XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP7013E: IPSEC AES-256-GCM

Extreme-Speed IPsec ESP packet encrypt and decrypt

Product Brief
ver. 1.0
March 6, 2024

sales@xiphera.com

Introduction

XIP7013E implements the IPsec (Internet Protocol Security) protocol ESP (Encapsulating Security Payload) packet[1] processing using AES-256-GCM as specified in [3], [4], and [5] with a streaming interface. The IPsec protocol defines a security infrastrucure for Layer 3 (as per the Open System Interconnect (OSI) model) traffic by assuring that a received packet 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.

XIP7013E uses Advanced Encryption Standard [1] with 256-bit key in Galois Counter Mode (AES-256-GCM) [2] to protect data confidentiality, data integrity and data origin authentication. The througput of XIP7013E is designed for scaleability, and it can be use either a 256-bit, or 512-bit wide bus with Xiphera's extreme-speed AES-GCM IP core XIP1113E-256-N or XIP1113E-512-N as the internal crypto engine.

The ESP packet processing can be used in five different modes allowing either payload authentication, encryption with or without optional IV (Initialisation Vector), or bypassing the payload as it is. In the default version of XIP7013E, the Internet Key Exchange version 2 (IKEv2) is executed in software on a processor[2]; contact sales@xiphera.com if FPGA- or ASIC-based support for IKEv2 is required.

XIP7013E is best suited for traffic on links from 10 Gbps to 200 Gbit/s links with high-end FPGAs or ASICs. XIP7013E 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.

XIP7013E has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP7013E does not rely on any FPGA manufacturer-specific features.

[1] The term "frame" is often used interchangeably for "packet" in both standards and literature; this datasheet uses the term "packet" consistently even if the term "frame" may have been in standards.

[2] The term "processor" in this context can also refer to an FPGA- or ASIC-based processor.

Key Features

- **Performance:** The extreme-speed XIP7013E achieves a throughput exceeding 200 Gbps in modern high-end FPGAs and ASICs. Importantly, XIP7013E does not require any extra interpacket gap cycles even when it processes short packets. The latency of XIP7013E is fixed, and it does not depend on the length of the input packet.
- **Standard Compliance:** XIP7013E is compliant with RFC4303 [3]. The cipher suite (AES-256-GCM) is fully compliant with the Advanced Encryption Algorithm (AES) standard [1], as well as with the Galois Counter Mode (GCM) standard [2].
- **Easy Interfacing:** XIP7013E uses a streaming interface for payload data and side-channel signalling for the required ESP packet parameters.

Functionality

The functionality of XIP7013E is to encrypt and authenticate IPsec ESP (Encapsulating Security Payload) packets in the Transmit (Tx) direction and to decrypt and validate the authenticity of IPsec ESP packets in the receive (Rx) direction.

The structure of an ESP packet is described in Figure 1, and the high-level functionality of XIP7013E in both encryption (Tx) and decryption (Rx) directions is described at high-level in Figure 2

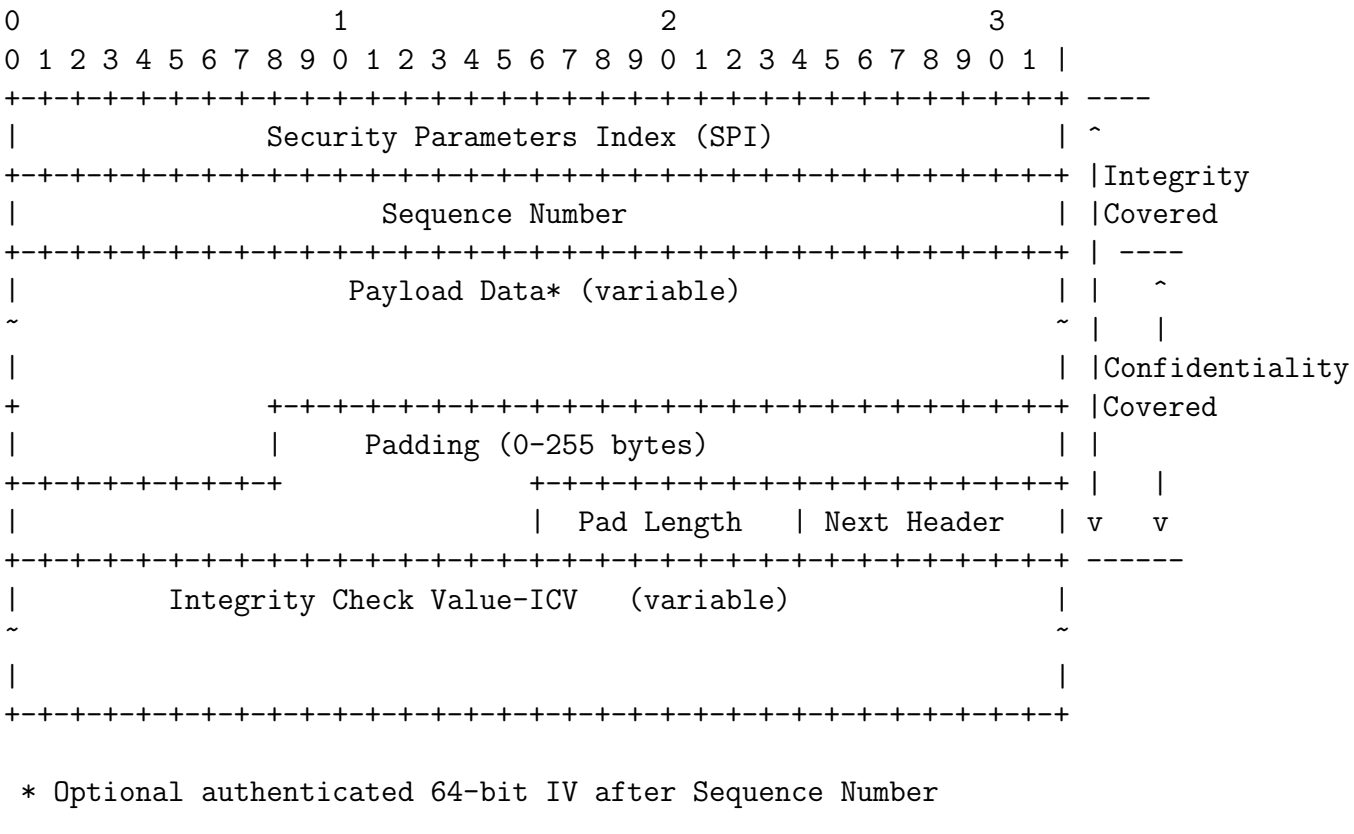

Figure 1: Top-level structure of ESP packet (See also [3]).

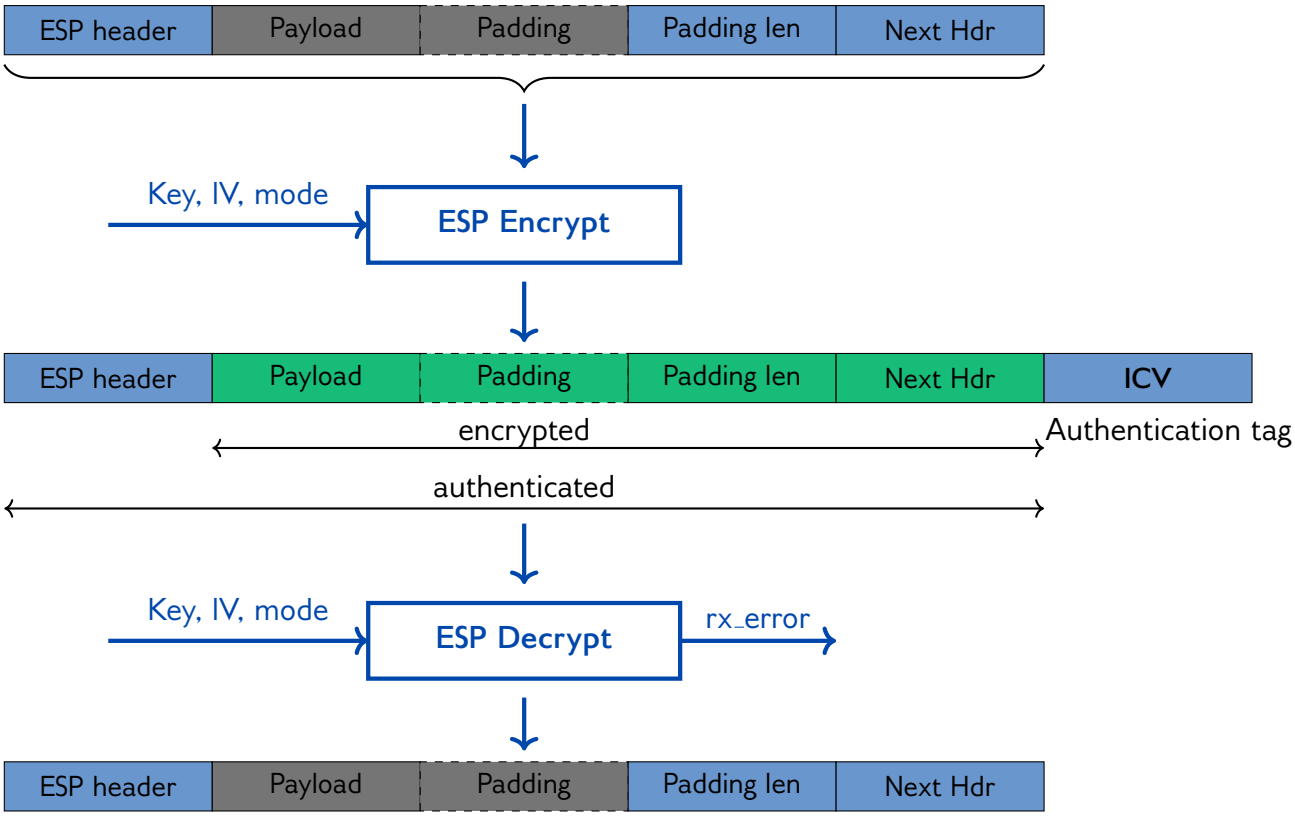

Figure 2: High-level functionality of XIP7013E.

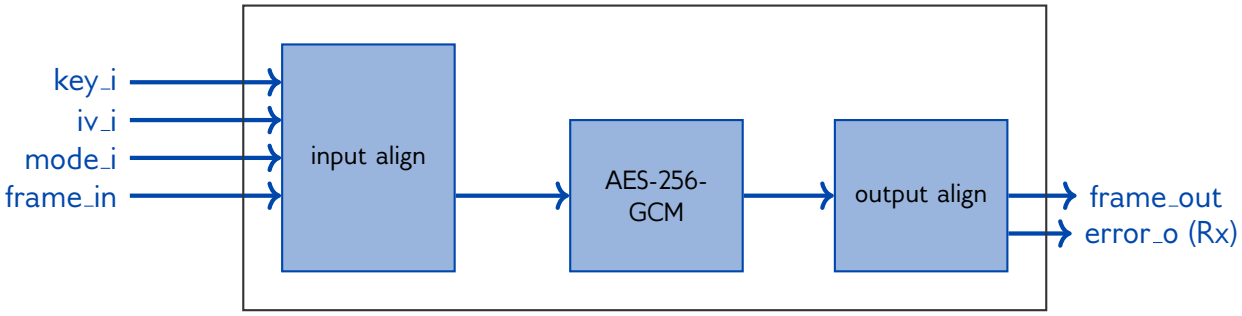

Figure 3: Internal high-level block diagram of either Rx or Tx direction in XIP7013E.

Block Diagram

Internally, XIP7013E consists of two independently operating blocks, working either in the Receive (Rx) (also known as decryption[3]) and Transmit (Tx) (also known as encryption[4]) directions. The internal high-level block diagram of both Rx and Tx blocks is practically identical, and it is depicted in Figure 3 with the only differences being the value of the `ENCDEC_P` Verilog parameter and using the `error_o` output signal. Importantly, the AES-256-GCM crypto engines in the Rx and Tx directions do not necessarily need to have identical performance.¸

[3]Decryption also includes the ICV (Integrity Check Value) calculation and verification of the calculated ICV value with the received ICV value.

[4]Encryption also includes the ICV (Integrity Check Value) calculation.

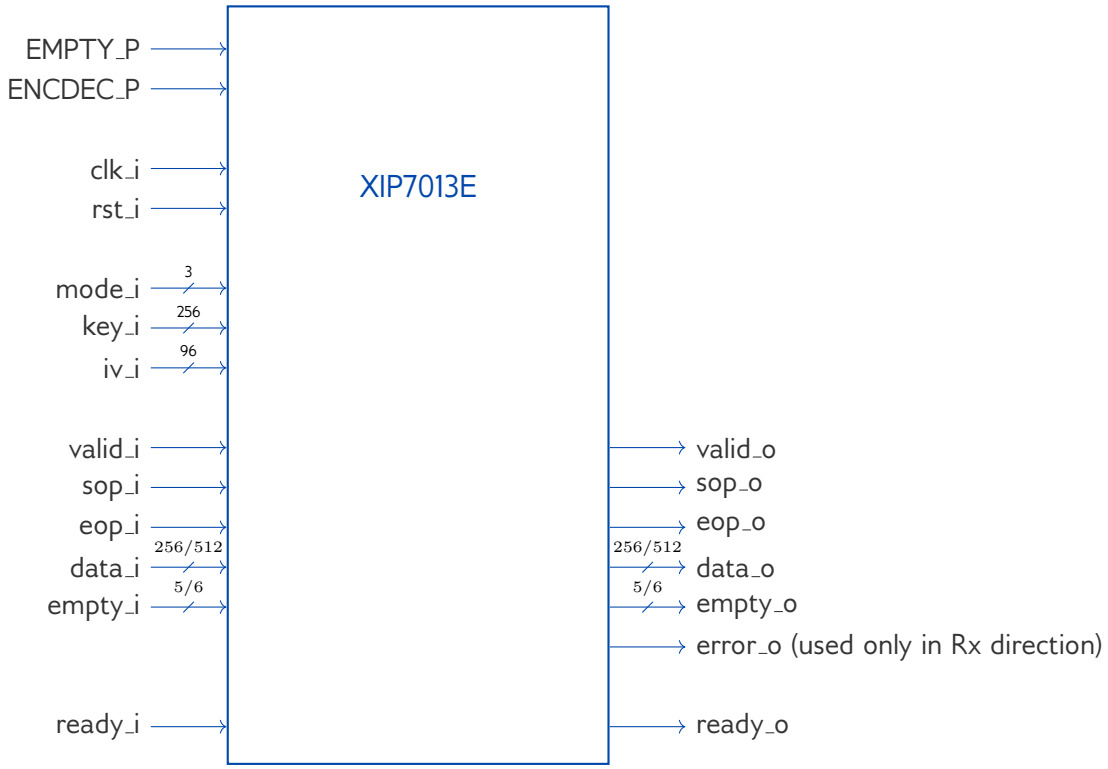

Figure 4: External interfaces of XIP7013E with either 256 or 512-bit interface.

Interfaces

The external interfaces of XIP7013E are depicted in Figure 4, which describes the connectivity of both Rx and Tx directions with the only difference being the use of `error_o` output signal.The width of the data bus in XIP7013E is defined by the Verilog parameter `EMPTY_P`, the encryption (Tx) or decryption (Rx) direction is defined by the Verilog parameter `ENCDEC_P`, and the functionality of XIP7013E is defined by the value on `mode_i[2:0]` as described in Table 1..

`mode_i[2:0]`	Mode of operation
`'000'`	Authenticated without optional IV (Initialisation Vector)
`'001'`	Authenticated with optional IV
`'010'`	Encrypted without optional IV
`'011'`	Encrypted with optional IV
`'1xx'`	Bypass mode, no processing for the packet

Table 1: Functionality of XIP7013E as defined by `mode_i[2:0]`

.

FPGA Resources and Performance

Table 2 presents the FPGA resource requirements on Intel Agilex® 7 family. On request, the resource estimates can also be supplied for other FPGA families.

[5] $Throughput = f_{MAX}$*databus width bits; achieved asymptotically with long packets.

FPGA family	Resources	f_{MAX}	databus width	Max. Throughput[5]
Intel Agilex® 7	87169 ALMs, 4 M20K	463.39 MHz	encrypt 512-bit	237.3 Gbps
Intel Agilex® 7	86128 ALMs, 4 M20K	445.04 MHz	decrypt 512-bit	227.9 Gbps
Intel Agilex® 7	50112 ALMs, 4 M20K	486.38 MHz	encrypt 256-bit	124.5 Gbps
Intel Agilex® 7	52478 ALMs, 4 M20K	494.56 MHz	decrypt 256-bit	126.6 Gbps
AMD Kintex™Ultrascale+™	92221 LUT	404.53 MHz	encrypt 512-bit	207.1 Gbps
AMD Kintex™Ultrascale+™	92286 LUT	419.99 MHz	decrypt 512-bit	215.0 Gbps
AMD Kintex™Ultrascale+™	56721 LUT	470.36 MHz	encrypt 256-bit	120.4 Gbps
AMD Kintex™Ultrascale+™	55938 LUT	450.34 MHz	decrypt 256-bit	108.4 Gbps

Table 2: Resource usage and performance of XIP7013E on Intel Agilex® 7 family.
Target device: AGFA006R162I1V, Quartus version. = 23.2
AMD target device: xcku15p-ffva1156-3-e, Vivado version v2023.1

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP7013E can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, a comprehensive SystemVerilog testbench and a detailed datasheet are included.

Export Control

XIP7013E protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP7013E is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP7013E 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.

About Xiphera

Xiphera specializes in secure and efficient implementations of standardized cryptographic algorithms on Field Programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs). Our fully in-house designed 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 and institutional investors.

Contact

Xiphera Oy
Tekniikantie 12
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] 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.

[3] Stephen Kent. IP Encapsulating Security Payload (ESP). RFC 4303, December 2005.

[4] John Viega and David McGrew. The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP). RFC 4106, June 2005.

[5] Paul Wouters, Daniel Migault, John Preuß Mattsson, Yoav Nir, and Tero Kivinen. Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH). RFC 8221, October 2017.

A Revision history

Version	Date	Changes
0.9.0	2024-01-19	Preliminary version.
0.9.1	2024-01-22	Updated interfaces.
1.0	2024-03-04	First published version