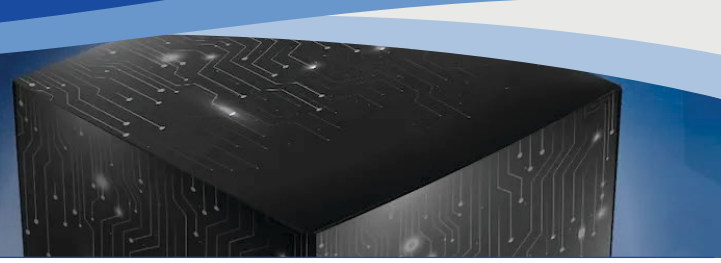
XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD



nQrux® Secure Boot

Product code: XIP7410B

nQrux® Secure Boot enhances system security by enabling quantum-secure authenticated boot, crucial for verifying the authenticity and integrity of binary images during the processor boot sequence. The protection is rooted in a hybrid digital signature scheme that utilises both ECDSA and ML-DSA. ML-DSA signatures are designed to counter threats from quantum computing, while ECDSA provides a reliable fallback to guard against potential vulnerabilities in the newer quantum-resistant algorithms.

KEY FEATURES

- Trusted computing enabler
- Secure cryptographic base for Root of Trust
- Digital signature verification for binaries
- Hybrid security mechanism (ECDSA/ML-DSA) protects against classical and quantum attacks
- Implements NIST standard FIPS 204 for quantum-secure digital signatures
- Secure from side-channel attacks
- Efficient and optimized architecture
- Pure digital logic with no CPU or software components
- Easy integration with 32-bit interface
- Vendor agnostic ASIC/FPGA implementation

APPLICATIONS

Quantum-resistant Secure Boot for:

- Secure system initialisation
- Data centers, edge, and cloud
- Space and satellite infrastructures
- Mission-critical applications
- Industrial and IoT environments
- Root of Trust

nQrux® Secure Boot

Quantum-Secure Authenticated Boot

Xiphera's nQrux® Secure Boot is implementable across FPGA and ASIC-based systems and incorporates a process-agnostic design approach.

This IP core is an essential solution for securing systems against both contemporary and emerging cryptographic threats, ensuring that only fully authenticated software is executed during system startups.

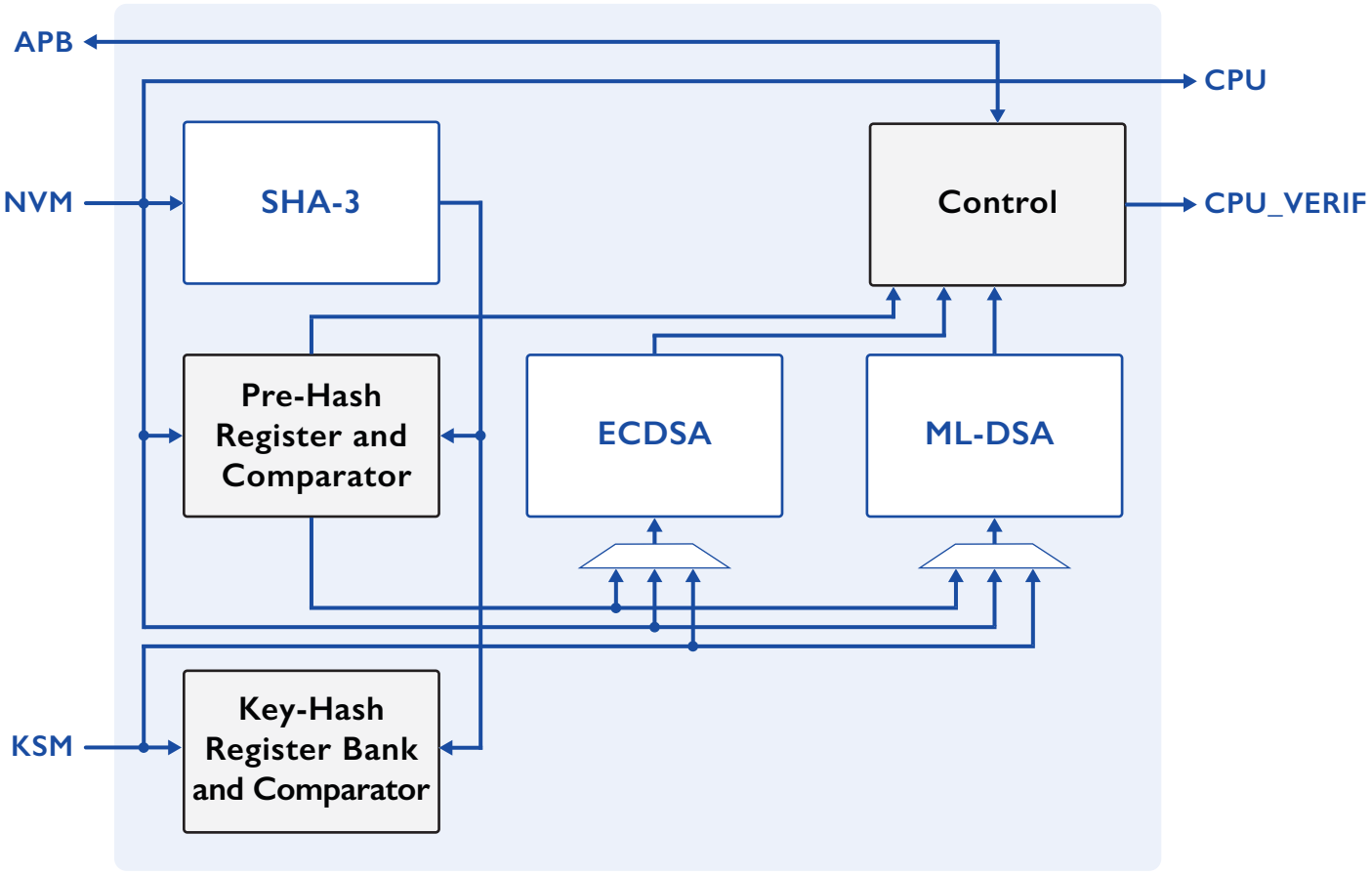
BALANCED

XIP7410B

- Supports all security levels (ECDSA-256/384/521 and ML-DSA-44/65/87)
- Moderate resource requirements (a few thousand LUTs in a typical FPGA setup)
- Fast performance with thousands of signature verifications/sec

XIPHERA

nQrux® Secure Boot



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