XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP1123B: VERSATILE AES-256 IP CORE

Advanced Encryption Standard (256-bit key), ECB, CBC, OFB, CFB, and CTR Mode of Operation

Product Brief
ver. 1.0
September 20, 2023

sales@xiphera.com

Introduction

XIP1123B from Xiphera is a balanced[1] and versatile Intellectual Property (IP) core implementing the Advanced Encryption Standard (AES) [1] with a 256-bit key in five dynamically selectable modes of operation: Electronic Codebook (ECB) [2], Cipher Block Chaining (CBC) [2], Cipher Feedback (CFB) [2], Output Feedback (OFB) [2], and Counter (CTR) [2].

The four different modes of operation (CBC, CFB, OFB, and CTR) all protect data confidentiality, and are widely used in numerous security designs and cryptographic protocols. XIP1123B also supports the ECB mode of operation as a building block for other AES modes of operation, but importantly the standalone use of ECB is not recommended for cryptographically secure applications. The design of XIP1123B allows for every individual 128-bit data block (`din` —plaintext in encryption mode, ciphertext in decryption mode) to use a different key, a different Initialization Vector (IV)[2], and a different mode of operation[3].

XIP1123B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP1123B does not rely on any FPGA manufacturer-specific features.

[1] Xiphera's balanced (denoted by 'B' at the end of the ordering code) IP cores strike a balanced compromise between performance and FPGA resource usage.

[2] ECB mode of operation does not use an IV.

[3] If less than the default 5 (five) modes of operation are required the FPGA resource requirements are reduced; contact info@xiphera.com for details.

Key Features

- **Moderate** resource requirements: The entire XIP1123B requires 4051 4-input Lookup Tables (4LUTs) (Microchip® PolarFire®), and does not require any multipliers or DSPBlocks[4].
- **Performance:** XIP1123B achieves an impressive throughput in the Gbps range, for example 1.30+ Gbps in Microchip® PolarFire® .
- **Standard Compliance:** XIP1123B is fully compliant with both the Advanced Encryption Algorithm (AES) standard [1], as well as with the ECB, CBC, CFB, OFB, and CTR modes of operation [2].
- **Versatility:** The key, initialization vector (IV), and the mode of operation can dynamically updated for every 128-bit data block.

Functionality

XIP1123B supports five different AES modes of operation: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). The four modes of operation (CBC, CFB, OFB, and CTR) use an internal AES256-ECB block as the encryption/decryption engine, but the internal connectivity between 128-bit data block, initialization vector, and the AES256-ECB block inputs and outputs is different; additionally the modes differ in the interdependencies between successsive encryption/decryption rounds.

The high-level flow diagrams of CBC, CFB, OFB, and CTR in encryption mode are presented in Figures 1, 2, 3, and 4.

When decrypting ciphertext blocks into plaintext, the CBC mode of operation requires the internal AES256-ECB block to operate in decryption mode, whereas the other three supported modes of operation (CFB, OFB, and CTR) use the internal AES256-ECB block in encryption mode. This means that if CBC support is not required, a considerable amount of FPGA resources can be saved; contact info@xiphera.com for details.

Block Diagram

The internal high-level block diagram of XIP1123B is depicted in Figure 5.

Interfaces

Primary interface

The external interfaces of XIP1123B are depicted in Figure 6.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP1123B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP1123B, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

[4]The AES S-boxes can be implemented either in Microchip® FPGA logic or internal memory blocks depending on the customer's preference

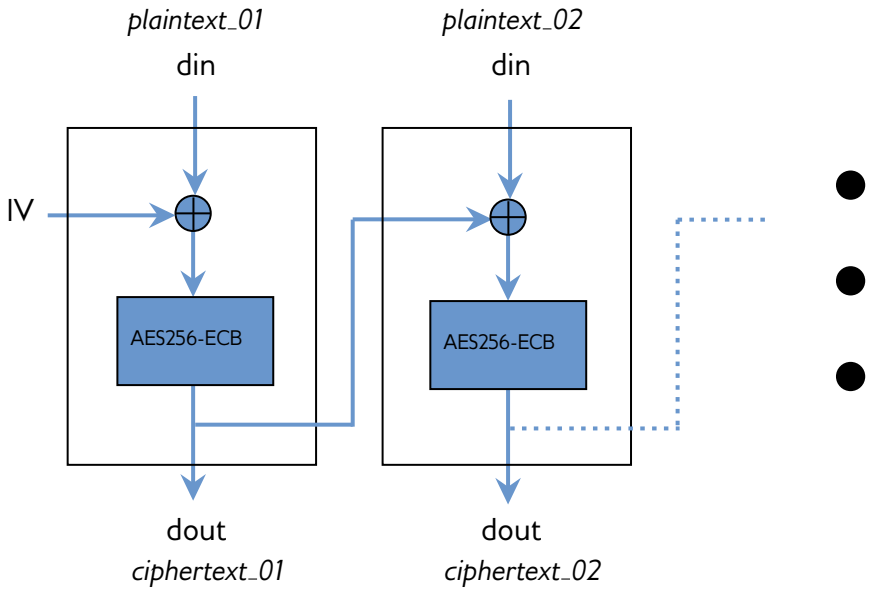

Figure 1: XIP1123B in CBC mode of operation, encryption.

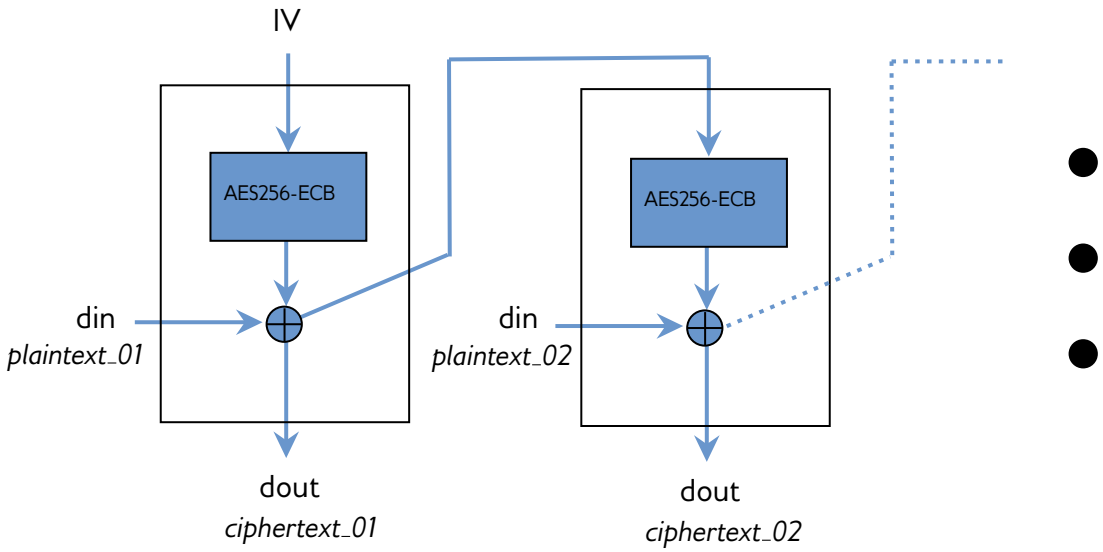

Figure 2: XIP1123B in CFB mode of operation, encryption.

AXI4 Lite subordinate interface

Xiphera provides standard AMBA® AXI4 Lite register based wrapper to XIP1123B interface. The primary interface is translated into control and data registers accessable by the AXI4 lite interface. The data width of the interface is 32 bits by default.

The address space of the interface is described in the Table 1. The address space is eight bits wide and unlisted addresses are reserved.

Control and Status registers

AXI4 Lite interface control register located at address offset $0x00$ and status register located at address $0x04$. The control register is write only and status register is read only.

Table 2 describes the contents of the registers.

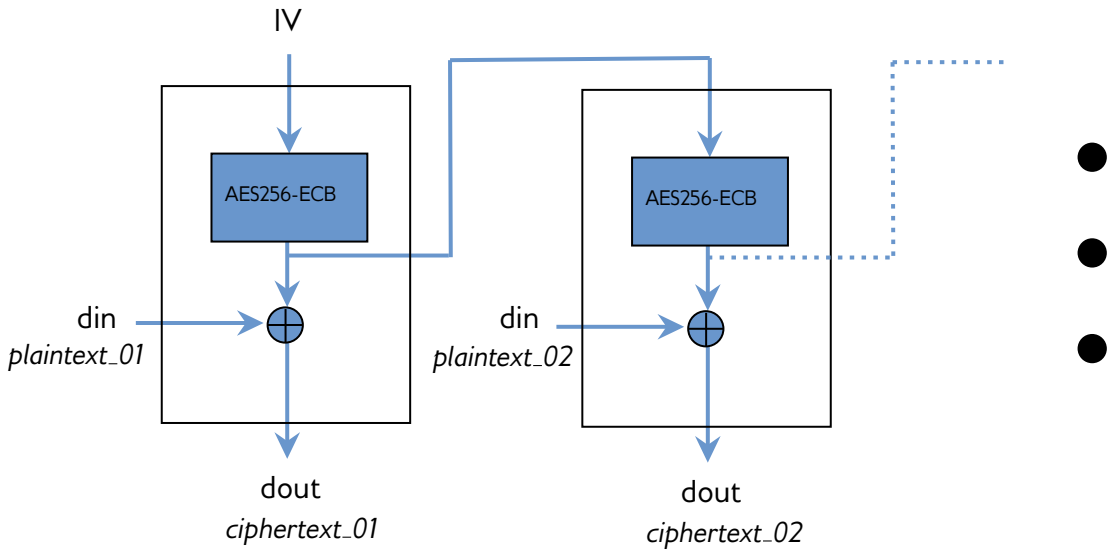

Figure 3: XIP1123B in OFB mode of operation, encryption.

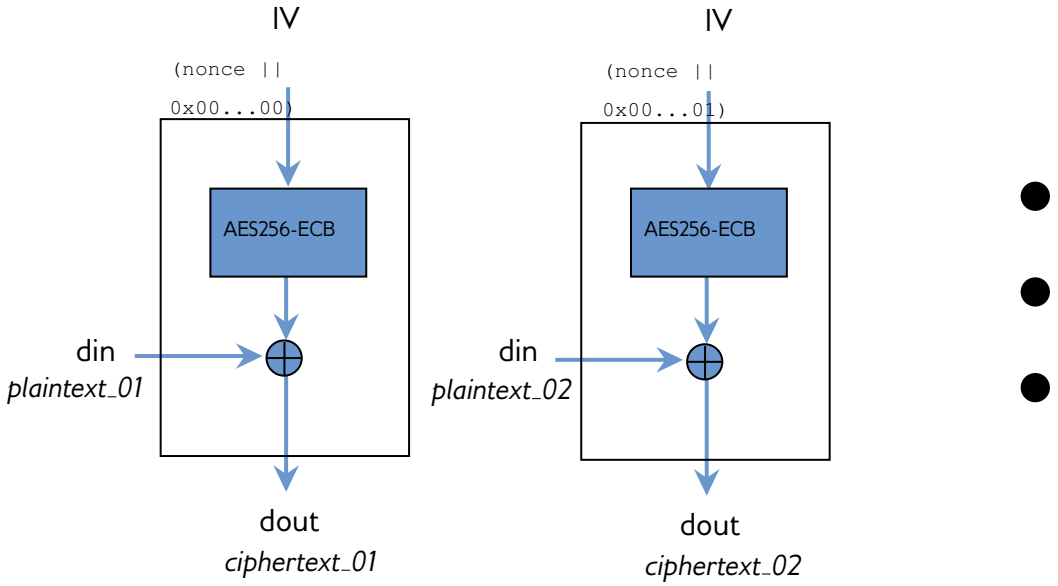

Figure 4: XIP1123B in CTR mode of operation, encryption.

FPGA Resources and Performance

Table 3 presents the Microchip® FPGA resource requirements for representative implementations on different Microchip® FPGA architectures. On request, the resource estimates can also be supplied for other Microchip® FPGA families.

XIP1123B can also be customized to support a subset —or just one —of the modes of operations; this will lead to reduction in the required Microchip® FPGA resources. Contact info@xiphera.com for details.

*$Throughput = \frac{f_{MAX} * 128\ bits}{16\ clock\ cycles}$

†Libero 2022.1.0.10, default compilation settings, industrial speedgrade.

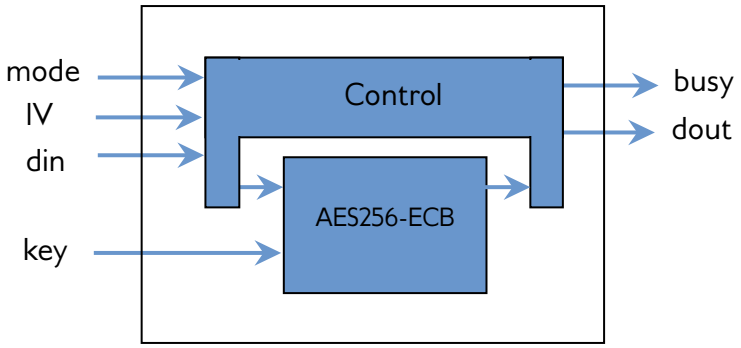

Figure 5: Internal high-level block diagram of XIP1123B

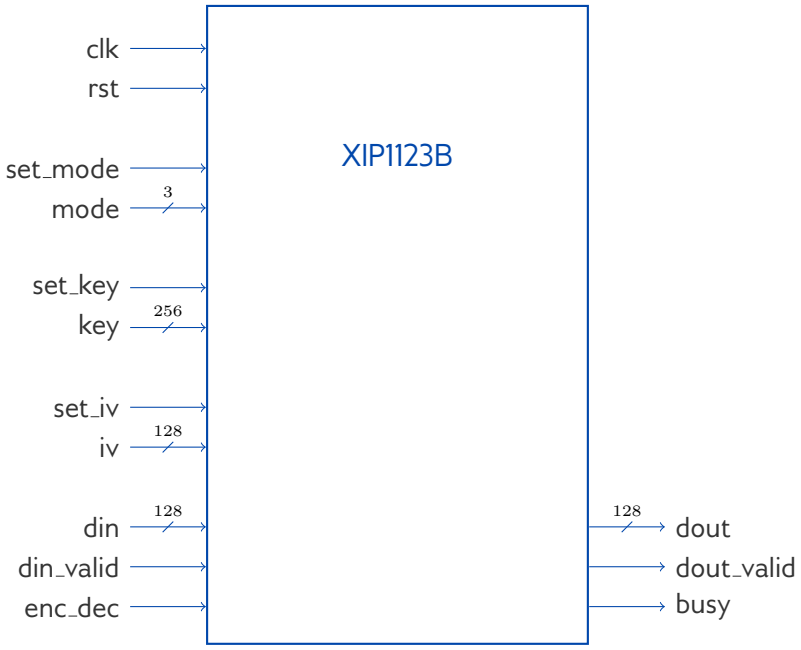

Figure 6: External interfaces of XIP1123B

Example Use Cases

XIP1123B protects the confidentiality of the encrypted plaintext in CBC, CFB, OFB, and CTR mode of operation. To additionally provide authenticity protection XIP1123B should be used in combination with a keyed message authentication code, such as Xiphera's XIP3322B (SHA-256 HMAC) IP core.

If multiple tens of gigabits per second encryption/decryption speeds are required, Xiphera's high-speed AES256-CTR (XIP1103) or AES256-GCM (XIP1113H) IP cores are recommended.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP1123B 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.

Offset	Register Name	Access Type	Description
0x00	CONTROL	W	Control register for mode, reset and enc/dec selection.
0x04	STATUS	R	Status register for busy and data out valid.
0x10	KEY_0	W	First word of the key. Bits 31 through to bit 0 (31 downto 0).
0x14..0x28	KEY_1...KEY_6	W	Corresponding key segments.
0x2C	KEY_7	W	Last word of the key. Bits 255 through to bit 224 (255 downto 224). Writing to this address asserts the set_key signal.
0x30	IV_0	W	First word of the initialisation vector (IV). Bits 31 through to bit 0 (31 downto 0).
0x34	IV_1	W	Second word of the IV. Bits 63 through to bit 32 (63 downto 32).
0x38	IV_2	W	Third word of the IV. Bits 95 through to bit 64 (95 downto 64).
0x3C	IV_3	W	Last word of the IV. Bits 127 through to bit 96 (127 downto 96). Writing to this address asserts the set_iv signal.
0x40	DIN_0	W	First word of the data input. Bits 31 through to bit 0 (31 downto 0).
0x44	DIN_1	W	Second word of the data input. Bits 63 through to bit 32 (63 downto 32).
0x48	DIN_2	W	Third word of the data input. Bits 95 through to bit 64 (95 downto 64).
0x4C	DIN_3	W	Last word of the data input. Bits 127 through to bit 96 (127 downto 96). Writing to this address asserts the set_iv signal.
0x50	DOUT_0	R	First word of the data output. Bits 31 through to bit 0 (31 downto 0).
0x54	DOUT_1	R	Second word of the data output. Bits 63 through to bit 32 (63 downto 32).
0x58	DOUT_2	R	Third word of the data output. Bits 95 through to bit 64 (95 downto 64).
0x5C	DOUT_3	R	Last word of the data output. Bits 127 through to bit 96 (127 downto 96). Reading from this register clears the data valid and output registers.

Table 1: Address space and register description for the XIP1123B AXI4 Lite interface.

Export Control

XIP1123B protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP1123B is controlled by Council Regulation (EC) No

Bit(s)	Name	Reset	Description
Control register			
31-6	Reserved	0	Reserved for future use.
5	Reset	1	Internal reset for the XIP1123B. Needs to be deasserted after system reset. Active high.
4	Enc / Dec	0	Encryption or decryption selection.
3	Set mode	0	Asserts the `set_mode`.
2-0	AES mode	0	Sets the AES mode for the XIP1123B.
Status register			
31-5	Reserved	0	Reserved for future use.
4-2	Error code	0	Errors occurred.
1	Data out valid	0	Indicates valid data in DOUT address space.
0	Busy	1	Indicates that core is busy calculating AES block operation. Data cannot be loaded into DIN_3 address.

Table 2: AXI4 Lite Control and Status register contents described.

Device	Resources	f_{MAX}	Max. throughput*
Microchip® PolarFire® †	4051 4LUT, 11 uSRAM	161.97 MHz	1.30 Gbps

Table 3: Resource usage and performance of XIP1123B on representative Microchip® FPGA families. AES S-boxes implemented either in internal memory blocks or lookup tables (4 and 6 inputs supported).

428/2009 of 5 May 2009 and its subsequent changes.

XIP1123B 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 800-38A 2001 Edition. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. Technical report, Gaithersburg, MD, United States, 2001.