xQlave®

Post-Quantum Cryptography

Quantum computers pose an inescapable threat for cybersecurity architectures. Xiphera's xQlave® family of Post-Quantum Cryptography (PQC) secures hardware platforms against both traditional and quantum attacks, without the need for quantum computing - or software components.

Quantum resilience

- The xQlave® family offers ML-KEM (Kyber) key encapsulation mechanism and ML-DSA (Dilithium) digital signature algorithms
- PQC algorithms can be implemented together with Xiphera's traditional public-key IP for full hybrid cryptographic protection

Standard compliance

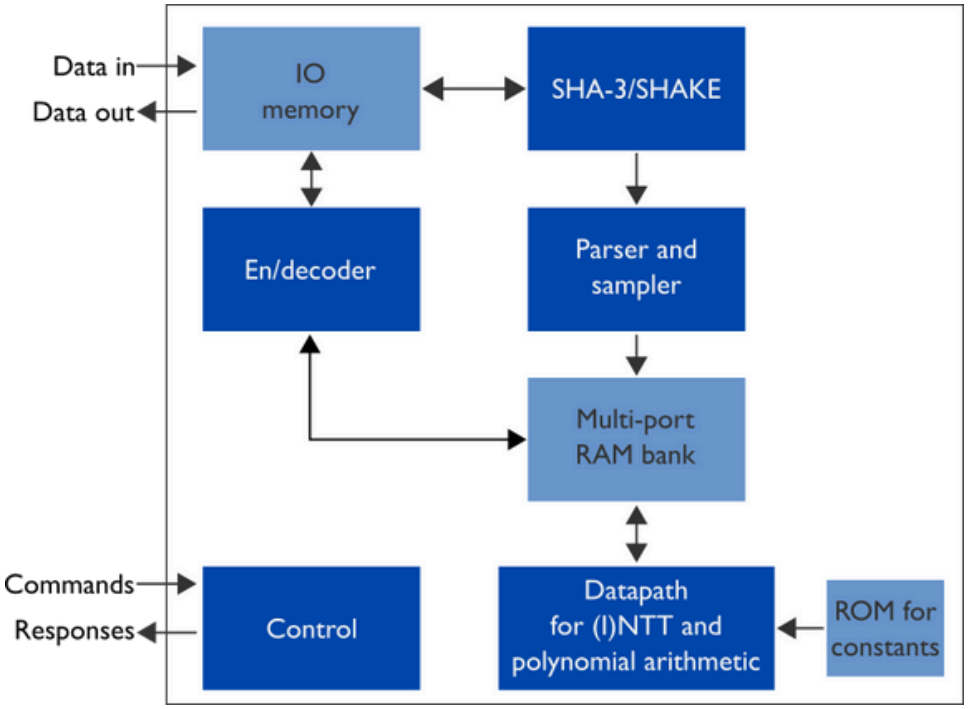
- xQlave® IP cores follow the PQC standards from NIST
- Xiphera is dedicated to update the IP cores in the xQlave® family along the NIST standardisation process

Optimised architecture

- IP cores are optimised for resource usage and performance
- Implementation in pure RTL code without software components for performance, security, and ease of validation

XIPHERA

High-level block diagram of xQlave® ML-KEM (Kyber) IP core



About Xiphera

Xiphera designs and implements proven cryptographic security for embedded systems. Our strong cryptographic expertise and extensive experience in digital system design enable us to help our customers to protect their most valuable assets. We offer secure and highly optimised cryptographic Intellectual Property (IP) cores, designed directly for FPGAs and ASICs without software components. Our broad, fully in-house designed, and up-to-date portfolio enables cost-effective development projects with fast time-to-market – providing peace of mind in a dangerous world.