SHA-3

SHA-3 Secure Hash Crypto Engine

Microsemi

The SHA-3 is a high-throughput, area-efficient hardware implementation of the SHA-3 cryptographic hashing functions, compliant to NIST's FIPS 180-4 and FIPS 202 standards.

The core implements all the fixed-length and extendable hashing functions provisioned by these standards. The hashing function is synthesis-time configurable; a version supporting run-time hashing function selection can be made available upon request.

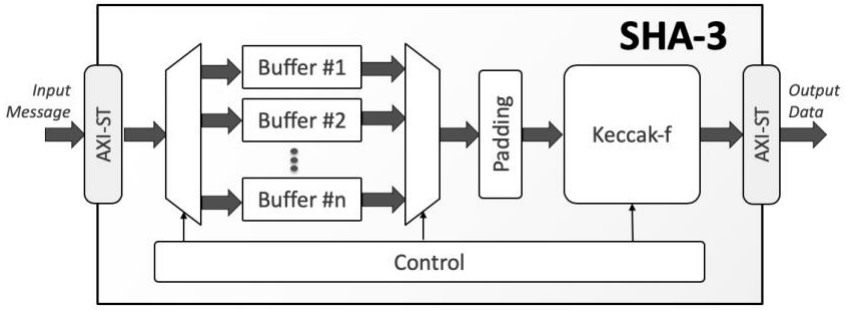
The SHA-3 core's processing bit rate is impressively high even in its minimum throughput configuration, for which it processes 24 to 56 bits per cycle depending on the hashing function. This high throughput can scale to practically meet any processing rate. The number of hashing rounds per clock is configurable at synthesis time, allowing users to scale performance at the cost of silicon resources when desired.

The core is designed for ease of use and integration and adheres to industry best-standards coding and verification practices. It requires no assistance from a host processor, and uses standard AMBA® AXI4-Stream interfaces for input and output data. Technology mapping, and timing closure are trouble-free, as the core contains no multi-cycle or false paths, and uses only rising-edge-triggered D-type flip-flops, no tri-states, and a single-clock/reset domain. Its reliability and low risk have been proven through rigorous verification and FPGA validation.

Applications

The SHA-3 IP core can ensure data integrity and/or user authentication in a range of applications including IPsec and TLS/SSL protocol engines, encrypted data storage, secure processing systems, e-commerce, and financial transaction systems.

Block Diagram



Sample Implementation Results

The SHA-3 can be mapped to any Microsemi device, provided sufficient silicon resources are available. Sample implementation results for a limited set of configurations implemented on a RTG4 (STD speed grade) device are provided in the following table. Please note that the figures on this table do not represent the highest clock frequency or smallest area possible for the core.

Hash Function	Rounds per Cycle	Number of Buffers	4LUTs	Freq. (MHz)	Gbps
SHA3-224	1	1	7,411	50	2.40
SHA3-224	4	1	20,161	50	5.76
SHA3-256	1	1	7,124	50	2.27
SHA3-384	1	1	7,297	40	1.39
SHA3-512	1	1	5,752	50	1.20
SHAKE-128	1	1	7,768	50	2.80
SHAKE-256	1	1	7,147	40	1.81

FEATURES

Standards Support

- FIPS 202: SHA-3 - Permutation-Based Hash and Extendable-Output Function
- FIPS 180-4: Secure Hash Functions (limited to SHA-3 use)
- All four fixed-length SHA-3 Hash Functions:
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
- Both SHA-3 Extendable Output Functions (XOF):
  - SHAKE-128
  - SHAKE-256

Performance

- User-selectable (1 to 4) permutation rounds per clock cycle, resulting in a throughput of:
  - SHA3-224: 48.0. to 192 Mbits/MHz
  - SHA3-256: 45.3 to 181.2 Mbits/MHz
  - SHA3-384: 34.7 to 138.8 Mbits/MHz
  - SHA3-512: 24.0 to 96 Mbits/MHz
  - SHAKE-128: 56.0 to 224 Mbits/MHz
  - SHAKE-256: 45.3 to 181.2 Mbits/MHz
- Intelligent buffers management optionally allows receiving new input while processing the previous message

Interfaces

- AMBA® AXI4-Stream

Fully autonomous operation

- Requires no assistance from the host processor
- Automatic padding insertion

Configuration Options

- Hashing function (bit-rate, capacity, number of permutation rounds)
- Input & output bus bit-width
- Number of input buffers
- Number of rounds per cycle

Deliverables

- Verilog RTL source code or targeted FPGA netlist
- Integration Test-Bench
- Bit Accurate C Model
- Simulation & synthesis scripts
- User documentation

Sourced from BEYOND SEMICONDUCTOR