XIP1103H: AES256-CTR

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

Product Brief
ver. 1.0
September 8, 2020

sales@xiphera.com

Introduction

XIP1103H from Xiphera is a high-speed Intellectual Property (IP) core implementing the Advanced Encryption Standard (AES) [1] in Counter Mode (CTR) [2].

The Counter mode of operation effectively turns a block cipher into a stream cipher, and provides a number of advantages from an implementation point of view. These include the ability to use the same key expansion functionality and datapath for both encryption and decryption, and the possibility to parallelize the FPGA-based implementation by unrolling and pipelining.

XIP1103H has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP1103H does not rely on any FPGA manufacturer-specific features.

Key Features

- **Moderate** resource requirements: The entire XIP1103H requires less than 14000 Adaptive Lookup Modules (ALMs) (Intel® Cyclone®V), and does not require any multipliers or DSPBlocks[1].
- **Performance:** Despite its moderate size, XIP1103H achieves a throughput in the tens of Gbps range, for example 100+ Gbps in Xilinx® Virtex® UltraScale+™ FPGA family.
- **Standard Compliance:** XIP1103H is fully compliant with both the Advanced Encryption Algorithm (AES) standard [1], as well as with the Counter Mode (CTR) standard [2].
- **128-bit and 256-bit Interfaces** ease the integration of XIP1103H with other FPGA logic and/or control software.

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

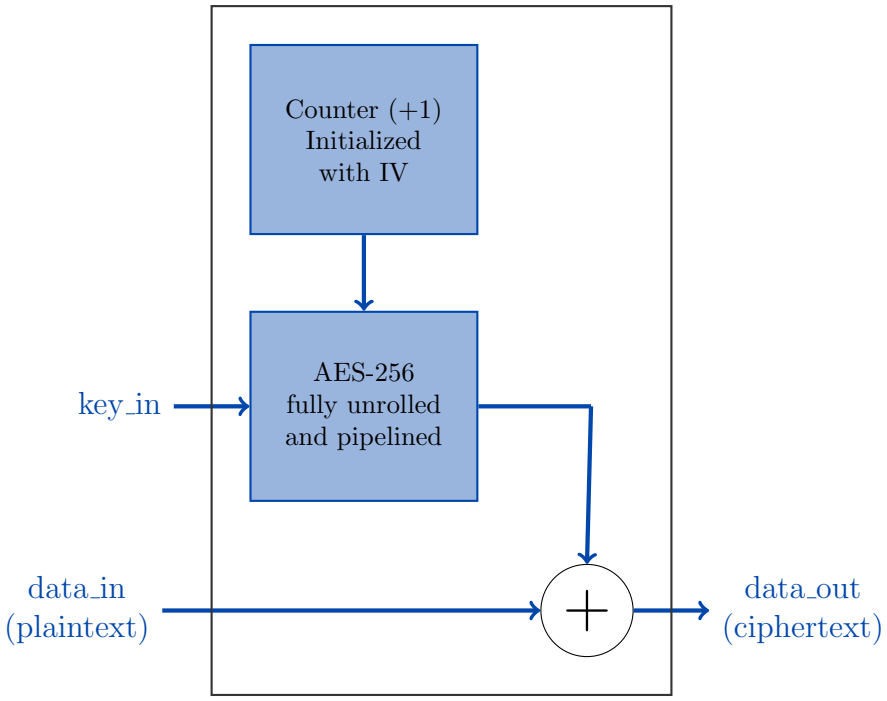

Figure 1: Internal high-level block diagram of XIP1103H, encryption mode

Functionality

XIP1103H encrypts[2] the incoming 128 bits long plaintext blocks by XORing (exclusive-OR) them with the encrypted successive values of a counter. The counter is initialized with a 128 bits long initialization vector[3], which is then incremented by one after each encryption with the same secret key.

XIP1103H is a high-speed version of the Counter mode of operation, and due to the full unrolling of the AES datapath can output a 128 bits long ciphertext block every clock cycle. The key expansion —which is identical for both encryption and decryption operation —is performed on-the-fly and if the same key is used for successive plaintext blocks does not affect the throughput or latency of XIP1103H.

Block Diagram

The internal high-level block diagram of XIP1103H is depicted in Figure 1.

Interfaces

The external interfaces of XIP1103H are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP1103H. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP1103H, example simulation

[2]The operation is identical in the decryption direction, where the only difference is decrypting ciphertext into plaintext.

[3]The initialization vector consists of a 32 bits long nonce, and a 96 bits long initial value.

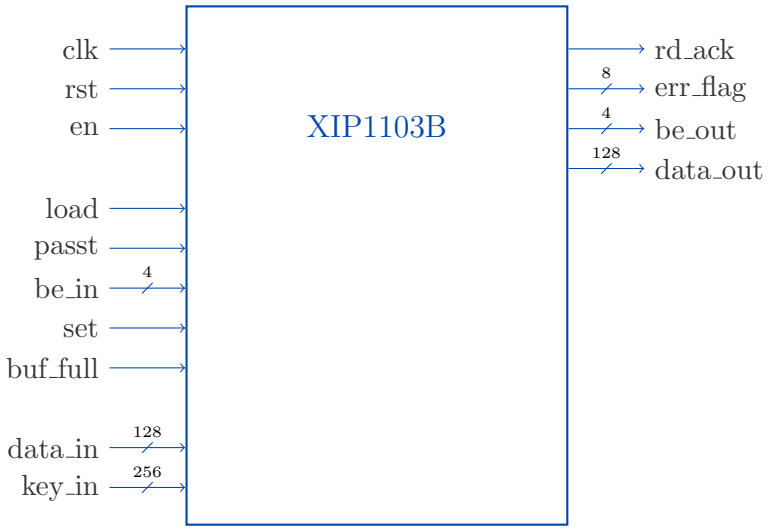

Figure 2: External interfaces of XIP1103H

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 two different FPGA architectures. On request, the resource estimates can also be supplied for other FPGA families.

Device	Resources	f_{MAX}	Max. throughput[‡]
Intel® Cyclone®V [†]	13645 ALM	246 MHz	31.5 Gbps
Xilinx® Virtex® UltraScale+™[⋆]	15414 LUT	782 MHz	100.1 Gbps

[†] Quartus II Prime 19.1., default compilation settings, industrial speedgrade.
[⋆] Vivado 2019.1., performance optimized compilation settings, fastest speedgrade.
[‡] $Throughput = f_{MAX} * 128\ bits$

Table 1: Resource usage and performance of XIP1103H on representative FPGA families.

Example Use Cases

XIP1103H protects the confidentiality of the encrypted plaintext, and to additionally provide authenticity protection XIP1103H can be used as a building block in AES-GCM (Galois Counter Mode) (for example, Xiphera's IP cores XIP1113B and XIP1113H have XIP1103H for confidentiality protection). An alternative way to protect both confidentiality and authenticity is to use XIP1103H in combination with a keyed message authentication code (such as Xiphera's KMAC IP core).

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP1103H 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

XIP1103H protects data confidentiality and is a dual-use product as defined in the Wassenaar Arrangement. Consequently, the export of XIP1103H is controlled by Council Regulation (EC) No 428/2009 of 5 May 2009 and its subsequent changes.

XIP1103H 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). 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.

Contact

Xiphera Oy
Otakaari 5
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.