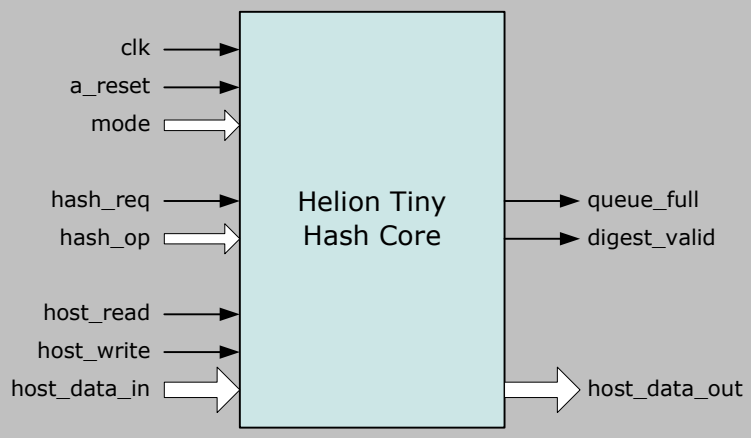
Helion Technology

FULL DATASHEET – Tiny 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
- Supports Keyed Hashing for Message Authentication (HMAC) to FIPS 198-1
- Supports state unload/reload operations to optimise hashing of interleaved message streams
- Highly optimised for use in Altera FPGA technology
- Provides high functionality for low resource in low data rate applications
- Ideally suited for use as a hash co-processor in embedded FPGA applications
- Choice of 8 or 32-bit host system interface data bus width

Deliverables

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

Overview

The Helion Tiny Hash Core family for Altera FPGA offers a combination of high functionality and low resource usage for lower data rate applications than the Helion Fast Hash Core family. The core is available in versions which support one or more of the five NIST approved cryptographic hashing algorithms described in FIPS 180-3; SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512, plus the legacy MD5 algorithm described in RFC 1321.

It can optionally support the standard Keyed Hash-based Message Authentication Code (HMAC) algorithm described in FIPS 198-1 which is widely used for data authentication and integrity checking in a number of data security protocols. Support for full hash state unload and reload also greatly improves system throughput when hashing interleaved or packetised message streams. A simple synchronous host system interface ensures easy connection into any end user application whether employed as a hardware hashing accelerator for an embedded processor, or connected directly into the datapath.

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

Functional Description

The Helion Tiny Hash core family can be provided in versions which implement one or more of the NIST approved hashing algorithms specified in FIPS 180-3; namely SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 and also supports the legacy MD5 hash algorithm to RFC 1321. In addition, each supported algorithm may be selected as the underlying hash function used to calculate the standard Keyed-Hash Message Authentication Code (HMAC) defined in FIPS 198-1.

The core is able to switch mode dynamically between messages, allowing any hash algorithm (with or without HMAC) to be selected on a message by message basis. Additionally using the state unload/reload functionality, the core may also switch between messages on a block by block basis in order to facilitate efficient handling of multiple interleaved message streams which require independent authentication.

For standard hash operations, the host loads message data into the core whenever the core indicates there is room in its message queue i.e. *queue_full* is deasserted. The core starts hash processing whenever a whole message block is available and the user has requested the hash operation defined by *hash_op* while asserting *hash_req*.

Further message blocks may be loaded into the message queue by the host whilst the core is still busy processing previous blocks. Once hashing of the final message block is complete the core indicates that the message digest is valid by asserting *digest_valid*. The host system may then read the calculated message digest from the core before starting to process the next message.

For HMAC operations, the host first loads the HMAC key into the core. The core then performs key pre-processing to ready itself for the subsequent hash operations, whilst the host is free to load the first blocks of message data. Once key pre-processing is complete, the core proceeds as described above for hash operations, with any additional internal HMAC processing hidden from the host. When the HMAC computation is complete the core indicates that the MAC result is valid by asserting *digest_valid*. The host system may then read the calculated MAC value from the core before starting to process the next message.

Core versions

The Tiny Hash core family is available in a number of versions, each sharing a common user interface whilst providing support for one or more hashing algorithms, optionally including HMAC processing.

Measured typical resource utilisation and maximum performance for a variety of Altera FPGA device families are detailed for four versions of the core in the tables below. Please note: These standard core versions do not include HMAC support, the addition of which increases the logic resource used slightly. The cores are available for all current and legacy Altera device families; please contact Helion for details of versions not shown, or for details of typical resource and performance for other Altera FPGA devices.

The core can also be provided with host data interface widths of either 8 or 32 bits. As standard the core is supplied with a 32 bit host data interface; all resource figures in the tables below assume this version.

Logic Utilisation and Performance

	Cyclone III/IV			Cyclone V		
Core version	Resource	Max clock	Max data rate	Resource	Max clock	Max data rate
SHA-1 only	560 LEs 2 M9K	180 MHz	45 Mbps	380 ALMs 2 M10K	179 MHz	45 Mbps
SHA-256 only	756 LEs 2 M9K	164 MHz	38 Mbps	448 ALMs 2 M10K	163 MHz	38 Mbps
SHA-1/256	966 LEs 2 M9K	162 MHz	40 Mbps	624 ALMs 2 M10K	166 MHz	41 Mbps
SHA-1/256/384/512	1577 LEs 2 M9K	171 MHz	42 Mbps	1026 ALMs 2 M10K	171 MHz	42 Mbps

Logic Utilisation and Performance (continued)

	Arria II GX			Stratix V		
Core version	Resource	Max clock	Max data rate	Resource	Max clock	Max data rate
SHA-1 only	382 ALMs 2 M9K	331 MHz	82 Mbps	382 ALMs 2 M20K	335 MHz	82 Mbps
SHA-256 only	443 ALMs 2 M9K	250 MHz	59 Mbps	446 ALMs 2 M20K	295 MHz	69 Mbps
SHA-1/256	642 ALMs 2 M9K	260 MHz	65 Mbps	620 ALMs 2 M20K	300 MHz	75 Mbps
SHA-1/256/384/512	1037 ALMs 2 M9K	271 MHz	67 Mbps	989 ALMs 2 M20K	310 MHz	77 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