XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

AES
Symmetric Encryption

Product codes
AES-GCM: XIP1113B, XIP1113H, XIP1113E
AES-CTR: XIP1103H
Versatile AES: XIP1123B
AES-XTS: XIP1183B, XIP1183H
SIDE-CHANNEL PROTECTED AES: XIP1113B

Xiphera's AES symmetric encryption IP cores ensure robust encryption and decryption, providing data confidentiality and integrity with the Advanced Encryption Standard algorithm. These solutions support various AES modes and offer versatile functionality for secure data communication and storage protection. Xiphera's in-house designed AES encryption engines are optimised for efficiency and high performance in both FPGA and ASIC implementations.

KEY FEATURES

- Optimised resource requirements
- High throughput - up to 100s of Gbps
- Compliant with NIST standards
- CAVP validated by NIST
- Support for various AES modes including GCM, CTR, XTS, ECB, CBC, CFB, and OFB
- Pure RTL without hidden CPU or software components
- Easy system integration
- Vendor agnostic FPGA/ASIC implementation
- Side channel protection

APPLICATIONS

Enhance your security with advanced AES encryptions:

- Secure data communication
- Data protection in storage
- MACsec/IPsec/TLS
- Optical transport
- WPA3 support
- IoT device security
- Automotive security

AES Symmetric Encryption

Cutting-edge AES encryption solutions

Our AES IP cores offer various modes, ensuring performance, flexibility, and robust security.

AES-GCM

BALANCED *(XIP1113B)*
- Hundreds of Mbps
- ~3 kLUTs

HIGH-SPEED *(XIP1113H)*
- Up to 100 Gbps
- ~26 kLUTs

EXTREME-SPEED *(XIP1113E)*
- 100s of Gbps
- Starting from 60 kLUTs

AES-CTR

HIGH-SPEED *(XIP1103H)*
- Up to 100 Gbps
- ~15 kLUTs

VERSATILE AES

BALANCED *(XIP1123B)*
- Several Mbps
- Only ~4 kLUTs

AES-XTS

BALANCED *(XIP1183B)*
- Several Mbps
- Only ~6 kLUTs

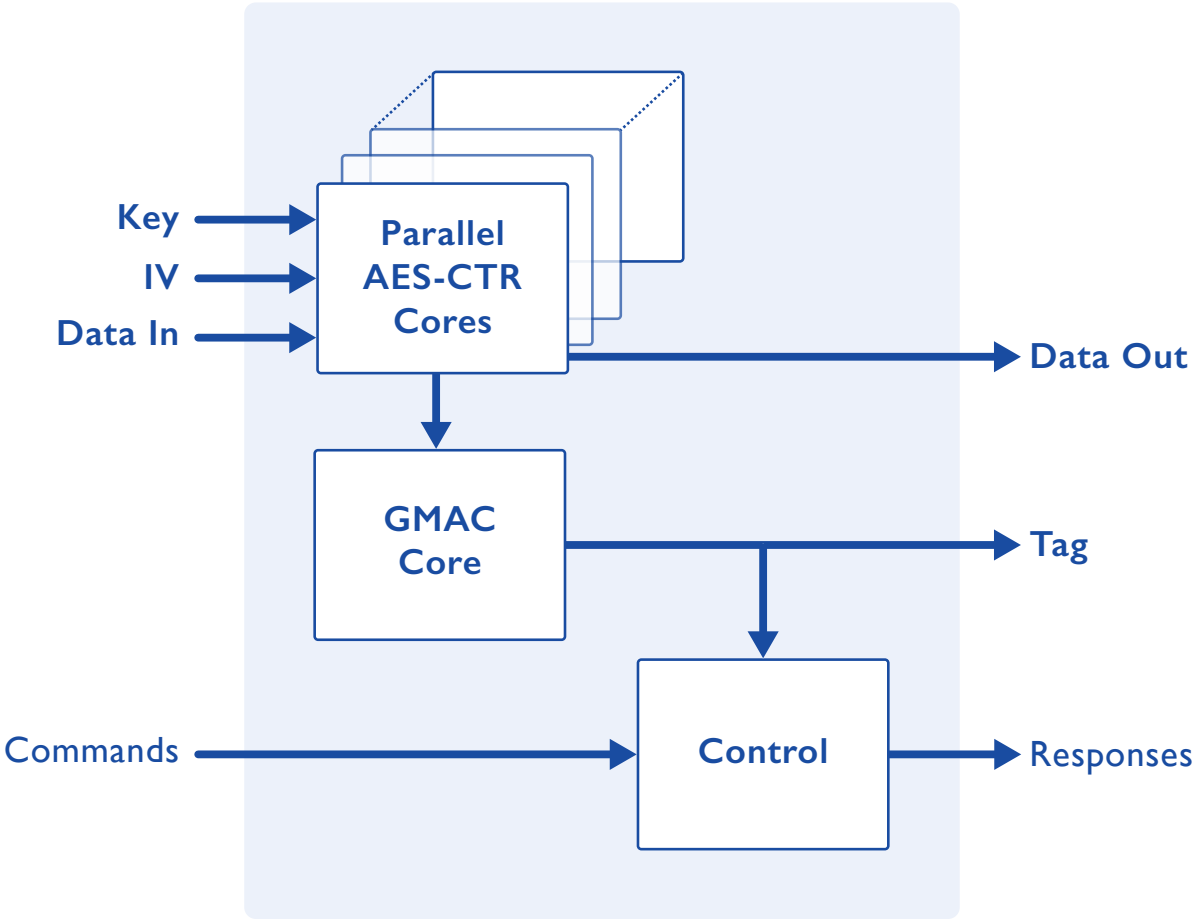
HIGH-SPEED *(XIP1183H)*
- 10s of Gbps
- ~33 kLUTs

Side-Channel Protected AES

BALANCED *(XIP1133B)*
- Side-channel counter measures

We also offer ChaCha20-Poly1305 and Ascon symmetric encryption solutions. For more details, please see our dedicated product flyer.

AES-GCM Extreme-speed Symmetric Encryption



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

Email: sales@xiphera.com
Phone: +358 20 730 5252
Web: www.xiphera.com