SHA-3

SHA-3 Secure Hash Crypto Engine

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.

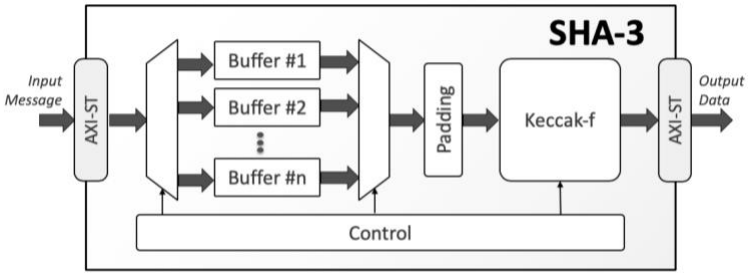
The number of SHA-3 permutation rounds per clock cycle is configurable at synthesis time, allowing users to trade throughput for silicon resources. Under its minimum configuration of one permutation per cycle, the core processes 24 to 56 bits per cycle depending on the hashing function. This throughput can scale by a factor of 2x, 3x, or 4x by implementing 2, 3, or 4 permutations per cycle respectively, enabling throughputs in excess of 100Gbps in modern ASIC technologies.

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, timing closure, and scan insertion 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

Sample implementation results for a limited set of the SHA3 core configurations are provided in the following table.

Configuration	Rounds per Cycle	Number of Buffers	Target Technology	Area (kGates)	Freq. (MHz)	Gbps
SHAKE-128	1	1	TSMC 7nm	49.8	1,800	100.8
SHAKE-256	1	1	TSMC 7nm	43.5	1,800	81.6
SHA-512	1	1	TSMC 7nm	36.7	1,900	45.6
SHA-384	1	1	TSMC 7nm	43.7	1,900	65.9
SHA-256	1	1	TSMC 7nm	44.4	1,800	81.6
SHA3-224	1	1	TSMC 7nm	47.3	1,800	86.4
SHA3-224	2	1	TSMC 7nm	83.3	1,300	124.8
SHA3-224	4	1	TSMC 7nm	120.8	700	192.0
SHA3-224 (12-rounds)	3	2	TSMC 7nm	110.9	900	259.0

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
- Throughput in excess of 100 Gb/s in modern ASIC technologies
- 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