XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

IPsec

Product codes: XIP7213E, XIP7013E

IPsec (Internet Protocol Security) is a widely implemented protocol to secure communications across the Internet. Xiphera’s IPsec core enhances secure communication at layer three (Network) of the OSI model, ensuring the authenticity and confidentiality of data traffic. It leverages the Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) with a 256-bit key length, to secure device communications with the IPsec protocol.

Xiphera's scalable extreme-speed IPsec IP core is tailored for high-bandwidth applications, ranging from 10 Gbps to 200 Gbps links. Designed for seamless integration, our IP core supports a vendor-agnostic design methodology, making it adaptable across various high-end FPGA or ASIC environments.

KEY FEATURES

- Moderate resource requirements
- High throughput up to 100s of Gbps
- Compliant with RFC 4303
- Powered by AES256-GCM
- Supports encryption and decryption
- Tunnel and Transport modes
- Streaming interface for simple integration
- Independent Transmit and Receive channels
- Up to 256 Security Associations (SA's)
- Constant Latency
- Efficient and optimised architecture
- Easy system integration
- Vendor agnostic FPGA/ASIC implementation

APPLICATIONS

Enhance your network with advanced IPsec protections for:

- Data Center, Cloud, and Edge Security
- Virtual Private Networks (VPNs)
- FPGA-based SmartNICs

IPsec AES256-GCM

Secure and high-performance device communications over networks

STANDALONE IPsec

XIP7213E

- Standalone IPsec protocol implementation
- Compliant with RFC 4303 and RFC 4035
- Tunnel and Transport mode support
- Up to 256 Security Associations
- Flexible key management interface

ESP FRAME AEAD

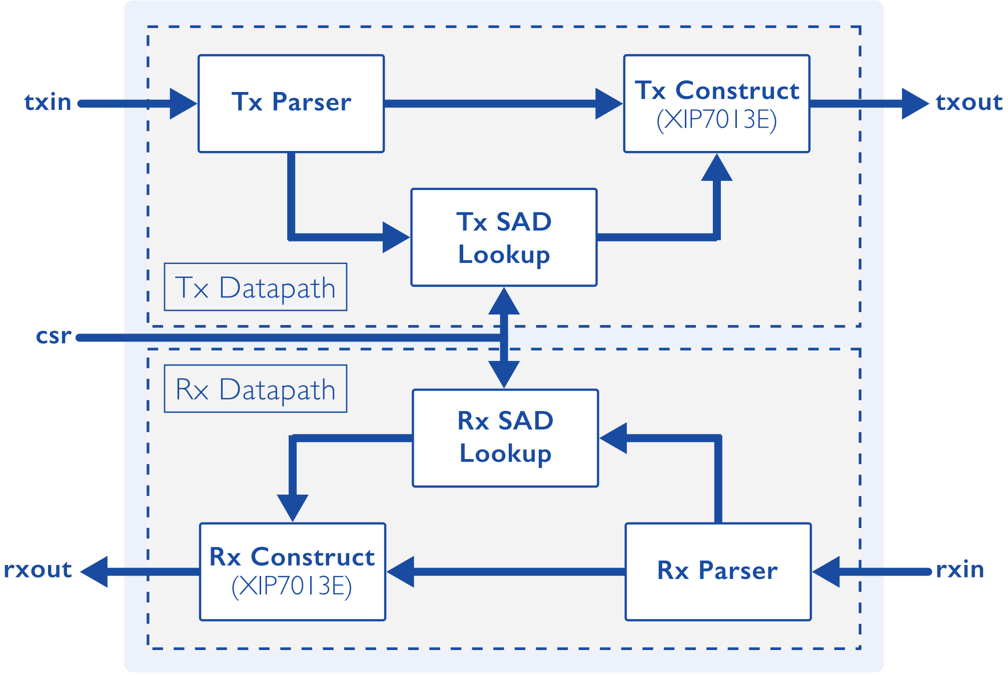
XIP7013E

- Moderate resource requirements with no multipliers or DSP blocks
- Encapsulating Security Payload (ESP) frame AEAD processing
- Compliant with RFC 4303

- Packet processing performed in five different modes: authentication and encryption with or without Initialisation Vector, or passing payload as it is.
- Flexible packet processing enables authentication and encryption with or without Initialisation Vector, or passing payload as it is.
- IPsec implementation can be adapted with enhancements and optimisations, based on customer requirements and the selected hardware architecture.
- Optimisable implementation adapts to customer requirements and hardware architecture.

XIPHERA

Standalone IPsec IP Core - XIP7213E



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