SHA-3

Secure Hash Crypto Engine

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

The accelerator core requires no assistance from a host processor and uses standard AMBA® AXI4-Stream interfaces for input and output data. An AXI4-Stream to AXI4 Memory Mapped bridge, with or without DMA capabilities, can be used with the core and is separately available from CAST. A single instance of the core implements all fixed-length and extendable-output hash functions. The cryptographic function, the length of the extendable output function (up to 2GB) is chosen at run time via AXI4-Stream side-band signals and can be different for every input message.

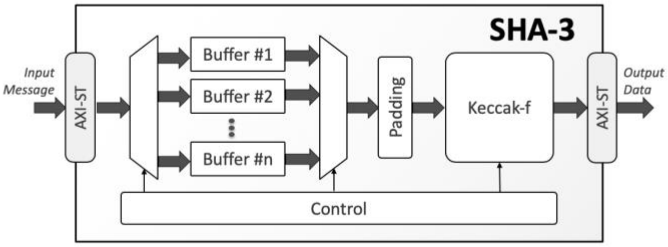
The SHA-3 core is also highly configurable at synthesis time, to ease integration in systems with different requirements. The data-bus width of the input and output interfaces is configurable at synthesis time. The number of SHA-3 permutation rounds per clock cycle is also configurable at synthesis time, allowing users to trade throughput for silicon resources. Under its minimum configuration of one permutation per cycle, the core processes 50 bits per cycle depending on the hashing function. Its throughput can scale by implementing 2, 3, or 4 permutations per cycle respectively, enabling high throughputs even in low-end FPGA devices.

The core is designed for ease of use and integration and adheres to industry-best coding and verification practices.

Applications

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

Block Diagram



Sample Implementation Results

The SHA-3 IP core can be implemented in any Microsemi FPGA provided sufficient resources are available. Sample implementation results for a limited set of configurations are provided in the following table. Please, note that the list of configurations is not exhaustive, and that the indicated clock frequency is not the highest possible.

FPGA Device	Configuration			Logic Resources	Memory Resources	Freq. (MHz)
	Input / Output Bit-Width	Rounds per Cycle	Number of Buffers			
RTG4 rt4g150-std	32	1	0	7,162 4LUT	–	85
RTG4 rt4g150-std	64	1	1	9,302 4LUT	–	85
RTG4 rt4g150-std	64	1	2	9,687 4LUT	–	80
RTG4 rt4g150-std	128	2	2	15,185 4LUT	–	65

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
  - Up to 50 Mbits/MHz for one permutation per cycle
  - Up to 150 Mbits/MHz for four permutations per cycle
- Intelligent buffers management optionally allows receiving new input while processing the previous message
- Optional dynamic control of the number of permutation rounds

Interfaces

- AMBA® AXI4-Stream

Fully autonomous operation

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

Configuration Options

- Input & output bus bit-width
- Number of input buffers
- Number of permutations per cycle
- Enable/disable dynamic control of permutation rounds

Deliverables

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