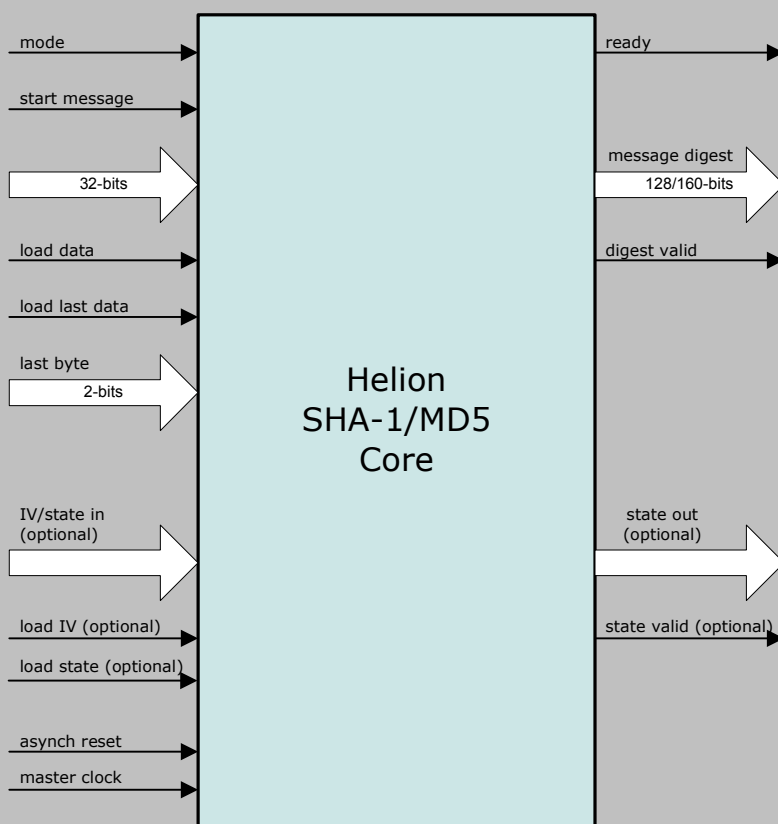


Helion Technology

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

Unlike most FPGA core vendors, Helion is both a certified Xilinx AllianceCORE IP provider and Xilinx Alliance Program consultancy. We therefore take great care when implementing our Xilinx cores, and as a result our cores have been designed from the bottom up to be highly optimal in each Xilinx FPGA technology - they are not simply based on a synthesised generic ASIC design.

The Helion Fast Dual SHA-1/MD5 Hash core makes use of Xilinx-specific architectural features in order to achieve high performance combined with efficient logic resource utilisation. It is available for all current Xilinx FPGA technologies.

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. Please contact Helion for full details if the configuration, device type or speed grade you require is not shown below.

	Dual SHA-1/MD5 (no reload)			
technology	Spartan3 -5	Spartan3E -5	Virtex4 -11	Virtex5 -3
logic resource	889 slices 1 RAMB16	939 slices 1 RAMB16	867 slices 1 RAMB16	356 slices
max clock	71 MHz	73 MHz	112 MHz	171 MHz
max throughput (SHA-1)	443 Mbps	455 Mbps	699 Mbps	1067 Mbps
max throughput (MD5)	550 Mbps	566 Mbps	868 Mbps	1326 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