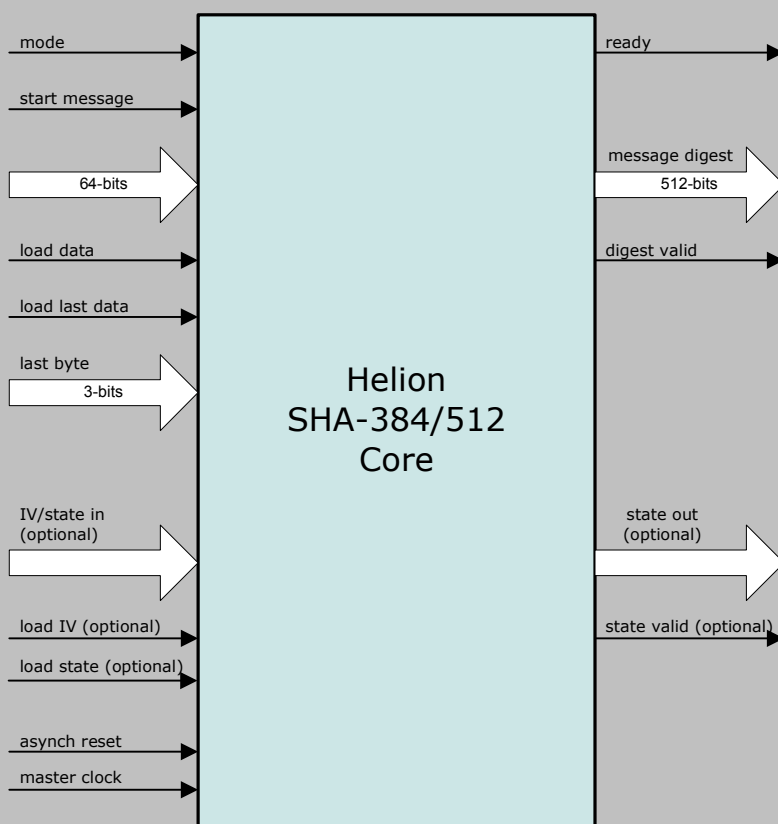


Helion Technology

DATASHEET - Fast Dual SHA-384/SHA-512 Hash Core for Altera FPGA



Features

- Implements SHA-384 and SHA-512 secure hash algorithm to FIPS 180-2
- Fast operation – each 1024-bit block requires only 82 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-384 and SHA-512 secure hash algorithms according to NIST FIPS 180-2. 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 1024-bit blocks, and produce as output a compressed representation of the message data in the form of either a 384-bit (SHA-384) or a 512-bit (SHA-512) message digest.

Applications for the core include implementations of the standard keyed-Hash Message Authentication Code (HMAC) described in NIST FIPS 198. Both algorithms have been proposed for use in the IPsec and TLS/SSL protocols, as well as Digital Signature applications, where a hash function is required to ensure both data integrity and origin authentication. The SHA-384 algorithm has also been specified by the NSA as part of the Suite B set of cryptographic algorithms for protecting classified US Government information.

Helion Technology Limited

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



Functional Description

The Helion Fast SHA-384/512 Dual-hash core implements the latest NIST secure hash algorithms, which are used wherever data integrity and/or origin authentication is a requirement. Both process an arbitrary length message by operating on successive 1024-bit blocks of data, producing as output either a 384-bit or 512-bit message digest.

The core contains an internal 1024-bit block store which may be 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 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 digest of the message 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 SHA-384/512 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-384/512 (no reload)			
technology	Cyclone II C6	Cyclone III C6	Stratix II C3	Stratix III C2
logic resource	3363 LEs 8x M4k	3458 LEs 8x M9K	2153 ALUTs 8x M4K	2071 ALUTs 8x M9K
max clock	87 MHz	101 MHz	140 MHz	184 MHz
max throughput	1086 Mbps	1261 Mbps	1748 Mbps	2297 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