SHA-256

256-bit SHA Cryptoprocessor Core

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.

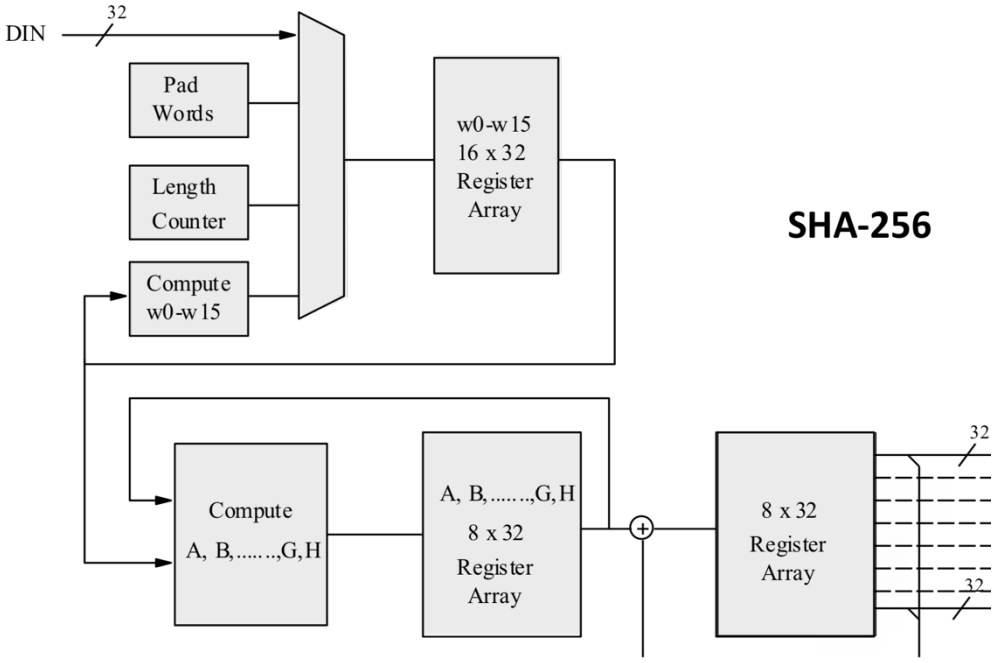
Developed for easy reuse in ASIC and FPGA applications, the SHA-256 is available optimized for several technologies with competitive utilization and performance characteristics. Support for the AMBA bus interface is available as an option.

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



Features

- Designed according to the FIPS 180-2 Standard
- 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

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 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.

Related Products

A SHA-1 is also available as a stand-alone core.

Export Permits

This core is approved for export to Australia and the United States for military applications, and to all other countries for non-military applications, except for the following:

Cuba	Iran	Iraq	Libya
North Korea	Sudan	Syria	

It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing the SHA-256 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.

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 ASIC version includes

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

CAST
info@cast-inc.com
www.cast-inc.com

CAST, Inc. 50 Tice Blvd, Suite 340
Woodcliff Lake, NJ 07677 USA
tel 201-391-8300 fax 201-391-8694

The SHA-256 core is sourced from Technology Partner Ocean Logic.