XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP1113E: AES256-GCM

Extreme-Speed IP Cores for AES256-GCM Authenticated Encryption

Product Brief
ver. 1.0
October 31, 2023

sales@xiphera.com

Introduction

XIP1113E is a family of extreme-speed IP cores designed for AES256-GCM (Advanced Encryption Standard with a 256-bit key and Galois Counter Mode) authenticated encryption as defined in the NIST (National Institute of Standards and Technology) standards FIPS PUB 197 [1] and Special Publication 800-38D [2]. AES-GCM is a widely used cryptographic algorithm for Authenticated Enryption with Associated Data (AEAD) purposes, as it provides both data confidentiality and authenticity. XIP1113E has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP1113E does not rely on any FPGA manufacturer-specific features.

Key Features

- **High Security:** XIP1113E implements AES256-GCM authenticated encryption as defined in the NIST standards FIPS PUB 197 [1] and Special Publication 800-38D [2], and offers a security level of 256 bits.
- **Extremely High Throughput:** XIP1113E offers extremely high throughput for a single stream of data as it processes one 32/64/128-byte block per clock cycle and has a high maximum clock frequency. The IP cores of XIP1113E achieve throughputs of hundreds of Gbps depending on the target Intel® FPGA.
- **Constant Latency:** XIP1113E offers constant latency for every data block and has a deterministic latency that facilitates an easy integration to various systems.
- **Secure Design:** XIP1113E executes encryption and decryption in constant time (that is, independent of the value of the key), and therefore provides full protection against timing side-channel attacks.

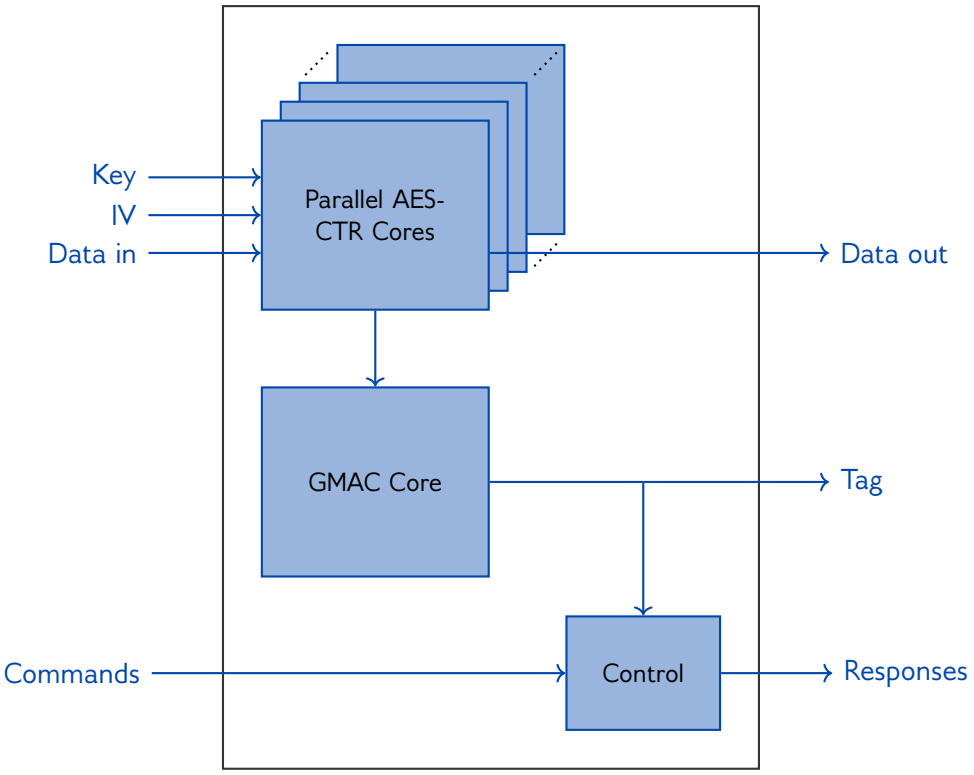

Figure 1: Internal high-level block diagram of XIP1113E

Functionality

The main functionality of XIP1113E depends on the mode of operation. When XIP1113E operates in the encryption and authentication tag calculation mode, it encrypts the incoming plaintext blocks into ciphertext blocks, and in addition to this also calculates an at most 128-bit authentication tag from both the incoming plaintext and associated data. When XIP1113E operates in the decryption and tag validity cheching mode, it decrypts the incoming ciphertext blocks into plaintext blocks, and validates the received authentication tag value by calculating the tag from the incoming ciphertext and associated data blocks and comparing the resulting tag value with the received tag value.

XIP1113E cores are available with different data widths starting from 256 bits and these widths directly influence the speed (throughput) of the core. XIP1113E are available as non-blocking versions, where the core is constantly free to accept new messages after the writing of the previous message has ended regardless of the length of the messages, and normal variants, where short idle periods are needed after short messages. The latter have slightly smaller footprint. XIP1113E have constant latency for all data processing and, therefore, they are compatible with timing sensitive applications and are protected against timing side-channel attacks.

Block Diagram

The internal high-level block diagram of XIP1113E is depicted in Figure 1.

Interfaces

The external interfaces of XIP1113E are depicted in Figure 2.

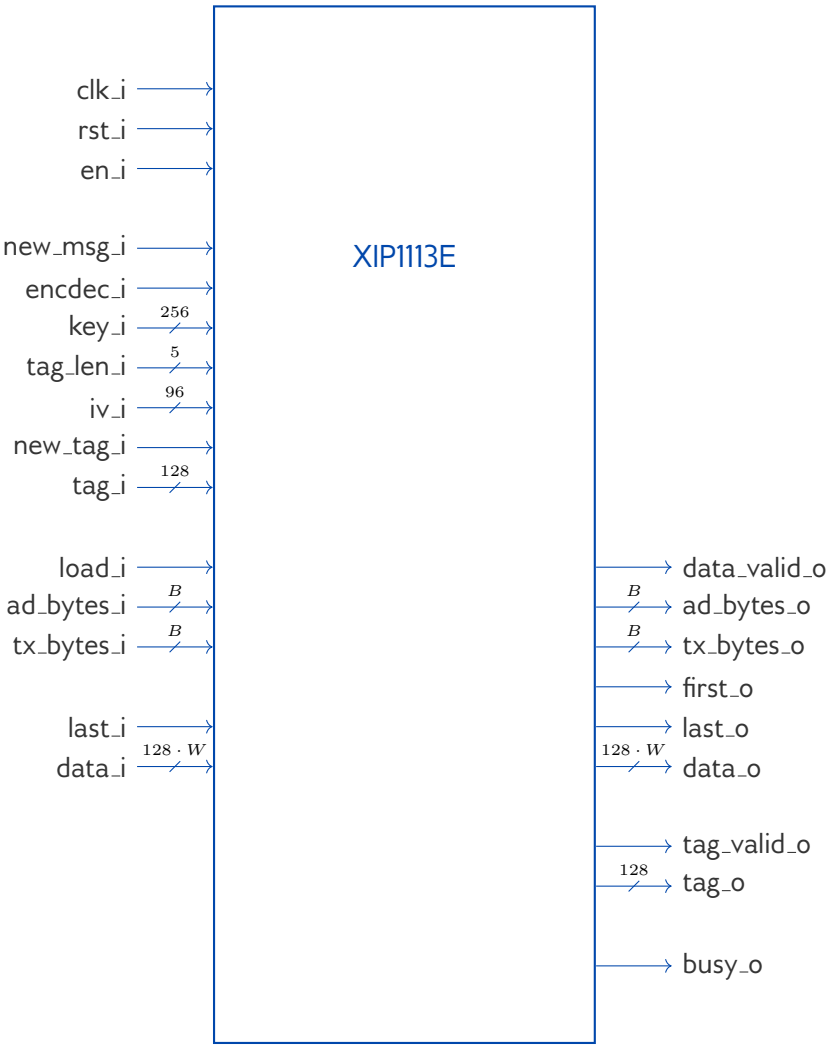

Figure 2: External interfaces of XIP1113E

This Product Brief describes a high-level overview of the functionality and capabilities of XIP1113E. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP1113E, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

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

*$Throughput = f_{MAX} * 128\ bits * W$; achieved asymptotically with long packets.
†Quartus® Prime Pro 22.4.0, default compilation settings, industrial speedgrade.

Device	Resources	f_{MAX}	Max. throughput*
XIP1113E-1024			
Intel® Agilex® F†	159153 ALM	352.86 MHz	361.33Gbps
Intel® Stratix® 10 GX†	162762 ALM	251.51 MHz	257.55Gbps
XIP1113E-256			
Intel® Agilex® F†	45726 ALM	381.53 MHz	97.67Gbps
Intel® Stratix® 10 GX†	46798 ALM	294.55 MHz	75.40Gbps
XIP1113E-256-N			
Intel® Agilex® F†	52837 ALM	379.22 MHz	97.08Gbps
Intel® Stratix® 10 GX†	53654 ALM	279.72 MHz	71.61Gbps
XIP1113E-512			
Intel® Agilex® F†	79040 ALM	376.93 MHz	192.99Gbps
Intel® Stratix® 10 GX†	80587 ALM	277.09 MHz	141.87Gbps
XIP1113E-1024-N			
Intel® Agilex® F†	190469 ALM	376.51 MHz	385.55Gbps
Intel® Stratix® 10 GX†	188515 ALM	227.17 MHz	232.62Gbps
XIP1113E-512-N			
Intel® Agilex® F†	92211 ALM	373.97 MHz	191.47Gbps
Intel® Stratix® 10 GX†	93297 ALM	259.61 MHz	132.92Gbps

Table 1: Resource usage and performance of XIP1113E on representative Intel® FPGA families.

Example Use Cases

XIP1113E has several applications, as AES-GCM is a popular AEAD algorithm in a number of standardized communications protocols, including IPsec, MACsec and TLS (Transport Layer Security) versions 1.2 and 1.3. Additionally, AES-GCM is used in fibre channel communications and tape storage applications.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP1113E can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, synthesis scripts, a comprehensive testbench, and a detailed datasheet including an integration guide are included.

Export Control

XIP1113E protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP1113E is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP1113E 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.