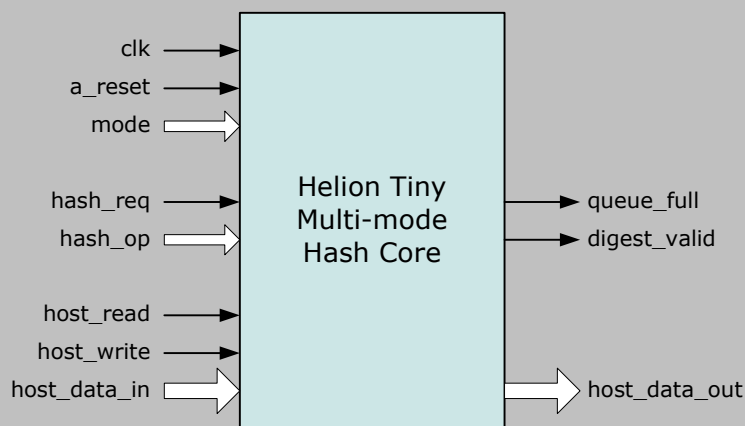


Helion Technology

FULL DATASHEET – Tiny Multi-mode Hash Core for Altera FPGA



Features

- Supports MD5, SHA-1, SHA-224 and SHA-256 hash algorithms
- Supports Keyed Hashing for Message Authentication (HMAC) to RFC 2104 for all hash algorithms
- Supports state unload/reload operations to optimise processing of fragmented message streams
- Highly optimised for use in Altera FPGA technology
- Provides high functionality for low resource in lower rate applications
- Ideally suited for use as a hash co-processor in NIOS II applications
- Choice of 8, 16 or 32-bit host system interface

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 Multi-mode Hash Core for Altera FPGA offers high functionality and low resource usage for lower rate applications than the Helion Fast Hash Core family.

The core implements four of the most widely used hashing algorithms; MD5, SHA-1, SHA-224 and SHA-256. It also supports the popular Internet standard HMAC mechanism used for data authentication and integrity checking in a number of secure protocols such as IPsec. Full support for hash state unload and reload also greatly improves system throughput for fragmented message streams.

A simple synchronous host system interface enables easy connection into any end user application whether employed as a hardware accelerator in a microprocessor system, or connected directly into a design datapath.

Helion Technology Limited

Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England



Functional Description

The Helion Multi-mode hash core implements four of the most popular hashing algorithms; MD5, SHA-1, SHA-224 and SHA-256. In addition, each algorithm may be selected as the underlying hash function used to calculate the Internet standard HMAC. This provides the core with eight possible modes - any of the four hash algorithms, with or without HMAC. The core can switch mode dynamically between messages, allowing any algorithm 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 facilitating efficient handling of fragmented message streams.

The host system may load message data into the core whenever it indicates there is room in its message queue. The core starts processing whenever a full 512-bit message block is available for hashing. Further message data may be loaded into the message queue whilst the core is busy. Once hashing is complete the core indicates that the resulting digest is valid. The host system can then read the 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 the necessary key pre-processing for the subsequent HMAC hash operations. The host then loads message data and proceeds as described above for hash operations, with any additional HMAC processing within the core hidden from the host.

Logic Utilisation and Performance

Helion has a long history in high-end FPGA design, and we therefore take great care when implementing our IP cores. As a result they have been designed from the ground up to be highly optimal in Altera FPGA technology - they are not simply based on a synthesised generic RTL ASIC design like much of the competition.

The Tiny Multi-mode Hash core has been specially micro-coded and handcrafted to be highly optimal in all Altera FPGA designs to give high functionality for the logic resources used. As such it makes use of Altera-specific architectural features in order to achieve highly efficient logic resource utilisation. It is aimed at lower data rate applications than our higher performance Altera Fast Hash core family and is available for all of the current Altera device families including legacy Cyclone and Stratix devices.

	Multi-Mode Hash			
technology	Cyclone II C6	Cyclone III C6	Stratix II C3	Stratix III C2
logic resource	1310 LEs 4x M4K	1285 LEs 2x M9K	910 ALUTs 4x M4K	906 ALUTs 2x M9K
max clock	140 MHz	146 MHz	208 MHz	306 MHz
throughput (MD5)	44 Mbps	46 Mbps	65 Mbps	96 Mbps
throughput (SHA-1)	28 Mbps	29 Mbps	42 Mbps	61 Mbps
throughput (SHA-256)	23 Mbps	24 Mbps	34 Mbps	51 Mbps

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