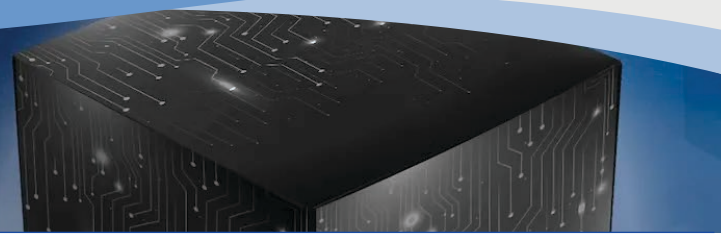
XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD



nQrux® Crypto Module

Product code: XIP7500

Xiphera's nQrux® Crypto Module IP core provides a comprehensive security platform that allows for customisation of top-notch cryptographic services, suitable for both microcontrollers and SoC systems. Choose the ideal security solution from an extensive selection of cryptographic features to protect data confidentiality, maintain integrity, and ensure authenticity within your systems. Cryptographic algorithms are based on CAVP-verified implementations. Crypto Module is designed for easy integration with ASIC and FPGA designs in a vendor agnostic design methodology.

KEY FEATURES

- Customisable security platform
- Optimised for microcontrollers & SoCs
- Comprehensive data protection
- Robust encryption & hashing
- Quantum-safe crypto option
- Pure RTL with no hidden CPU/software
- Industry standard compliance
- Efficient and optimised architecture
- Easy system integration
- Vendor agnostic ASIC/FPGA implementation

APPLICATIONS

Offload and accelerate cryptographic algorithms for:

- Secure communications
- Data integrity and authenticity
- Data at rest encryption
- HSM (Hardware Security Module)
- Cryptographic co-processor for SoC
- Key generation
- Secure Boot
- Root of Trust

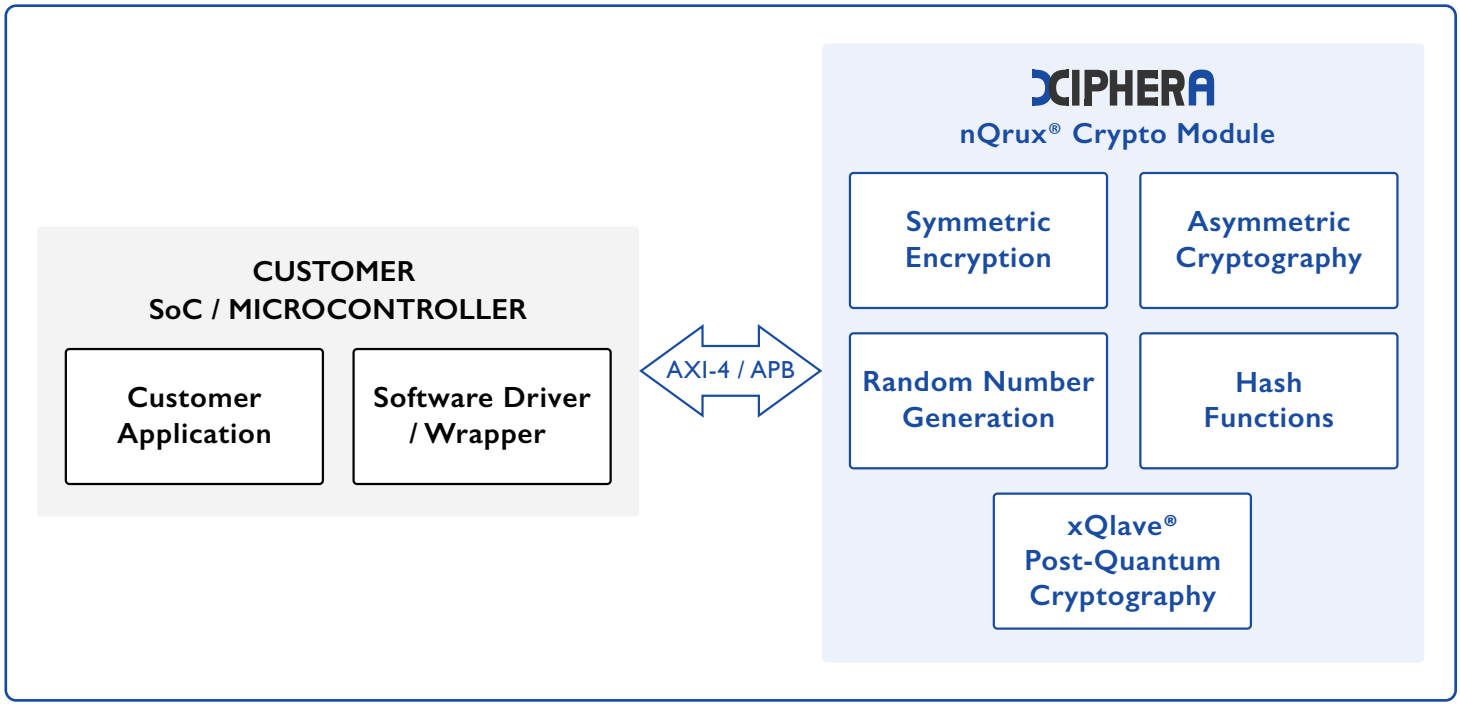
Selectable IP Cores for nQrux® Crypto Module

xQlave® PQC	• xQlave® ML-KEM (Kyber) • xQlave® ML-DSA (Dilithium)
Symmetric Encryption	• AES-128/256 - Various modes of operation e.g. GCM, CTR, XTS • ChaCha20-Poly1305 • Ascon
Asymmetric Cryptography	• ECDH(E)/ECDSA • X25519/Ed25519 • RSA Signature Verification

Hash Functions	• SHA-2
	  - HMAC + KHDF
	• SHA-3
	  - (c)SHAKE128/256

Random Number Generation	• True Random Number Generator • Pseudorandom Number Generator

The solution can be configured to reach the area & performance level required by your application



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