

# xQlave<sup>®</sup> PQC ML-DSA (Dilithium)

Product code: XIP6220B

The xQlave<sup>®</sup> ML-DSA (Dilithium) Digital Signature Algorithm IP core secures critical infrastructures and operations against the threat of quantum computing. This IP core is engineered to provide robust, quantum-secure digital signatures, ensuring the integrity of data and authenticity of identities. It is designed to comply with the standard set by the U.S. National Institute of Standards and Technology (NIST). The xQlave<sup>®</sup> ML-DSA solution is tailored for high performance and moderate resource usage, ensuring your systems are future-proof and ready to face the challenges of tomorrow's cryptographic landscape.

## KEY FEATURES

- Quantum-secure digital signatures for future-proof security
- Compliant with ML-DSA standard by U.S. NIST
- Pure RTL without hidden CPU or software components
- Execution time is independent of any secret values
- Easy system integration with 64-bit interface
- Vendor agnostic FPGA/ASIC implementation

## APPLICATIONS

Quantum-resistant network and data security for:

- Digital signature generation and verification
- Secure communications
- Secure boot
- Secure data storage and transmission
- Quantum-resistant cryptographic protocols

## xQlave<sup>®</sup> ML-DSA-44-65-87 (CRYSTALS-Dilithium)

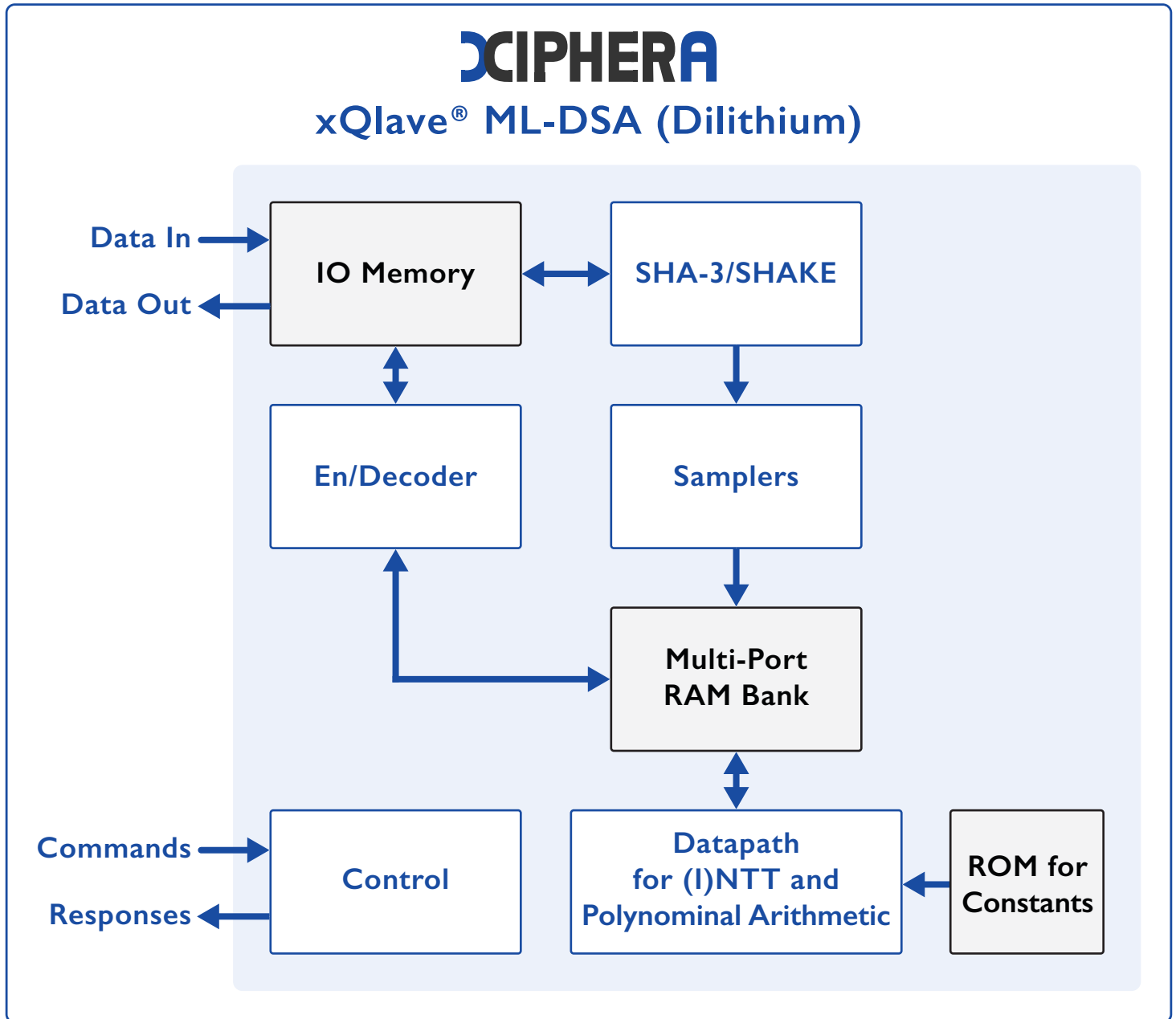
Xiphera's xQlave<sup>®</sup> PQC product family features quantum-secure cryptographic IP cores designed to protect against future quantum threats, all without relying on embedded CPUs or software components.

Our ML-DSA (Dilithium) Digital Signature Algorithm IP core, part of the xQlave<sup>®</sup> PQC family, is a powerful solution for secure digital signatures and it is designed to withstand attacks from quantum computers.

## BALANCED

XIP6220B

- Supports all security levels (ML-DSA-44/65/87)
- Moderate resource requirements (a few thousand LUTs in a typical FPGA setup)
- Fast performance with thousands of signatures/sec



## Deliverables

<ul style="list-style-type: none"> <li>✓ Encrypted RTL or source code</li> </ul>	<ul style="list-style-type: none"> <li>✓ Optional netlist</li> </ul>
<ul style="list-style-type: none"> <li>✓ Sample synthesis scripts</li> </ul>	<ul style="list-style-type: none"> <li>✓ Instantiation file</li> </ul>
<ul style="list-style-type: none"> <li>✓ Comprehensive simulation test bench, scripts &amp; guide</li> </ul>	<ul style="list-style-type: none"> <li>✓ Detailed datasheet and integration guide</li> </ul>

### 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.