OL_SHA256
SHA-256 Processor
Rev 0.9

General Description

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

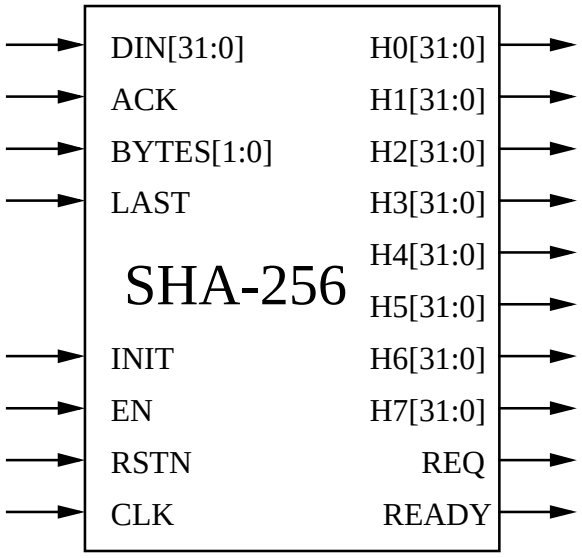
Applications

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

Features

- FIPS 180-2 compliant.
- Suitable for data authentication applications.
- Fully synchronous design.
- Available as fully functional and synthesizable VHDL or Verilog soft-core.
- FPGA 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 acknowledge.
LAST	Input	Last input data word indication.
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
REQ	Output	Requests input data.
READY	Output	Output data valid.
H0-H7[31:0]	Output	256 bit Hash value

General Description

The OL_SHA256 core is a fully compliant hardware implementation of the SHA-256 algorithm, suitable for a variety of applications.
The SHA-256 algorithm is an upgraded version of the SHA-1 algorithm and it offers improved security. It operates on message blocks of 512 bits for which a 256-bit (8 x 32-bit words) message digest (hash value) is produced. Corresponding 32-bit words of the hash values from consecutive message blocks are added to each other to form the message of the whole message. The block diagram of the core is shown in Figure 1.

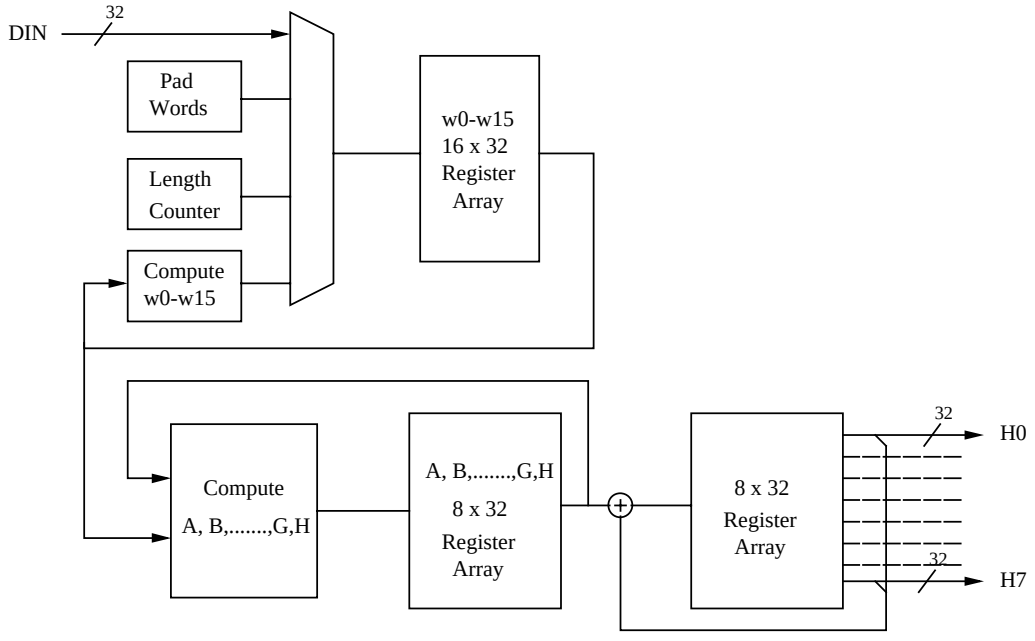


Figure 1: Block Diagram for the SHA-256 processor

Functional Description

Figure 2 shows the first message block of sixteen words being clocked into the core.
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.

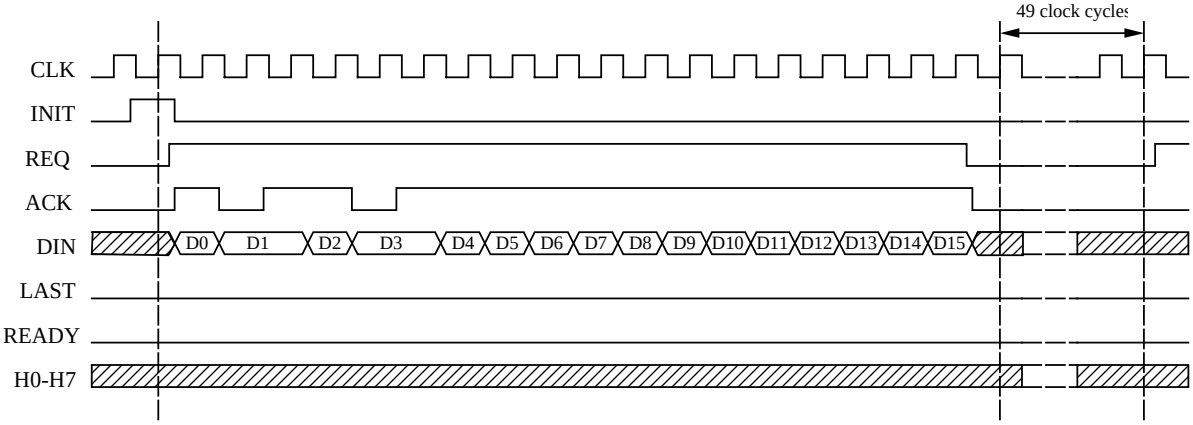


Figure 2 Timing diagram for first message block input

The standard specifies that the maximum number of bits in the message is 2^{64} - 1. Therefore, 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.

Figure 3 shows the last message block being clocked into the core. 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. See the signal list to see how the core interprets this signal.

If the total number of input words plus three is not a multiple of 16, 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. Note the three clock cycle delay for adding the pad and length words.

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.

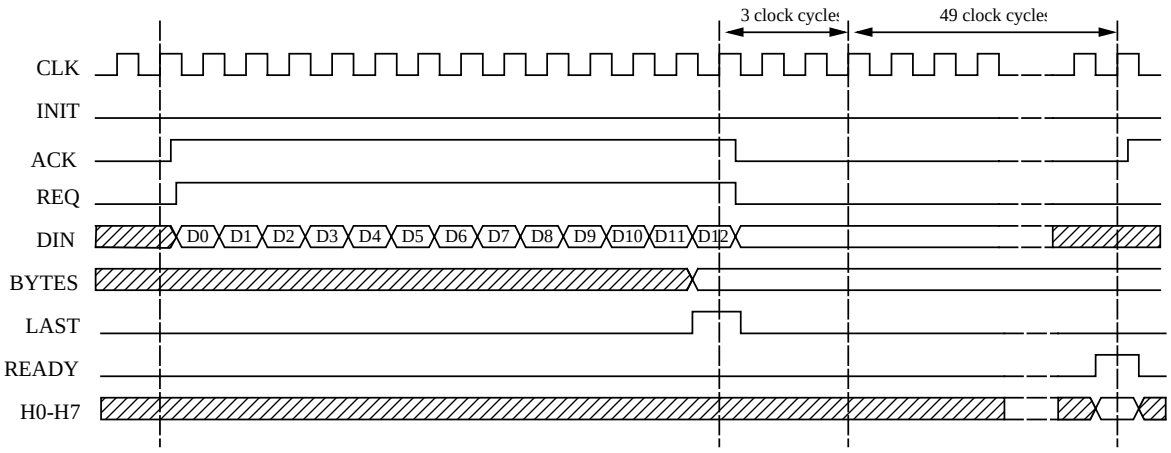


Figure 3 Timing diagram showing last message block input.

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.

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_MD5 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/