISCV or CortexM core) and, in addition, data registers of crypto-processors can be accessed also by a specific interface to Secure DMA (Direct Memory Access) controller. Dedicated SW drivers will be developed to integrate the HW acceleration offered by the Crypto-Tile in the secure GPP Operating System Kernel. The Crypto-Tile IP can be connected through an AXI full memory-mapped interface. Synthesis results on Artisan 7nm TSMC technology demonstrate that the Crypto-Tile IP can run up to several GHz (e.g. ECC@1.8GHz, SHA@5GHz, AES@3GHz) ensuring a throughput in data encryption and signature verification orders of magnitude higher than what achievable via SW on ARMv8 64b architecture.

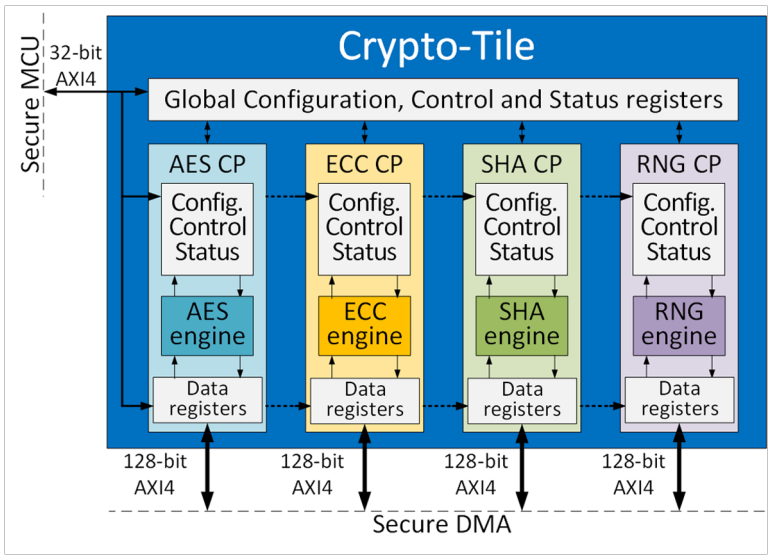

Fig. 2. Outline of Crypto-Tile architecture

www.european-processor-initiative.eu
European Processor Initiative
@EuProcessor
European Processor Initiative

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826647