BEYOND SHA-3 IP CORE

Hardware Secure Hash Algorithm-3 Implementation

OVERVIEW

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

Providing all four hash functions, Beyond's SHA-3 hardware implementation has been optimized for applications that require fast block processing without excessive logic utilization. Simple input / output interface, adjustable bus widths and module properties, allow designers to seamlessly adapt the core to desired architectures, meeting demanding speed and area requirements.

The Beyond SHA-3 IP core is delivered as a firm core to any library requested by customer. The package includes fully synthesisable RTL source code, verification suites, simulation model, and documentation.

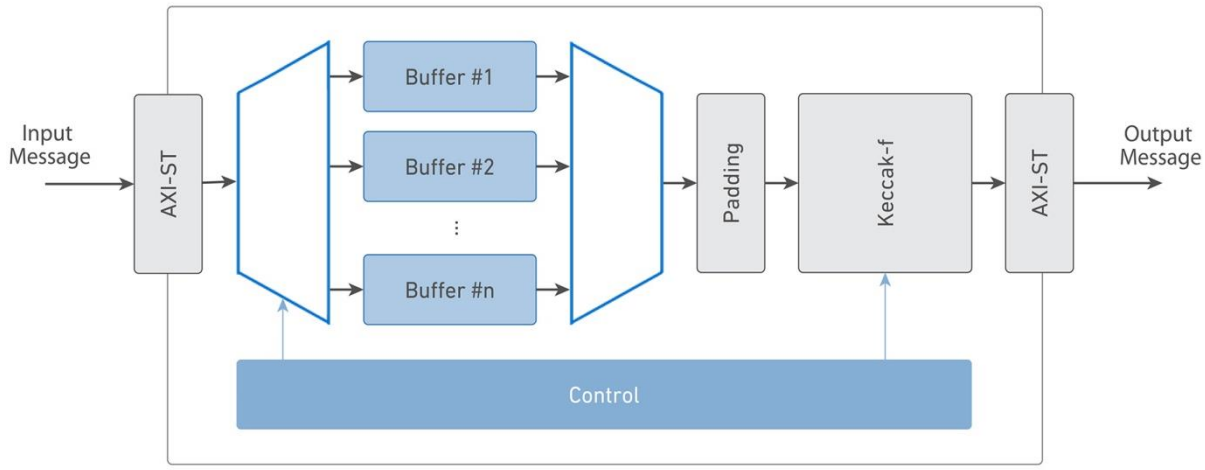
KEY BENEFITS

- Simple and adjustable input/output bus width
- Fast operation - one clock cycle per each hash round
- Streamed data hashing supported and error handling
- High-throughput buffers implemented
- Fully autonomous operation: automatic padding insertion
- Minimal latency

APPLICATIONS

- IPsec and TLS/SSL protocols
- Digital signature applications
- Encrypted data storage
- Secure processing
- E-commerce

BLOCK DIAGRAM



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

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

Performance

- High throughput: single cycle per hashing round
  - 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

Deliverables

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

SAMPLE IMPLEMENTATION RESULTS

Technology	Area (Gates)						Freq. (MHz)	Number of In. Buffers
	SHA3-224	SHA-256	SHA3-384	SHA3-512	SHAKE-128	SHAKE-256		
TSMC 28nm hpm-sc9-svt-c31	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.

BEYOND SEMICONDUCTOR

Beyond Semiconductor is addressing challenges of systemic complexity in today's electronic devices, empowering its customers to create new experiences for end users.
Initially known for its processor expertise, Beyond quickly gained acceptance among top semiconductor companies and evolved into global company leveraging processing, software and system-wide view competence to provide its customers with effectively designed IP and ASICs.

Brnčičeva ulica 41G, SI-1231 Ljubljana-Črnuče, Slovenija

Email: sales@beyondsemi.com , Tel: +386 5 90 90 100

