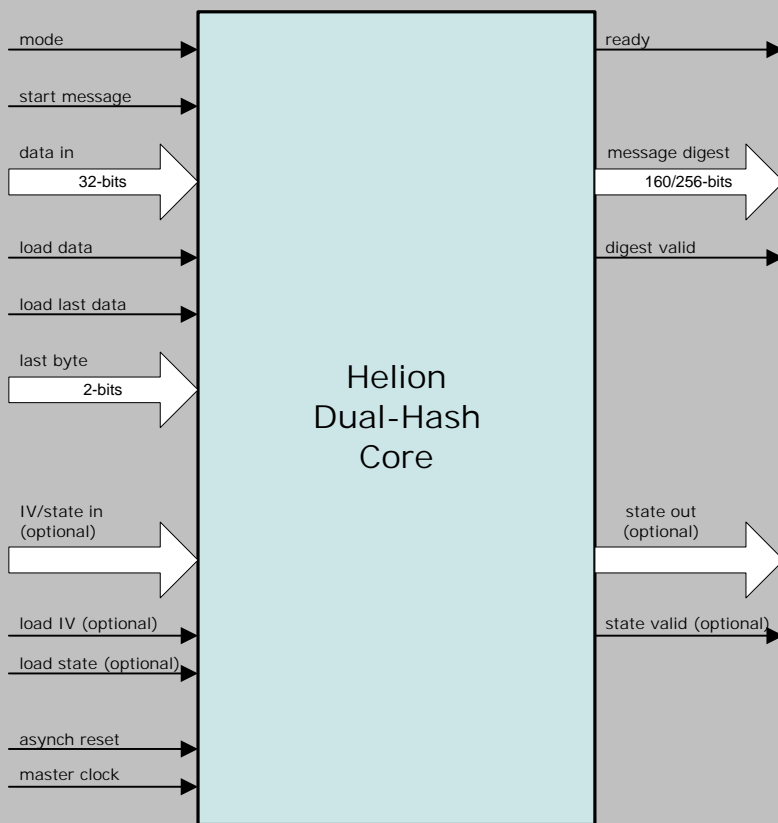


Helion Technology

DATASHEET - Fast Dual SHA-1 and SHA-256 Hash Core for Actel FPGA



Features

- Implements both SHA-1 and SHA-256 secure hash algorithms to NIST FIPS Publication 180-2
- Fast operation – each 512-bit block requires only 82 (SHA-1) or 66 (SHA-256) master clock cycles
- Performs automatic message length calculation and padding insertion
- Optional user initialisation of IVs for optimised HMAC support
- HMAC wrapper available to make implementations quick and easy
- Optional state unload/reload feature for handling fragmented messages
- Simple external interface
- Highly optimised for use in Actel FPGA technologies

Deliverables

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

Overview

This high performance core from Helion is intended exclusively for use in Actel FPGA, and implements both the SHA-1 and SHA-256 secure hash algorithms to NIST FIPS Publication 180-2.

Both hash algorithms take as input a message of arbitrary length, process the message in 512-bit blocks, and produce as output either a 160-bit (SHA-1) or 256-bit (SHA-256) 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 Internet standard HMAC (RFC 2104) used in the IPsec and SSL protocols, and in digital signature applications where a hash function is used to generate and verify signatures for data integrity and origin authentication .

Helion Technology Limited

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

Copyright © 2005 Helion Technology Limited. Revision 1.1 (29/11/2005)



Functional Description

The Helion dual hash core implements two 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 160-bit (SHA-1) or 256-bit (SHA-256) 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 and Resource Requirements

Helion also has a long history in high-end FPGA design, and we therefore take our FPGA implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Actel FPGA technology; they are not simply based on a synthesised generic ASIC design like much of the competition.

The Helion Fast SHA-1/SHA-256 core makes use of Actel-specific architectural features in order to achieve high performance and efficient logic resource utilisation. It is available for any of the current families including Axcelerator and ProASIC3.

Example performance and logic utilisation figures are shown below, targeting Actel Axcelerator and ProASIC3 devices. Obviously, different device families will yield different performance results; we would be pleased to provide details specific to your own applications on request. Note: the figures below are for the most popular version of the core, without the state unload/reload capability.

	—ProASIC3-2—	—Axcelerator-2—
resource	7126 Tiles	1274 R-cells 2275 C-cells
	8 RAMs	4 RAMs
max clock	57 MHz	78 MHz
throughput		
SHA-1	356 Mbps	487 Mbps
SHA-256	442 Mbps	605 Mbps

The logic utilisation figures above assume that FPGA RAM resource is available for the SHA-1/SHA-256 core. This will not always be the case for some applications, so Helion also has a variant of the core which does not require RAM resource for which utilisation figures are available upon request.

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

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

tel: +44 (0)1223 500 924 email: info@heliontech.com

fax: +44 (0)1223 880 169 web: www.heliontech.com

Copyright © 2005 Helion Technology Ltd; All rights reserved. This document contains Proprietary Trade Secrets of Helion Technology Limited; its receipt or possession does not convey any right to reproduce, disclose its contents, or to use its contents to manufacture, use, or sell anything that it may describe without the written authorisation of Helion Technology Limited. The products described in this document are subject to continuous development and all information is supplied strictly "as is" with no warranties implied or expressed and Helion Technology Limited shall not be liable for any loss or damage arising from the use of any information contained in this document.