XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

CRYPTO QUANTIQUE

nQrux® Hardware Trust Engines with QDID PUF

Quantum-resilience and immutable device identity for cryptographic hardware modules

nQrux® Hardware Trust Engines, together with QDID PUF (Physically Unclonable Function), provide quantum-resistance and immutable device identity for cryptographic hardware modules.

Xiphera's nQrux® Hardware Trust Engines offer customisable cryptographic security modules, isolating cryptographic operations and application data into secure hardware elements. nQrux® solutions protect against both traditional and quantum computer attacks with Post-Quantum Cryptography (PQC).

QDID PUF from Crypto Quantique generates quantum-derived, secure, unclonable identities based on manufacturing variations unique to each semiconductor chip. The PUF, alongside other cryptographic primitives, forms the essential hardware root-of-trust in security implementations.

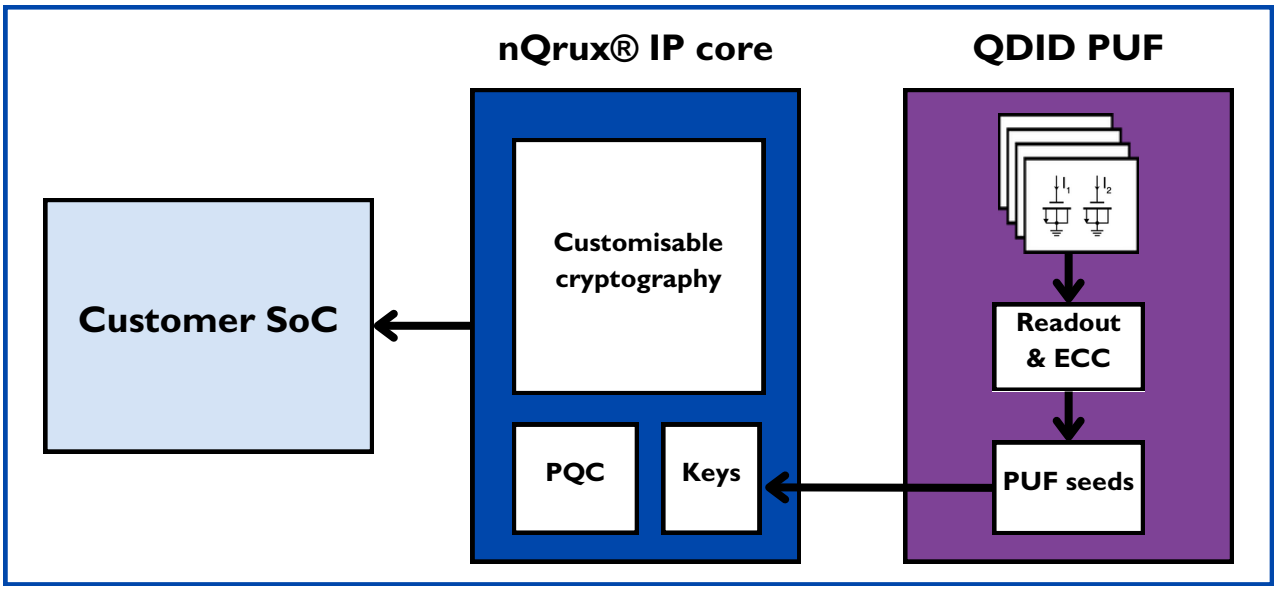
The combination of nQrux® Hardware Trust Engines and QDID PUF provides the adaptability and upgradeability required to secure the connected devices. QDID creates random numbers on demand, and the PUF technology reduces the size of flash memory needed, reducing power consumption and saving silicon area. As many industrial and governmental entities recommend implementing quantum-resilient hardware now, upgrading critical components with quantum-resilient nQrux® IP cores and QDID PUF protects the identities and core security of hardware devices into the foreseeable future.

Key features

- Pure hardware design with no hidden CPU or software components
- Implements Post-Quantum Cryptography (PQC)
- Unique device identity with PUF
- Standard compliance (NIST, IETF, IEEE)
- CAVP validation from NIST

Target industries

- Space and satellite technology
- Mission-critical infrastructure
- Automotive
- Industrial and IoT environments
- Medical



Use cases

- Secure communications
- Data integrity and authenticity
- Data at rest encryption
- HSM (Hardware Security Module)
- Key generation
- Secure boot
- Root of Trust
- Trusted computing

Benefits

- Protection against quantum attacks
- Customer-specific tailoring
- Extensive and modern portfolio of cryptographic algorithms
- Reduced power consumption and silicon area
- High security and ease of validation with HW-based cryptography

About Xiphera

Xiphera designs and implements hardware-based security using proven cryptographic algorithms. They offer secure and highly optimised cryptographic Intellectual Property (IP) cores, designed directly for FPGAs and ASICs without software components. The broad, fully in-house designed, and up-to-date portfolio, including implementations of Post-Quantum Cryptography, enables cost-effective development projects with fast time-to-market.

www.xiphera.com
sales@xiphera.com

About Crypto Quantique

Crypto Quantique is the first software and IP (Intellectual Property) company to create end-to-end IoT security that can be seamlessly integrated from chip design to cloud connectivity. It has partnerships with major semiconductor companies including STMicroelectronics, Microchip, and Renesas and OEMs like Würth Elektronik. Crypto Quantique is headquartered in London, UK, and has offices in the US, Europe and Taiwan.

www.cryptoquantique.com
info@cryptoqantique.com