



PEACE OF MIND IN A DANGEROUS WORLD

XIP113H: AES256-GCM

Advanced Encryption Standard (256-bit key), Galois Counter Mode IP Core

Product Brief

ver. 1.2

September 20, 2023

sales@xiphera.com

Introduction

XIP113H from Xiphera is a high-throughput Intellectual Property (IP) core implementing the Advanced Encryption Standard (AES) [2] in Galois Counter Mode (GCM) [3]. AES-GCM is a widely used cryptographic algorithm for Authenticated Encryption with Associated Data (AEAD) purposes, as it provides both data confidentiality and authenticity.

XIP113H has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP113H does not rely on any FPGA manufacturer-specific features.

Key Features

- **Moderate** resource requirements: The entire XIP113H requires 24673 Adaptive Lookup Modules (ALMs) (Intel® Stratix® 10 GX), and does not require any multipliers, DSPBlocks or internal memory in a typical FPGA implementation.
- **Optimized Implementation** utilizing unrolling, pipelining, optimized AES S-box design, and GMAC calculation based on pipelined Karatsuba multipliers enable extremely high performance.
- **Performance:** XIP113H achieves a throughput in the tens of Gbps range¹, for example 49.63+ Gbps in Intel® Stratix® 10 GX.
- **Standard Compliance:** XIP113H is fully compliant with both the Advanced Encryption Algorithm (AES) standard [2], as well as with the Galois Counter Mode (GCM) standard [3].

¹As is typical for AEAD algorithms, the highest throughput is achieved for long messages.

- **Test Vector Compliance:** XIP1113H passes all test vectors specified in [1].
- **128-bit and 256-bit Interfaces** ease the integration of XIP1113H with other high-speed FPGA logic.

Functionality

The main functionality of XIP1113H depends on the mode of operation. When XIP1113H 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 a 128 bits long authentication tag from both the incoming plaintext and associated data. When XIP1113H operates in the decryption and tag validity checking 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. As defined by the GCM mode of operation, associated data is included in the authentication tag calculation.

XIP1113H can also operate with zero-length associated data, meaning that XIP1113H treats all signals on the input `data_in` as plaintext to be encrypted or as ciphertext to be decrypted. XIP1113H can also operate with zero-length plaintext or ciphertext, in which case it acts only as an authenticator or authentication validity checker.

XIP1113H outputs first the associated data, followed by encrypted plaintext or decrypted ciphertext (depending on the mode of operation), and as the last output the tag value and associated status signals.

Block Diagram

The internal high-level block diagram of XIP1113H is depicted in Figure 1.

Interfaces

The external interfaces of XIP1113H are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP1113H. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP1113H, 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.

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

†Quartus® Prime Pro 21.1.0, default compilation settings, industrial speedgrade.

‡Quartus® Prime Pro 22.4.0, default compilation settings, industrial speedgrade.

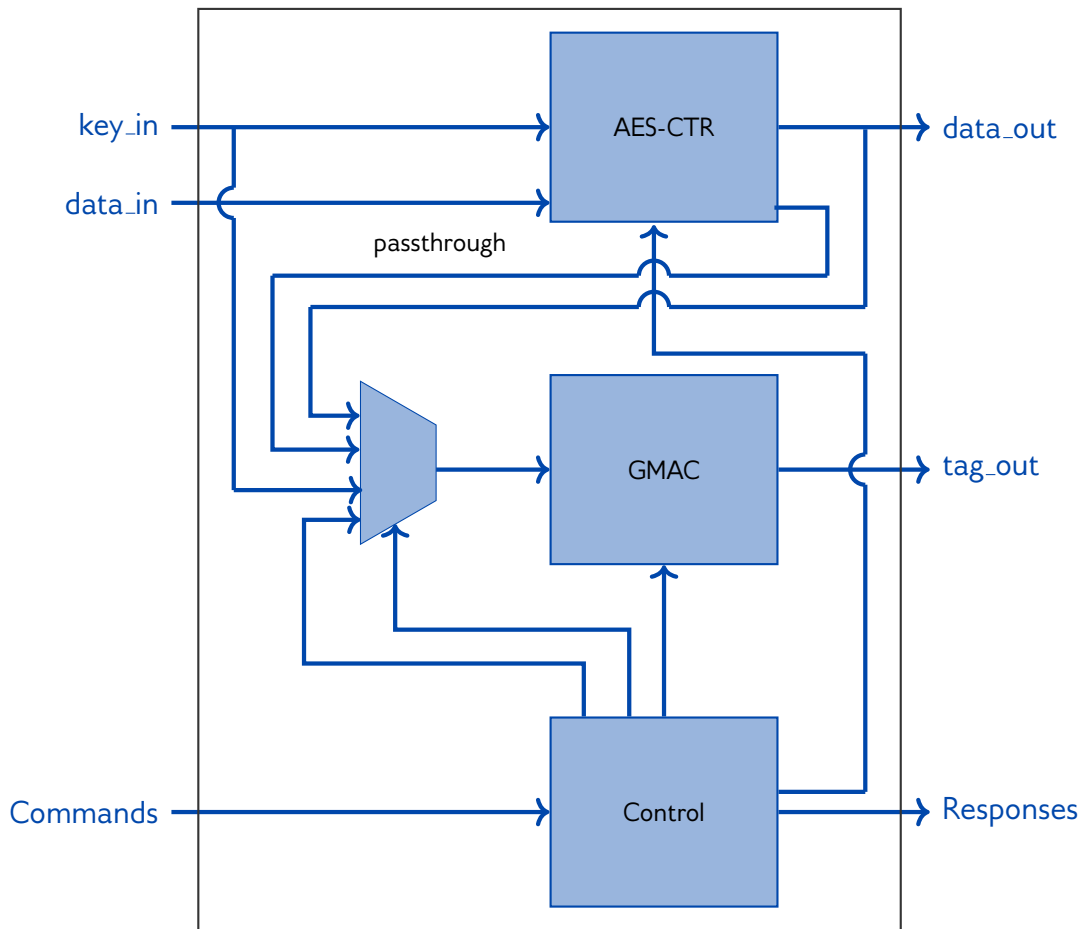


Figure 1: Internal high-level block diagram of XIP1113H

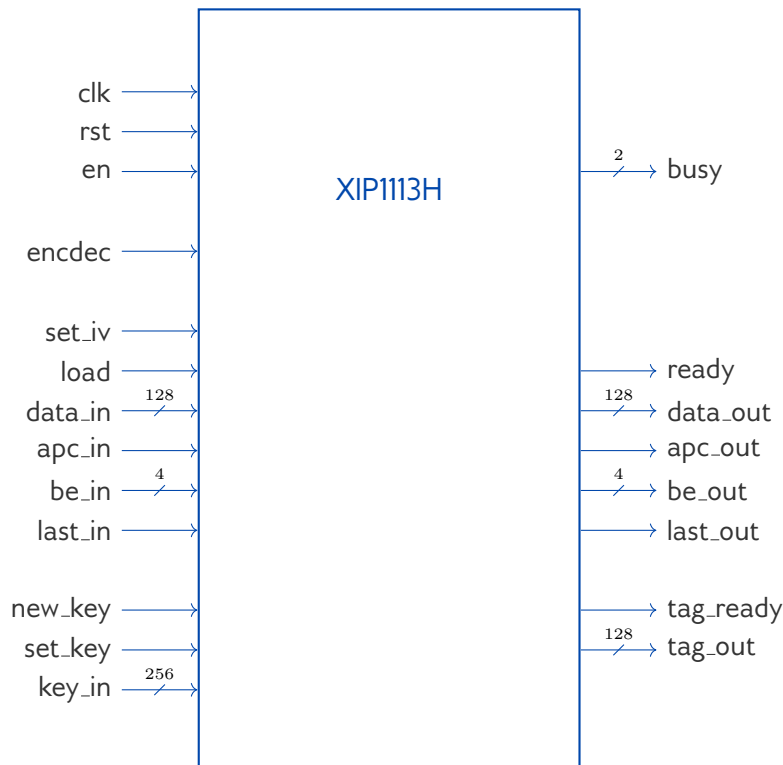


Figure 2: External interfaces of XIP1113H

Device	Resources	f_{MAX}	Max. throughput*
Intel® Stratix® 10 GX†	24673 ALM, 4 M20K	387.75 MHz	49.63 Gbps
Intel® Agilex® F†	24562 ALM, 4 M20K	600.60 MHz	76.88 Gbps
Intel® Cyclone® 10 GX‡	21922 ALM, 4 M20K	316.76 MHz	40.55 Gbps

Table 1: Resource usage and performance of XIP1113H on representative Intel® FPGA families.

Example Use Cases

XIP1113H 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. XIP1113H 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

XIP1113H protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP1113H is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP1113H 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] MACsec GCM-AES Test Vectors. <http://www.ieee802.org/1/files/public/docs2011/bn-randall-test-vectors-0511-v1.pdf>.
- [2] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.
- [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.