xQlave® PQC ML-KEM (Kyber)

Product code: XIP6110B

The xQlave® ML-KEM (Kyber) Key Encapsulation Mechanism IP core provides quantum-resistant key exchange, offering a secure solution against the growing threat posed by quantum computing. As a member of the xQlave® Post-Quantum Cryptography (PQC) product family, this IP core is designed to meet the security standards set by the U.S. National Institute of Standards and Technology (NIST), ensuring that your systems are equipped to handle the cryptographic challenges of the future. The xQlave® ML-KEM solution combines high performance with minimal resource usage, making it an ideal choice for secure, scalable, and efficient key exchange.

KEY FEATURES

◉ Quantum-resistant key exchange for future-proof security

◉ Compliant with NIST's ML-KEM standard

◉ Pure RTL without hidden CPU or software components

◉ Optimised architecture with constant-time execution

◉ Easy system integration with 64-bit interface

◉ Vendor agnostic FPGA/ASIC implementation

APPLICATIONS

Quantum-resistant network and data security for:

◉ Cryptographic key exchange

◉ Secure communications

◉ Secure data storage and transmission

◉ Quantum-resistant cryptographic protocols

xQlave® ML-KEM-512/768/1024 (CRYSTALS-Kyber)

Xiphera's xQlave® PQC product family features quantum-secure cryptographic IP cores designed to protect against future quantum threats, all without relying on embedded CPUs or software components.

Our ML-KEM (Kyber) Key Encapsulation Mechanism IP core, part of the xQlave® PQC family, is a powerful solution for secure key exchange and it is designed to withstand attacks from quantum computers.

BALANCED
XIP6110B

• Supports all security levels
• Minimal resource requirement (less than 10 kLUT)
• Fast performance with thousands of operations/sec

XIPHERA

xQlave® ML-KEM (Kyber)
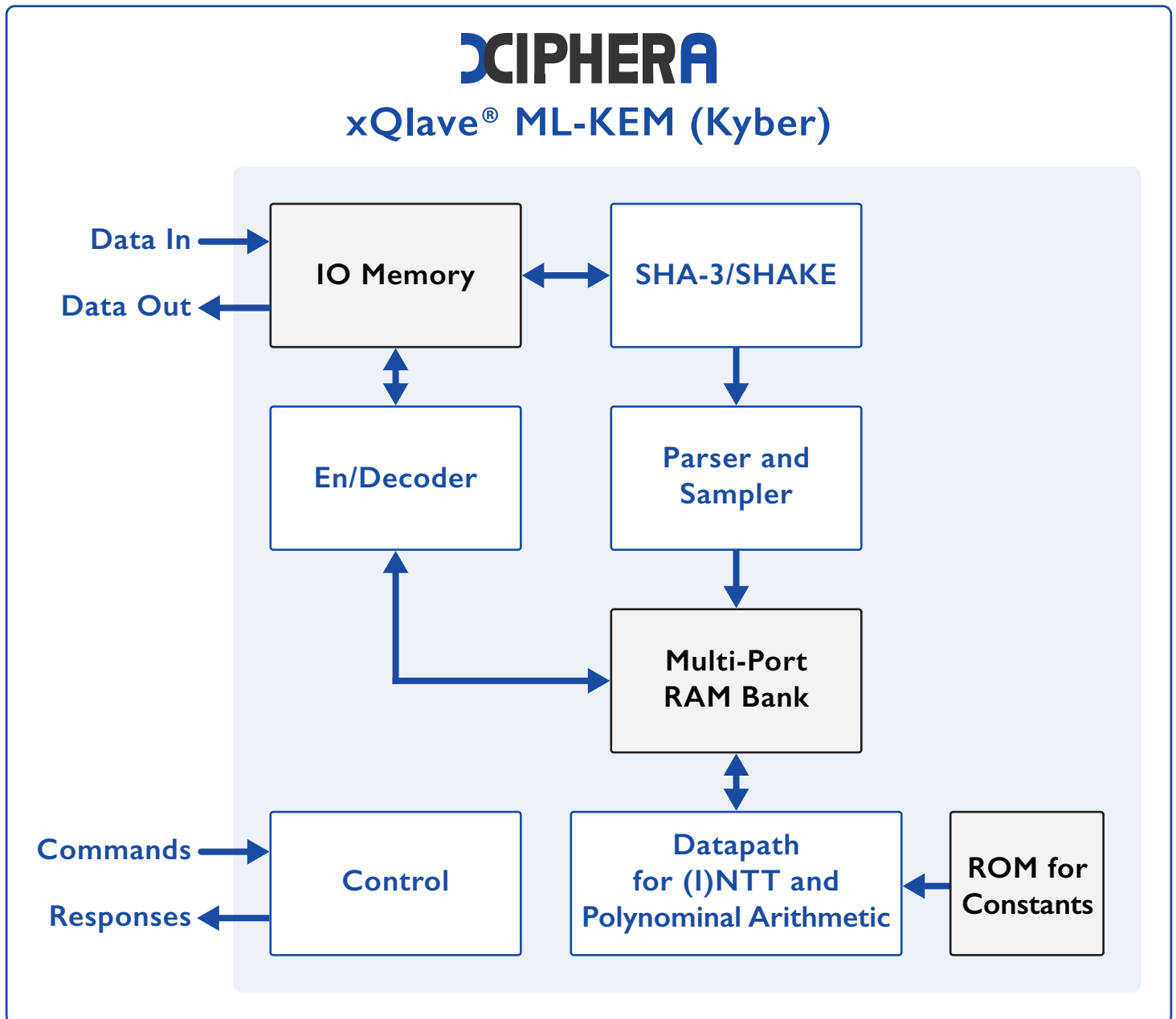
Deliverables

⊘ Encrypted RTL or source code	⊘ Optional netlist
⊘ Sample synthesis scripts	⊘ Instantiation file
⊘ Comprehensive simulation test bench, scripts & guide	⊘ Detailed datasheet and integration guide

About Xiphera

Xiphera, Ltd, is a Finnish company designing hardware-based security solutions using standardised cryptographic algorithms. Our product portfolio consists of secure and efficient cryptographic Intellectual Property (IP) cores, designed directly for ASICs and FPGAs. Our strong cryptographic expertise, extensive experience in system design, and deep knowledge in the field of reprogrammable logic enable us to offer our customers peace of mind in a dangerous world.

XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

Tekniikantie 12
02150 Espoo
Finland

Email: sales@xiphera.com
Phone: +358 20 730 5252
Web: www.xiphera.com