

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 the AMBA bus interface is available as an option.

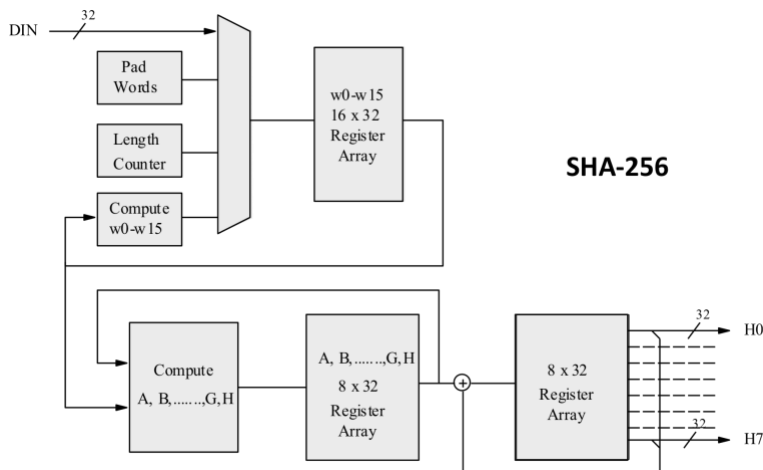
The SHA-256 core has been robustly verified and is silicon-proven.

Applications

The SHA-256 can be utilized for a variety of encryption applications including:

- Electronic Funds Transfer
- Authenticated Electronic data transfer
- Encrypted data storage

Block Diagram



Functional Description

The INIT signal is asserted at the start of each message. The SHA-256 core is ready to accept data when REQ is asserted.

Each 32-bit word is clocked into the core on the rising edge of CLK when ACK is asserted. The ACK signal is used to acknowledge a data request from the core. If the ACK is LOW when the core requests a new data with REQ HIGH, the core stalls.

The main difference between EN and ACK is that ACK only stalls the core when a data is being requested, whereas EN low suspends all the core operations.

After a block of 16 words has been input, REQ is deasserted as the SHA-256 core computes the message digest.

After another 49 clock cycles, the message digest for that 16 word block is computed and REQ is asserted again to indicate that more words can be clocked in.

The standard specifies that the maximum number of bits in the message is $2^{64} - 1$. Therefore, maximum number of 32-bit words that can be clocked in is $2^{59} - 1$. The core can cope with any number of words up to $2^{59} - 1$ being input.

The INIT signal is asserted at the start of each message. The SHA-256 core is ready to accept data when REQ is asserted.

Each 32-bit word is clocked into the core on the rising edge of CLK when ACK is asserted. The ACK signal is used to acknowledge a data request from the core. If the ACK is LOW when the core requests a new data with REQ HIGH, the core stalls.

FEATURES

- Encrypts and decrypts using the AES Rijndael Block Cipher Algorithm
- Implemented according to the IEEE P1619™/D16 standard
- NIST Certified
- Maximum message length up to $(2^{59} - 1)$ bits
- Suitable for data authentication application
- Simple, fully synchronous, reusable design
- Available as fully functional and synthesizable VHDL or Verilog, or as a netlist for popular programmable devices
- Complete deliverables include test benches, C model and test vector generator

Functional Description (cont.)

The LAST signal is asserted by the user when clocking in the last word. At least one pad, and two length words need to be added to the end of the message as part of the SHA-256 calculation.

Note that the BYTES signal is considered valid and sampled by the core when the LAST signal is high. This signal is used by the core to determine how many bytes in the last word are part of the input data.

If the total number of input words plus three is not a multiple of 16, the core adds additional pad bytes to calculate the message digest as specified in the standard.

The two Length words that contain the bit length of the original message are also added by the core.

The 256-bit message digest is output on H0-H7 when READY is asserted. READY indicates that the digest calculation is complete and it remains asserted until INIT is raised.

The core can be asynchronously reset by lowering the RSTN input port.

The clock enable signal is asserted high for normal operation. Registers are not updated when EN is forced to 0.

Implementation Results

The SHA-256 can be mapped to any Intel device (provided sufficient silicon resources are available). The following are sample Intel results with all core I/Os assumed to be routed on-chip.

Family	Logic	RAM bits	Freq. (MHz)	Throughput (Mbps)
MAX 10 (-7)	2,068 LEs	0	125	895
Arria 10 GX (-1)	893 ALMs	0	125	895
Stratix V (-3)	901 ALMs	0	200	1,575
Stratix V (-1)	900 ALMs	0	225	1,772

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.

Related Products

The SHA-3 Secure Hash Crypto Engine is also available as a standalone core.

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.

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.

Verification

The core has been verified through extensive synthesis, place and route and simulation runs. It has also been embedded in several products, and is proven in FPGA technologies.

Deliverables

The core is available in ASIC (RTL) or FPGA (netlist) forms, and includes everything required for successful implementation. The Intel version includes

- Targeted FPGA netlist
- Sophisticated HDL Testbench (self checking)
- C Model & test vector generator
- Simulation script, vectors & expected results
- Synthesis script
- User documentation