Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Crypto Solutions > SCZ_CS_CW_PQC

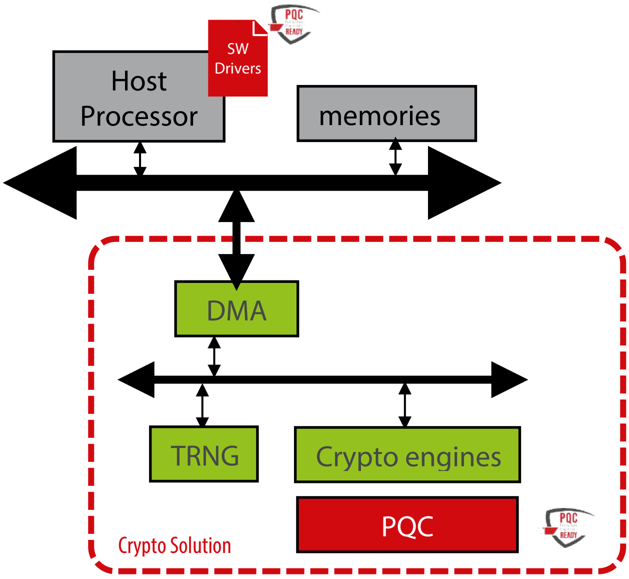
CRYPTO COPROCESSORS WITH POST-QUANTUM CRYPTOGRAPHY

The Crypto Coprocessors are 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 coprocessors can be used to accelerate/offload IPsec, VPN, TLS/SSL, disk encryption, or any custom application requiring cryptography algorithms.

Post-Quantum Cryptographic algorithms are including in the solutions to accelerate/offload security operations based on XMSS for FW verification, or on Crystals Kyber for secure Key Exchange, or also on Crystals Dilithium for Digital Signature.

General description
The Coprocessors platform integrates your desired selection of our cryptographic IP cores (including our TRNG solutions), additional interfacing, DMA and software layers providing a complete solution.
Depending on needs, the solution can be configured to embed only accelerators required for PQC algorithms, or a hybrid solution embedding both PQC algorithms and traditional cryptography.



Applications

Secure Communication (TLS, IPSec, BLE, Zigbee, others…)	Secure boot support	Secure storage

Compliances

FIPS 203 (Crystals-Kyber)	FIPS 204 (Crystals-Dilithium)	RFC8391 (XMSS)

Key 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
- DPA countermeasures Full software/driver support
- Easy integration with AXI interfaces
- FIPS 140-2 validated: CAVP #C742
- Embedded DMA to optimize memory access
- Embedded TRNG for random seed generation
- Supported Traditional Cryptographic algorithms:
  - AES/SM4
  - SHA1/SHA2/SHA3/SM3 with HMAC
  - RSA/ECC/SM2
  - Chacha20-Poly1305
  - ARIA
  - Kasumi
  - Snow3G
  - ZUC
  - DES
- Supported Post-Quantum Cryptographic algorithms :
  - Crystals-Kyber/Crystals-Dilithium
  - XMSS
  - LMS
  - SPHINCS$^+$

Deliverables

RTL code	SW Drivers	Scripts for implementation	Self-checking RTL test-bench	Documentation

Related products

SCZ_CS_S10_neo / SCZ_CS_S30_neo	SCZ_IP_PQC_Lattice	SCZ_IP_PQC_XMSS

V1.0

SECURE-IC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com

EMEA
sales-EMEA@seure-ic.com

AMERICAS
sales-US@seure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

CONTACT US
www.secure-ic.com