XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

We protect your critical systems by designing security directly into hardware.

HARDWARE SECURITY IP SOLUTIONS

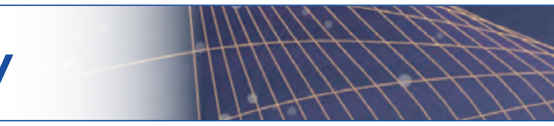
At Xiphera, we specialise in designing cutting-edge, hardware-based security solutions using standardised cryptographic algorithms. With our extensive expertise in cryptography, deep knowledge of reprogrammable logic, and vast experience in system design, we are dedicated to protecting your critical information and assets.

ASIC / FPGA

CYBERSECURITY™
MADE IN EUROPE

www.xiphera.com

xQlave® Post-Quantum Cryptography



xQlave® 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.

xQlave® ML-KEM-512/768/1024 (CRYSTALS-Kyber)

A powerful solution for secure key exchange, designed to withstand attacks from quantum computers.

Balanced: XIP6110B

xQlave® ML-DSA-44-65-87 (CRYSTALS-Dilithium)

A quantum-safe solution for digital signatures, designed to protect data authenticity and integrity.

Balanced: XIP6220B

nQrux® Hardware Trust Engines

nQrux® Hardware Trust Engines provide hardware-based cryptographic solutions tailored for high-security environments. These engines offer full hardware isolation for cryptographic operations, ensuring performance and security in critical applications without relying on software.

nQrux® Crypto Module

Offers a range of cryptographic features for protecting data, and ensuring confidentiality, integrity & system authenticity.

Selectable IP Cores for nQrux® Crypto Module:

- xQlave® PQC
- Symmetric Encryption
- Asymmetric Cryptography
- Hash Functions
- Random Number Generation

Code: XIP7500

nQrux® Secure Boot

Provides quantum-resistant authentication, ensuring boot sequence authenticity and integrity.

Balanced: XIP7410B

nQrux® CCE (Confidential Computing Engine)

Protects data, code execution, and AI models with TLS 1.3 for secure communication.

Code: XIP7700

Security Protocols

High-performance protection for communications across critical layers of the OSI model. These protocols ensure data integrity, confidentiality, and robust protection against cyber threats.

MACsec AES256-GCM

Secures point-to-point communications with AES-GCM encryption.

Balanced: XIP1213B
High-speed: XIP1213H
Extreme-speed: XIP1213E

IPsec AES256-GCM

Protects network traffic with AES-GCM for speeds up to 200 Gbps.

Extreme-speed: XIP7013E

TLS 1.3

Ensures secure client-server connections over the Internet.

Compact: XIP7131C

Random Number Generation

Random number generation IP cores for providing high-quality, hardware-based entropy sources for cryptographic operations.

True Random Number Generator (TRNG)

Balanced: XIP8001B

Pseudorandom Number Generator (PRNG)

Balanced: XIP8103B / **High-speed:** XIP8103H

Symmetric Encryption

High-performance, energy-efficient cryptography, ensuring data confidentiality and integrity with compact resource use.

AES-GCM

Balanced: XIP1113B / **High-speed:** XIP1113H / **Extreme-speed:** XIP1113E

AES-CTR

High-speed: XIP1103H

AES-XTS

Balanced: XIP1183B / **High-speed:** XIP1183H

VERSATILE AES

Balanced: XIP1123B

ChaCha20-Poly1305

Balanced: XIP2113B / **High-speed:** XIP2113H

Ascon

Balanced: XIP2201B

Asymmetric Cryptography

The asymmetric cryptography IP cores offer robust, hardware-based solutions for key exchange, digital signatures, and encryption.

ECC Accelerator

High-speed: XIP4200H

NIST P-256/P-384 ECDH+ECDSA

Compact: XIP41X3C

Curve25519 Key Exchange

Compact: XIP4001C

Curve25519 Key Exchange & Digital Signature

Compact: XIP4003C

RSA Signature Verification

Compact: XIP5012C

Hash Functions

Hash function IP cores ensure data security and integrity, supporting both SHA-2 and SHA-3 algorithms.

SHA-3

Compact: XIP3030C / **High-speed:** XIP3030H

SHA-2

Compact: XIP3327C / **Balanced:** XIP3322B, -23B, -24B

Your trusted partner for hardware-based security solutions

Xiphera's product portfolio consists of efficient Intellectual Property (IP) cores for proven cryptographic primitives and security protocols. Our pure hardware-based design philosophy offers performance advantages and first grade security.

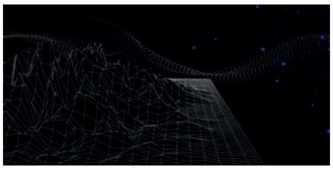
xQlave® Post-Quantum Cryptography

nQrux® Hardware Trust Engines

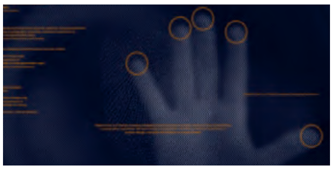
Security Protocols

Random Number Generation

Symmetric Encryption



Asymmetric Cryptography



Hash Functions

Contact us

Our global sales network covers continents around the world, enabling us to offer global customer service and support.

HEADQUARTERS
Tekniikantie 12
02150 Espoo, Finland
Tel: +358 20 730 5252
e-mail: sales@xiphera.com

North America
Akyra Pagoulatos
Tel: +1 408 887 2261
e-mail: akyra.pagoulatos@xiphera.com

Europe
Tomi Jalonen
Tel: +31 6 45540652
e-mail: tomi.jalonen@xiphera.com

Japan
Spinnaker Systems Inc.
Tel: +81 3 6277 4985
e-mail: info_s@spinnaker.co.jp

Israel
IPro Silicon IP Ltd.
Tel: +972 (545) 441579
e-mail: mauro@ipro-great-ip.com

India
Muspark Technologies
Tel: +91 98800 39083
e-mail: parag.kulkarni@musparktech.com

Taiwan
Kaviaz Technology
Tel: +886 3 516 3168
e-mail: info@kaviaztech.com

XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

www.xiphera.com