SECURE-iC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

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

XMSS POST-QUANTUM CRYPTOGRAPHY

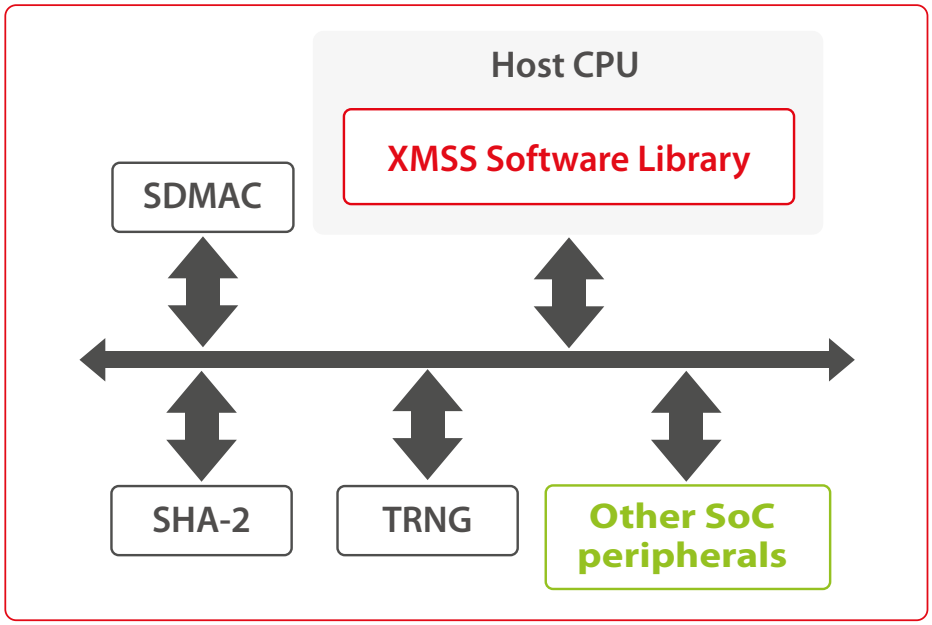
XMSS is a Post-Quantum Cryptographic (PQC) algorithm, meaning it is mathematically designed to be robust against a cryptanalytic attack using a quantum computer. XMSS is a stateful Hash-Based Signature Scheme that has been recommended by NIST in 2020.

The XMSS IP is a software IP that may run on the Host CPU. It uses HASH IP resources, which may be implemented either in software (for a full software XMSS implementation) or in Hardware, to a mixed Hardware/Software implementation.

The figure below shows the IP block diagram in its system environment, in case of an implementation using a Hardware HASH IP: the hardware SHA-2 IP, and a portable software library.

Secure-IC TRNG IP for XMSS keys generation and SDMAC IP are also used.

The interconnection is ensured by an AMBA bus.



Standards

- XMSS is standardized by IRTF in RFC8391: XMSS: eXtended Merkle Signature Scheme
- It has been recommended as 'Stateful Hash-Based Signature Scheme' in SP 800-208
- The XMSS function has been implemented using only RFC8391
- The variants XMSS-SHA2_10_256 and XMSS-SHA2_16_256 have been implemented, for hybrid hardware/ software implementation based on Secure-IC HASH IP
- Key generation, Signature and Verification operations are supported. Performance depends on the system resources, in particular for Key generation and Signature

Applications

- XMSS is designed to resist cryptanalysis using either classical or quantum computers, in applications such as:
  - Secure communications systems
  - Secure Boot
- For Signature, XMSS IP ensures:
  - Key Generation
  - Signature
  - Signature verification

XMSS is recommended for Post-Quantum Firmware signature in the US National Security Agency's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) document.

Deliverables

- Specifications
- User guide
- Test report documentation
- XMSS software library

Related products (must be purchased separately)

- Secure-IC SHA IP (SCZ_IP_HMAC)
- Secure-IC TRNG IP (SCZ_IP_TRNG_DRBG)
- Secure-IC SDMAC IP (SCZ_IP_SDMAC)

V4.0

CONTACT US

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

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