BERTEN
Secure Communications

SHA3-B219 IP Core

SHA-3 Hash Crypto Engine

High Throughput
Low Resource Utilisation
Register-based Configuration

Features

- Cryptographic Hashing
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- Extendable-Output Functions
  - SHAKE128, cSHAKE128
  - SHAKE256, cSHAKE256
- KMAC Support
- Context Switching
- FIPS 202, FIPS 140-3 Compliant
- Portable to any FPGA or ASIC
- AMBA AXI Interfaces

Applications

- Digital Signature
- User Authentication
- Encrypted Data Storage
- Secure Communications
- Post-Quantum Cryptography

The **SHA3-B219** is a crypto IP Core for hardware offloading of Hash algorithms in FPGA, SoC, and ASIC technologies.

The engine implements the Secure Hash Algorithm 3 (SHA-3) family according to FIPS 202 standard, including fixed-length (SHA3-224, SHA3-256, SHA3-384, SHA3-512) and extendable-output functions (SHAKE128, SHAKE256). It also supports the cSHAKE and KMAC (KECCAK Message Authentication Code) operations according to NIST 800-185.

SHA3-B219 implements the KECCAK sponge construction, including the insertion of the domain separation suffix, message padding, and data permutation functions.

With the context switching functionality, the internal state of the KECCAK engine can be saved and restored as needed to process other data.

Portable to any Xilinx, Intel, or Microsemi device, the IP Core is compliant with FIPS 140-3 and provides the highest performance in a minimum area.

SHA3-B219 includes AMBA AXI interfaces and a register map with user-programmable parameters to select the Hash function, the length of the XOFs digest, and the cSHAKE / KMAC configuration. ANSI C drivers are provided for a fast integration into the target platform.

© BERTEN DSP S.L.

www.bertendsp.com sales@bertendsp.com +34 942 18 10 11

SHA-3 Functions

The SHA3-B219 IP Core implements the following cryptographic algorithms specified in the FIPS 202 and NIST 800-185 standards:

- Fixed-Length Hash Functions
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- Extendable-Output Functions (XOFs)
  - SHAKE128, cSHAKE128
  - SHAKE256, cSHAKE256
- Keyed Hash Functions
  - KMAC128
  - KMAC256

Based on the KECCAK algorithm, the IP Core implements the sponge construction of the SHA-3 standard, which includes the insertion of the domain separation suffix, padding of the input string, and permutation using the KECCAK-*p* mathematical function.

Performance

For each SHA-3 function, the following table provides the performance considering a clock reference of 300 MHz.

Function	Performance, Gbps @300MHz
SHA3-224	14.4
SHA3-256	13.6
SHA3-384	10.4
SHA3-512	7.2
SHAKE128, cSHAKE128	15.5
KMAC128	15.5
SHAKE256, cSHAKE256	13.6
KMAC256	13.6

Interfaces

The IP Core includes three 64-bit AXI4-Stream interfaces for high-speed transfer of the input message, the KMAC key, and the output hash value. The AXI4-Lite interface provides access to the register map for selecting the SHA-3 function, the length of the SHAKE digest, and the cSHAKE / KMAC parameters.

Resources

Resource utilisation for different devices is provided in the table below. Metrics for any Xilinx, Intel, or Microsemi FPGA or SoC are available as required.

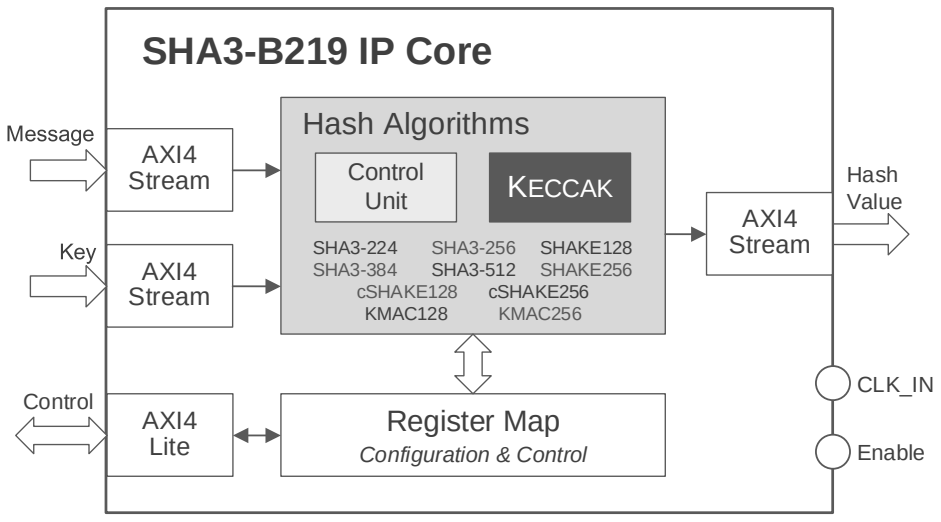
	Device Family	LUT	Register
Xilinx	Spartan-7, Artix-7, Kintex-7, Virtex-7	5.2K	4.5K
	Kintex/Virtex Ultrascale	5.2K	4.5K
	Artix/Kintex/Virtex Ultrascale+	5.2K	4.5K
	Versal ACAP	4.9K	4.5K
Intel	MAX 10, Cyclone 10 LP	8.4K	4.5K
	Cyclone V	5.5K	4.5K
	Arria 10	5.5K	4.5K
	Stratix V	5.5K	4.5K

Licensing

The IP Core is provided as encrypted netlist for one device family, under a perpetual Site Licence. It includes 12 months of maintenance and support for the integration of the module in your platform.

Deliverables

- Targeted, timing closed Netlist
- Design Constraints
- Simulation Model
- User Manual
- ANSI C drivers



© BERTEN DSP S.L.

www.bertendsp.com sales@bertendsp.com +34 942 18 10 11