XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

XIP3030C: SHA-3

A Compact Versatile Core for SHA-3-224/256/384/512 and (c)SHAKE-128/256

Product Brief
ver. 1.1.0
April 4, 2024

info@xiphera.com

Introduction

XIP3030C is a compact IP core designed for versatile support of all variants of the SHA-3 hash function and related extendable-output function SHAKE as well as the SHA-3 derived function cSHAKE and its variants KMAC, TupleHash and ParallelHash (including their arbitrary-length output variants). SHA-3 and SHAKE are defined in the NIST (National Institute of Standards and Technology) standard FIPS PUB 202 [1] and cSHAKE, KMAC, TupleHash and ParallelHash are specified in NIST Special Publication 800-185 [2]. Because of the versatile algorithm support, XIP3030C can be used in various applications that require SHA-3 hashing or other supported SHA-3 based functionalities. XIP3030C consumes only small amounts of FPGA resources that allows it to be used even in settings where resources are scarce. SHA-3 plays a central role also in post-quantum cryptography schemes. The design is device-agnostic and fully compliant with various FPGA platforms. XIP3030C offers high level of implementation security and is fully protected against timing attacks as its execution time does not depend on the values of the inputs.

The interface of XIP3030C is pin-wise compatible with XIP3030H, the high-speed versatile SHA-3 core with the same functionalities. The only differences are in performance (latency) and resource requirements. XIP3030C has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP3030C does not rely on any FPGA manufacturer-specific features.

Key Features

- **Minimal Resource Requirements:** XIP3030C requires 673 LUTs with Altera Cyclone® V SX SoC or 1003 6-input LUTs with AMD Zynq-7000® and use only some internal memory blocks in a typical AMD® FPGA implementation.

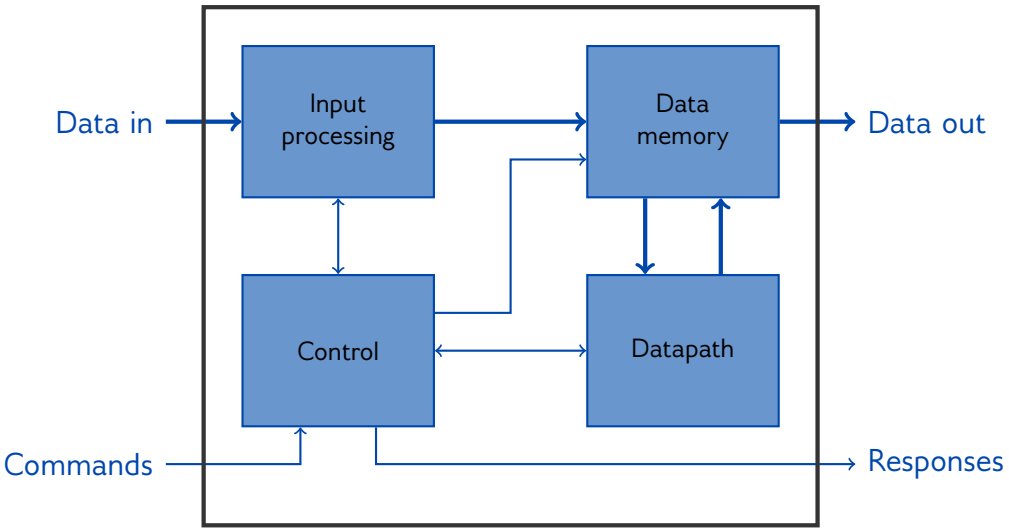

Figure 1: Internal high-level block diagram of XIP3030C

- **Versatile Algorithm Support:** XIP3030C supports SHA-3-224/256/384/512, SHAKE-128/256, and cSHAKE-128/256. That is, XIP3030C covers all algorithms defined in [1] and also all algorithms included in [2] are supported via cSHAKE.
- **Secure Architecture:** The execution time of XIP3030C is independent of the input values and, consequently, provides full protection against timing-based side-channel attacks.
- **Standard Compliance:** XIP3030C is compliant with FIPS 202 [1] and SP 800-185 [2]. XIP3030C can be used as a part of numerous systems and protocols that require SHA-3 or its derivatives.
- **Easy Integration:** The 64-bit interface of XIP3030C supports easy integration to various systems.

Functionality

The main functionality of XIP3030C is to calculate a SHA-3 message digest (also commonly known as a hash value). SHA-3 is a family of hash functions that NIST has standardized in FIPS PUB 202 [1] in August 2015.

In addition to basic hash functions SHA-3-224/256/384/512 with outputs (hashes) of different predefined lengths, XIP3030C supports SHAKE-128 and SHAKE-256. They are *extendable-output functions* (XOFs) defined in [1], and they allow a user to query arbitrary-length output data from the functions while maintaining the security levels of 128 and 256 bits, respectively. Additionally, XIP3030C supports also NIST Special Publication 800-185 [2] by supporting cSHAKE-128 and cSHAKE-256 XOFs.

The XIP3030C is optimised for low resource usage and compact footprint.

Block Diagram

The internal high-level block diagram of XIP3030C is depicted in Figure 1.

Interfaces

The external interfaces of XIP3030C are depicted in Figure 2.

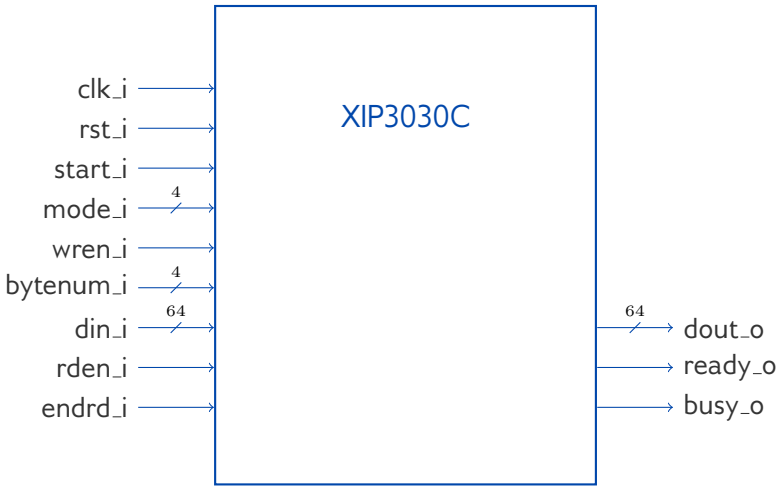

Figure 2: Interface diagram of XIP3030C.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP3030C. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP3030C, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

FPGA Resources and Performance

Table 1 presents the amd® FPGA resource requirements for representative implementations on different amd® FPGA architectures. On request, the resource estimates can also be supplied for other amd® FPGA families. For in-depth perfomance figures please request and consult the datasheet.

Device	Resources	f_{MAX}	Max. throughput*
AMD® Zynq-7000® †	1003 LUT, 1/1 RAMB36/18	151.70 MHz	68.97 Mbps
AMD® Spartan-7® †	977 LUT, 1/1 RAMB36/18	171.38 MHz	77.92 Mbps
AMD® Artix-7® †	978 LUT, 1/1 RAMB36/18	173.88 MHz	79.06 Mbps

Table 1: Resource usage and performance of XIP3030C on representative amd® FPGA families.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP3030C 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.

*$Throughput = \frac{1088}{2376+17} * f_{MAX}$; for SHA3-256 mode.
†Vivado 2022.1, default compilation settings, industrial speedgrade.

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] NIST Computer Security Division. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. FIPS Publication 202, National Institute of Standards and Technology, U.S. Department of Commerce, August 2015.

[2] John Kelsey, Shu jen Chang, and Ray Perlner. SP 800-90A Rev.1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2015.