SECURE-iC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ Security IP > Tunable Crypto > PQC > SCZ_IP_PQC_Lattice

ML-KEM / ML-DSA POST-QUANTUM CRYPTOGRAPHY

ML-KEM (Crystals-Kyber) and ML-DSA (Crystals-Dilithium) are Post-Quantum Cryptographic (PQC) algorithms, meaning they are mathematically designed to be robust against a cryptanalytic attack using a quantum computer. Both have been standardized by the NIST in it post-quantum cryptography project.

The security of ML-KEM and ML-DSA algorithms is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices.

ML-KEM belongs to Key Encapsulation Mechanism (KEM) family, KEM is an encryption technique designed to secure symmetric cryptographic keys (e.g. AES key) for transmission using asymmetric algorithms (e.g. RSA in classical cryptography), or for more security, using post-quantum cryptography with ML-KEM.

ML-DSA is a digital signature algorithm.

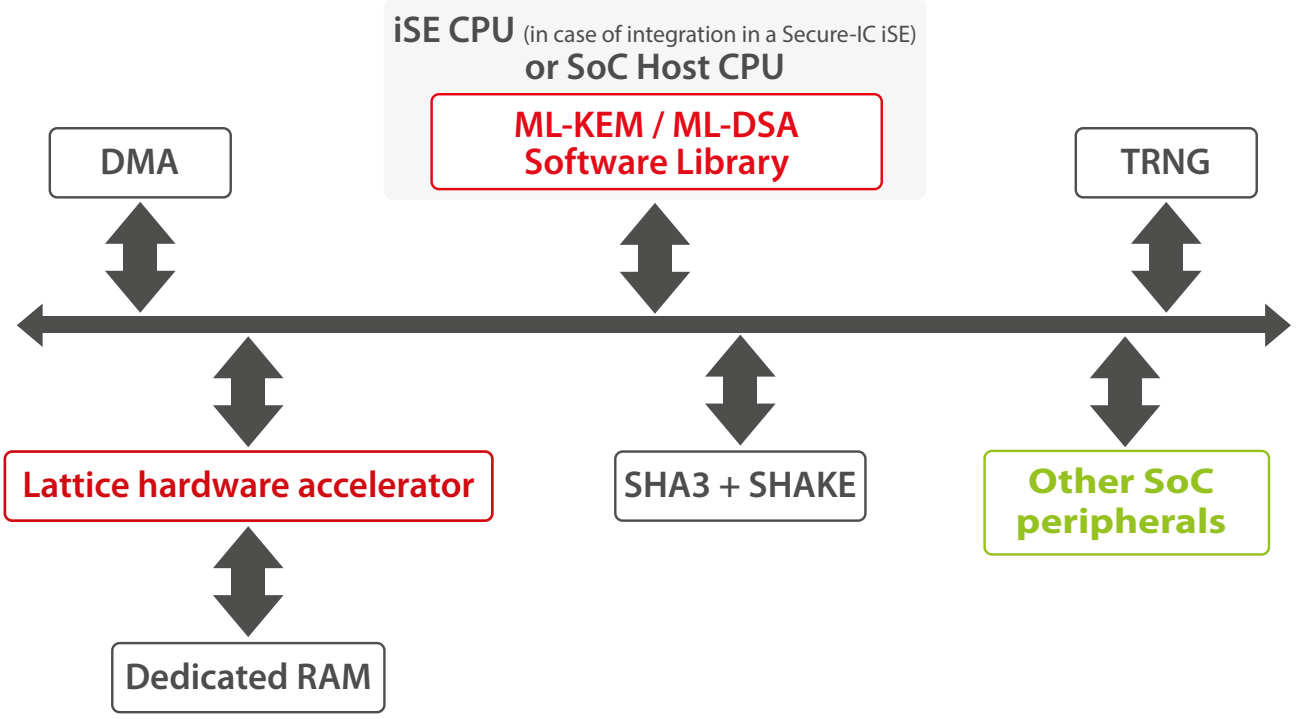
The Lattice Hardware accelerator can be used to realize the ML-KEM Key Encapsulation Mechanism and the ML-DSA signature scheme, with the appropriate software library.

To implement the ML-KEM and ML-DSA functions, five elements are needed:

- The Hardware Lattice Accelerator SCZ_IP_PQC_Lattice and its dedicated RAM
- A Software library which is running on the Securyzr iSE CPU, in case the IP is intergated in a SoC as a stand-alone IP and not in a Secure-IC iSE, the software library then must run on the SoC CPU
- A SHA3/SHAKE Hardware accelerator (*)
- A DMA to optimize memory accesses (*)
- A TRNG for random seed generation (*)

(*) The TRNG, DMA and SHA3+SHAKE Hardware IPs are available as part of Secure-IC's Crypto Solutions. They are not provided in a context of SCZ_IP_PQC_Lattice standalone IP.

The figure below shows the IP block diagram in its system environment: the hardware accelerator, and a portable software library.



Applications

- The ML-KEM IP and ML-DSA may be used both in quantum computing and classical computing context for:
  - Secure communications systems
  - Secure Boot
- For Signature, ML-DSA ensures
  - Keys generation
  - Signature
  - Verification
- For Key Encryption Mechanism, ML-KEM ensures:
  - Key Generation
  - Key Encapsulation
  - Key Decapsulation

Key features

ML-KEM and ML-DSA have been selected by the NIST post-quantum cryptography project.
The US National Security Agency also recommends to implement those algorithms in its Commercial National Security Algorithm Suite 2.0 (CNSA 2.0).
The present product is based on the version of ML-KEM and ML-DSA selected by the NIST at the end of round 3 and is aligned with NIST reference implementation.

Security features

- ML-KEM-512, ML-KEM-768, ML-KEM-1024.
- ML-DSA-II, ML-DSA-III, ML-DSA-V.
- Implementation protected against Side-Channel Attack (Key Generation and Key Decapsulation operations are sensitive):
  - o Simple Power Analysis (SPA)
  - o Differential Power Analysis (DPA)
  - o Differential Electromagnetic Analysis (DEMA)
  - o Correlation Power Analysis (CPA)
  - o Correlation Electromagnetic Analysis (CEMA)
- Optional: health tests for integrity verification.

Other features

- Hybrid hardware-software solution.
- Optimized in performance or power/area.
- Performs Key Generation, Key Encapsulation and Key Decapsulation functions
- Performs Key generation, Signature and Verification.
- Memory can be shared or dedicated.
- Easy to integrate into the system thanks to AMBA AXI wrapper.
- The control interface of the hardware accelerator is the AMBA AXI interface

Deliverables

- RTL of the AMBA wrapper
- VHDL RTL source code
- ML-KEM / ML-DSA software libraries
- Self-checking RTL Testbench based on reference scenario for simulation*

**Simulation scripts are adapted to Questasim, any change of Simulator shall be taken care of by the Licensee*

Related products (must be purchased separately)

- Secure-IC SHA IP for SHA3 and SHAKE (SCZ_IP_SHA3)
- Secure-IC TRNG IP (SCZ_IP_TRNG)
- Secure-IC Crypto Solutions

V4.0

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@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

TAIWAN
sales-TAIWAN@secure-ic.com

CONTACT US
www.secure-ic.com