XIPHERA

CAVP-Validated Post-Quantum Security

CAVP validation tests a cryptographic implementation against NIST requirements, so customers can rely on it meeting the standards.

Xiphera's ML-KEM and ML-DSA implementations are successfully validated under NIST CAVP.

Future-Proof Your Security with PQC

Protects your critical data and communications today and tomorrow.

Prevents quantum attacks from stealing or exploiting sensitive information..

Secures critical infrastructures across defense, energy, telecom, and space environments.

Xiphera's **xQlave® Post-Quantum Cryptography product family**: includes ML-KEM & ML-DSA.

ML-KEM Post-Quantum Key Encapsulation

Quantum-resistant key exchange to protect sensitive data in transit

Pure hardware (RTL) design and no hidden software for high performance and security

Optimised constant-time execution for predictable performance

Designed for critical system deployments on FPGA and ASIC

ML-DSA Post-Quantum Digital Signatures

Quantum-secure digital signatures for device and user authentication

Protects critical data and system integrity against emerging quantum computing threats

Pure hardware (RTL) design and no hidden software for high performance and security

Efficient IP core implementation designed for critical system integration

Xiphera's xQlave®

PQC product family

Standardized. Validated.

High-performance.

www.xiphera.com