XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP1183B: AES256-XTS

Advanced Encryption Standard (256-bit key), XTS mode IP Core

Product Brief
ver. 1.0
July 4, 2022

sales@xiphera.com

Introduction

XIP1183B from Xiphera is a balanced[1] Intellectual Property (IP) core implementing the Advanced Encryption Standard (AES) [1] with 256 bits long key in XTS [2] mode.

AES-XTS is block-oriented cipher used primarily for protecting the confidentiality of data at rest. Consequently, AES-XTS is widely used for encrypting the contents of hard drives and other storage devices.

AES-XTS is a *tweakable* block cipher, and as it instantiates the underlying AES block cipher twice, the key material for AES-XTS is twice longer than for the constituent individual AES block ciphers.

The encrypted data depends not only on the plaintext and encryption key, but also on the logical address of the data on the storage device. This means that identical plaintexts get encrypted differently at different logical addresses.

XIP1183B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP1183B does not rely on any FPGA manufacturer-specific features.

Key Features

- **Moderate** resource requirements: The entire XIP1183B requires 6074 Adaptive Lookup Modules (ALMs) (Intel® Cyclone® 10 GX), and does not require any multipliers or DSPBlocks[2].

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

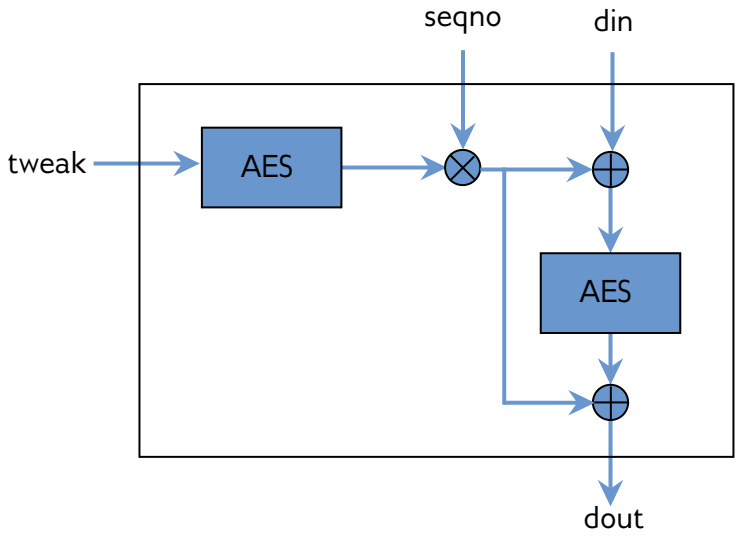

Figure 1: Internal high-level block diagram of XIP1183B

- **Performance:** XIP1183B achieves an impressive throughput in the Gbps range, for example 2.79+ Gbps in Xilinx® Zynq® MPSoC.
- **Standard Compliance:** XIP1183B is compliant with both the Advanced Encryption Algorithm (AES) standard [1], and the XTS standard [2] .
- Optional **Ciphertext stealing** support as defined in [2].
- **Increase Performance** can be achieved by paralle instantiations of XIP1183B.

Functionality

AES256-XTS works by first encrypting the tweak value[3] with an AES block. The encrypted tweak value is then multiplied[4] with a value derived from the Block Sequence Number[5] of the 128 bits long block inside the data unit.

The resulting value is then used in an Exlusive OR (XOR) operation both at the input and output of another AES block ("datapath AES"), which uses a different 256 bits long key from the AES block responsible for encrypting the tweak value.

Decryption is an identical operation to encryption, with the exception that the datapath AES operates in decryption mode.

Block Diagram

The internal high-level block diagram of XIP1183B is depicted in Figure 1.

[3]The AES-XTS standard [2] defines the tweak as a 128 bits long value used to represent the logical position of the data being encrypted or decrypted, which in practice is most often the address of an individual sector on the storage media.

[4]The multiplication is performed in Galois field $GF(2^{128})$ defined by the polynomial $x^{128} + x^7 + x^2 + x + 1$.

[5]The default configuration of XIP1183B uses a 4kB sector size, but this can be easily parameterized.

Interfaces

The external interfaces of XIP1183B are depicted in Figure 2.

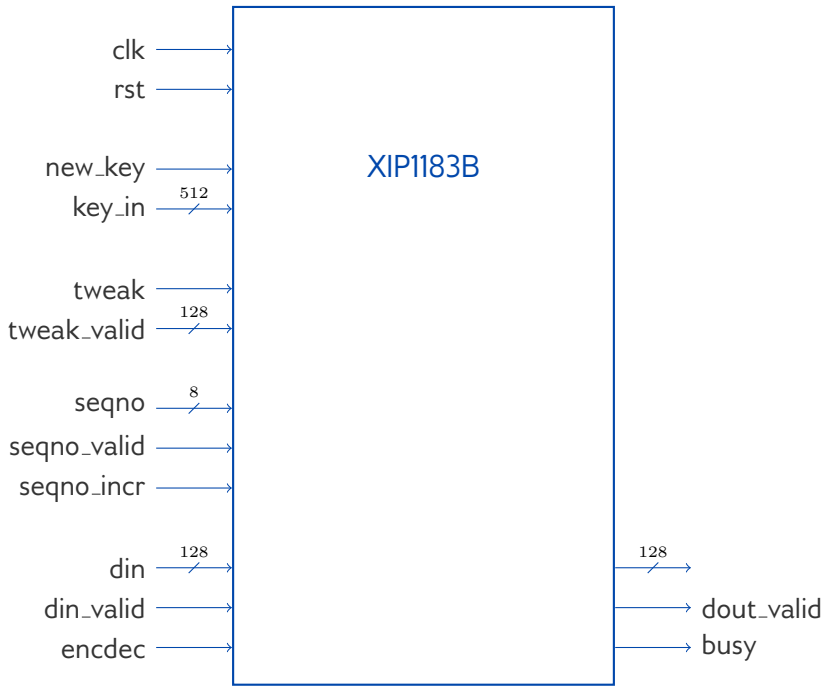

Figure 2: External interfaces of XIP1183B

This Product Brief describes a high-level overview of the functionality and capabilities of XIP1183B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP1183B, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

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

Device	Resources	f_{MAX}	Max. throughput*
Intel® Cyclone® 10 GX†	6074 ALM	282.97 MHz	2.26 Gbps
Intel® Stratix® 10 GX†	6125 ALM, 8 M20K	305.81 MHz	2.45 Gbps
Intel® Agilex® F†	6079 ALM, 8 M20K	455.37 MHz	3.64 Gbps
Intel® Arria® 10 GX†	5958 ALM, 6 M20K	284.09 MHz	2.27 Gbps
Xilinx® Zynq® MPSoC‡	6961 LUT	349.16 MHz	2.79 Gbps
Xilinx® Kintex® UltraScale+‡	6932 LUT	400.48 MHz	3.20 Gbps

Table 1: Resource usage and performance of XIP1183B on representative FPGA families. AES S-boxes implemented either in internal memory blocks or lookup tables (4 and 6 inputs supported).

*$Throughput = \frac{f_{MAX} * 128\ bits}{16\ clock\ cycles}$, achieved for encrypting/decrypting an entire sector.

Mention configuration

Example Use Cases

XIP1183B protects the confidentiality of the encrypted plaintext, and identical plaintext is encrypted into a different ciphertext at different memory addresses.

When using XIP1183B with storage media whose natural bit width is smaller than 128 bits, it is recommended to integrate XIP1183B with a memory controller IP core to enable encrypting and decrypting 128-bits data units.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP1183B can be shipped in a number of formats, including netlist, source code, or encrypted source code. Additionally, a comprehensive VHDL testbench and a detailed datasheet are included.

Export Control

XIP1183B protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP1183B is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP1183B 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 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
Otakaari 5
FIN-02150 Espoo
Finland
sales@xiphera.com

[†]Quartus® Prime Pro 21.1.0, default compilation settings, industrial speedgrade.
[‡]Vivado 2020.2, default compilation settings, industrial speedgrade.

+358 20 730 5252

References

[1] Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, 2001.

[2] IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. *IEEE Std. 1619-2018*, 2018.