

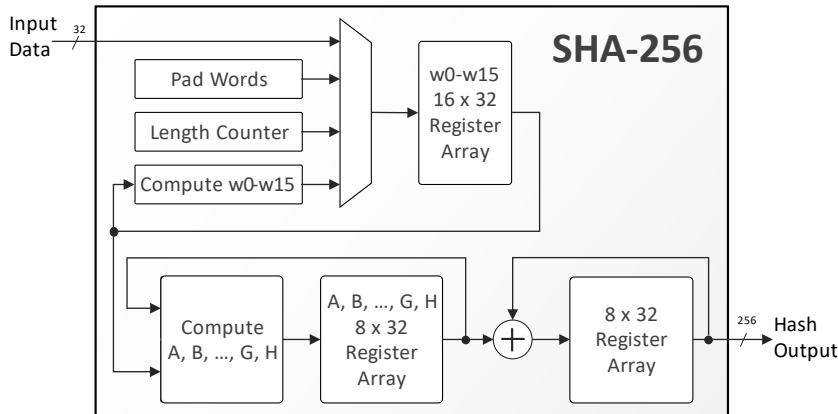
SHA-256

256-bit SHA Secure Hash Crypto Engine

The SHA-256 encryption IP core is a fully compliant implementation of the Message Digest Algorithm SHA-256. It computes a 256-bit message digest for messages of up to $(2^{64} - 1)$ bits.

Developed for easy reuse in ASIC and FPGA applications, the SHA-256 is available optimized for several technologies with competitive utilization and performance characteristics. Support for AMBA bus interfaces and integration with an external DMA are available as options.

Block Diagram



Applications

The SHA-256 can be used in various applications for ensuring data integrity, and authenticity. Some examples are on-chip communication, electronic fund transfers, digital signatures, password storage, blockchain technology and data backup.

Implementation Results

The SHA-256 can be mapped to any ASIC technology or FPGA device. The following are sample ASIC pre-layout results reported from synthesis with a silicon vendor design kit under typical conditions, with all core I/Os assumed to be routed on-chip.

Technology	Logic Resources	Memory Resources	Fmax (MHz)	Throughput (Gbps)
TSMC 28nm HPM	14,674 eq. gates	-	1,000	7.877
TSMC 16nm	17,963 eq. gates	-	1,400	11.028

The provided figures do not represent the higher speed or smaller area for the core. Please contact CAST to get characterization data for your target configuration and technology.

Verification

The core has been verified through extensive synthesis, place and route and simulation runs. It has also been production-proven in several ASIC and FPGAs designs.

FEATURES

- NIST-Validated SHA-256 implementation compliant to FIPS 180-4
- Input length up to $(2^{64} - 1)$ bits
- High throughput:
 - 65 clock-cycles per 512-bit input block
 - Over 10Gbps on modern ASIC technologies
 - Throughput scaling with multiple clock instances.
- Small Silicon footprint: 15k-20k Gates
- Easy integration & implementation
 - Fully synchronous, uses only the rising clock-edge, single-clock domain, no false or multiclock timing paths, scan-ready, LINT-clean, re-usable design
 - Simple input and output interface, optionally bridged to AMBA™ interfaces or integrated with a DMA engine.
- Available in VHDL or Verilog source code format, or as a targeted FPGA netlist
- Complete deliverables include test benches, C model, and test vector generator
- Multiple times production proven in ASIC and FPGA designs

Support

The core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

Deliverables

The core is available in RTL (VHDL or Verilog) source code, or as a targeted FPGA netlist. Its deliverable package includes the following:

- Sophisticated self-checking HDL testbench
- C Model & test vector generator
- Sample simulation & synthesis scripts
- User documentation

Export Permits

This core implements encryption functions and as such it is subject to export control regulations. Export to your country may or may not require a special export license. Please contact CAST to determine what applies in your specific case.