XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Asymmetric Cryptography

Product codes
ECC Accelerator: XIP4200H
ECDH/ECDSA: NIST Curves: XIP41X3C
Curve25519: XIP4001C, XIP4003C
RSA Signature Verification: XIP5012C

Xiphera's Asymmetric Cryptography IP cores provide cutting-edge security solutions designed for robust public-key operations, including encryption, digital signatures, and key exchanges. These solutions are optimised for both performance and resource efficiency, offering versatile functionality across various cryptographic protocols. All of these Xiphera in-house designed IP cores are optimised for efficiency and optimal performance in both FPGA and ASIC implementations.

KEY FEATURES

- Moderate resource requirements
- High throughput
- Compliant with FIPS 186-5, SP 800-186, SP 800-56A, RFC 7748, RFC 8446, and more
- Supports all NIST P curves and user-specified elliptic curves
- Secure architecture with side-channel protections
- Fully RTL-based with no CPU or software components
- Efficient and optimised architecture
- Easy system integration
- Vendor agnostic FPGA/ASIC implementation

APPLICATIONS

Versatile solutions for secure environments:

- Secure data communication
- Digital signature verification
- Key exchange protocols
- High-performance cryptographic operations

Asymmetric Cryptography

ECC Accelerator

HIGH-SPEED *(XIP4200H)*

- >1K ops/sec for key generation on NIST P-256
- ~36 kLUTs
- Supports all NIST P Curves
- Protections against multi-trace side-channel attacks

NIST P-256/P-384 ECDH + ECDSA

COMPACT *(XIP41X3C)*

- Several 100s key agreements or signatures/sec
- ~1.12 kLUTs

Curve25519 Key Exchange

COMPACT *(XIP4001C)*

- More than 100 key exchange ops/sec
- ~1 kLUTs

Curve25519 Key Exchange & Digital Signature

COMPACT *(XIP4003C)*

- More than 100 key exchange or signatures ops/sec
- ~1 kLUTs

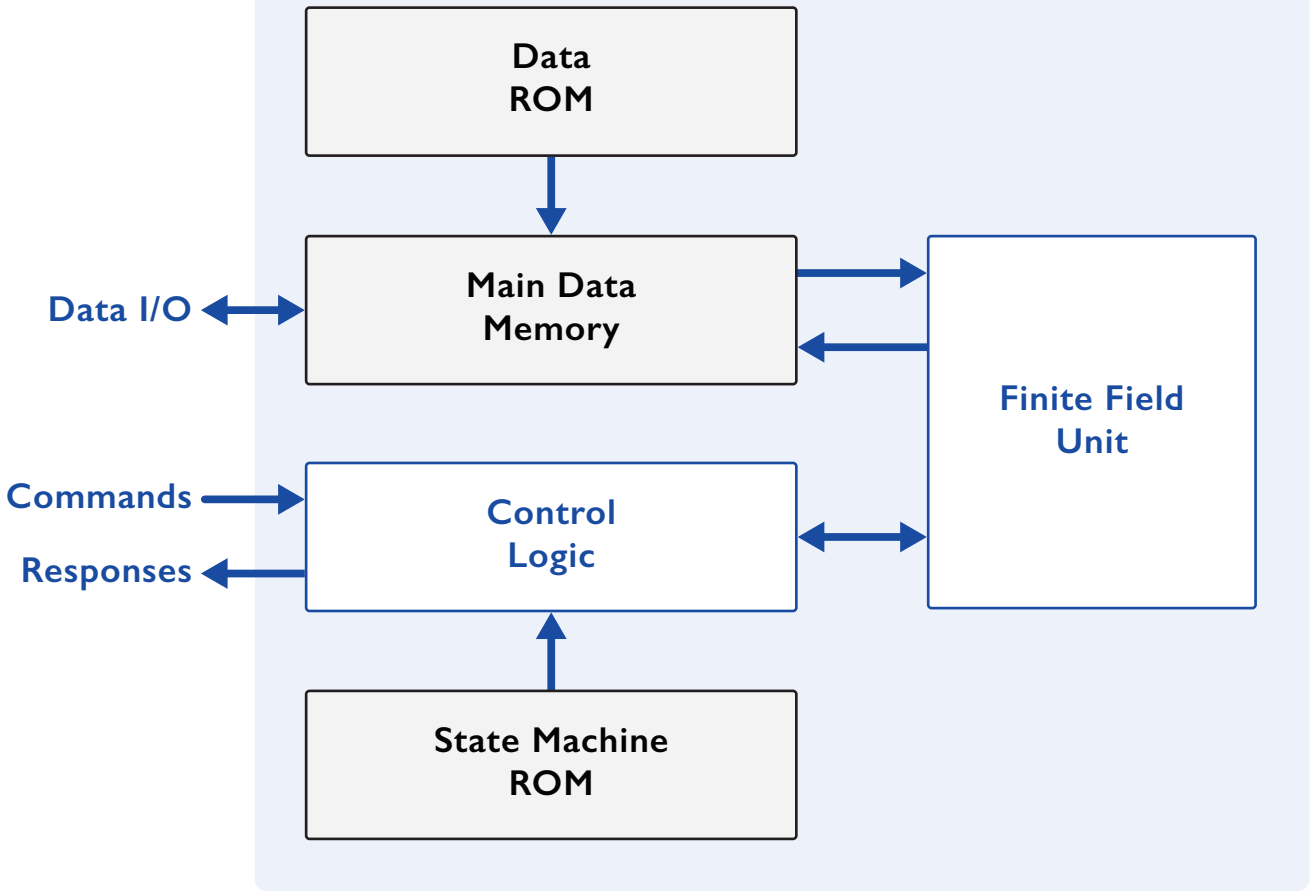
RSA Signature Verification

COMPACT *(XIP5012C)*

- More than 10 signatures verification ops/sec
- ~0.5 kLUTs

XIPHERA

ECC Accelerator



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