XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

Hash Functions

Product codes
SHA-3: XIP3030C, XIP3030H
SHA-2: XIP3322B, XIP3323B, XIP3324B, XIP3327C

Xiphera's comprehensive hash function IP portfolio ensures the security and integrity of data through robust cryptographic standards. Supporting both SHA-2 and SHA-3 algorithm families, these solutions provide versatile functionality for various applications, from data integrity verification to password security. Our hash function portfolio is powered by Xiphera's in-house designed IP cores, optimised for efficiency and high performance in FPGA and ASIC implementations.

KEY FEATURES

- Optimised resource requirements
- High throughput - several 10s of Gbps on single instance
- Constant latency
- Compliant with relevant NIST standards
- CAVP validated by NIST
- Supports SHA-3, SHA-2, and related functions
- Pure RTL without hidden CPU or software components
- Efficient and optimised architecture
- Easy system integration
- Vendor agnostic FPGA/ASIC implementation

APPLICATIONS

Boost your security with advanced hash functions:

- Data integrity verification
- Password security
- Digital signatures
- Key derivation
- Securing blockchain transactions

Hash Functions

Reliable, versatile, and secure solutions

Our hash function IP cores support multiple variants, offering flexibility and robust security features.

SHA-3

Our IP cores support SHA3-224, SHA3-256, SHA3-384, SHA3-512, and related functions such as SHAKE, cSHAKE, KMAC, TupleHash, and ParallelHash.

COMPACT
XIP3030C
- 10s of Mbps
- Only ~1 kLUTs (FPGA)

HIGH-SPEED
XIP3030H
- 10s of Gbps
- Below 7 kLUTs (FPGA)

SHA-2

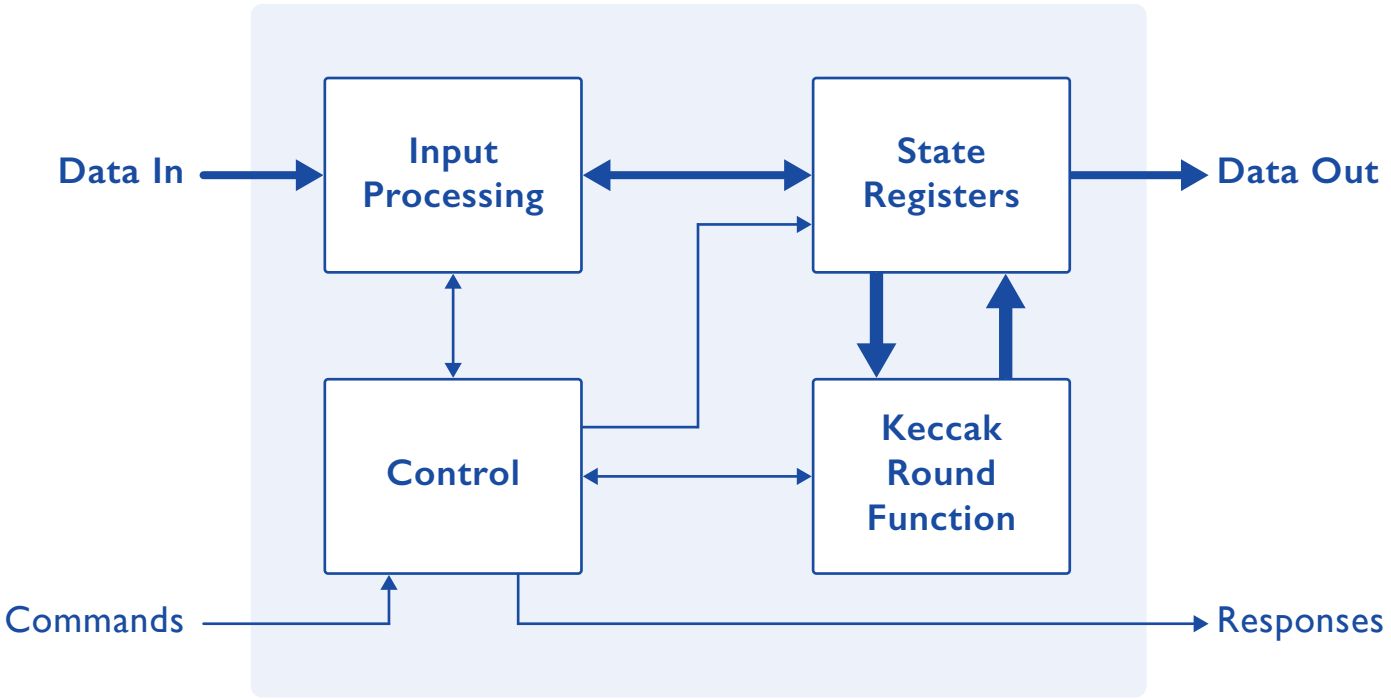
The SHA-2 IP cores support SHA-256, SHA-384, and SHA-512. All variants have support for HMAC and HKDF.

COMPACT
XIP3327C
- SHA-256 / 512
- 10s of Mbps
- From 1.2 kLUTs (FPGA)

BALANCED
XIP3322B, -23B, -24B
- SHA-256 / 384 / 512
- 100s of Mbps
- From 1.4 kLUTs (FPGA)

XCIPHERA

SHA-3 Hash Function - High-speed



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.

XCIPHERA
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