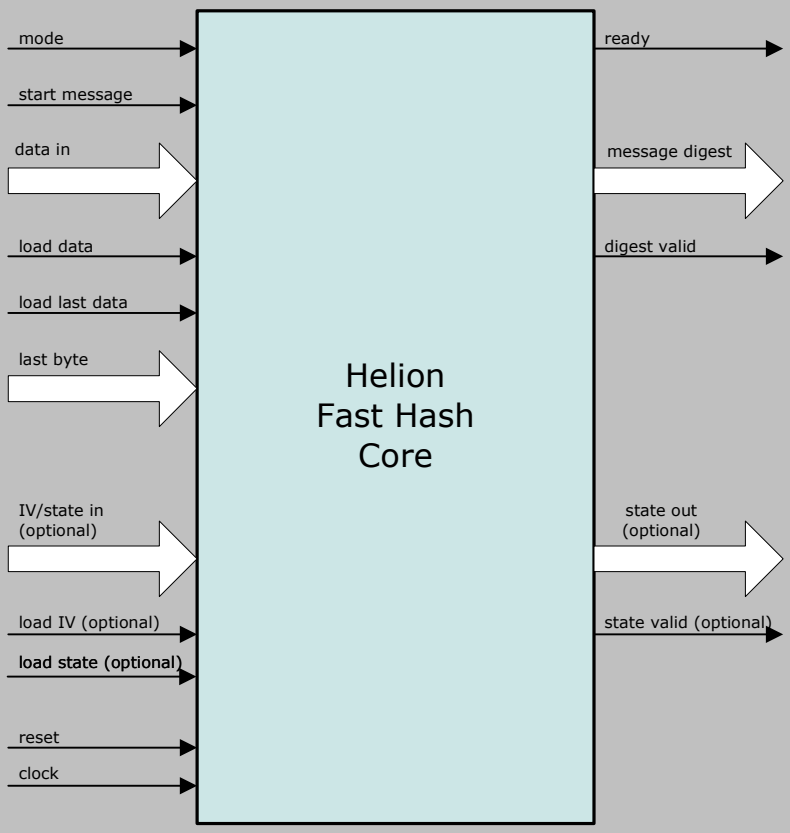
Helion Technology

PRODUCT BRIEF | **Fast Hash IP cores for ASIC**



Features

- Implements one or more of SHA-1, 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 accelerated HMAC support
- HMAC wrapper available for quick and easy implementation
- Optional state unload/reload feature for handling fragmented messages
- Simple external interface
- Optimised for use in ASIC

Deliverables

- Fully synthesisable RTL source code
- VHDL/Verilog simulation model and testbench
- User documentation

Overview

The Helion Fast Hash core family implements the NIST approved SHA-1, 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 dual algorithm versions and have been designed specifically for use in 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

Background
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 a message digest as the output. The resulting digest varies in length (and thus security) with hash algorithm.

These cores implement the NIST approved hashing algorithms specified in FIPS 180-3; namely SHA-1, SHA-256, SHA-384 and SHA-512, as well as the legacy MD5 hash algorithm described in RFC 1321. The cores implement single hashing algorithms, or certain pairs of algorithms, in which case the core is able to switch mode dynamically between messages, allowing the hash algorithm to be changed on a message by message basis. Please see the "Ordering Information" section overleaf for a list of valid algorithm pairings supported.

The Helion Fast Hash core family comes with input data interface widths of 32-bit (SHA-1, SHA-256 and MD5) or 64-bit (SHA-384 and SHA-512) in keeping with the underlying hash algorithm to ensure maximum data throughput. The message digest output is a full width parallel port, and so varies with the digest size of the supported hashing algorithm.

Supporting HMAC
An optional HDL wrapper is available from Helion which contains all of the additional logic (including key storage) required to simply 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.

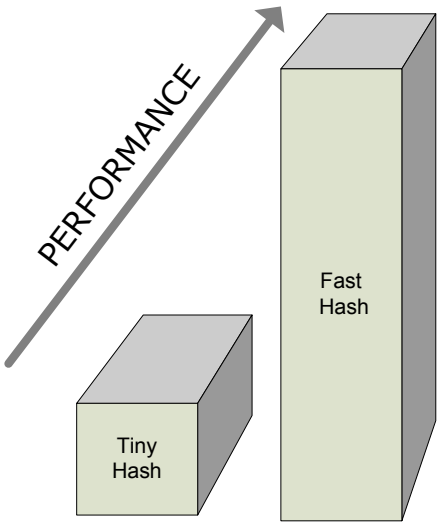
Core Operation
Hash algorithms process data in blocks – these are 512-bits in size for SHA-1, SHA-256 and MD5, and 1024-bits in the case of SHA-384 and SHA-512. The cores contain an internal block store which may be loaded with message data under the control of external logic whenever the core indicates it is ready. Once the block store is full, the core will indicate that it is busy, and will execute the next phase of the hash algorithm internally. On completion, the core will indicate that it is ready to accept the next message block, so this process may repeat.

The user application logic is responsible for informing the core when the last message word is present at the data input and the location of the last message byte within that last word. This allows the core to calculate the exact message length and append message padding accordingly, which is a necessary part of the hashing algorithm. When the last message block has been processed, the core will output the resulting message digest and will indicate its validity. The core is then ready and available to start work on the next message.

Extra Features
One available core option is support for unload and reload of the hash state at message block boundaries. This allows the full hash core state to be stored externally and subsequently reloaded at a future time to provide for efficient hashing of fragmented messages.

These versions of the cores also allow 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. One application for this is to allow accelerated implementation of the Keyed-Hash Message Authentication Code (HMAC) described in FIPS 198-1, where key pre-processing is available.

Core Choice



The **Fast** Hash core is one of two hashing solutions available from Helion, and is aimed at higher throughput applications - up to low Gbps rates – where it can support high clock rates and rapid block processing without excessive logic utilisation.

Within the Fast Hash core family there are a number of core versions, each supporting one or two hashing algorithms – the latter can be dynamically selected in use. More detail on the available options is shown overleaf.

Where only low throughput rates are required, Helion also offer a lower area **Tiny** Hashing core family, which is covered in a separate datasheet. Please see http://heliontech.com/tiny_hash.htm for more details on this solution.

Core Throughput

The tables below show the number of cycles and the maximum data throughput as a function of core clock frequency, for each of the supported algorithms running in the Fast Hash core.

algorithm	SHA-1	SHA-256 or MD5	SHA-384 or SHA-512
size of hash block	512-bits	512-bits	1024-bits
clock cycles used per hash block	82	66	82
data throughput (Mbps per MHz)	6.24	7.75	12.48

For any specific application, the above figures may be used with an appropriate and achievable core clock frequency to determine actual message processing time. Note that if HMAC support is being planned, there are "per message" overheads associated with this algorithm, which can become significant particularly when short messages are being handled. In this case additional performance margin may be required. Please contact Helion to discuss this in more detail.

Logic Utilisation and Performance

The table below shows typical area and maximum clock rates for popular configurations of the Helion Fast Hash core.

	Helion Fast Hash cores			
version	SHA-1	SHA-256	SHA-512	SHA-1/SHA-256
typical gatecount	<13k gates	<19k gates	<41k gates	<21k gates
typical max clock rate (65nm)	450MHz	400MHz	300MHz	400MHz

Note that exact figures will depend significantly on the target library used, as well as the synthesis method and options, so these numbers should be treated as preliminary guidance only.

Only need Low Data Rates?

The Helion Fast Hash core is designed specifically for higher data rate applications, where its optimised wide datapath allows very high clock rates and fast block processing times. However where data throughput requirements are more modest, a more compact, lower rate solution may be appropriate.

Helion offer a Tiny Hash core family which has been optimised for lowest logic area and offers a rich feature set, supporting multiple hash algorithms at rates of 100 to 200 Mbps as well as inbuilt HMAC processing. Please take a look at our Tiny Hash webpage at http://www.heliontech.com/tiny_hash.htm, or contact Helion for more information on low resource hashing core solutions.

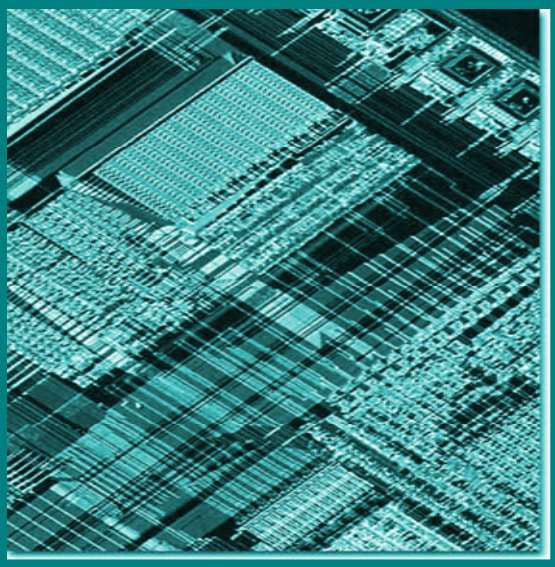
Ordering Information

Before ordering, the first thing to decide is which algorithms you would like to support. Supported combinations are as follows; SHA-1 only, SHA-256 only, SHA-384 only, SHA-512 only, MD5 only, SHA-1/SHA-256 dual-mode, SHA-1/MD5 dual-mode and SHA-384/SHA-512 dual mode.

If you require simple support for HMAC, this should also be specified at time of order. This is supported by way of an optional wrapper that sits on top of the hashing engine, and takes care of the key storage, additional processing and control required to implement an HMAC.

If some of these choices are unclear, or you would just like to go over the options available, we are always happy to discuss the alternatives and help select the best solution for your application.

HELION



**"Helion's products and services have consistently fit a variety of our needs.
They are superbly easy to work with, answering questions in clear straightforward terms.
The organization of their deliverables - particularly the concise and sensible documentation - provide for fast successful integration of their IP.
I deal with many vendors, Helion is currently my favorite by every conceivable metric."**

Jeff Harms
IP Procurement Lead
Microchip Technology

About Helion

Founded in 1992, Helion is a long established British company based in Cambridge, England. We offer a range of product-proven Data Security and Lossless Compression IP cores, backed by a team of highly experienced engineers, proudly developing and supporting a world-class portfolio.

Our aim is to offer our customers…

Innovation
Helion works hard to anticipate, understand and then deliver great solutions for its customers. As an example, Helion offered the world's first commercial AES core back in 2001, even before the industry had fully adopted the algorithm. This process continues unabated today, with new products in development that will lead the field.

High Performance
Helion IP is specially designed and optimised for each target technology. This means lots of work for us, but this approach yields amazing results for our customers. We always aim for the best in class performance and lowest utilisation in any given ASIC or FPGA target.

High Quality
IP should be problem free, so we always go the extra mile to ensure a smooth and trouble free integration phase for our products. We realise that our customers are putting their faith in us, and want to repay that with an outstandingly easy deployment.

Ease of Use
Helion engineers have many years of real product development experience, and so our IP is designed to be used in realistic situations. It is flexible and well thought through - the result being that it is simple to drop into your system.

See how we achieve all this by visiting our Clients page at http://www.heliontech.com/clients.htm

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