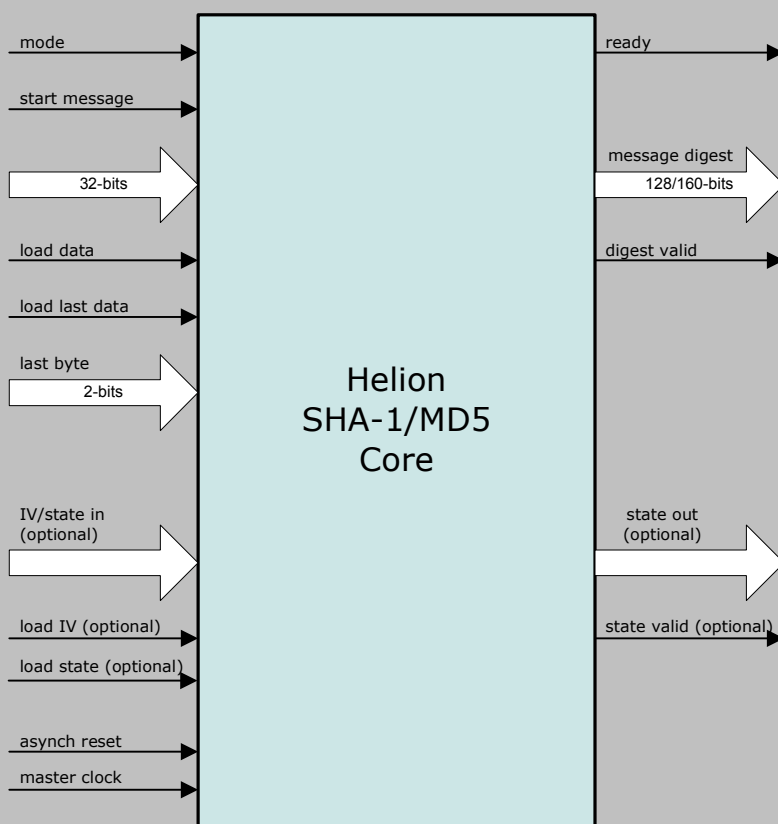


Helion Technology

FULL DATASHEET - Fast Dual SHA-1/MD5 Hash Core for Altera FPGA



Features

- Implements both SHA-1 and MD5 secure hash algorithms
- Fast operation – each 512-bit block requires only 82 (SHA-1) or 66 (MD5) master clock cycles
- Performs automatic message length calculation and padding insertion
- Optional user initialisation of IVs for optimised HMAC support
- HMAC wrapper available to make implementations quick and easy
- Optional state unload/reload feature for handling fragmented messages
- Simple external interface
- Highly optimised for use in Altera FPGA technologies

Deliverables

- Target specific netlist or fully synthesisable RTL VHDL/Verilog
- VHDL/Verilog simulation model and testbench with FIPS test vectors
- Comprehensive user documentation

Overview

The Helion Fast Dual-Hash core implements both the SHA-1 hash algorithm described in FIPS PUB 180-2, and the MD5 hash algorithm described in RFC 1321. It is a high performance core which has been designed especially for use in Altera FPGA. Both algorithms take as input a message of arbitrary length, process the message as a series of 512-bit blocks, and produce as output a compressed representation of the message data in the form of either a 160-bit (SHA-1) or a 128-bit (MD5) message digest.

Applications for the core include implementations of the standard keyed-Hash Message Authentication Code (HMAC) described in FIPS 198. Both algorithms have been employed in a variety of security applications including the IPsec and TLS/SSL protocols, as well as Digital Signature applications, where the hash function is used to ensure data integrity and origin authentication.

Helion Technology Limited

Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England



Functional Description

The Helion Fast SHA-1/MD5 Dual-hash core implements two of the most common secure hash algorithms which are used where data integrity and/or origin authentication is a requirement. Both process an arbitrary length message by operating on successive 512-bit blocks of data, producing as output either a 160-bit or 128-bit message digest.

The core contains an internal 512-bit block store which may be loaded with message data under the control of external logic or a microprocessor while the core indicates it is ready. Once the block store is full the core indicates it is busy and executes the hash 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 resulting message digest and indicates its validity.

Optionally, whilst loading the first message word, the external logic may also 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); loading of these incurs no throughput penalty since they have their own dedicated input port. In addition, the internal hash state can be made accessible, so that it may be stored externally and subsequently reloaded; this may be a useful option where fragmented messages are being hashed.

Logic Utilisation and Performance

Helion has a long history in high-end FPGA design, and we therefore take great care when implementing our IP cores. As a result they have been designed from the ground up to be highly optimal in Altera FPGA technology - they are not simply based on a synthesised generic RTL ASIC design like much of the competition.

The Helion Fast Dual SHA-1/MD5 core makes use of Altera-specific architectural features in order to achieve high performance and efficient logic resource utilisation. It is available for all of the current Altera device families including legacy Cyclone and Stratix devices.

The table below shows typical logic area and performance figures for the most popular version of the core which does not include the state unload/reload capability. Alternative versions of the core are available for Stratix II which uses M512 instead of M4K RAM blocks, and for Stratix III which uses Memory LABs (MLAB) instead of M9K RAM blocks.

	Dual SHA-1/MD5 (no reload)			
technology	Cyclone II C6	Cyclone III C6	Stratix II C3	Stratix III C2
logic resource	1942 LEs 4x M4K	1907 LEs 4x M9K	1367 ALUTs 4x M4K	1322 ALUTs 4x M9K
max clock	83 MHz	98 MHz	151 MHz	202 MHz
max throughput (SHA-1)	518 Mbps	612 Mbps	942 Mbps	1261 Mbps
max throughput (MD5)	643 Mbps	760 Mbps	1171 Mbps	1567 Mbps

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 Technology Limited

Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

tel: +44 (0)1223 500 924 email: info@heliontech.com
fax: +44 (0)1223 500 923 web: www.heliontech.com