



XIP1211H: MACSEC AES128-GCM

MACsec (IEEE 802.1AE) IP Core

Product Brief
ver. 1.0.1
March 2, 2020

sales@xiphera.com

Introduction

XIP1211H from Xiphera is a high-speed¹ Intellectual Property (IP) core implementing the MACsec protocol as standardized in IEEE Std 802.1AE-2018 [2].

The MACsec protocol defines a security infrastructure for Layer 2 (as per the OSI model) traffic by assuring that a received frame has been sent by a transmitting station that claimed to send it. Furthermore, the traffic between stations is both encrypted to provide data confidentiality and authenticated to provide data integrity.

XIP1211H uses Advanced Encryption Standard [1] with 128 bits long key in Galois Counter Mode (AES-GCM) [3] to protect data confidentiality, data integrity and data origin authentication. The cipher suite is denoted either as GCM-AES-XPN-128 if the eXtended Packet Numbering (XPN)² is in use, or as GCM-AES-128 if XPN is not in use. Both GCM-AES-128 and GCM-AES-XPN-128 use Xiphera's IP core XIP1111H as the underlying building block for AES-GCM.

XIP1211H is best suited for traffic on 10/25/40 Gbps links³. XIP1211H can also in selected cases be retrofitted to existing FPGA designs without requiring a board re-spin, either if there are enough FPGA resources available or if a pin-compatible FPGA with additional resources can be used.

Key management (including key exchange) lies outside the scope of 802.1AE, and hence the functionality of XIP1211H is based on the assumption that key management is performed by externally to XIP1211H.

XIP1211H has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP1211H does not rely on any FPGA manufacturer-specific features.

¹Xiphera's high-speed (denoted by 'H' at the end of the ordering code) IP cores are designed to maximize the achievable FPGA performance.

²The eXtensible Packet Numbering (XPN), which was added to the MACsec standard in 2013, extends the packet number (PN) to 64 bits from the original 32 bits.

³The maximum achievable linerate depends on the FPGA.

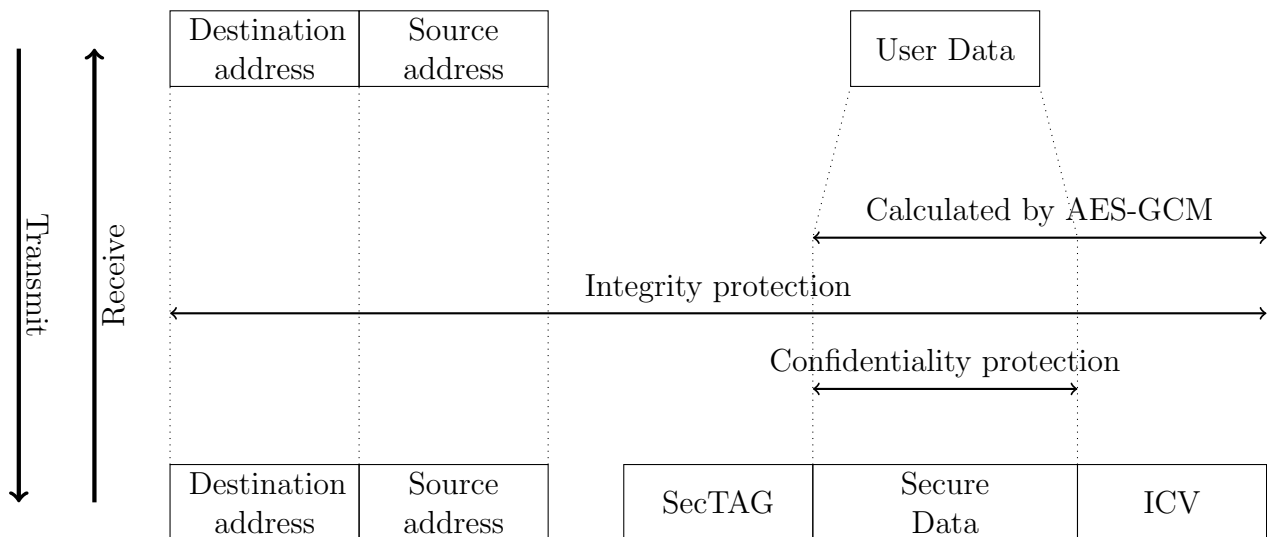


Figure 1: MACsec frame structure. Adapted from Figure 8-1 in [2].

Key Features

- **Moderate** resource requirements: The entire XIP1211H requires less than 37000 Adaptive Lookup Modules (ALMs) (Intel[®] Stratix[®]10), and does not require any multipliers or DSPBlocks in a typical FPGA implementation.
- **Performance:** XIP1211H achieves a throughput in the tens of Gbps range⁴, for example up to 40+ Gbps in Xilinx[®] UltraScale+[™] MPSoC family.
- **Standard Compliance:** XIP1211H is fully compliant with the MACsec protocol as standardized in IEEE Std 802.1AE-2018 [2]. The cipher suite (GCM-AES-128 or GCM-AES-XPB-128) is fully compliant with the Advanced Encryption Algorithm (AES) standard [1], as well as with the Galois Counter Mode (GCM) standard [3].
- **Test Vector Compliance:** XIP1211H passes the relevant test vectors specified in Annex C of IEEE Std 802.1AE-2018 [2].

Functionality

The functionality of XIP1211H is divided into the transmit (Tx) and receive (Rx) datapaths, which operate independently of each other. The underlying cipher suite GCM-AES-(XPB)-128 is consequently instantiated twice, both for the Rx and Tx datapaths. The high-level structure of MACsec frame is presented in Figure 1 with the goal of understanding better the functionality of both datapaths.

MACsec operation is based on the concepts of unidirectional Secure Channels (SC) and Security Associations (SA) within each channel. Each SA uses its own Secure Association Key (SAK); establishing and managing keys is not part of the MACsec standard.

A high-level functionality of the Tx datapath (See also Figure 2) includes the SAK key lookup based on the Association Number (AN)⁵ value. Additionally, a monotonically increasing

⁴The highest throughput is achieved for long messages.

⁵AN is a two bits long value identifying up to four different SAs within the context of an SC.

Packet Number (PN)⁶ is calculated, and this will be used as the Initialization Vector (IV) by the cipher suite.

The cipher suite in the transmit datapath of XIP1211H operates in the encryption and Integrity Check Value (ICV) calculation mode, meaning that it encrypts the incoming plaintext blocks into ciphertext blocks, and additionally calculates a 128 bits long ICV value from both the incoming plaintext and associated data. The original Ethernet frame is updated by adding a Security Tag (SecTAG)⁷ starting with the MACsec type (0x88E5), encrypting the original EtherType with the payload, and appending the calculated ICV to the end of the original message.

After receiving an incoming MACsec frame, the first functionality of the Rx datapath is the SAK key⁸ lookup. After the right SAK has been identified, the cipher suite in the receive path of XIP1211H operates in the decryption and tag validity checking mode. This means that the cipher suite decrypts the incoming ciphertext blocks into plaintext blocks, and validates the received ICV by calculating the ICV from the incoming ciphertext and associated data blocks and comparing the resulting value with the received ICV value. As defined by the GCM mode of operation, associated data is included in the ICV calculation. If the ICV checking is successful, the receive datapath returns the original frame by removing the SecTAG and ICV, and replacing the MACsec type with the original EtherType.

XIP1211H also supports the bypass mode, where an incoming packet passes through the XIP1211H unaltered.

Block Diagram

The internal high-level block diagram of XIP1211H is depicted in Figure 2.

Interfaces

The external interfaces of XIP1211H are depicted in Figure 3, and they can be grouped into five logical groups:

- One Control and Status Register interface, I/O signal names beginning with `csr`
- Two Transmit interfaces, I/O signal names beginning with `txin` and `txout`
- Two Receive interfaces, I/O signal names beginning with `rxin` and `rxout`

This Product Brief describes a high-level overview of the functionality and capabilities of XIP1211H. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

Table 1 presents the FPGA resource requirements for representative implementations on two different FPGA architectures. On request, the resource estimates can also be supplied for other

⁶PN was originally standardized as 32 bits long, but support for XPN has extended it to 64 bits.

⁷The length of the SecTAG is either 8 or 16 bytes.

⁸The number of SAKs is parameterizable in XIP1211H with the default value being eight (8).

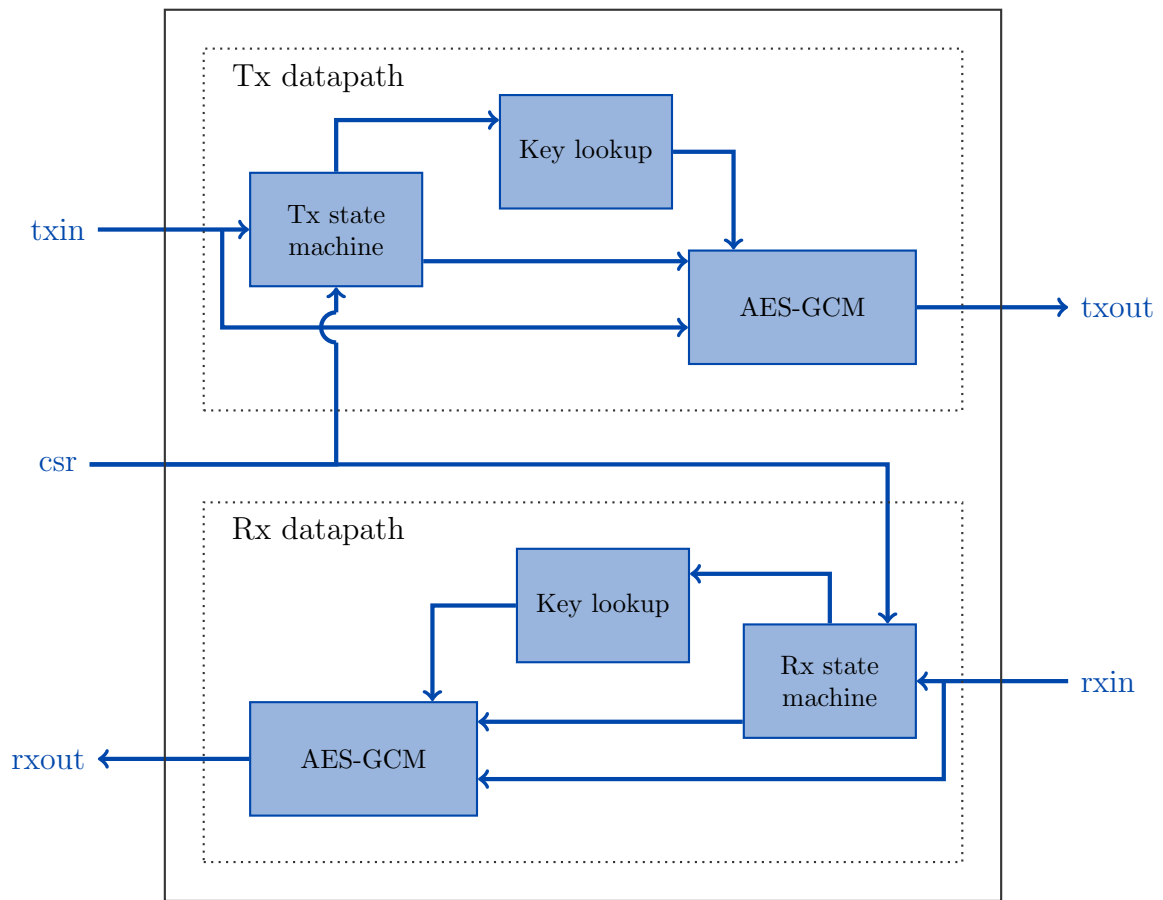


Figure 2: Internal high-level block diagram of XIP1211H

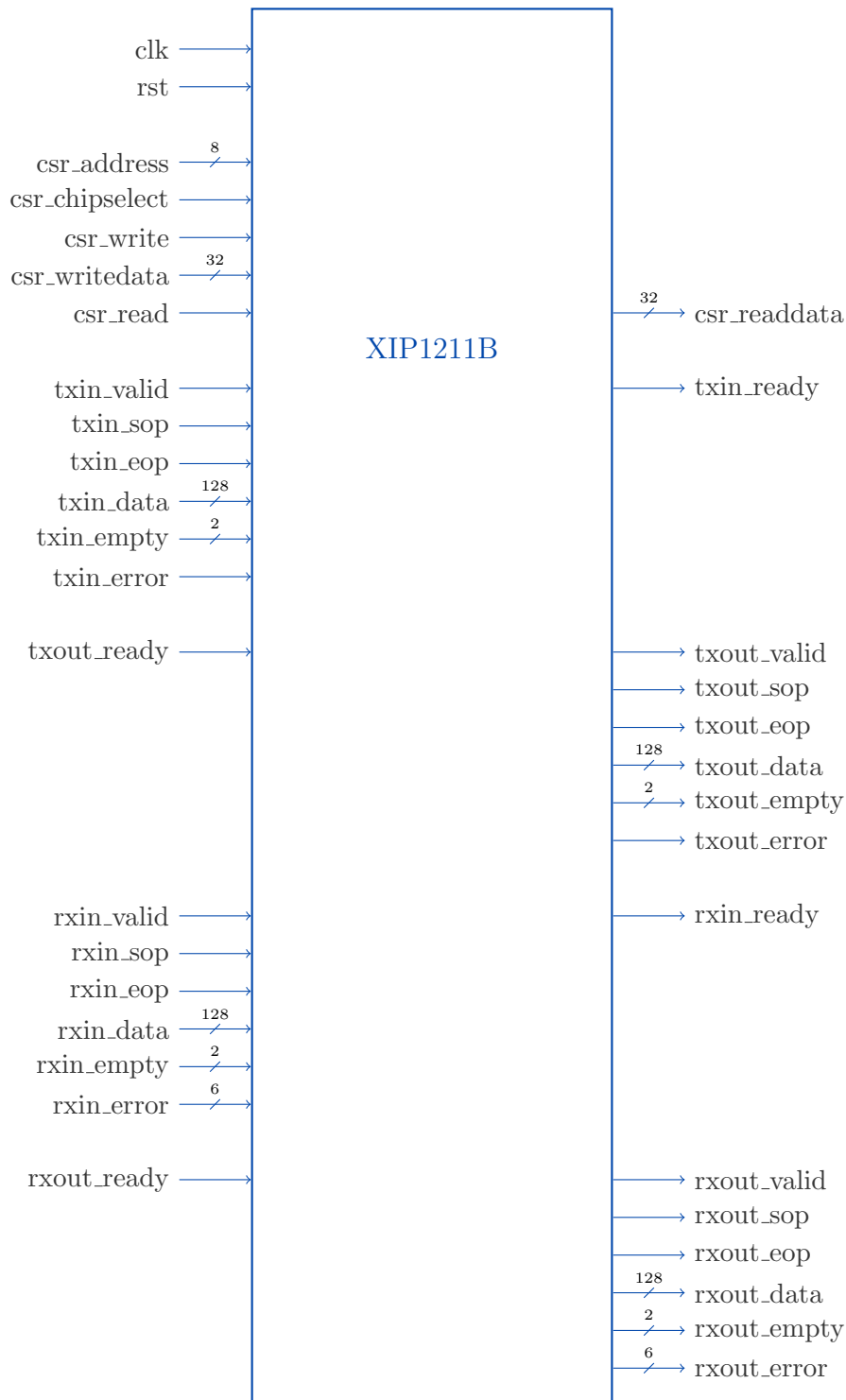


Figure 3: External interfaces of XIP1211H

FPGA families. The results in Table 1 were obtained by implementing the AES S-boxes in logic, and the internal memory blocks are used to implement the internal input and output FIFOs⁹.

⁹The size of the FIFOs is parameterizable.

Device	Resources	f_{MAX}	Max. throughput [‡]
Intel® Stratix®10 [†]	36748 ALM, 16 M20K	275 MHz	35.2 Gbps
Xilinx® UltraScale+™ MPSoC [*]	43704 LUT, 8 BRAM	405 MHz	51.8 Gbps

[†] Quartus II Prime 19.1., default compilation settings, industrial speedgrade

^{*} Vivado 19.1., default compilation settings, industrial speedgrade

[‡] $Throughput = f_{MAX} * 128 \text{ bits}$; achieved asymptotically with long packets.

Table 1: Resource usage and performance of XIP1211H on representative FPGA families.

Example Use Cases

The primary application of XIP1211H is provide for confidentiality and integrity of data as well as source authentication for Layer 2. Consequently, XIP1211H is typically connected via an Ethernet MAC IP core to an external 10/25/40 Gbps link, and the CSR (Control and Status Register) interface is connected to a processor¹⁰. An example use case is presented in Figure 4.

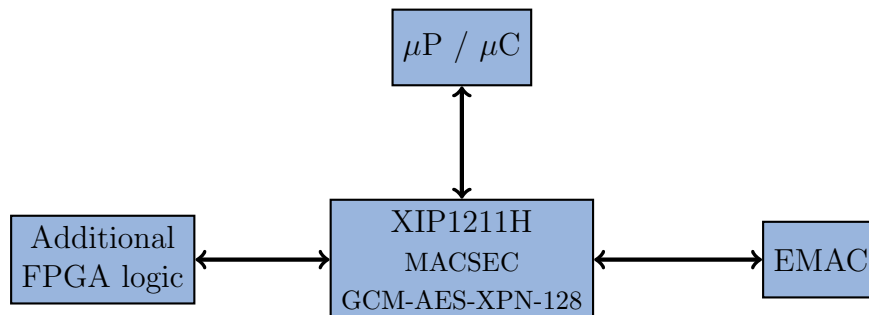


Figure 4: Example use case for XIP1211H.

If the end application requires slower linerates (for example, 1 Gbps), the balanced MACsec IP cores XIP1211B and XIP1213B from Xipherra are the recommended design choice.

Ordering and Deliverables

Please contact sales@xipherra.com for pricing and your preferred delivery method. XIP1211H can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, a comprehensive VHDL testbench and a detailed datasheet are included.

Export Control

XIP1211H protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP1211H is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP1211H can be immediately shipped to all European Union member states, Australia, Canada, Japan, New Zealand, Norway, Switzerland, United Kingdom, and the United States.

Export to other countries requires authorization from The Ministry for Foreign Affairs of Finland, and a typical processing time for an export authorization is a few weeks.

¹⁰The processor can also be an FPGA-based soft processor.

About Xiphera

Xiphera specializes in secure and efficient implementations of standardized cryptographic algorithms on Field Programmable Gate Arrays (FPGAs). Our product portfolio includes individual cryptographic Intellectual Property (IP) cores, as well as comprehensive security solutions built from a combination of individual IP cores.

Xiphera is a Finnish company operating under the laws of the Republic of Finland, and is fully owned by Finnish citizens.

Contact

Xiphera Oy
Otakaari 5
FIN-02150 Espoo
Finland
sales@xiphera.com
+358 20 730 5252

References

- [1] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.
- [2] IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security. *IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006)*, pages 1–239, Dec 2018.
- [3] Morris J. Dworkin. SP 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Technical report, Gaithersburg, MD, United States, 2007.