XIPHERA
PEACE OF MIND IN A DANGEROUS WORLD

MACsec

Product codes: XIP1213B, XIP1213H, XIP1213E

MACsec is a point-to-point protocol located on layer two (Data Link) of the OSI model. Xiphera's comprehensive MACsec solution portfolio safeguards the confidentiality and integrity of data transmitted over point-to-point communication links, assured by the Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) with 256-bit key length. The underlying cryptographic engines in the MACsec solutions are powered by Xiphera's in-house designed AES-GCM Intellectual Property (IP) cores.

KEY FEATURES

- Optimised resource requirements
- High throughput up to 100s of Gbps
- Compliant with IEEE 802.1AE-2018
- Powered by AES256-GCM
- Pure RTL without hidden CPU or software components
- Efficient and optimised architecture
- Easy system integration
- Vendor agnostic FPGA/ASIC implementation

APPLICATIONS

Leverage MACsec for advanced network security:

- Interconnect security for cloud services and data centers
- Enhanced IP/MPLS network protection
- IoT device protection within LAN
- Automotive ethernet communication
- Secure point-to-point video links

MACsec AES256-GCM

Tailored for every network requirement

BALANCED

XIP1213B

- Minimal resource use with 9,891 ALMs, optimised for cost-effective FPGAs
- Up to several Gbps

HIGH-SPEED

XIP1213H

- 53,842 ALMs; designed for efficiency in typical FPGA setups
- Up to tens of Gbps, ideal for 10/25/40 Gbps links

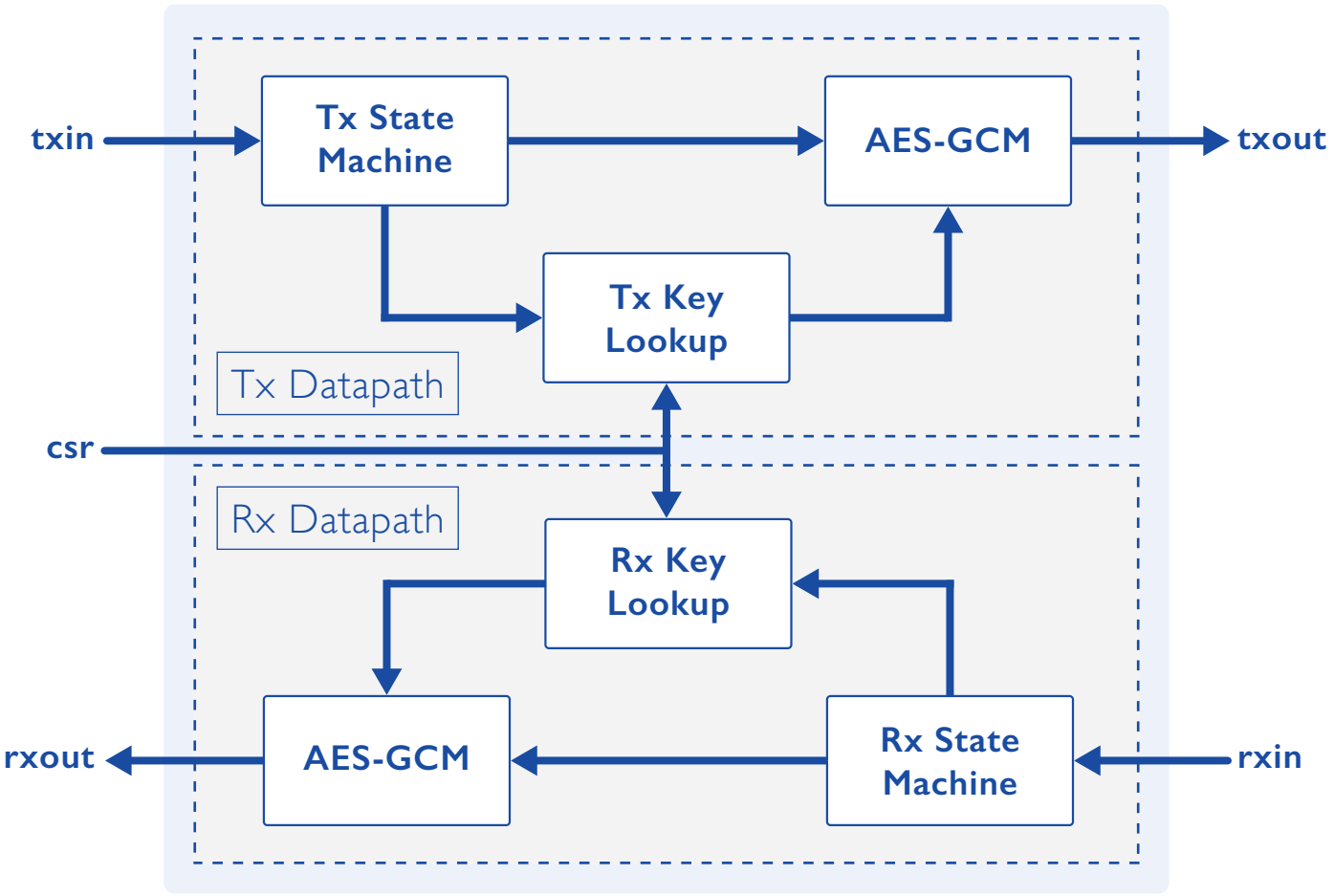
EXTREME-SPEED

XIP1213E

- 217,213 ALMs; no multipliers/DSP blocks
- Constant latency
- Scalable databus width (128/256/512-bit)
- Hundreds of Gbps, suitable for ultra-fast networks and data centres

XIPHERA

MACsec



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