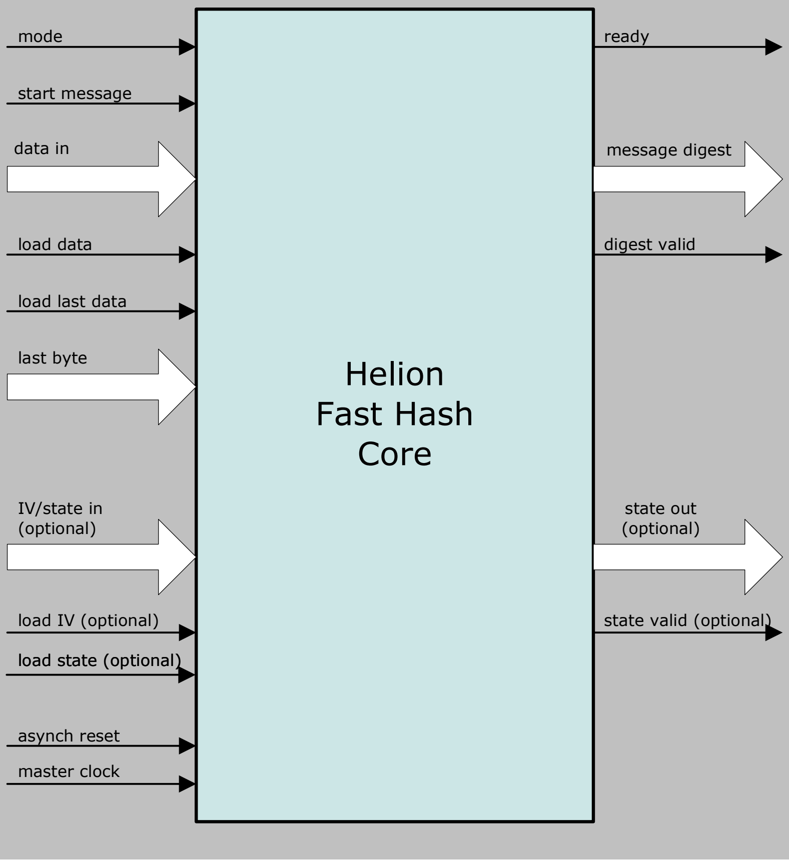
Helion Technology

FULL DATASHEET - Fast Hash Core Family for Altera FPGA



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
- Highly optimised for use in Altera FPGA technologies

Deliverables

- Target specific netlist or fully synthesisable HDL source code
- VHDL/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 use in Altera FPGA.

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 source code wrapper is available 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 data width of the underlying hash algorithm to ensure maximum data throughput. The message digest output width also varies with the digest size of the hashing algorithm.

The measured resource utilisation and maximum performance figures for a selection of Altera FPGA device families are shown in the tables below for the four most popular versions of the Fast Hash core family NB. The standard versions shown in the tables do not include state unload/reload or HMAC functionality, both of which further increase the logic resource used. Other versions are also available which are not shown in the tables, including MD5 legacy solutions. All versions of the core are available for all current and legacy Altera devices, so please contact Helion for details of other core versions, or for resource and performance metrics for Altera FPGA devices not shown.

In keeping with all Helion IP cores, the Fast Hash core family has been highly optimised for the lowest logic resource usage and maximum performance in Altera FPGA.

Logic Utilisation and Performance

	Cyclone IV			**Arria II GX**		
Core version	Resource	Max clock	Max data rate	Resource	Max clock	Max data rate
SHA-1 only	1263 LEs 3 M9Ks	179 MHz	1117 Mbps	541 ALMs 3 M9Ks	296 MHz	1848 Mbps
SHA-256 only	1804 LEs 4 M9Ks	138 MHz	1070 Mbps	830 ALMs 4 M9Ks	227 MHz	1760 Mbps
Dual SHA-1/256	2272 LEs 4 M9Ks	138 MHz	1070 Mbps	956 ALMs 4 M9Ks	197 MHz	1528 Mbps
Dual SHA-384/512	3265 LEs 8 M9Ks	105 MHz	1311 Mbps	1337 ALMs 8 M9Ks	178 MHz	2170 Mbps

Logic Utilisation and Performance (continued)

	Stratix IV			Stratix V		
Core version	Resource	Max clock	Max data rate	Resource	Max clock	Max data rate
SHA-1 only	545 ALMs 3 M9Ks	371 MHz	2316 Mbps	601 ALMs 3 M20Ks	467 MHz	2916 Mbps
SHA-256 only	827 ALMs 4 M9Ks	272 MHz	2110 Mbps	932 ALMs 4 M20Ks	313 MHz	2428 Mbps
Dual SHA-1/256	972 ALMs 4 M9Ks	252 MHz	1955 Mbps	1033 ALMs 4 M20Ks	313 MHz	2428 Mbps
Dual SHA-384/512	1378 ALMs 8 M9Ks	216 MHz	2697 Mbps	1528 ALMs 8 M20Ks	259 MHz	3234 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.

Helion has a very long history in working with high performance FPGAs, so we take our Altera implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Altera FPGA; they are not simply based on a generic ASIC design like much of the competition.

Most Helion IP cores make use of Altera-specific architectural features; in fact in many cases we build-up custom internal logic structures by hand, in order to achieve the very highest performance and most efficient logic resource utilisation. The benefits of this dedicated approach 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