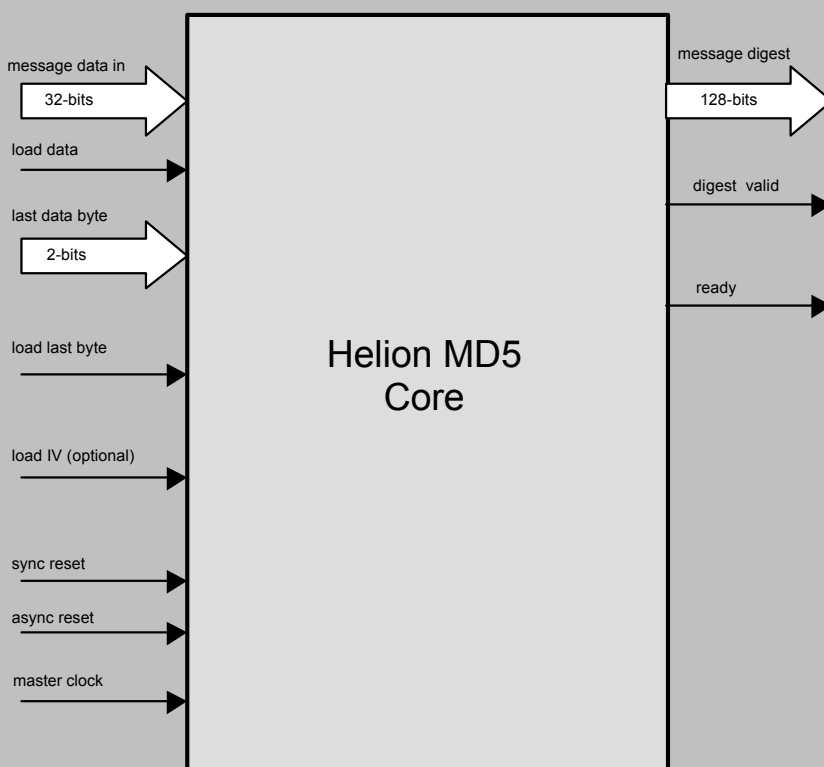


Helion Technology

DATASHEET – High Performance MD5 Hash Core for ASIC



Features

- Implements the MD5 secure hash algorithm to RFC 1321
- Fast operation – each 512-bit block requires 65 master clock cycles (1 clock per algorithm step + 1 clock load)
- Performs automatic message length calculation and padding insertion
- Optional user initialisation of IVs for efficient HMAC support
- Simple external interface
- Suitable for use in ASIC or fine-grain FPGA technologies

Deliverables

- RTL VHDL code for synthesis
- VHDL testbench
- Synopsys synthesis scripts
- User documentation

Overview

This high performance core from Helion is intended for use in ASIC and fine-grain FPGA technologies, and implements the MD5 secure hash algorithm as described in RFC 1321.

The MD5 algorithm takes as input a message of arbitrary length, processes the message in 512-bit blocks, and produces as output a 128-bit message digest. It is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted. Applications include hardware implementations of the Internet standard HMAC (RFC 2104) used for IP security and SSL.

Helion Technology Limited

The Granary, Home End, Fulbourn, Cambridge CB1 5BS, UK.



Functional Description

The Helion MD5 core implements the secure hash algorithm described in RFC 1321 which processes an arbitrary length input message in successive 512-bit blocks producing as output a 128-bit message digest. The algorithm consists of four rounds of processing each of 16 iterations. Once all 64 processing steps are complete, four 32-bit intermediate variables are updated and the next message block is processed. At the end of processing of the last message block the final variable values represent the 128-bit message digest.

The MD5 core contains an internal 16x32-bit block store which is loaded with message data under the control of external logic or a microprocessor when the core indicates it is ready. Once the block store is full the core indicates it is busy (not ready) and executes the 64 rounds of the MD5 algorithm; on completion the core indicates it is ready to accept a further message block. The external logic is responsible for informing the core when the last message word is available at the data inputs and the location of the last message byte within the last word. This allows the core to calculate the exact message length and append message padding accordingly. When the last message block has been processed the core outputs the 128-bit digest of the message and indicates its validity to the external logic.

Optionally, prior to loading the first message word the external logic may load customised initial values into the core. This allows pre-computed initial values to be used for efficient implementation of a Hash-based Message Authentication Code (HMAC).

Core Performance

This core has been designed for efficient implementation in both ASIC and fine-grain FPGA designs.

For ASIC applications, the illustrative gate count and speed figures shown below have been based on synthesis with Synopsys Design Compiler targeting a generic 0.18um CMOS technology library.

For fine-grain FPGA applications, performance and gate count will be dependant on the specific technology targeted; hence no figures are quoted here, but we would be happy to supply specific details on request.

| | |
|--------------------------------|-------------------------|
| technology | 0.18um CMOS ASIC |
| typical core gate count | 16k gates |
| max master clock | 145 MHz |
| max data rate | 1140 Mbps |

Rev 1.0.5

More information

For more detailed information on this or any of our other products and services, please contact Helion and we will be pleased to discuss how we can assist with your individual requirements.



Helion are very proud to be original members of the Xilinx Xpert Consultancy programme, having gained certification right from its inception.



Helion Technology Limited
The Granary, Home End, Fulbourn, Cambridge CB1 5BS, UK.

tel +44 (0)1223 500 924 fax +44 (0)1223 880 169
email info@heliontech.com web www.heliontech.com