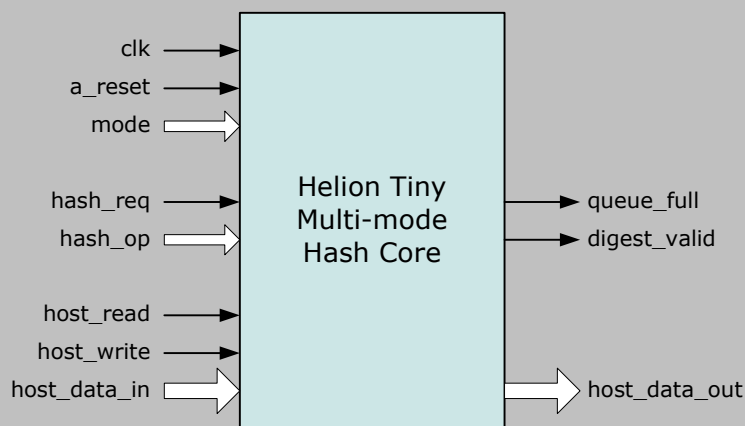


Helion Technology

FULL DATASHEET – Tiny Multi-mode Hash Core for 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 each individual FPGA technology
- Provides high functionality for low resource in lower rate applications
- Ideally suited for use as a hash co-processor
- 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 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 Tiny 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 for each individual FPGA technology - they are not simply based on a synthesised generic RTL ASIC design. The Helion Tiny Multi-mode hash core makes use of the architectural features available in each FPGA technology to achieve the highest performance combined with the most efficient logic resource utilisation.

The latest logic area, performance figures, and datasheets for the Helion Tiny Multi-mode hash core in a range of different technologies are available at <http://www.heliontech.com/multihash.htm>. Please feel free to contact us should you require further details.

About Helion

Helion is a long established British company based in Cambridge, England, offering a range of product-proven Data Security silicon IP cores backed up by our 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 headline IP vendors who try to supply a very diverse range of solutions, being specialists we can offer much more than just the IP core itself.

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.

The quality of our IP is however the main reason our customers keep coming back for more. We passionately believe that if you are buying IP, it should have been designed with the ultimate in care, crafted to achieve the ultimate performance in each target technology, and thoroughly tested to ensure compliance with any associated standards. All this comes as standard with IP from Helion.

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