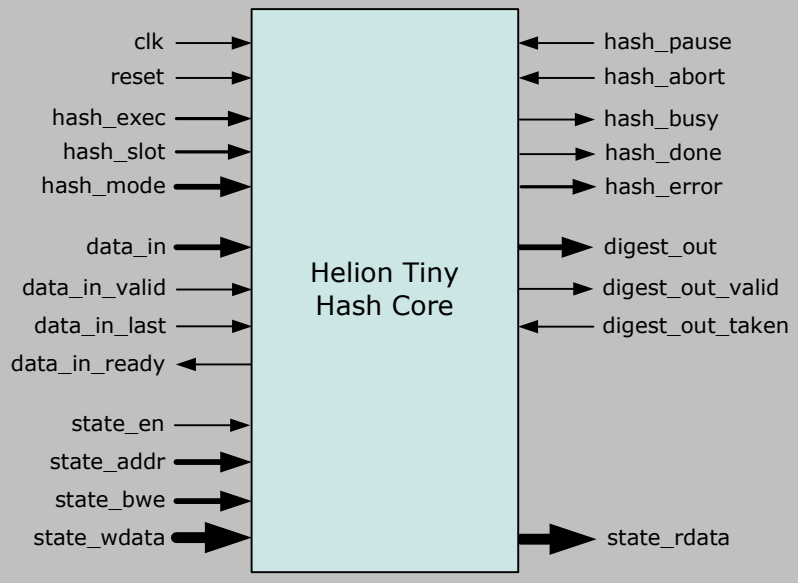
Helion Technology

FULL DATASHEET – Tiny Hash Core for ASIC



Features

- Implements one or more of SHA-1, SHA-224, SHA-256, SHA-384 & SHA-512 secure hash algorithms defined in FIPS PUB 180-3
- Supports Keyed Hashing for Message Authentication (HMAC) to FIPS 198-1
- Performs full message padding according to FIPS PUB 180-3
- Provides high functionality for low resource, low data rate applications
- Supports four concurrent hashes each using different hash algorithms
- Supports full state unload/reload to optimise hashing of interleaved data
- Highly optimised, smallest available hashing core for use in ASIC

Deliverables

- Fully synthesisable RTL Verilog
- Self-checking Verilog testbench with SHA Validation Suite test vectors
- Comprehensive User documentation

Overview

The Helion Tiny Hash Core family for ASIC 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 any combination of the secure hashing algorithms described in the Secure Hash Standard, FIPS PUB 180-3; namely SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. It can support the standard Hash-based Message Authentication Code (HMAC) algorithm described in FIPS PUB 198-1 which is widely used for data authentication and integrity checking in a number of common data security protocols.

The core supports up to four hash calculations, or two HMAC calculations, with full core state unload and reload to greatly improve system throughput when processing interleaved or packet-based data streams is a requirement. Simple synchronous interfaces ensure easy system integration whether employed as a hashing accelerator for an embedded processor, or connected directly into a datapath.

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

Functional Description

The Helion Tiny Hash core for ASIC is fully configurable and can implement any combination of the NIST secure hashing algorithms specified in FIPS PUB 180-3; namely SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. It can also support the newer SHA-512-224 and SHA-512-256 hash algorithms defined in DRAFT FIPS PUB 180-4.

The core is able to switch hash algorithm dynamically between message blocks; allowing any of the hash algorithms supported by the core to be selected for use on a message block by block basis. The core internally provides support for four concurrent hash calculations each using a different hash algorithm as standard, enabling up to four message streams to be hashed simultaneously. Additionally, using the optional state unload and reload interface the core can very efficiently handle more than four interleaved message streams using external state storage.

For hash operations, the user initiates a new hash operation on the *hash_exec* input; the *hash_mode* and *hash_slot* inputs indicating the hash algorithm and internal memory slot to be used for the operation. The core then indicates its readiness to accept input data and the user may load message data into the core using the *data_in_valid* and *data_in_ready* handshake signalling. At the end of the message, the user flags the last byte of the final message block by asserting the *data_in_last* marker input and the core appends padding as required by FIPS PUB 180-3.

Once the core has completed hashing of the final message block it indicates that the resulting message digest output is valid by asserting *digest_out_valid*. The host system may then read the message digest from *digest_out* using the *digest_out_taken* handshake signal before starting the next hash operation.

The Tiny Hash core indicates an operation is in progress by asserting *hash_busy* following acceptance of a valid hash operation request on the *hash_exec* input. Once a hash operation is complete the core de-asserts the *hash_busy* output and pulses the *hash_done* output at which point the user may read the final message digest or internal state from the core.

Two further control inputs are provided to allow suspension of the current hash operation; *hash_pause* stops the current core operation at the end of the present message block for state unload and reload operation; and *hash_abort* halts the current operation immediately and returns the core to its idle state. A new hash operation may be requested in the very next clock cycle.

Core versions

The Tiny Hash core is fully configurable allowing a number of possible core variants to be synthesized by the user; each variant sharing a common user interface whilst providing support for a different combination of secure hashing algorithms, with or without HMAC. The size and performance of the core varies with the configured algorithm support since logic associated with unused algorithms is not implemented during synthesis.

Typical resource utilisation and performance when targeting a standard 0.13um CMOS ASIC process are shown in the tables below for six different variants of the core to illustrate the relationship between the configured hash algorithm(s) and the resulting resource area. The core has been designed to use the absolute minimum area for each user configuration and very efficiently makes uses of a small single-port RAM or register file to implement the internal state storage necessary for all secure hash algorithms.

Logic Utilisation and Performance

	SHA-1	SHA-256	SHA-1/256
technology	0.13 um	0.13 um	0.13 um
logic resource + SPRAM	<6k gates 32x32	<8k gates 40x32	<9k gates 40x32
clock constraint	200 MHz	200 MHz	200 MHz
max SHA-1 rate	>100 Mbps	N/A	>100 Mbps
max SHA-256 rate	N/A	>100 Mbps	>100 Mbps
max SHA-384/512 rate	N/A	N/A	N/A

Logic Utilisation and Performance (continued)

	SHA-384/512	SHA-256/384/512	SHA-1/224/256/384/512
technology	0.13 um	0.13 um	0.13 um
logic resource + SPRAM	<13k gates 40x64	<15k gates 40x64	<17k gates 40x64
clock constraint	200 MHz	200 MHz	200 MHz
max SHA-1 rate	N/A	N/A	>100 Mbps
max SHA-224/256 rate	N/A	>100 Mbps	>100 Mbps
max SHA-384/512 rate	>150 Mbps	>150 Mbps	>150 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