



PEACE OF MIND IN A DANGEROUS WORLD

# XIP3324B: HKDF/HMAC/SHA-512

## SHA-512 IP Core with Extended Functionalities

Product Brief  
ver. 1.0  
September 20, 2023

sales@xiphera.com

---

### Introduction

XIP3324B from Xiphera is a versatile Intellectual Property (IP) core designed for SHA-512 cryptographic hash function with extended support for HMAC message authentication code and HKDF key derivation function that are based on using SHA-512. SHA-512 is one of the most commonly used hash functions and is used in numerous cryptographic applications. XIP3324B offers a good balance between performance and resource requirements.

XIP3324B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP3324B does not rely on any FPGA manufacturer-specific features.

### Key Features

- **Versatility:** XIP3324B supports the widely used cryptographic hash function SHA-512. It also has native support for commonly used message authentication code (HMAC) based on SHA-512 and key derivation function (HKDF) based on HMAC. This allows using XIP3324B for multiple cryptographic functions —for example, TLS 1.3 [4] —more easily and efficiently than an IP core that supports only SHA-512.
- **Constant Latency:** The execution time of XIP3324B is independent of the message and key values (apart from message length), and consequently provides protection against timing-based side-channel attacks.
- **Performance:** XIP3324B provides high performance and reaches hashing speeds of several hundreds of Mbps.
- **Compact Size:** XIP3324B has compact size (for example, 2483 ALMs and, 6 M20K blocks in Intel® Cyclone® 10 GX family) permitting integration into resource constrained FPGA designs.

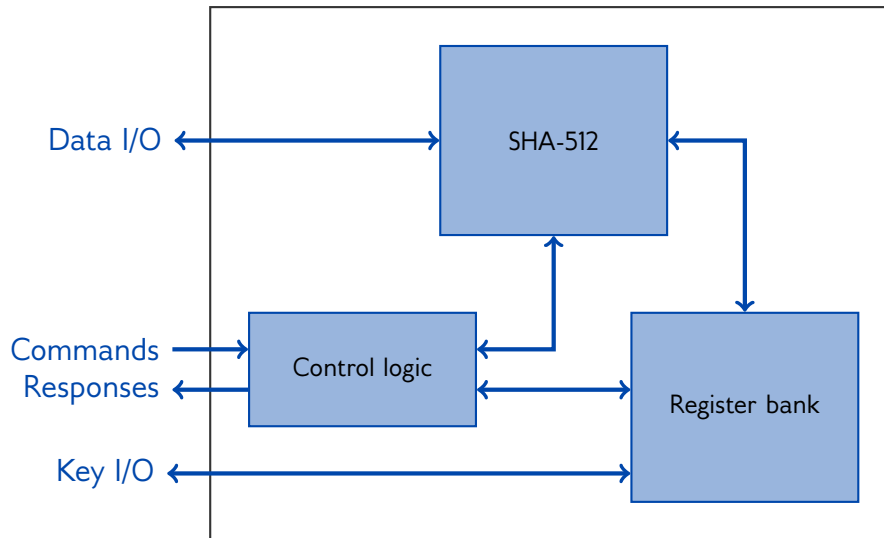


Figure 1: Internal high-level block diagram of XIP3324B

- **Standard Compliance:** XIP3324B 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, XIP3324B can be used in multiple cryptographic applications.

## Functionality

XIP3324B supports four main functionalities:

- **SHA-512:** Computes a SHA-512 hash for an input message.
- **HMAC:** Computes an HMAC 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.

XIP3324B has a convenient 64-bit FIFO interface allowing for easy integration with rest of the FPGA design. The data inputs are loaded into XIP3324B with byte-level granularity using the `numbytes` signal that denotes the number of active bytes in a 64-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 XIP3324B is depicted in Figure 1.

## Interfaces

The external interfaces of XIP3324B are depicted in Figure 2.

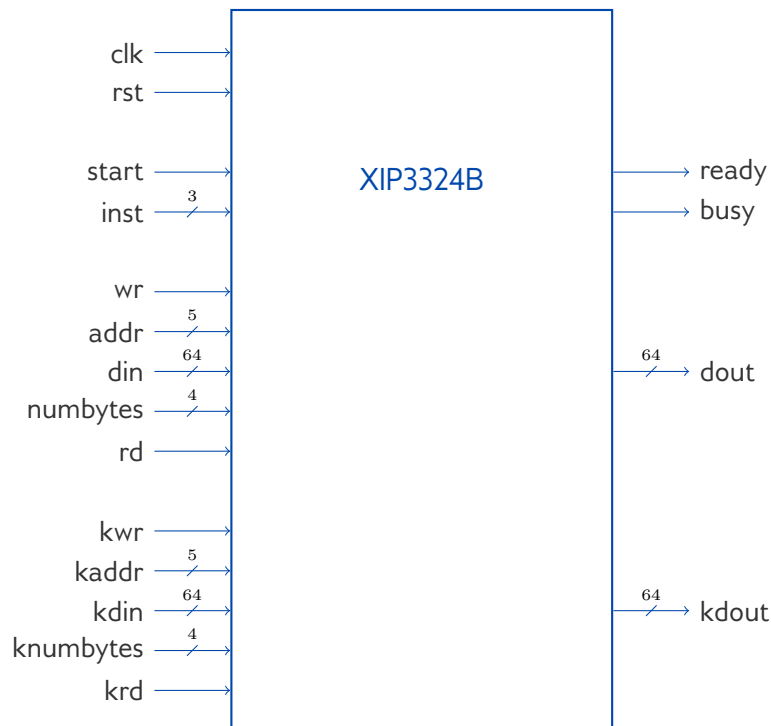


Figure 2: External interfaces of XIP3324B

This Product Brief describes a high-level overview of the functionality and capabilities of XIP3324B. Please contact [sales@xiphera.com](mailto:sales@xiphera.com) for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP3324B, 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® 10 GX*	2483 ALM, 6 M20K	181.32 MHz
Intel® Arria® 10 GX*	2483 ALM, 6 M20K	183.45 MHz
Xilinx® Zynq® MPSoC <sup>†</sup>	2969 LUT, 2 RAMB36	281.85 MHz
Xilinx® Kintex® UltraScale+ <sup>†</sup>	2879 LUT, 2 RAMB36	339.56 MHz
Lattice® ECP5® ‡	4087 LUT4, 6 EBR	87.42 MHz
Microchip® PolarFire® §	5074 4LUT, 6/8 uSRAM/LSRAM	99.33 MHz

Table 1: Resource usage and performance of XIP3324B on representative FPGA families.

The general performance characteristics for different functionalities are as follows:

\*Quartus® Prime Pro 21.1.0, default compilation settings, industrial speedgrade.

<sup>†</sup>Vivado 2022.1, default compilation settings, industrial speedgrade.

- **SHA-512:** XIP3324B can perform SHA-512 hash computations with an asymptotic maximum throughput of  $\frac{f_{MAX} * 1024 \text{ bits}}{86}$  and minimum latency of 95 clock cycles (for at most 64 bit messages)
- **HMAC:** An authentication tag computation requires two iterations of SHA-512, but the throughput of the computation approaches the throughput of SHA-512 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. XIP3324B 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.

## 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. FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC). Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2008.

<sup>‡</sup>Diamond 3.12.0, default compilation settings, synthesised with Synplify.

<sup>§</sup>Libero 2022.1.0.10, default compilation settings, industrial speedgrade.

- [2] NIST Computer Security Division. 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.