OL_SHA
SHA-1 Processor
Rev 1.3

Overview

This 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. Simple, fully synchronous design with low gate count.

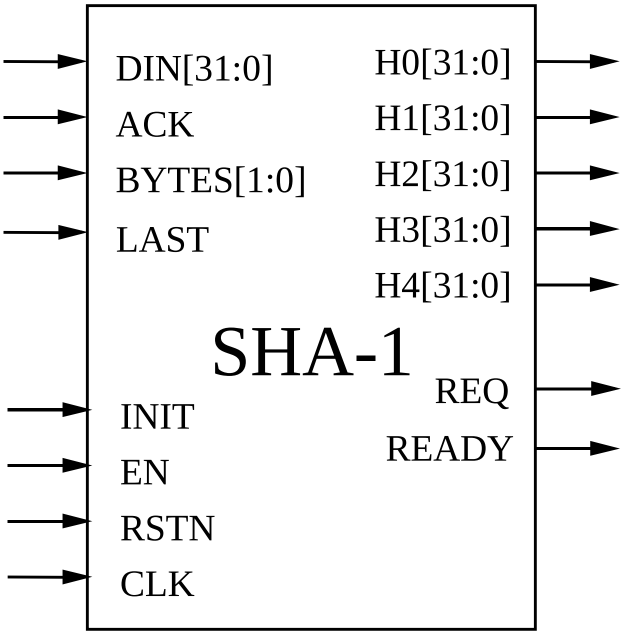
Applications

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

Features

- Suitable for data authentication applications.
- Fully synchronous design.
- Available as fully functional and synthesizable VHDL or Verilog soft-core.
- Xilinx and Altera netlist available for various devices.

Symbol



Pin Description

Name	Type	Description
RSTN	Input	Asynchronous Core reset. Active LOW.
CLK	Input	Core clock signal.
EN	Input	Synchronous enable signal. When LOW the core ignores all its inputs.
INIT	Input	Initializes message digest calculation.
DIN[31:0]	Input	Input data.
ACK	Input	Input data enable.
BYTES[1:0]	Input	Number of bytes valid in last input word. 00 : DIN[31:24] valid 01 : DIN[31:16] valid 10 : DIN[31:8] valid 11 : DIN[31:0] valid
LAST	Input	Last input data word indication.
REQ	Output	Ready for input.
READY	Output	Output data valid.
H0[31:0]	Output	First message digest word
H1[31:0]	Output	Second message digest word
H2[31:0]	Output	Third message digest word
H3[31:0]	Output	Fourth message digest word
H4[31:0]	Output	Fifth message digest word

General Description

The OL_SHA core is a fully compliant hardware implementation of the SHA-1 algorithm, suitable for a variety of applications.

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 digest of the whole message. The block diagram of the core is shown in Figure 1.

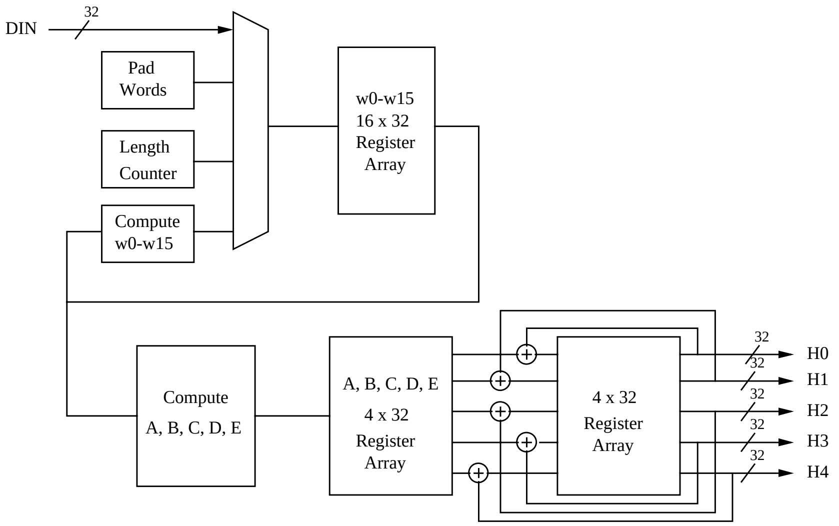


Figure 1: Block Diagram for the SHA-1 processor

Functional Description

Figure 2 shows the first message block of 512 bits, comprising sixteen 32-bit words, being clocked into the core.

The INIT signal is asserted at the start of each message to initialise the logic for calculating a new message digest. The SHA 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 have been input, REQ is deasserted as the SHA 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.

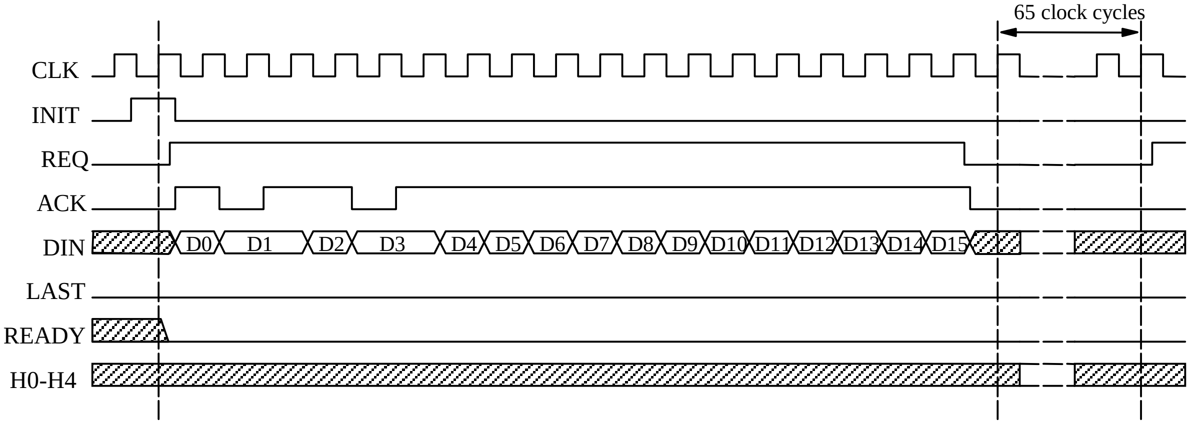


Figure 2 Timing diagram for first message block input

The standard specifies that the maximum number of bits in the message is 2^{64} - 1. Therefore, the maximum number of bytes in a message is 2^{61} - 1. The core can cope with any number of bytes 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.

Figure 3 shows the last message block being clocked into the core. The LAST signal is asserted when clocking in the last word.

At least one pad byte, 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, additional pad bytes are added by the core 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. There is a three clock cycle delay for adding the pad and length words as shown in Figure 3.

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.

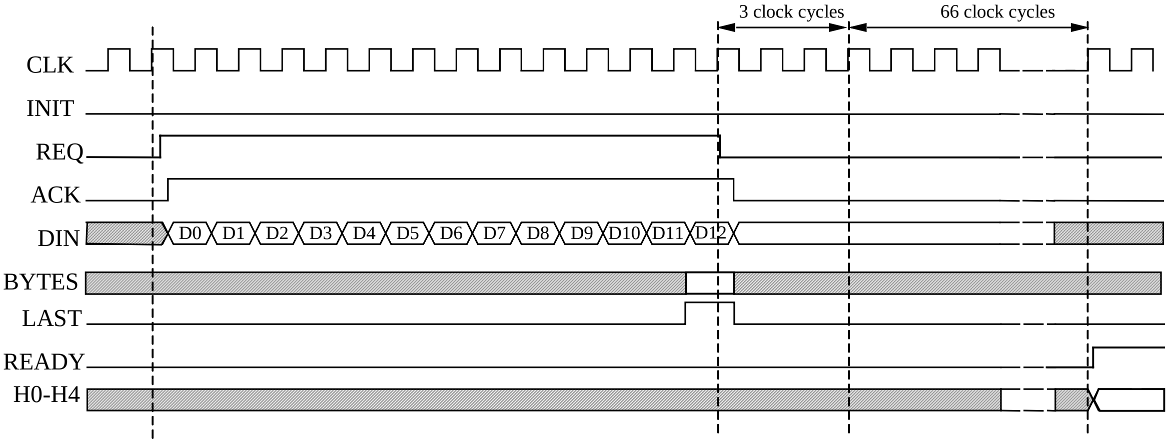


Figure 3 Timing diagram showing last message block input

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

Performance

Performance figures of the core implemented with some particular technologies, are shown in the table below

Technology	Area	Speed	Throughput
ASIC 0.18 u			
Virtex II			
Virtex 4			

Table 1 Performance of the OL_SHA core.

Export Permits

The core is available for export to all the countries of the world with the exception of the following:

Iran	North Korea	Libya	Cuba	Sudan
Syria	Iraq			

It is the customer’s responsibility to check with relevant authorities regarding the re-export of equipment containing this technology.

Ocean Logic Pty Ltd
PO BOX 768 - Manly NSW 1655 - Australia
Tel: +61-2-99054152 Fax: +61-2-99050921
E-Mail: info@ocean-logic.com URL : http://www.ocean-logic.com/