XIPHERA

XIP3026B: SHA512, SHA384, SHA512/216 AND SHA512/224

Secure Hash Algorithm (SHA512, SHA384, SHA512/256 and SHA512/224) IP Core

Product Brief
ver. 1.0.1
February 27, 2020

sales@xiphera.com

Introduction

XIP3026B from Xiphera is a balanced Intellectual Property (IP) core implementing the secure hash algorithms SHA512, SHA384, SHA512/216 and SHA512/224 as specified in the Secure Hash Standard published by the National Institute of Standards and Technology (NIST) [1]. The message[1] is parsed and padded into 1024 bits long message blocks, and the resulting message digest (hash value) is either 512, 384, 256 or 224 bits long.

XIP3026B has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP3026B does not rely on any FPGA manufacturer-specific features.

Key Features

- **Compact** resource requirements: The entire XIP3026B requires less than 3200 lookup tables (LUTs) (Xilinx® UltraScale+™ MPSoC), and does not require any multipliers, DSPBlocks or internal memory in a typical FPGA implementation.
- **Performance:** Despite its compact size, XIP3026B achieves a throughput in the Gbps range[2], for example 2.5+ Gbps in Xilinx® UltraScale+™ MPSoC.
- **Standard Compliance:** XIP3026B is fully compliant with the Secure Hash Standard published by the National Institute of Standards and Technology (NIST) [1], and passes the test vectors published by NIST.

[1] The maximum total message size is $2^{128} - 1$ bits.

[2] As is typical for sequential hash algorithms, the highest throughput is achieved for long messages.

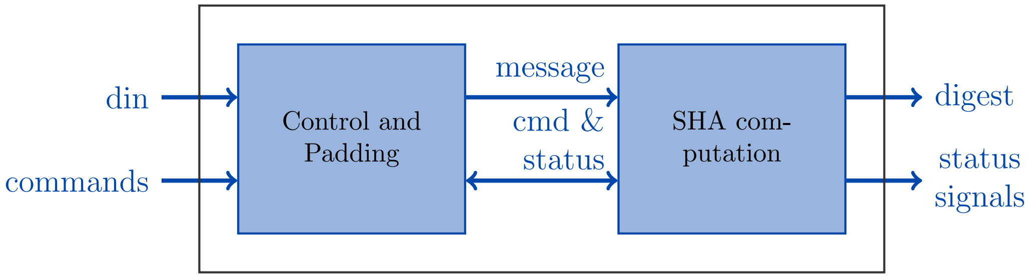

Figure 1: Internal high-level block diagram of XIP3026B

- Byte-orientated **64-bit Interface** eases the integration of XIP3026B with other FPGA logic and/or control software.

Functionality

The main functionality of XIP3026B is to calculate a message digest (also commonly known as a hash value) with a length of either 512 bits (SHA512), 384 bits (SHA384), 256 bits (SHA512/256), or 224 bits (SHA512/224). XIP3026B pads and parses the incoming message into 1024 bits long message blocks as specified in the Secure Hash Standard [1], and adds the length information to the last 64 bits of the last 1024 bits long message block.

After the message digest has been calculated, the result is output during consecutive eight (SHA512), six (SHA384), or four (both SHA512/256 and SHA512/224) clock cycles on the 64 bits wide `digest` output signal.

After the message digest has been output, the hash algorithm in use for the next message can be controlled by changing the value on the input signal `sha_mode`,

Block Diagram

The internal high-level block diagram of XIP3026B is depicted in Figure 1.

Interfaces

The external interfaces of XIP3026B are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP3026B. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP3026B, 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 two different FPGA architectures. On request, the resource estimates can also be supplied for other FPGA families.

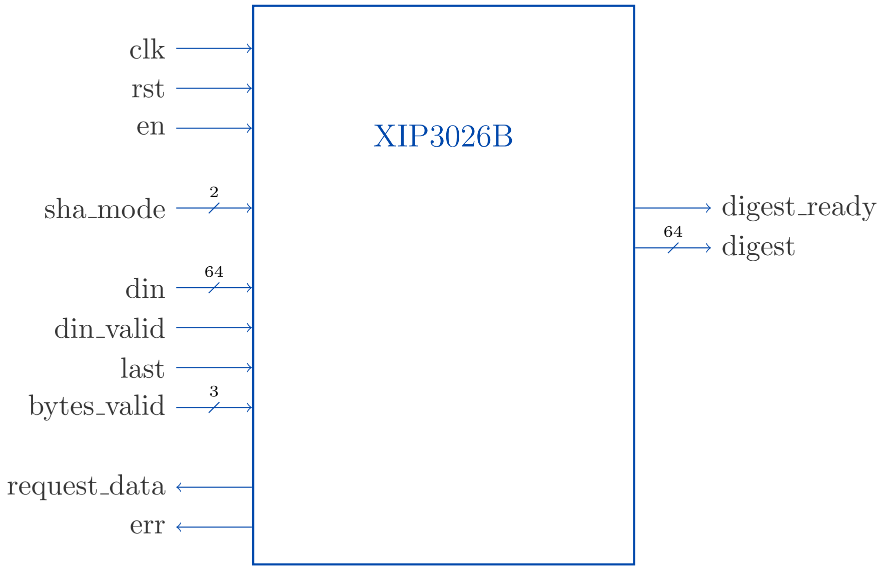

Figure 2: External interfaces of XIP3026B

Device	Resources	f_{MAX}	Max. throughput[‡]
Intel® Cyclone®V [†]	2645 ALM, 2403 REG	56 MHz	691 Mbps
Xilinx® UltraScale+™ MPSoC [⋆]	3159 LUT, 1830 FF	205 MHz	2.53 Gbps

[†] Quartus II Prime 19.1., default compilation settings, industrial speedgrade

[⋆] Vivado 19.1., default compilation settings, industrial speedgrade

[‡] $Throughput = \frac{f_{MAX} * 1024\ bits}{83\ clock\ cycles}$; achieved asymptotically with long packets.

Table 1: Resource usage and performance of XIP3026B on representative FPGA families.

The resource requirements will decrease slightly if support for only hash algorithm (SHA512, SHA384, SHA512/256 or SHA512/224) is required from XIP3026B. Please contact sales@xiphera.com for additional details.

Example Use Cases

The hashing algorithms supported by XIP3026B (SHA512, SHA384, SHA512/256 and SHA512/224) have numerous use cases in communications message and stored data authentication, and XIP3026B can also be used in FPGA-based implementations of blockchain technology.

As per the Secure Hash Standard [1], XIP3026B implements a keyless message digest calculation algorithm. In case a keyed hashing algorithm is required, Xiphera IP cores XIP3322B (HKDF and HMAC based on SHA256) and XIP3327C (HKDF and HMAC-SHA256 and SHA256/512) are recommended.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP3026B 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 180-4 Secure Hash Standard (SHS). Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2015.