BERTEN
Digital Signal Processing

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
- SHAKE256

FIPS 202 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. It includes fixed-length (SHA3-224, SHA3-256, SHA3-384, SHA3-512) and extendable-output functions (SHAKE128, SHAKE256).

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

Portable to any Xilinx, Intel, or Microsemi device, the IP Core 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 and the length of the XOFs digest. ANSI C drivers are provided for a fast integration into the target platform.

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

SHA-3 Functions

The SHA3-B219 IP Core implements the cryptographic Hash algorithms specified in the FIPS 202 standard, including:

- Fixed-Length Hash Functions
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- Extendable-Output Functions (XOFs)
  - SHAKE128
  - SHAKE256

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	15.5
SHAKE256	13.6

Interfaces

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

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.

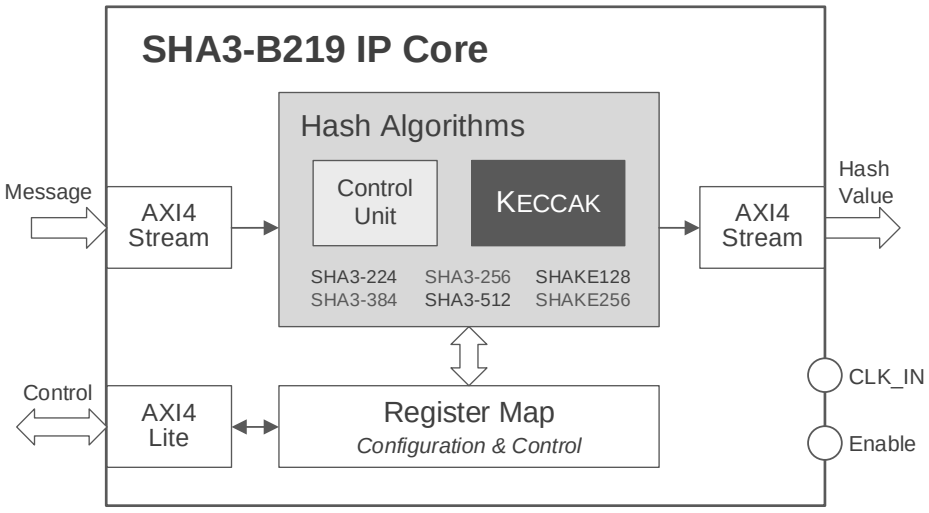
	Device Family	LUT	Register
Xilinx	Spartan-7, Artix-7, Kintex-7, Virtex-7	4.2K	3.6K
	Kintex/Virtex Ultrascale	4.2K	3.6K
	Kintex/Virtex Ultrascale+	4.2K	3.6K
	Versal ACAP	3.9K	3.6K
Intel	MAX 10 / Cyclone 10 LP	6.9K	3.6K
	Cyclone V	4.3K	3.6K
	Arria 10	4.3K	3.6K
	Stratix V	4.3K	3.6K

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
- User Manual
- ANSI C drivers



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