BERTEN
Secure Communications

SHA2-B209 IP Core

SHA-2 Hash Crypto Engine

High Throughput
Register-based Configuration
HMAC and HKDF Functions

Features

Cryptographic Hashing
- SHA-224
- SHA-256
- SHA-384
- SHA-512
- SHA-512/224
- SHA-512/256

HMAC, HKDF Support
FIPS 180-4, FIPS 140-3 Compliant
FIPS 198-1, RFC 2104 Compliant
RFC 5869 Compliant
Portable to any FPGA or ASIC
AMBA AXI Interfaces

Applications

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

The **SHA2-B209** is a crypto IP Core for hardware offloading of Hash algorithms in FPGA, SoC, and ASIC technologies.

The engine implements the Secure Hash Algorithm-2 (SHA-2) family according to FIPS 180-4 standard. It includes SHA-224, SHA-256, SHA-384, and SHA-512 functions, and the truncated variants SHA-512/224 and SHA-512/256.

SHA2-B209 supports HMAC (Keyed-Hash Message Authenticated Code) and HKDF (HMAC-based Key Derivation Function) operations, being possible to use any of the hash primitives as underlying function.

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.

SHA2-B209 includes AMBA AXI interfaces and a register map with user-programmable parameters to select the operation mode, hash algorithm, and HKDF output length. ANSI C drivers are provided for a fast integration into the target platform.

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

Hash Algorithms

The SHA2-B209 IP Core implements the following SHA-2 algorithms specified in the FIPS 180-4 standard:

- SHA-224
- SHA-256
- SHA-384
- SHA-512
- SHA-512/224
- SHA-512/256

The high-throughput SHA-2 engine executes these cryptographic primitives based on the Merkle-Damgård construction. Message padding according to FIPS 180-4 is applied to the input data.

Operation Modes

In addition to cryptographic hashing, the IP Core supports the following functions:

- HMAC, compliant with FIPS 198-1 and IETF RFC 2104 standards.
- HKDF, Extract and Expand operations according to IETF RFC 5869.

Performance

The following table provides the hashing performance considering a clock reference of 300 MHz.

Function	Performance, Gbps @300MHz
SHA-224, SHA-256	2.3
SHA-384, SHA-512, SHA-512/224, SHA-512/256	3.8

Interfaces

The IP Core includes three 64-bit AXI4-Stream interfaces for high-speed transfer of the key, input, and output data. An AXI4-Lite interface provides access to the register map for selecting the operation mode, SHA-2 algorithm, and HKDF-Expand output length. A Status port is available for event notification.

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.

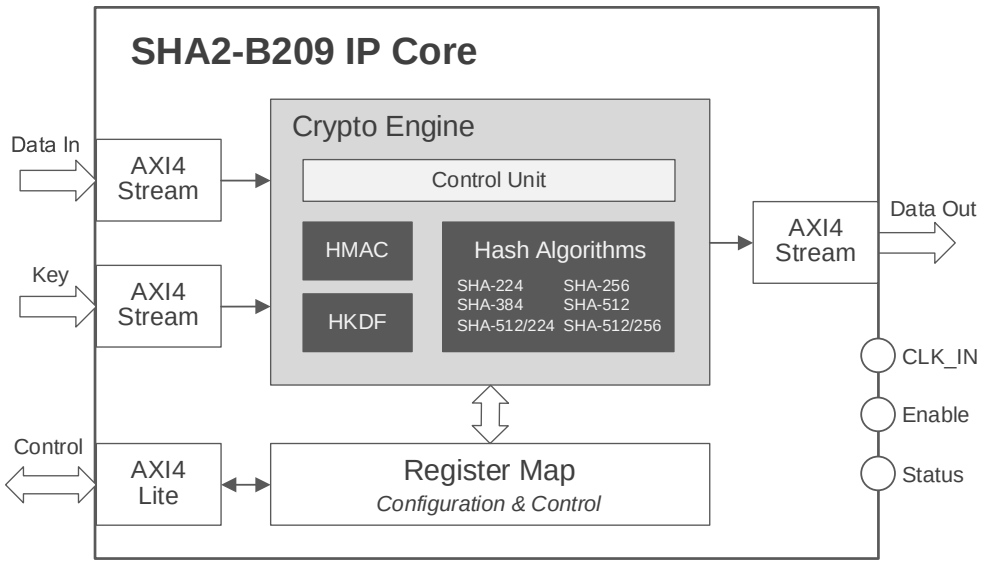
	Device Family	LUT	Register
Xilinx	Spartan-7, Artix-7, Kintex-7, Virtex-7	3.5K	2.6K
	Kintex/Virtex Ultrascale	3.5K	2.6K
	Artix/Kintex/Virtex Ultrascale+	3.5K	2.6K
	Versal ACAP	3.5K	2.6K
Intel	MAX 10, Cyclone 10 LP	5.8K	2.5K
	Cyclone V	3.7K	2.5K
	Arria 10	3.7K	2.5K
	Stratix V	3.7K	2.5K

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
- User Manual
- ANSI C drivers



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