XIP3327C: HKDF/HMAC/SHA-256/SHA-512

SHA-256 IP Core with Extended Functionalities

Product Brief
ver. 1.0
September 2, 2020
sales@xiphera.com

Introduction

XIP3327C from Xiphera is a versatile Intellectual Property (IP) core designed for SHA-256 and SHA-512 cryptographic hash functions with extended support for HMAC message authentication code and HKDF key derivation function that are based on using SHA-256. SHA-256 and SHA-512 are among the most commonly used hash functions and are used in numerous cryptographic applications. XIP3327C is optimized for low FPGA resource requirements.

XIP3327C has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP3327C does not rely on any FPGA manufacturer-specific features.

Key Features

- **Versatility:** XIP3327C supports the widely used cryptographic hash functions SHA-256 and SHA-512. It also has native support for commonly used message authentication code (HMAC) based on SHA-256 and key derivation function (HKDF) based on HMAC-SHA-256. This allows using XIP3327C for multiple cryptographic functions —for example, TLS 1.3 [4] —more easily and efficiently than an IP core that supports only SHA-256 or SHA-512.

- **Constant Latency:** The execution time of XIP3327C is independent of the message and key values (apart from message length), and consequently provides protection against timing-based side-channel attacks.

- **Compact Size:** XIP3327C has compact size (for example, approximately 1000 LUTs and a three memory blocks in Xilinx® Zynq UltraScale+® family) permitting integration into resource constrained FPGA designs.

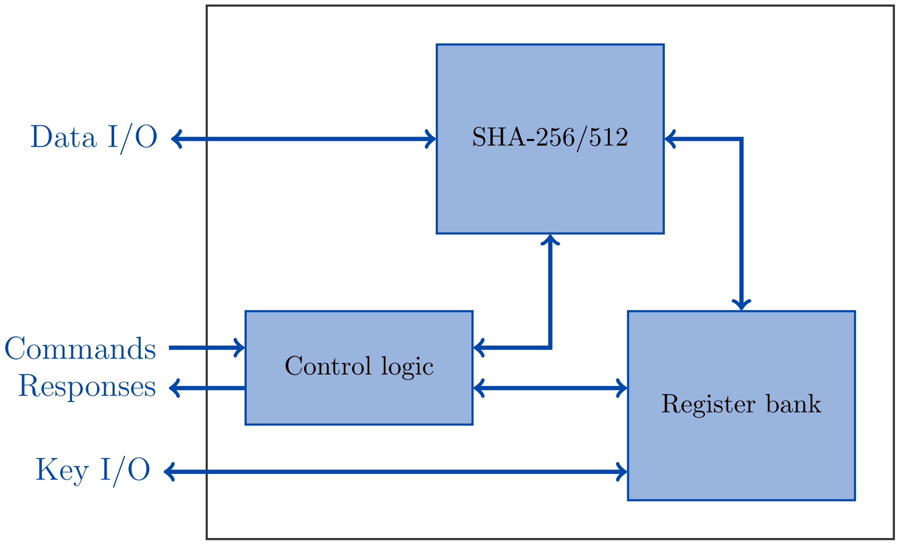

Figure 1: Internal high-level block diagram of XIP3327C

- **Standard Compliance:** XIP3327C is compliant with NIST FIPS 180-4 Secure Hash Standard (SHS) [2], FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC) [1], and RFC 5869 HMAC-based Extract-and-Expand Key Derivation Function (HKDF) [3]. Consequently, XIP3327C can be used in multiple cryptographic applications.

Functionality

XIP3327C supports five main functionalities:

- **SHA-256:** Computes a SHA-256 hash for an input message.
- **SHA-512:** Computes a SHA-512 hash for an input message.
- **HMAC:** Computes an HMAC-SHA-256 authentication tag for an input message using an authentication key.
- **HKDF-extract:** Computes the HKDF-extract function that calculates a pseudorandom key from initial key material.
- **HKDF-expand:** Computes the HKDF-expand function that expands the pseudorandom key to several additional pseudorandom keys of desired lengths for specific cryptographic algorithms.

XIP3327C has a convenient 32-bit FIFO interface allowing for easy integration with rest of the FPGA design. The data inputs are loaded into XIP3327C with byte-level granularity using the `numbytes` signal that denotes the number of active bytes in a 32-bit word (0. . . 4). The key inputs are loaded through a separate port allowing full isolation between keys and data.

Block Diagram

The internal high-level block diagram of XIP3327C is depicted in Figure 1.

Interfaces

The external interfaces of XIP3327C are depicted in Figure 2.

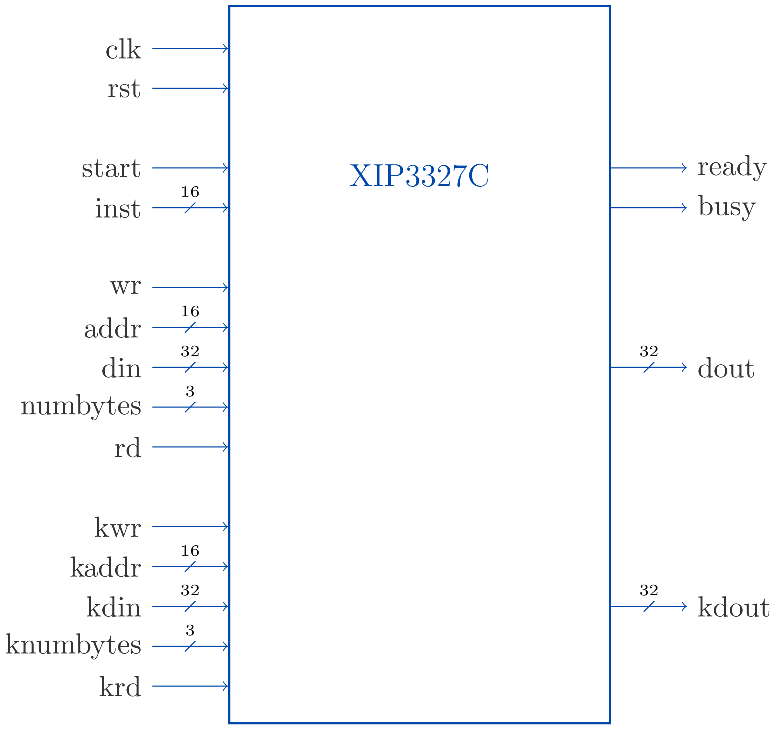

Figure 2: External interfaces of XIP3327C

This Product Brief describes a high-level overview of the functionality and capabilities of XIP3327C. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP3327C, 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 certain FPGAs from two leading FPGA manufacturers. On request, the resource estimates can also be supplied for other FPGA families.

Device	Resources	f_{MAX}
Intel® Cyclone® V†	1230 ALM, 6 M10K	127 MHz
Xilinx® Zynq UltraScale+® ⋆	1012 LUT, 3 BRAM	422 MHz

† Quartus II Prime 19.1, default compilation settings, industrial speedgrade
⋆ Vivado 2019.1., default compilation settings, industrial speedgrade

Table 1: Resource usage and performance of XIP3327C on representative FPGA families.

The general performance characteristics for different functionalities are as follows:

- **SHA-256:** 512-bit blocks of data are processed in 3191 clock cycles (excluding possible interfacing delays).

- **SHA-512:** 1024-bit blocks of data are processed in 9126 clock cycles (excluding possible interfacing delays).
- **HMAC:** An authentication tag computation requires two iterations of SHA-256, but the throughput of the computation approaches the throughput of SHA-256 for long messages.
- **HKDF:** HKDF-Extract and HKDF-Expand both require computation of a single HMAC and their performance is similar to HMAC with short messages.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP3327C 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). 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] FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC). Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2008.

[2] FIPS PUB 180-4 Secure Hash Standard (SHS). Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2015.

[3] Dr. Hugo Krawczyk and Pasi Eronen. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869, May 2010.

[4] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018.