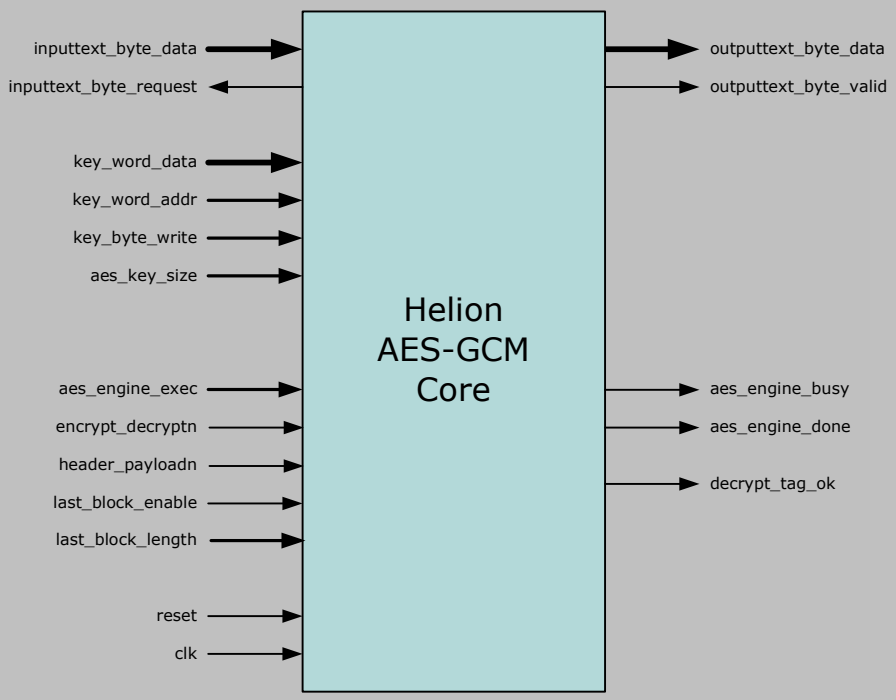
Helion Technology

FULL DATASHEET – Standard AES-GCM Core for Altera FPGA



Features

- Implements Galois/Counter (GCM) authenticated encryption mode to NIST 800-38D
- Supports all AES key sizes (128,192, and 256 bits) with integrated key expansion
- 96-bit Nonce/IV support
- Performs AES and GHASH functions needed for GCM including final block padding, tag appending and checking
- Simple 8-bit data interface for easy system integration
- Suitable for use in IPsec, MACsec, IEEE1619.1 and other applications
- Planned availability in multiple versions providing optimal area/ performance AES-GCM solutions

Deliverables

- Target specific netlist or fully synthesisable RTL VHDL/Verilog
- VHDL/Verilog simulation model and testbench
- User documentation

Overview

AES-GCM is an authenticated encryption block cipher mode which provides data confidentiality, integrity and origin authentication at potentially very high data rates, and is therefore an alternative to modes such as CCM, EAX & OCB. It is described formally in NIST Special Publication 800-38D. This particular implementation of GCM targets medium throughput applications with emphasis on low resource usage, and ease of use via a byte-wide interface.

The Helion AES-GCM core integrates all of the underlying functions required to implement AES in GCM mode including round-key expansion, counter mode logic, hash length counters, final block padding, and tag appending and checking features. The only external logic required is to form the Nonce block from various application specific packet header fields. Support is provided for both optional header and zero-length payload, and configurable tag length, making the core suitable for IPsec (RFC4106), MACsec (IEEE802.1ae) and Tape Storage (IEEE1619.1) applications.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

Functional Description

The Helion AES-GCM core uses AES-CTR operations to provide data encryption or decryption, and GHASH operations to provide message authentication. The master AES key is loaded into the core using the byte-writable 32-bit key interface. Key processing to derive the internal GHASH key is then initiated by the user issuing an EXEC_KEY command to the core (via aes_engine_exec) and indicating the AES key size to be used (aes_key_size).

Before the start of the message, the Nonce/IV must also be loaded by issuing an EXEC_INIT command to the core. The 128-bit Nonce/IV (96 bits used) is transferred into the core using the byte-wide data input interface. Message data processing is performed using multiple 128-bit block encrypt/decrypt operations which are initiated by issuing one or more EXEC_DATA commands to the core. Control inputs are used to indicate the direction (encrypt_decryptn) and data type (header_payloadn). The input block is transferred into the core using the byte-wide data input interface (inputtext_byte_data), and the resulting output block is transferred from the core using the byte-wide data output interface (outputtext_byte_data).

The last header or payload block may be less than 128 bits, and so its presence and length in bytes is indicated to the core using the last_block control inputs. Once the last message block has been encrypted/decrypted, the tag will either be appended to the output data (encrypt direction), or will be checked against the received tag (decrypt direction) and the tag check output flag (decrypt_tag_ok) driven accordingly.

Logic Utilisation and Performance

Helion has a very long history in working with high performance FPGAs. We therefore take great care when implementing our Altera cores, and as a result our cores have been designed from the bottom up to be highly optimal in each Altera FPGA technology - they are not simply based on a synthesised generic ASIC design. In this way we achieve the very best combination of low resource usage and high performance.

The Helion AES-GCM core is available for all popular Altera FPGA technologies. The tables below show typical logic area and performance figures for the first member of the 8-bit IO family with nominal 48-cycle operation:

	128-bit key version		**Allsizes key version**	
technology	CycloneIII -6	StratixII -3	CycloneIII -6	StratixII -3
logic resource	1925 LEs 3 M9K RAMs	1136 ALMs 3 M4K RAMs	2285 LEs 3 M9K RAMs	1274 ALMs 3 M4K RAMs
max clock	164 MHz	241 MHz	170 MHz	233 MHz
max throughput 128-bit AES key	437 Mbps	642 Mbps	453 Mbps	621 Mbps
max throughput 192-bit AES key	-	-	388 Mbps	532 Mbps
max throughput 256-bit AES key	-	-	340 Mbps	466 Mbps

Please note: Area and performance figures are available from Helion on request for other variants and for all device types and speed grades not shown in the tables above.

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