XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP2201B: ASCON

A Lightweight Cryptographic Suite for AEAD and Hashing

Product Brief
ver. 1.0
April 24, 2023

info@xiphera.com

Introduction

XIP2201B from Xiphera is an Intellectual Property (IP) core for Ascon [2] authenticated encryption with associated data (AEAD) and hashing. It supports three variants of AEAD as well as two variants of hashing and extendable output functions (XOF). Notably, XIP2201B provides three different cryptographic primitives all in one IP core. Ascon was selected by the National Institute of Standards and Technology (NIST) to be standardized as the lightweight cryptographic algorithm [1].

XIP2201B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP2201B does not rely on any FPGA manufacturer-specific features.

Key Features

- **Small Resource Requirements:** XIP2201B requires 2009 Adaptive Lookup Modules (ALMs) (Intel® Cyclone® V E) or 2309 Lookup Tables (LUTs) (Xilinx® Artix-7).
- **Versatile Algorithm Support:** XIP2201B supports ASCON-128/128a/80pq/Hash/Hasha as well as XOF and XOFa. In other words, XIP2201B supports all parameterized algorithms given in [2].
- **Secure Architecture:** The execution time of XIP2201B is independent of the input values and, consequently, provides full protection against timing-based side-channel attacks.
- **Standard Compliance:** XIP2201B is compliant with Ascon specification 1.2 (31.05.2021) [2] which is the version that was selected to be standardized by NIST [1]. Xiphera commits to update XIP2201B when the standardization proceeds to newer versions.

- **Easy Integration:** The 64-bit interface of XIP2201B supports easy integration to various systems.

Functionality

XIP2201B for authenticated encryption and decryption, hashing, and extendable output function operation for all Ascon variants defined in [2]. Ascon was selected as the lightweight cryptographic algorithm by NIST [1] and can thus be expected to see usage in the coming years. The algorithm itself is optimized to be small in size, support many features, and be especially efficient with small inputs.

The XIP2201B is optimized for both moderate resource usage and fast computation.

Block Diagram

The internal high-level block diagram of XIP2201B is depicted in Figure 1.

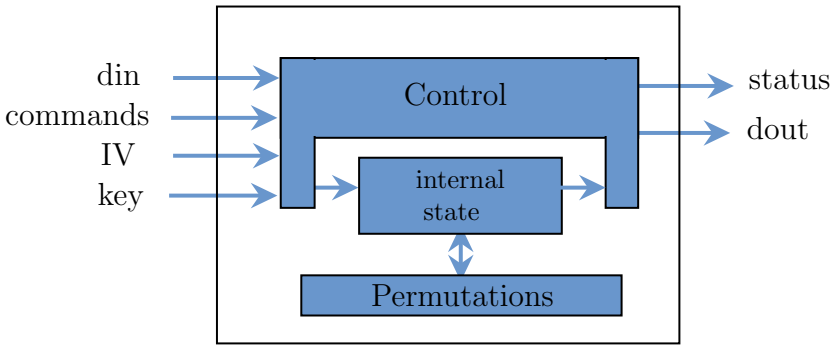

Figure 1: Internal high-level block diagram of XIP2201B

Interfaces

The external interfaces of XIP2201B are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP2201B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP2201B, 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. For in-depth perfomance figures please request and consult the datasheet.

*Throughput $= \frac{64\text{bits}}{13 \text{ clock cycles}} * f_{\text{MAX}}$; for Ascon-128 mode.

†Quartus® Prime Lite 21.1.1, default compilation settings, industrial speedgrade.

‡Vivado 2022.1, default compilation settings, industrial speedgrade.

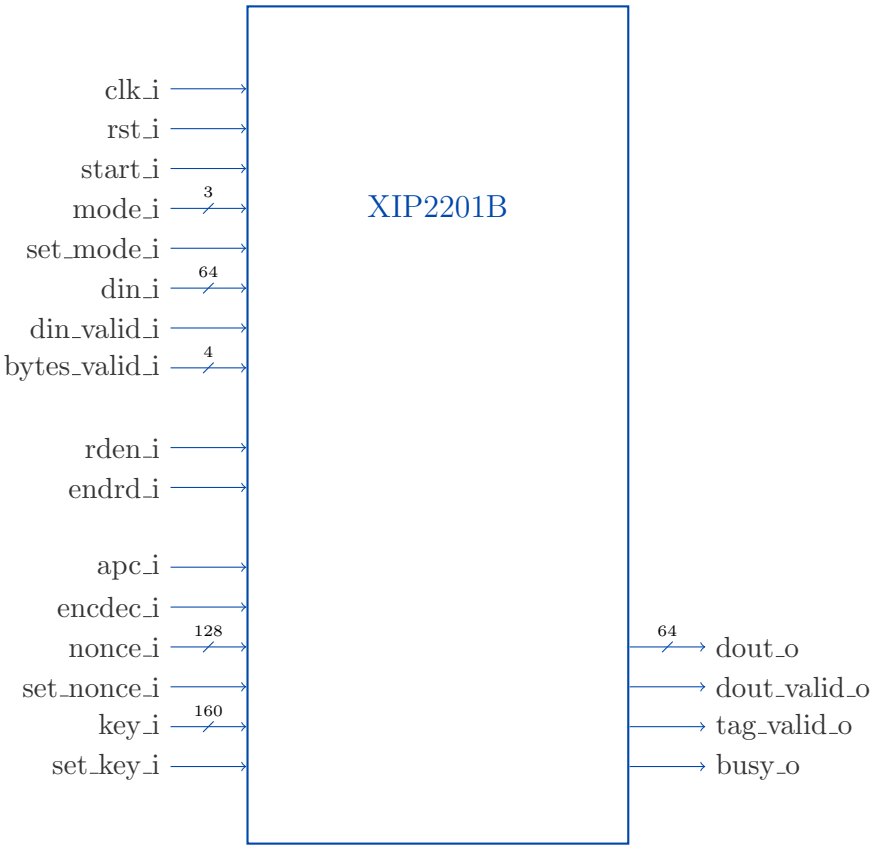

Figure 2: Interface diagram of XIP2201B.

Device	Resources	f_{MAX}	Max. throughput*
Intel® Cyclone® V E†	2009 ALM	180.40 MHz	888.12 Mbps
Xilinx® Artix-7‡	2309 LUT	188.79 MHz	929.4 Mbps
Xilinx® Zynq® Ultrascale+‡	2296 LUT	314.86 MHz	1.550 Gbps

Table 1: Resource usage and performance of XIP2201B on representative FPGA families.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP2201B 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.

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
Tekniikantie 12
FIN-02150 Espoo
Finland
sales@xiphera.com
+358 20 730 5252

References

[1] NIST: Lightweight Cryptography. https://csrc.nist.gov/Projects/lightweight-cryptography.

[2] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. ASCON v1.2 Submission to NIST. Technical report, 2021.