SHA-384/512

SHA-384 and SHA-512 Secure Hash Crypto Engine

The SHA-384/512 is a high-throughput, and compact hardware implementation of the SHA-384 and the SHA-512 cryptographic hash functions provisioned by the FIPS180-4 standard.

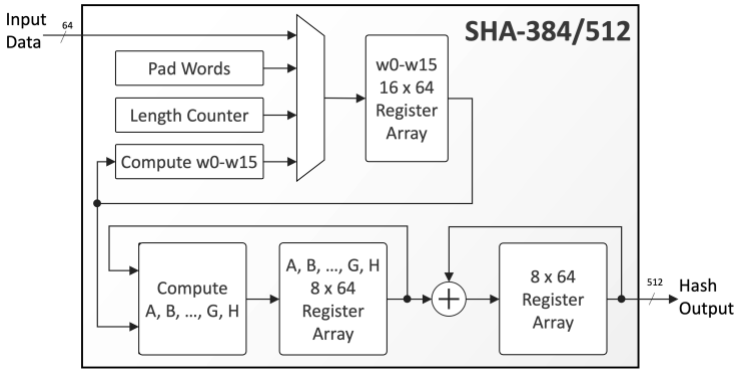
The core is designed for ease of use and integration and adheres to industry-best coding and verification practices. Technology mapping, and timing closure are trouble-free, as the core contains no multi-cycle or false paths, and uses only rising-edge-triggered D-type flip-flops, no tri-states, and a single-clock/reset domain. The SHA-384/512 core features a simple input and output data interface. Support for AMBA bus interfaces and integration with an external DMA are available as options.

The highly reliable SHA-384/512 has been production-proven in several ASIC and FPGAs designs.

FEATURES

- Custom-hardware accelerator for the SHA-384 and SHA-512 cryptographic hash functions
- Compliant to FIPS 180-4 with input message length up to (2^{128} – 1) bits
- High throughput:
  - 81 clock cycles per 1024-bit input block
  - Throughput scaling with multiple clock instances.
- Small silicon footprint: ~1,900 ALMs
- Easy integration & implementation
  - Fully synchronous, uses only the rising clock-edge, single-clock domain, no false or multicycle timing paths, scan-ready, LINT-clean, reusable design
  - Simple input and output interfaces, optionally bridged to AMBA™ interfaces or integrated with a DMA engine.
- Available in VHDL or Verilog source code format, or as a targeted FPGA
- Complete deliverables include test benches, C model, and test vector generator
- Multiple times production-proven in ASIC and FPGA designs

Block Diagram



Applications

The SHA-384/512 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-384/512 core can be mapped to any Intel® FPGA device (provided sufficient silicon resources are available). The following are sample results with all core I/Os assumed to be routed on-chip.

Family	Logic	Memory	Freq. (MHz)	Throughput (Mbps)
Agilex (-2)	1,872 ALMs	-	375	4,741
Arria 10 GX (-1)	1,930 ALMs	4 RAMB	250	3,160

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.

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.