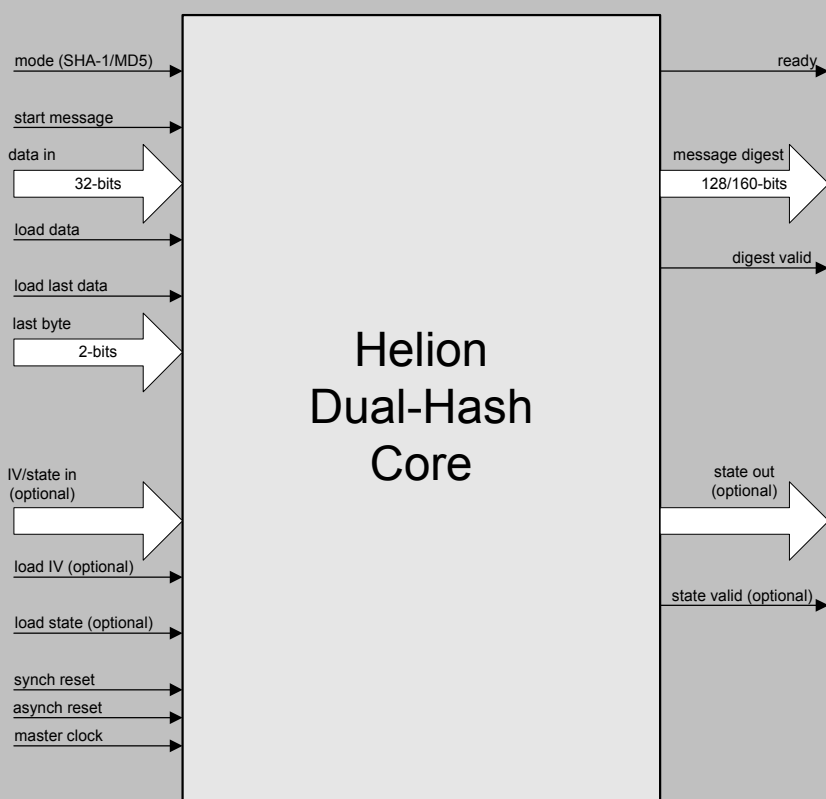


# Helion Technology

## DATASHEET – High Performance Dual MD5 and SHA-1 Hash Core for ASIC



### Features

- Implements both MD5 and SHA-1 secure hash algorithms
- Fast operation – each 512-bit block requires 82 (SHA-1) or 66 (MD5) master clock cycles
- Performs automatic message length calculation and padding insertion
- Optional user initialisation of IVs for efficient HMAC support
- Optional hash state unload/reload feature for handling fragmented messages
- Simple external interface
- Suitable for use in ASIC or fine-grain FPGA technologies

### Deliverables

- Fully synthesisable RTL source (VHDL or Verilog available)
- VHDL/Verilog testbench with FIPS/RFC test vectors
- Synopsys synthesis scripts
- Comprehensive user documentation

## Overview

This high performance core from Helion is intended for use in ASIC and fine-grain FPGA technologies, and implements both the MD5 and SHA-1 secure hash algorithms.

Both hash algorithms take as input a message of arbitrary length, process the message in 512-bit blocks, and produce as output either a 128-bit (MD5) or 160-bit (SHA-1) message digest. They are intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted. Applications include hardware implementations of the Digital Signature Algorithm where a hash function is used to generate and verify signatures for data integrity and origin authentication as specified in the Digital Signature Standard described in FIPS PUB 186, as well as the Internet standard HMAC (RFC 2104) used in IPsec and SSL.

## Helion Technology Limited

The Granary, Home End, Fulbourn, Cambridge CB1 5BS, UK.



## Functional Description

The Helion dual hash core implements the two most commonly used secure hash algorithms, sharing common resources to achieve dual-mode support whilst using fewer logic resources than two individual solutions. Both hash functions process an arbitrary length input message by operating on successive 512-bit blocks of data, producing as output either a 128-bit (MD5) or 160-bit (SHA-1) message digest.

The core contains an internal 16x32-bit block store which may be loaded with message data under the control of external logic or a microprocessor, when 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 a further message block. The external logic is responsible for informing the core when the last message word is available at the data inputs 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 digest of the message and indicates its validity to the external logic.

Optionally, whilst loading the first message word, the external logic may also load customised initial values into the core. This allows pre-computed initial values to be used for efficient implementation of a Hash-based Message Authentication Code (HMAC); loading of these incurs no throughput penalty since they have their own dedicated input port. In addition, the internal hash state can be made accessible, so that it may be stored externally and subsequently re-instated; this may be a useful option where fragmented messages are being hashed.

## Core Performance

This core has been designed for efficient implementation in both ASIC and fine-grain FPGA designs, with particular emphasis on maximising the data throughput capabilities, whilst keeping the gatecount down to a reasonable level.

For ASIC applications, the illustrative gate count and speed figures shown below have been based on synthesis with Synopsys Design Compiler targeting a popular 0.13um CMOS technology library.

For fine-grain FPGA applications, performance and gate count will be dependant on the specific technology targeted; hence no figures are quoted here, but we would be happy to supply specific details on request.

<b>technology</b>	<b>0.13 um CMOS ASIC</b>
<b>typical core gate count</b>	< 20k
<b>max master clock</b>	> 200 MHz
<b>max data rate (MD5)</b>	> 1.55 Gbps
<b>max data rate (SHA-1)</b>	> 1.25 Gbps

### Other variants

This datasheet covers our fast "dual-mode" hash core, supporting both SHA-1 and MD5. However, we also have other variants available, offering single mode operation, or different tradeoffs between gatecount and throughput. Please feel free to contact us for with details of your particular requirements.

## 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.

