

Data sheet for MD5 Core

Functional Description

This document describes the MD5 message-digest algorithm. The algorithm takes as input a message of length which is a multiple of 512 bits and produces as output a 128-bit "fingerprint" or "message digest" of the input.

Features:

- Supports configurable clock rate
- Compatible with RFC 1321
- 512 bits takes 66 clock cycles

Block Diagram:

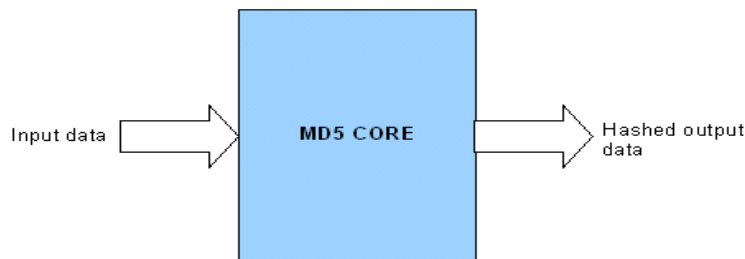


Figure 1: Block Diagram

Architectural Diagram:

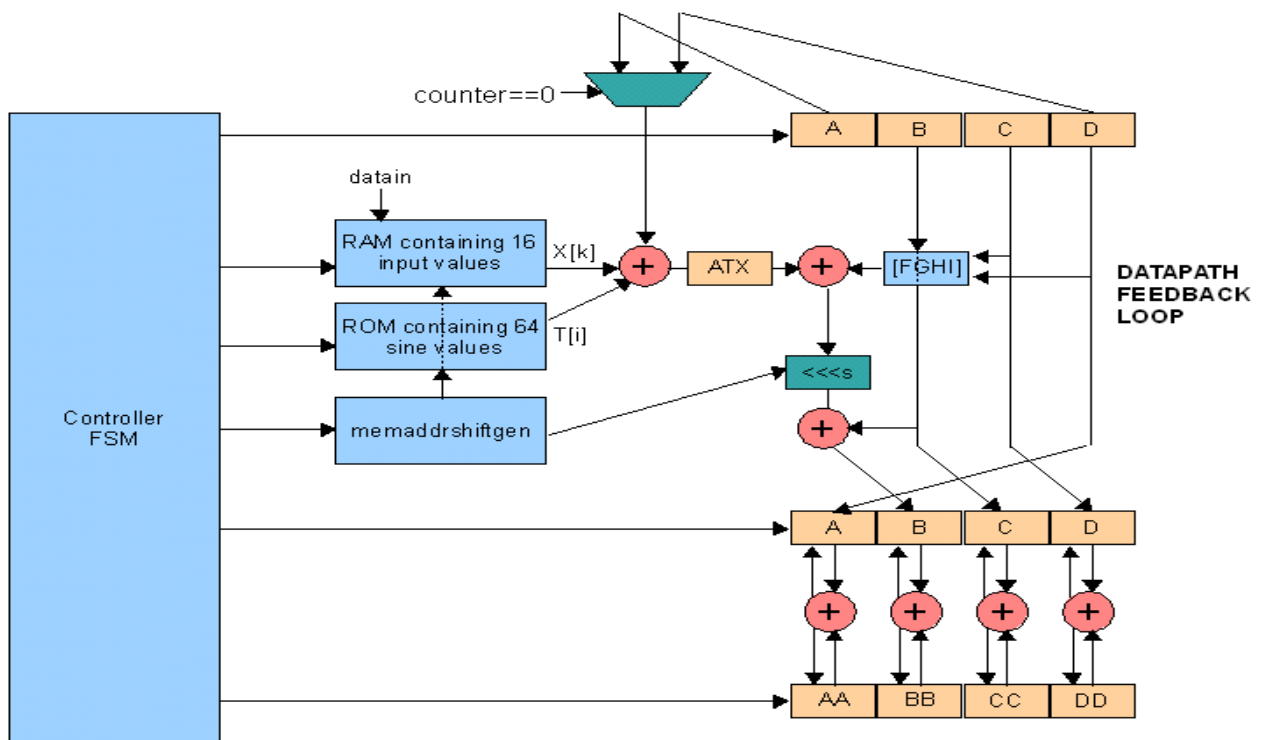


Figure 2: MD5 Architecture Diagram

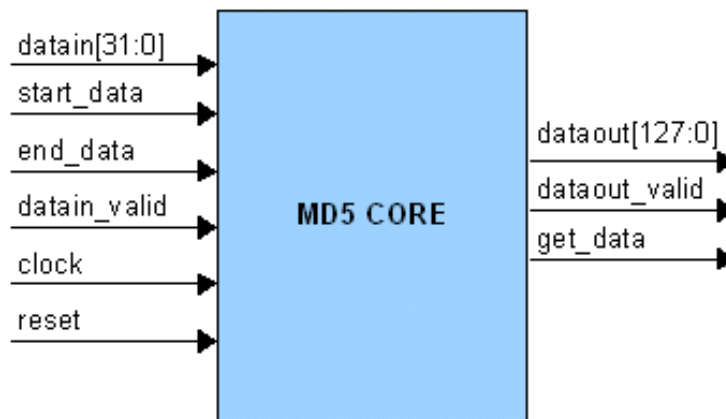
Description:

1. Data is given to the MD5 module when the 'get_data' signal is logic HIGH.
2. Sixteen words of 32 bits are given to the MD5 module in one chunk, along with the 'datain_valid' signal.
3. When the first chunk of of data is given to the MD5 module, a start_data pulse is held HIGH for one cycle.
4. When the last chunk of data is being fed to the module an 'end_data' pulse is HIGH for one cycle when the last word is being written.
5. When the valid data is ready to be outputted, the 'dataout_valid' signal is HIGH for one cycle.
6. The MD5 module takes 66 cycles to process one 512-bit chunk of data.

Signal definition table:

Signal	Direction	Description
clock	IN	This is the system clock.
reset	IN	This is the system reset.
datain[31:0]	IN	This is the data input.
datain_valid	IN	This signal is held HIGH when data is being fed to the module. One chunk of data has 16 words of 32 bits each. Thus this signal is HIGH for 16 consecutive cycles at one go.
start_data	IN	This signal is held HIGH for one cycle when the first data is given to the module.
end_data	IN	This signal is held HIGH for one cycle when the last 32-bit data is given to the module.
dataout[127:0]	OUT	This is the output of the module
dataout_valid	OUT	This signal is HIGH for one cycle when the output is valid.
get_data	OUT	Data should be fed to the module one cycle after this signal goes HIGH. When this signal is HIGH an entire 512-bit chunk consisting of 16 32-bit words should be given.

Schematic Symbol



Performance:

Device	Slice Register Count	Slice LUT Count	Frequency
Virtex-4	655	1374	90 MHz.
Virtex-5	553	979	166 MHz.

Verification:

The MD5 module has been verified with following approaches:

- Comparison with the test-cases given in the MD5 RFC 1321
- Exhaustive Functional/Timing simulation

Deliverables:

- Verilog RTL source code
- Test benches
- Synthesis and Simulation scripts.
- Detailed user documentation, including RTL source code documentation