SHA-1

Secure Hash Algorithm Cryptoprocessor Core

The SHA-1 encryption IP core is a fully compliant implementation of the Secure Hash Algorithm, SHA-1. It computes a 160-bit message digest for messages of up to $(2^{64} - 1)$ bits.

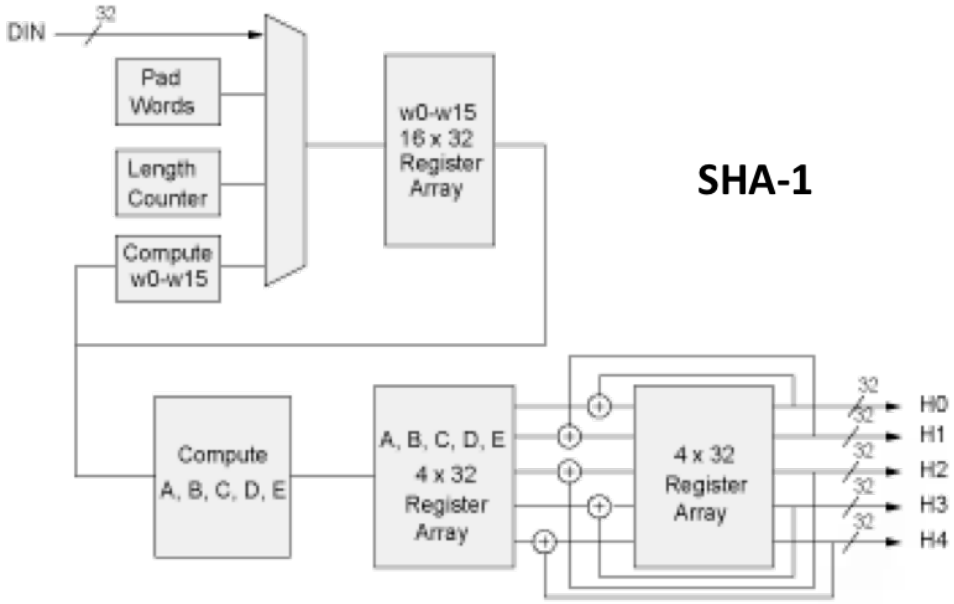
Developed for easy reuse in ASIC and FPGA applications, the SHA-1 is available optimized for several technologies with competitive utilization and performance characteristics. Support for the AMBA bus interface is available as an option.

Applications

The SHA-1 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 180-1 Standard
- Maximum message length up to $(2^{64} - 1)$ 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

July 2017

Functional Description

The SHA-1 algorithm is based on principles similar to those used by Professor Ronald L. Rivest of MIT when designing the MD4 message digest algorithm, and is closely modeled after that algorithm. It operates on message blocks of 512 bits for which a 160-bit (5 x 32-bit words) digest is produced. Corresponding 32-bit words of the digest from consecutive message blocks are added to each other to form the message of the whole message. =

The INIT signal is asserted at the start of each message to initialize the logic for calculating a new message digest. The SHA-1 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. After a block of 16 words has been input, *REQ* is deasserted as the SHA-1 core computes the message digest. After another 65 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, the maximum number of bits in a message is $2^{61} - 1$. The core can cope with any number of words up to $2^{61} - 1$ being input with the BYTES[1:0] input specifying the number of valid message bytes in the last input word.

The LAST signal is asserted 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 calculation.

If the total number of input bytes plus 9 is not a multiple of 64, 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.

Another 66 clocks later, READY is asserted together with the 160-bit message digest output on H0, H1, H2, H3, H4. These outputs remain valid until INIT or RSTN is asserted.

The core can be asynchronously reset by lowering the RSTN input port. After reset, READY and REQ are deasserted, and H0-H4 are set to 0. The clock enable (*EN*) signal is asserted high for normal operation. Registers are not updated when *EN* is forced to 0.

Related Product

A SHA-256 encryption IP core is also available as a stand-alone cryptoprocessor.

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 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-1 core is sourced from Technology Partner Ocean Logic.