XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

ChaCha20-Poly1305 / Ascon

Symmetric Encryption

Product codes
ChaCha20-Poly1305: XIP2113B, XIP2113H
Ascon: XIP2201B

Xiphera's ChaCha20-Poly1305 and Ascon symmetric encryption IP cores provide robust security for a wide range of applications. ChaCha20-Poly1305 combines the high-speed ChaCha20 stream cipher with the Poly1305 authenticator, delivering both encryption and authentication. Ascon, as a lightweight encryption algorithm, is ideal for constrained environments such as IoT devices. Both of these Xiphera in-house designed IP cores are optimised for efficiency and optimal performance in both FPGA and ASIC implementations.

KEY FEATURES

- Optimised resource requirements
- High throughput - up to 50 Gbps on ChaCha20-Poly1305
- Compliant with modern cryptographic standards
- Quantum-secure
- Pure RTL without hidden CPU or software components
- Easy system integration
- Vendor agnostic FPGA/ASIC implementation

APPLICATIONS

Enhance your security with advanced encryption engines:

- Data centres and cloud environments
- IPsec/TLS/DTLS/SSH protocols
- Data communications
- IoT devices
- Wearables
- Low-power devices and constrained environments

ChaCha20-Poly1305 / Ascon Symmetric Encryption

Our ChaCha20-Poly1305 and Ascon IP cores provide versatile encryption solutions, ensuring optimal performance, flexibility, and robust security.

ChaCha20-Poly1305

BALANCED

XIP2113B

- Several Gbps
- Only ~7.3 kLUTs

HIGH-SPEED

XIP2113H

- 10s of Gbps
- ~24 kLUTs

Ascon

The lightweight Ascon algorithm is ideal for constrained environments, such as IoT devices.

BALANCED

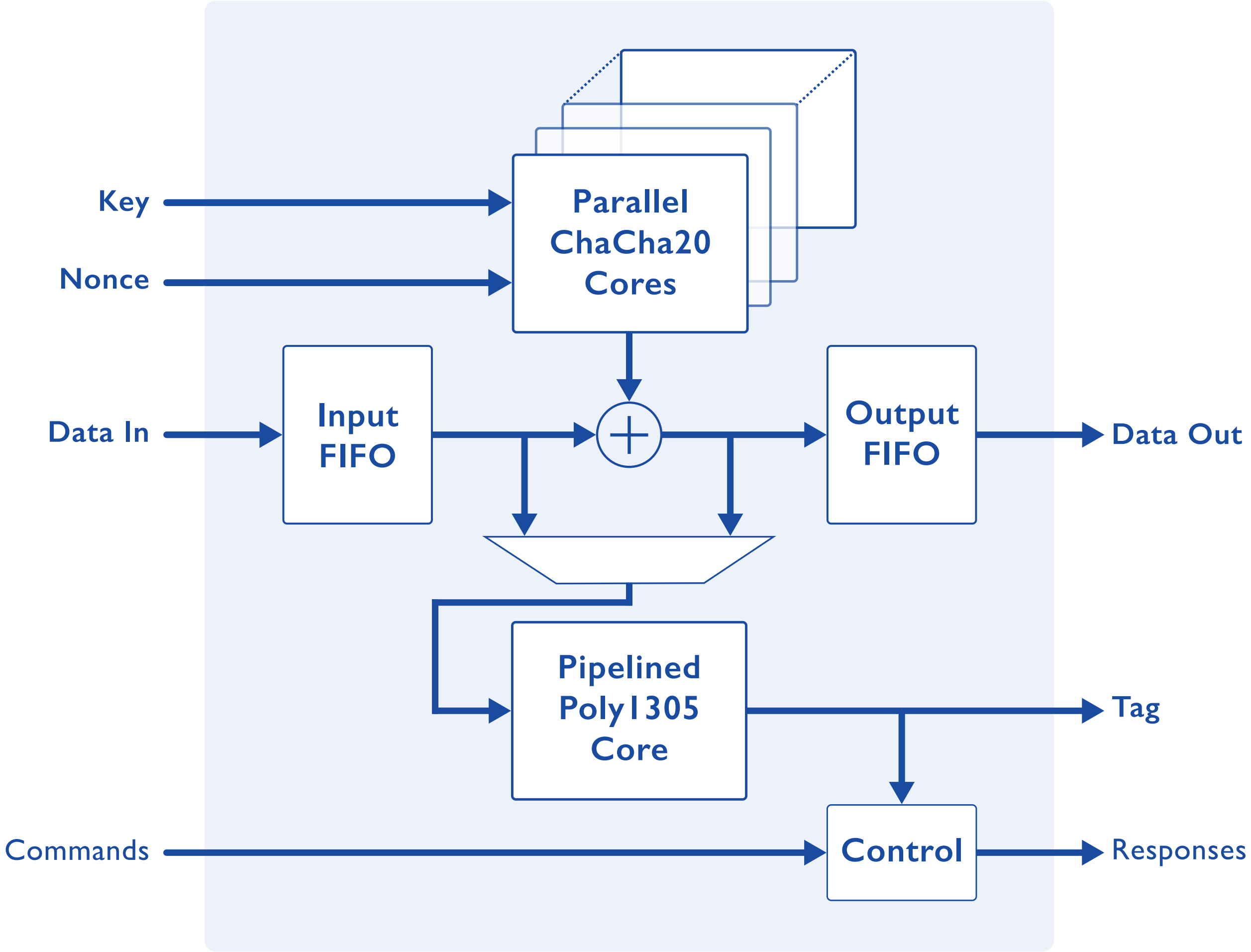
XIP2201B

- 100s of Mbps
- Only ~2.3 kLUTs

We also offer AES symmetric encryption solutions. For more details, please see our dedicated product flyer.

XIPHERA

ChaCha20-Poly1305 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

Tekniikantie 12
02150 Espoo
Finland

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