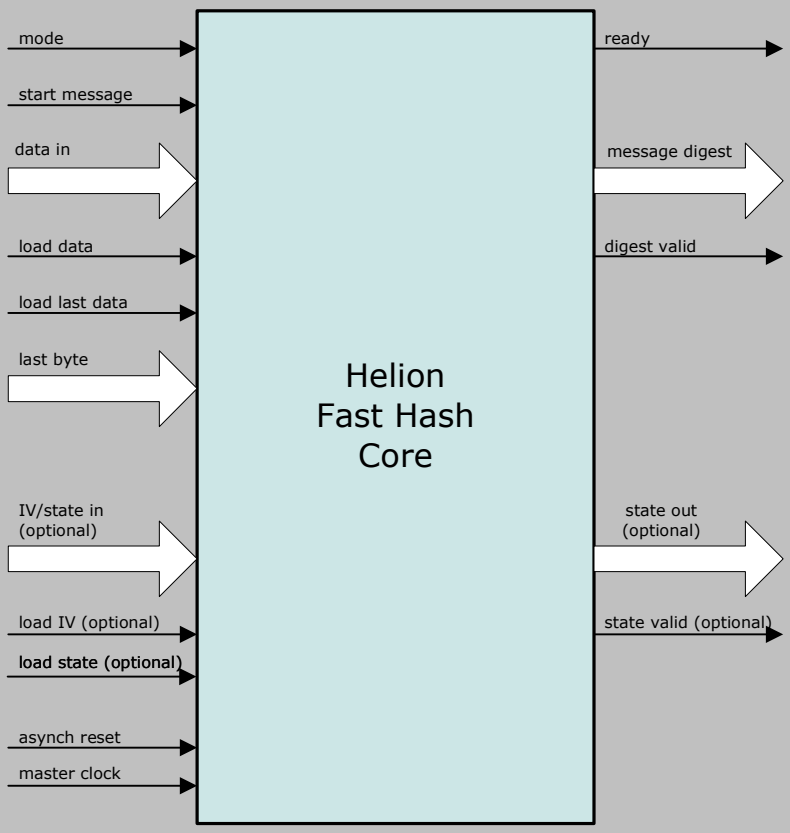
Helion Technology

FULL DATASHEET - Fast Hash Core Family for ASIC



Features

- Implements one or more of SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 & MD5 hash algorithms
- Fast operation – one clock per hashing algorithm round
- Performs automatic message length calculation and padding insertion
- Optional user initialisation of IVs for efficient HMAC support
- HMAC wrapper available for quick and easy implementation
- Optional state unload/reload feature for handling fragmented messages
- Simple external interface
- Suitable for use in ASIC or fine-grain FPGA technologies

Deliverables

- Fully synthesisable Verilog RTL
- Verilog simulation model and testbench with FIPS test vectors
- Comprehensive user documentation

Overview

The Helion Fast Hash core family implements the NIST approved SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 secure hash algorithms to FIPS 180-3 and the legacy MD5 hash algorithm to RFC 1321. These are high performance cores that are available in single or multi-mode versions and have been designed specifically for ASIC.

The hash algorithms take as input a message of arbitrary length, process the message as a series of 512 or 1024 bit blocks, and produce as output a compressed representation of the message data in the form of a message digest, the length of which varies with hash algorithm. Applications for the hashing cores include implementations of the standard Keyed-Hash Message Authentication Code (HMAC) described in FIPS 198-1. They are commonly used 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.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

Functional Description

The Helion Fast Hash core family implements the cryptographic hash algorithms which are used wherever data integrity and/or origin authentication is a system requirement. They process an arbitrary length message by operating on successive blocks of data, producing as output a message digest. The resulting digest varying in length with hash algorithm.

The cores contain an internal block store which may be loaded with message data under the control of external logic 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 the next message block. The user application logic is responsible for informing the core when the last message word is available at the data input 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.

The cores are optionally available in versions that support unload and reload of the hash state at the end of internal processing of each message block. This allows the full hash core state to be stored externally and subsequently reloaded at a future time to provide a very efficient mechanism for hashing of fragmented messages. This version of the cores also allows the user logic to preload custom initial hash values in the same cycle as the first message word is loaded. This allows pre-computed values to be programmed which override the default hash algorithm values, enabling efficient implementation of the Keyed-Hash Message Authentication Code (HMAC) described in FIPS 198-1.

HMAC

An optional HDL wrapper is available from Helion which contains all of the additional logic (including key storage) required to efficiently perform the FIPS 198-1 HMAC using the Fast Hash cores. The wrapper supports either HMAC or normal hashing operations using the underlying Fast Hash core directly. Please contact Helion for further details.

Core versions

The Helion Fast Hash core family is available in 32-bit and 64-bit data interface versions in keeping with the underlying hash algorithm to ensure maximum data throughput. The message digest output width also varies with the digest size of the underlying hashing algorithm.

Typical resource utilisation and performance targeting a standard 0.13um CMOS ASIC process using Synopsys Design Compiler are shown in the tables below for the four most popular versions of the core. Other versions are also available including single and multi-mode MD5 solutions, please contact Helion for details. Please note: The figures shown are for the standard versions of the core which do not include state unload/reload or HMAC support, which increase the logic resource used.

The tables illustrate the relationship between gate count and the synthesis clock constraint to show the variation in logic resource for different optimisation goals. All figures shown are for illustrative purposes only.

Logic Utilisation and Performance

	SHA-1			SHA-256		
logic resource	12.7K gates	13.2K gates	15.7K gates	17.8K gates	18.6K gates	22K gates
clock constraint	100 MHz	200 MHz	350 MHz	100 MHz	200 MHz	300 MHz
SHA-1 rate	624 Mbps	1248 Mbps	2185 Mbps	N/A	N/A	N/A
SHA-256 rate	N/A	N/A	N/A	775 Mbps	1551 Mbps	2327 Mbps
SHA-384/512 rate	N/A	N/A	N/A	N/A	N/A	N/A

Logic Utilisation and Performance (continued)

	SHA-1/256			SHA-384/512	
logic resource	20.1K gates	20.9K gates	24.6K gates	38.8K gates	41.5K gates
clock constraint	100 MHz	200 MHz	300 MHz	100 MHz	200 MHz
SHA-1 rate	624 Mbps	1248 Mbps	2185 Mbps	N/A	N/A
SHA-256 rate	775 Mbps	1551 Mbps	2327 Mbps	N/A	N/A
SHA-384/512 rate	N/A	N/A	N/A	1248 Mbps	2497 Mbps

About Helion

Founded in 1992, Helion is a well established British company based in Cambridge, England, offering a range of product-proven Data Security IP cores backed up by highly experienced and professional design service capabilities.

Although we specialise in providing the highest performance data encryption and authentication IP, our interest does not stop there. Unlike broadline IP vendors who try to supply a very diverse range of solutions, being specialists we can offer much more than just the IP core.

For instance, we are pleased to be able to supply up-front expert advice on any security applications which might take advantage of our technology. Many of our customers are adding data security into their existing systems for the first time, and are looking for a little assistance with how best to achieve this. We are pleased to help with suitable advice and support where necessary, and pride ourselves in our highly personal approach.

In addition, our Design Services team have an impressive track record in the development of real security products for our customers; we are proud to have been involved in the design of numerous highly acclaimed security products. This knowledge and experience is fed back into our IP cores, to ensure that they are easy to integrate into real systems, and perform appropriately for real engineering applications.

Unlike many broadline IP core vendors, Helion also spends a great deal of effort designing its cores at the very lowest level. We strongly believe that if you are buying IP, it should have been designed with the ultimate in care, and crafted to achieve the desired performance; not just put together at a high level to get the job done quickly. We find that this approach pushes the results much closer to the intended performance envelope.

For instance, if we are aiming for speed, we carefully optimise the datapath delays right down at the gate level; the result is a significantly faster core. Similarly, if we are aiming at reducing the gate count, we maintain a detailed understanding of gate budget throughout the design process. The benefits of this approach to design can be clearly demonstrated by direct comparison between Helion Data Security IP cores and the equivalents from other vendors.

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