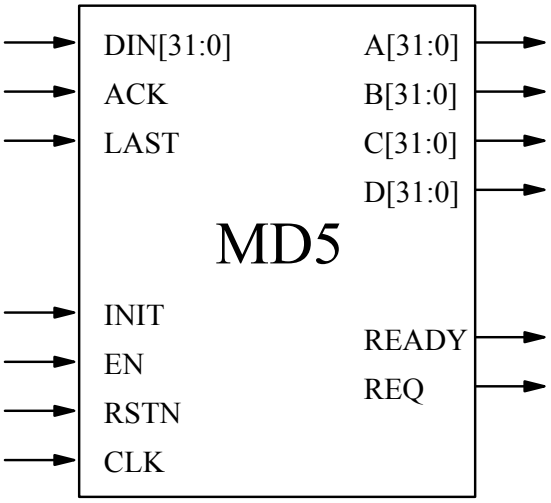
MD5 Processor Core

General Description

This core is a fully compliant hardware implementation of the Message Digest Algorithm MD5, suitable for a variety of applications. It computes a 120-bit message digest for messages of up to $(2^{64} - 1)$ bits.

The MD5 algorithm is an improved version of the MD4, created by Professor Ronald L. Rivest of MIT and is closely modeled after that algorithm. It operates on message blocks of 512 bits for which a 128-bit (4 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.

Symbol



Features

- RFC 1321 compliant
- Suitable for data authentication applications
- Fully synchronous design
- Available as fully functional and synthesizable VHDL or Verilog soft-core
- Test benches provided

Applications

- Electronic funds transfer
- Authenticated electronic data transfers
- Encrypted data storage

Pin Description

Name	Type	Description
RSTN	Input	Asynchronous reset, active low
EN	Input	Clock enable signal, active high
INIT	Input	Initialize message digest calculation
DIN[31:0]	Input	Input data
ACK	Input	Input data acknowledge
LAST	Input	Last input data word indication
REQ	Output	Requests input data
READY	Output	Output data valid
A[31:0]	Output	First message digest word
B[31:0]	Output	Second message digest word
C[31:0]	Output	Third message digest word
D[31:0]	Output	Fourth message digest word

Block Diagram

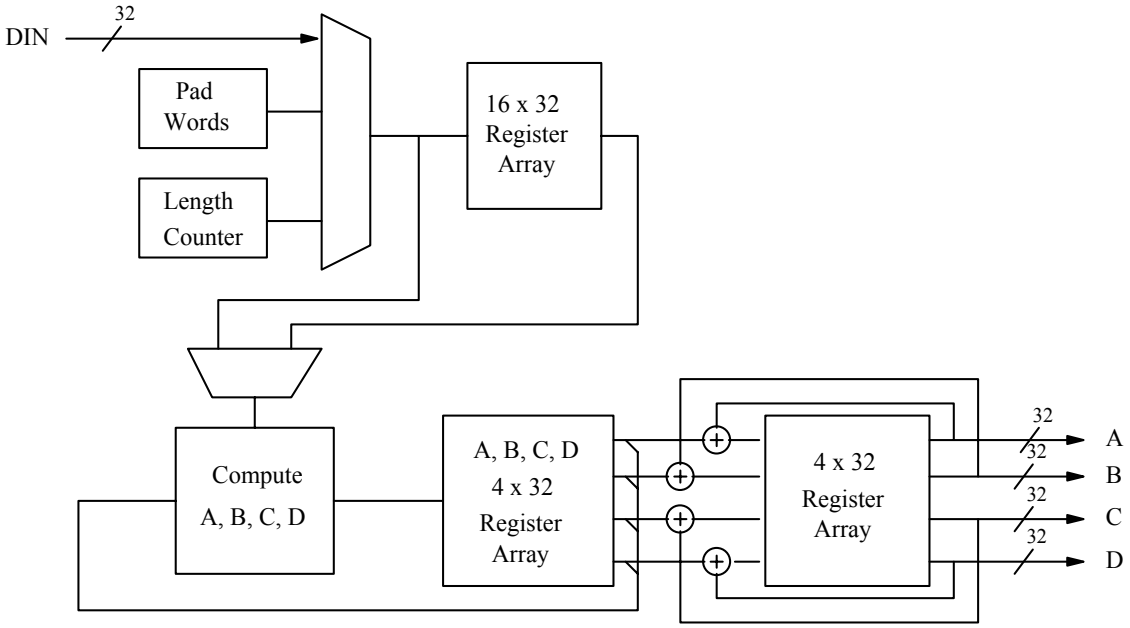


Figure 1: Block Diagram for the MD5 processor

Functional Description

The MD5 core is partitioned into modules as shown in figure 1 and described below.

Pad Words

This module pads the incoming data with the appropriate number of bits. According to the MD5 algorithm all data to be processed must be a multiple of 512 bits.

Length Counter

This module counts the number of bits being input. This information is also used to pad the incoming data to digest.

16x32 Register Array

Main storage for the 512 bits to be digested.

Compute A, B, C, D

This is a group of non-linear functions used by the MD5 algorithm to digest the data.

4x32 Registers arrays

These two arrays are used to compute the intermediate and the final results of the message digest.

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 MD5 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 MD5 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.

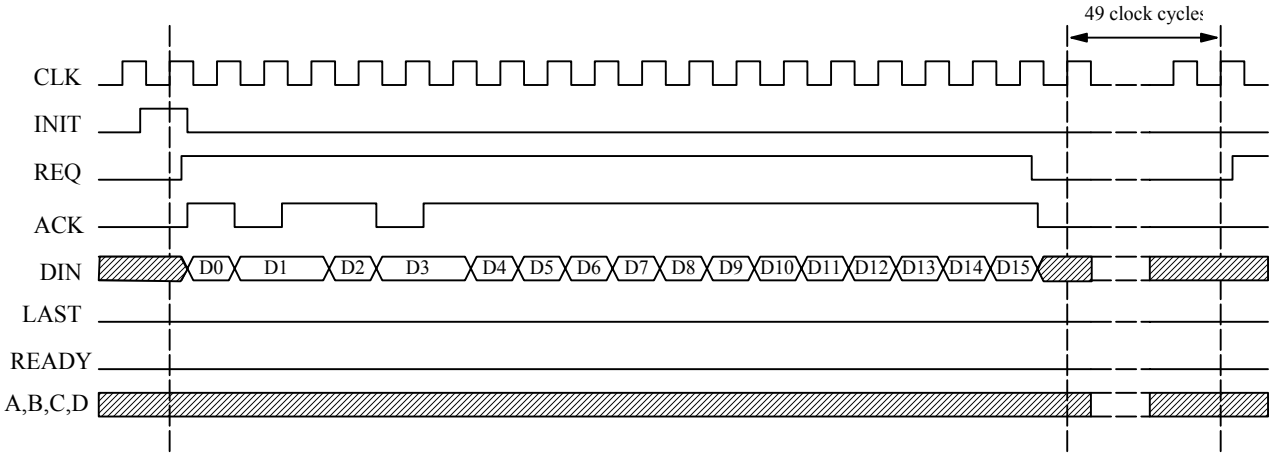


Figure 2: Timing diagram for first message block input

The standard specifies that the maximum number of bits in the message is 2^{64} - 1. Therefore the 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 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 MD5 calculation.

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 160-bit message digest is output on A, B, C, D when READY is asserted.

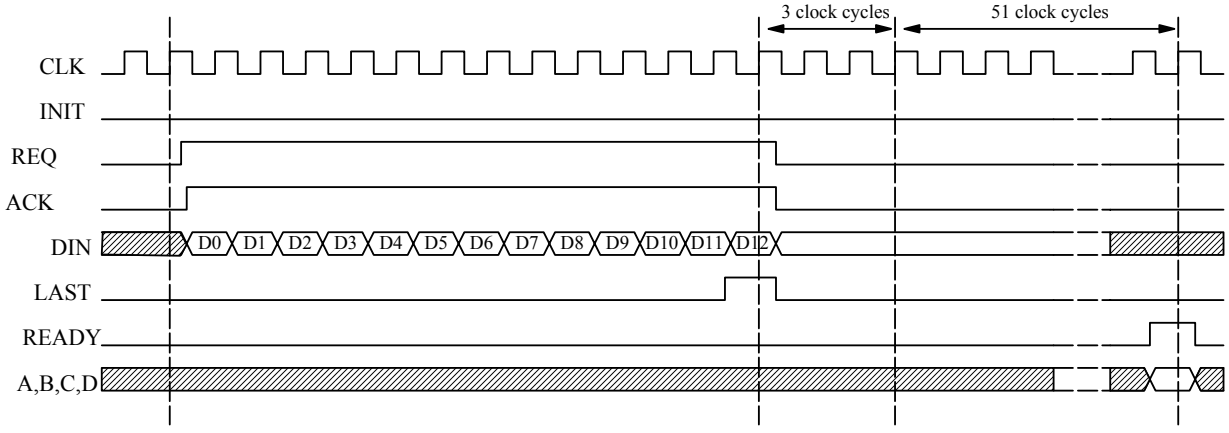


Figure 3 Timing diagram showing last message block input.

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.

Export Permits

The core is available for export in the following countries:

Australia	Austria	Belgium-Luxembourg	Brazil
Canada	China	Czech Republic	Denmark
Finland	France	Germany	Greece
Ireland	Israel	Italy	Japan
Malaysia	Netherlands	Norway	Portugal
Russia	Singapore	South Africa	South Korea
Spain	Sweden	Switzerland	Taiwan
United Kingdom	United States		

It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing the MD5 encryption technology.

Device Utilization & Performance

Supported Family	Device Tested	Slices[1]	Clock IOBs	IOBs[2]	RAM Blocks	Performance (MHz)
Spartan-IIE	2S50E-7	544	1	167	1	46
Spartan-3	3S200-4	535	1	167	1	41
Virtex-II	2V250-6	525	1	167	1	65
Virtex-IIP	2VP2-7	605	1	167	1	74

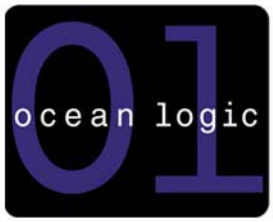
Notes:
1. Optimized for speed
2. Assuming all Core I/Os are routed off-chip
3. Results obtained using version ISE 5.2i of the Xilinx tools

Deliverables

- VHDL or Verilog (source code license)
- Post-synthesis EDIF (netlist license)
- Testbench (self checking)
- Vectors & expected results
- Place & Route Scripts (netlist license)
- Simulation & synthesis scripts
- Constraints file (netlist license)
- Instantiation templates

Contact Information

CAST, Inc.
11 Stonewall Court
Woodcliff Lake, New Jersey 07677 USA
Phone: +1 201-391-8300
Fax: +1 201-391-8694
E-Mail: info@cast-inc.com
URL: www.cast-inc.com



This core developed by the encryption experts at Ocean Logic Pty Ltd.

Copyright © CAST, Inc. 2003. All Rights Reserved. Contents subject to change without notice.