XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP1113B: AES256-GCM

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

Product Brief, ASIC version
ver. 1.0.1
July 31, 2023

sales@xiphera.com

Introduction

XIP1113B from Xiphera is a balanced 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 Enryption with Associated Data (AEAD) purposes, as it provides both data confidentiality and authenticity.

XIP1113B has been designed in pure digital RTL, and its functionality does not depend on any vendor or process node -specific features. This makes the integration of XIP1113B with the rest of the customer's ASIC design straightforward.

Key Features

- **Compact** resource requirements: The entire XIP1113B requires approximately 22 kGE (thousand Gate Equivalent)[1].
- **Performance:** Despite its moderate size, XIP1113B achieves a throughput in the Gbps range[2].
- **Standard Compliance:** XIP1113B is fully compliant with both the Advanced Encryption Algorithm (AES) standard [2], as well as with the Galois Counter Mode (GCM) standard [3].
- **Test Vector Compliance:** XIP1113B passes all test vectors specified in [1].
- **32-bit FIFO Interfaces**[3] ease the integration of XIP1113B with other ASIC logic and/or control software. On request, XIP1113B can also be delivered with an AXI-4 interface wrapper.

[1] The AES S-boxes can be implemented either in digital logic or internal memory depending on the customer's preference

[2] The maximum throughput is determined by the achieved f_{MAX} (See also Equation 1), which depends on the results of the place and route phase on the targeted ASIC process, the used design library, and the rest of the design.

[3] XIP1113B is also available with 128-bits long interfaces, please contact sales@xiphera.com for details.

Functionality

The main functionality of XIP1113B depends on the mode of operation. When XIP1113B 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 XIP1113B 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. As defined by the GCM mode of operation, associated data is included in the authentication tag calculation.

XIP1113B can also operate with zero-length associated data, meaning that XIP1113B treats all signals on the input `data_in` as plaintext to be encrypted or as ciphertext to be decrypted. XIP1113B can also operate with zero-length plaintext or ciphertext, in which case it acts only as an authenticator or authentication validity checker.

XIP1113B 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 XIP1113B is depicted in Figure 1.

Interfaces

The external interfaces of XIP1113B are depicted in Figure 2. On request, XIP1113B can also be shipped with an AXI-4 interface wrapper.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP1113B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP1113B, and example simulation waveforms.

Resources and Performance

Table 1 presents the resource requirements of XIP1113B synthesized on TSMC 16nm FinFET process. On request, Xiphera can work with the customer to attain the resource requirements also on another process.

IP Core	Gate Count	Memory Bits
XIP1113B	22069 *	0

* Synopsys Design Compiler, version 2022.03-SP5.

Table 1: Resource usage of XIP1113B on TSMC 16nm FinFET process.

The throughput[4] (in Gbps, gigabits per second) of XIP1113B depends on the achieved f_{MAX} as per the following formula:

[4] achieved asymptotically with long packets.

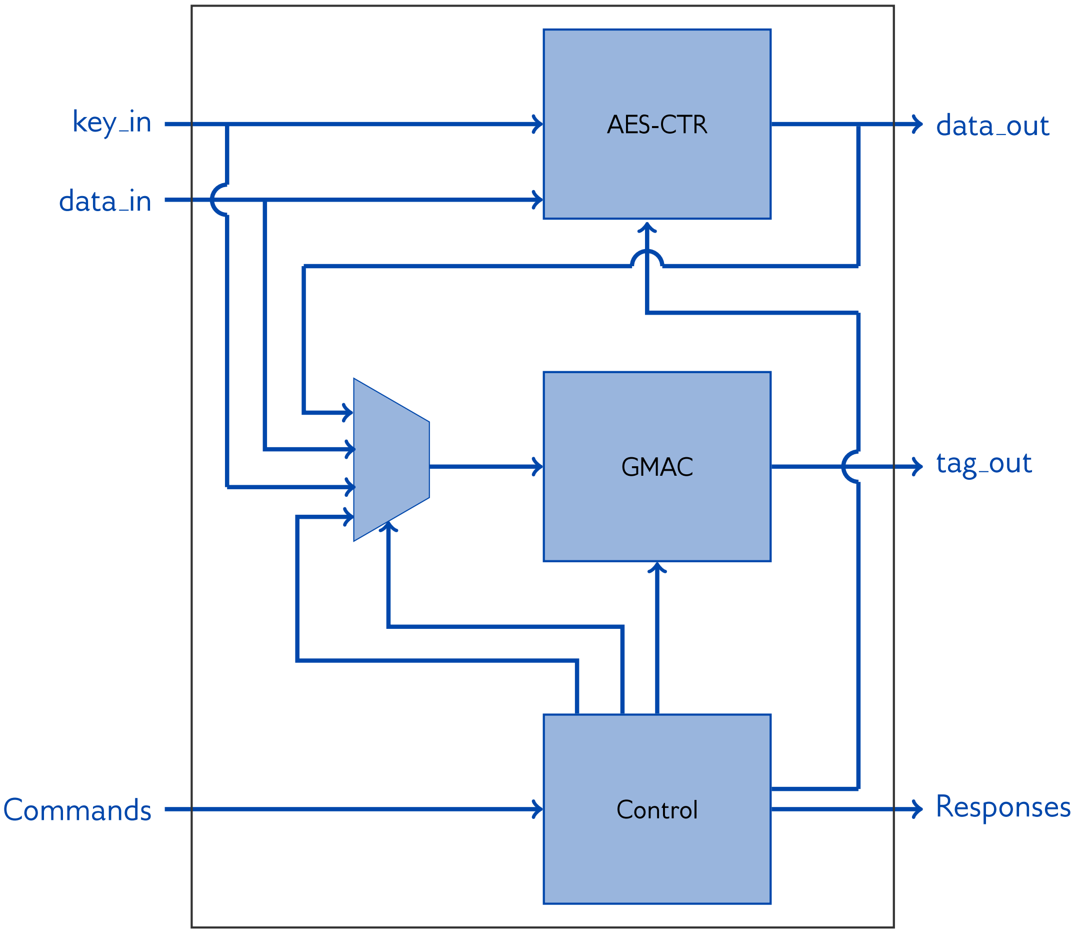

Figure 1: Internal high-level block diagram of XIP1113B

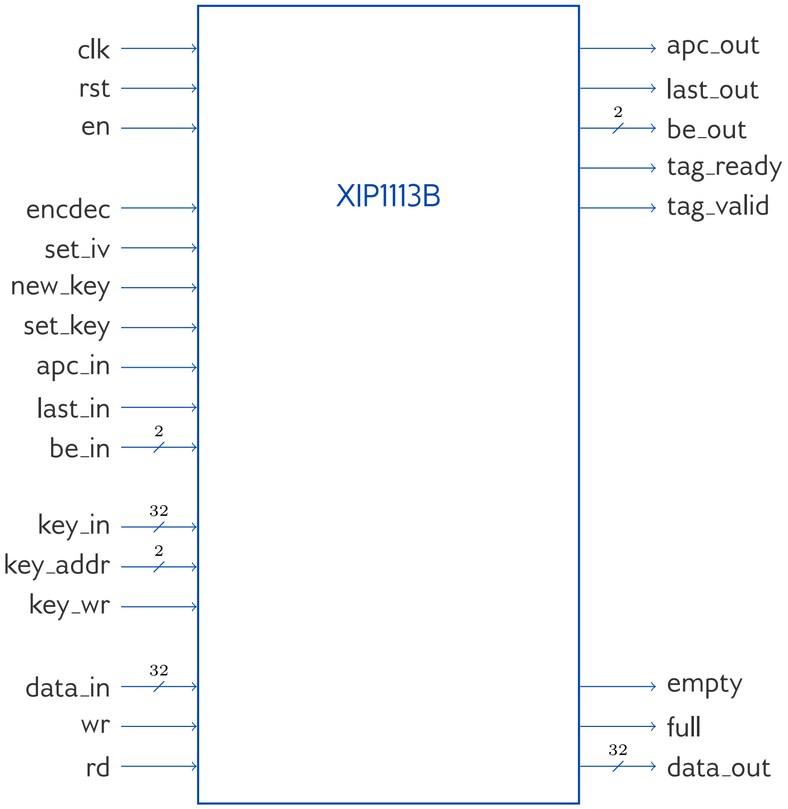

Figure 2: External interfaces of XIP1113B

$$Throughput = \frac{f_{MAX} * 128\ bits}{14\ clock\ cycles} \tag{1}$$

For example, for an f_{MAX} of 500 MHz, the throughput of XIP1113B is 4.57 Gbps[5].

Example Use Cases

XIP1113B 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. XIP1113B 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.

[5] The achieved f_{MAX} depends on the results of the place and route phase on the targeted ASIC process, the used design library, and the rest of the design; examples of achieved f_{MAX} on several FPGA families are available on Xiphera's product pages.

Export Control

XIP1113B protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP1113B is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP1113B 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.