SILEX INSIGHT

Product sheet
BA450

FIPS VALIDATED 140-2

CRYPTO COPROCESSOR

The Crypto Coprocessor is a hardware IP core platform that accelerates cryptographic operations in System-on-Chip (SoC) environment on FPGA or ASIC.

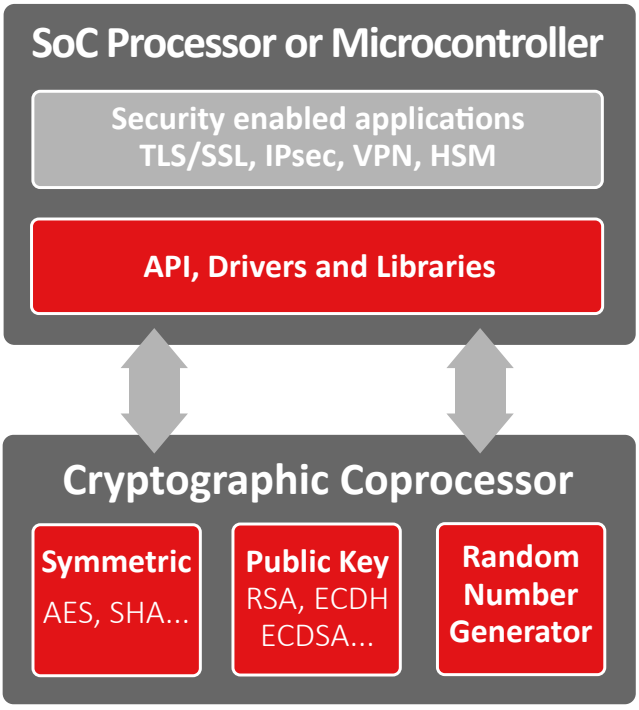
Symmetric operations are offloaded very efficiently as it has a built-in scatter/gather DMA. The coprocessor can be used to accelerate/offload IPsec, VPN, TLS/SSL, disk encryption, or any custom application requiring cryptography algorithms.

General description

The Coprocessor platform integrates your desired selection of our cryptographic IP cores (including our TRNG solutions), additional interfacing, DMA and software layers providing a complete solution.

The following cryptographic engines can be selected to be integrated:

- Public Key Cryptography (RSA, ECC, ECDSA, ECDH, SM2, ...)
- Random Number Generator (compliant with NIST-800-90A/B/C)
- AES (CTR, CCM, CMAC, GCM/GMAC, XTS, ECB, CBC, ...)
- Hash: SHA-1/SHA-2/SM3/HMAC, SHA-3
- Chacha20-poly1305
- SM4
- ARIA
- 3GPP security (ZUC, KASMI, SNOW_3G)
- DES and 3-DES (Ideal for legacy)



Features

- Scalable architecture and crypto engines for optimal performance/resource usage
- Configurable for perfect application fit
- 100% CPU offload with low latency and high throughput
- Optional DPA countermeasures for AES, PK and SM4
- Can use keys (from PUF or others) not visible by CPU
- Full software/driver support
  - mbedTLS integration
  - OpenSSL support
  - Linux drivers (Crypto API integration)
- Easy integration
  - AHB/AXI interfaces
- FIPS 140-2 validated: CAVP #C742
- Low power

Applications

- Secure Communication (TLS, IPSec, BLE, Zigbee, others...)
- Secure boot support
- Secure storage
- Key generation

Software Interfacing

The software API and drivers are interfacing with mbedTLS and the CryptoAPI from the Linux OS. They are provided with the co-processor to enable an easy integration with your application. Hardware offloading is directly available to applications using mbedTLs, OpenSSL or interfacing with the kernel through Cryptodev and AF_ALG.

Deliverables

- Netlist or RTL
- SW drivers (Linux) & OpenSSL
- Scripts for implementations
- Self-checking RTL test-bench based on FIPS vectors
- Documentation

Markets

WIRELESS COMMUNICATION

NETWORKING

AUTOMOTIVE

GENERAL PURPOSE MCU/MPU

DATA CENTER /CLOUD

Silex Insight
Rue Emile Francqui 11,
1435 Mont-Saint-Guibert, Belgium

Tel: +32 10 45 49 04
E-mail: contact@silexinsight.com
Web: www.silexinsight.com