XIP3034H: SHA3-512

Secure Hash Algorithm-3 (512 bit digest) IP Core

Product Brief
ver. 1.0.1
February 13, 2020

sales@xiphera.com

Introduction

XIP3034H from Xiphera is a high-speed Intellectual Property (IP) core implementing the Secure Hash Algorithm-3 [1] with a 512 bits long message digest (hash). The SHA-3 family of hash functions are based on the *Keccak* sponge function, and their internal structure is different from the SHA-2 family of hash functions which are based on the Merkle-Damgård structure. The hashing speeds achieved with FPGA-based implementations of SHA-3 are faster than those achieved with SHA-2, and consequently SHA-3 hash functions are a strong candidate for applications where the primary goal is to maximimize throughput.

XIP3034H has been designed for easy integration with FPGA- and ASIC-based designs in a vendor-agnostic design methodology, and the functionality of XIP3034H does not rely on any FPGA manufacturer-specific features.

Key Features

- **Performance:** Despite its modest size, XIP3034H achieves a throughput in the 10+ Gbps range[1], for example 11+ Gbps in Xilinx® UltraScale+™ MPSoC.
- **Modest Resource Requirements:** The entire XIP3034H requires 3.3k ALMs (Adaptive Lookup Modules), and does not require any multipliers, DSPBlocks or internal memory in a typical FPGA implementation.
- **Standard Compliance:** XIP3034H is fully compliant with the Secure Hash Algorithm-3 published by the National Institute of Standards and Technology (NIST) [1], and passes the test vectors published by NIST.
- Byte-orientated **64-bit Interface** eases the integration of XIP3034H with other FPGA logic and/or control software.

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

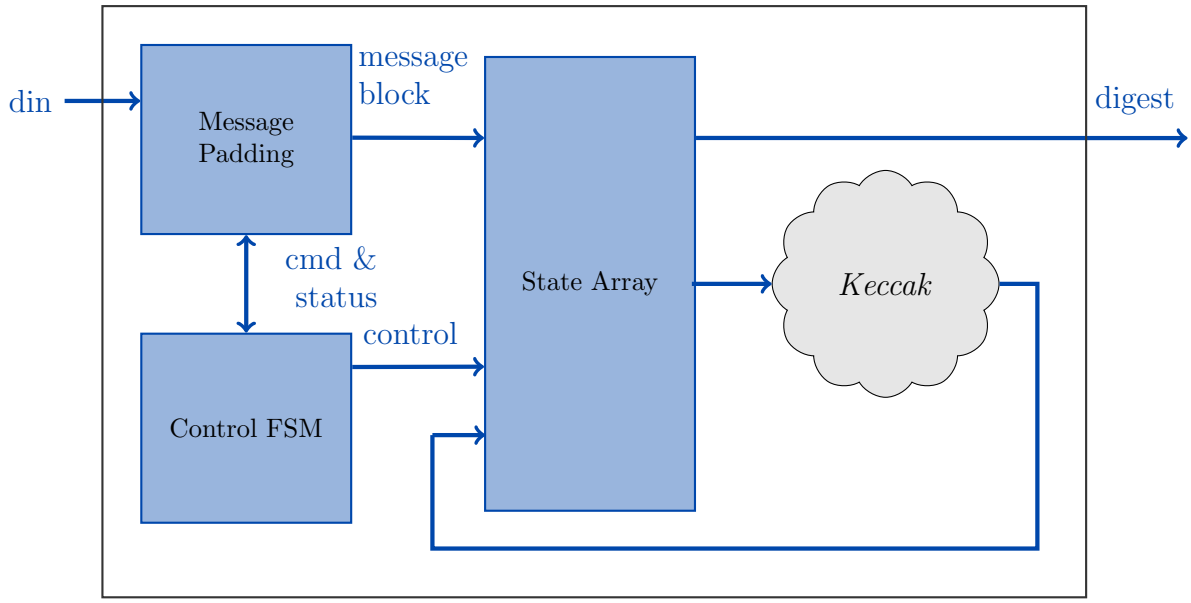

Figure 1: Internal high-level block diagram of XIP3034H

Functionality

The main functionality of XIP3034H is to calculate a message digest (also commonly known as a hash value) with a length 512 bits. XIP3034H pads the incoming message into 576 bits long message blocks[2] as specified in the Secure Hash Algorithm-3 [1], absorbs the message blocks into the 1600 bits long state array, and runs the *Keccak* algorithm for twenty-four (24) rounds after each message block has been absorbed[3].

After the last incoming message has been received, XIP3034H finalized the message digest calculation, and the resulting message digest is output during consecutive eight clock cycles on the 64 bits wide `digest` output signal.

Block Diagram

The internal high-level block diagram of XIP3034H is depicted in Figure 1.

Interfaces

The external interfaces of XIP3034H are depicted in Figure 2.

This Product Brief describes a high-level overview of the functionality and capabilities of XIP3034H. Please contact sales@xiphera.com for a complete datasheet with a detailed description of the input and output signals, startup procedure of XIP3034H, example simulation waveforms, and the FPGA resource requirements of your targeted FPGA family.

[2]This is also called the block size or rate of SHA3-512, and can be calculated as $1600 - capacity$, where 1600 is the size of the Keccak state array, and capacity is defined as twice the length of the digest (512 bits in the case of SHA3-512).

[3]The total number of clock cycles to process one message block is 25—*Keccak* for 24 clock cycles and one additional clock cycle for the absorbing phase.

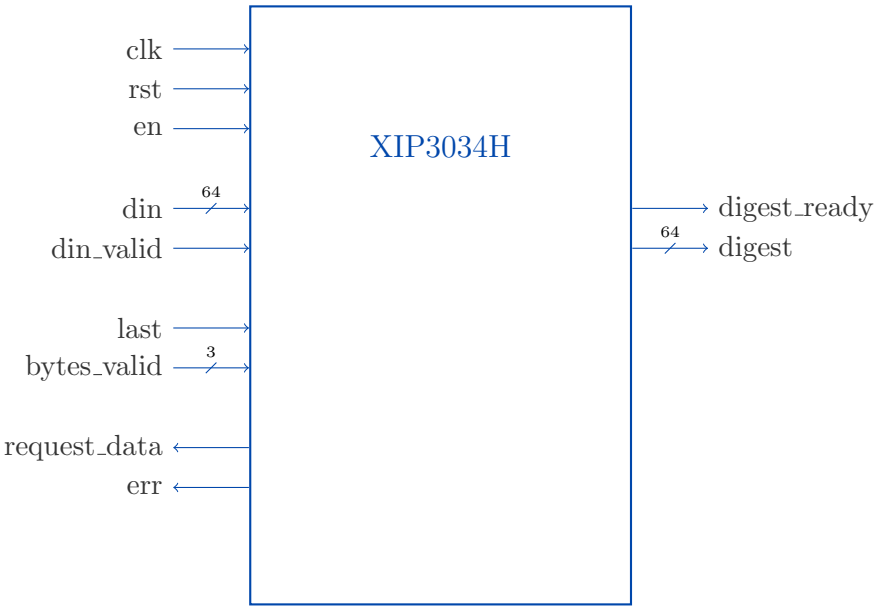

Figure 2: External interfaces of XIP3034H

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. The high throughput figures are mostly due to a highly optimized, efficient, and FPGA-friendly implementation of the *Keccak* algorithm..

Device	Resources	f_{MAX}	Max. throughput[‡]
Intel® Stratix®10 [†]	3279 ALM, 2276 REG	368 MHz	8.5 Gbps
Xilinx® UltraScale+™ MPSoC [⋆]	4156 LUT, 2285 FF	505 MHz	11.6 Gbps

[†] Quartus Prime Pro 19.3., default compilation settings, industrial speedgrade
[⋆] Vivado 19.1., default compilation settings, industrial speedgrade
[‡] $Throughput = \frac{f_{MAX} * 576\ bits}{25\ clock\ cycles}$

Table 1: Resource usage and performance of XIP3034H on representative FPGA families.

Example Use Cases

The SHA3-512 hashing algorithm supported by XIP3034H has numerous use cases in communications message and stored data authentication, and XIP3034H can also be used in FPGA-based implementations of blockchain technology.

XIP3034H implements a keyless message digest calculation algorithm. In case a keyed hashing algorithm based on the *Keccak* sponge function is required, please contact sales@xiphera.com for a KMAC (KECCAK Message Authentication Code) IP core.

Ordering and Deliverables

Please contact sales@xiphera.com for pricing and your preferred delivery method. XIP3034H 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] 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.