

CAST

SHA-3

SHA-3 Secure Hash Function Core

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

- Scalable throughput starting from:
 - SHA3-224: 48.0 Mbits/MHz
 - SHA3-256: 45.3 Mbits/MHz
 - SHA3-384: 34.7 Mbits/MHz
 - SHA3-512: 24.0 Mbits/MHz
 - SHAKE-128: 56.0 Mbits/MHz
 - SHAKE-256: 45.3 Mbits/MHz
- Intelligent buffers management optionally allows receiving new input while processing previous message
- Throughput over 20 Gb/s in most modern ASIC technologies

Interfaces

- AMBA® AXI4-Stream

Fully autonomous operation

- Requires no assistance from host processor
- Automatic padding insertion

Configuration Options

- Hashing function
- Input & output bus bit-width
- Number of input buffers
- Number of Hash rounds per cycle

Deliverables

- Verilog RTL source code or targeted FPGA netlist
- Integration Test-Bench
- Software C-Model
- User documentation

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.

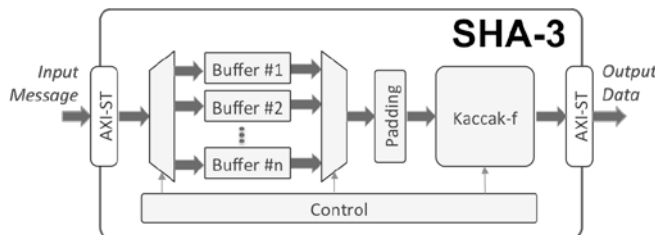
The SHA-3 core's processing bitrate is impressively high even in its minimum throughput configuration, for which it processes 24 to 56 bits per cycle depending on the hashing function. This high throughput can scale to practically meet any processing rate. The number of hashing rounds per clock is configurable 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-practices 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 the minimum throughput configuration of the core implemented on a 28nm technology (TSMC hpm-sc9-svt-c31) are provided in the following table.

Area (Gates)						Freq. (MHz)	Number of In. Buffers
SHA3-224	SHA3-256	SHA3-384	SHA3-512	SHAKE-128	SHAKE-256		
33.3k	30.0k	29.1k	27.8k	32.5k	30.4k	700	0
48.3k	46.8k	42.8k	36.8k	52.6k	47.6k	700	2

Note that these sample implementation figures do not represent the highest speed or smallest area possible for the core.