Helion Technology

FULL DATASHEET – AES-GCM Core family for Xilinx FPGA

inputtext_byte_data

inputtext_byte_request

key_word_data

key_word_addr

key_byte_write

aes_key_size

Helion
AES-GCM
Core

aes_engine_exec

encrypt_decryptn

header_payloadn

last_block_enable

last_block_length

reset

clk

outputtext_byte_data

outputtext_byte_valid

aes_engine_busy

aes_engine_done

decrypt_tag_ok
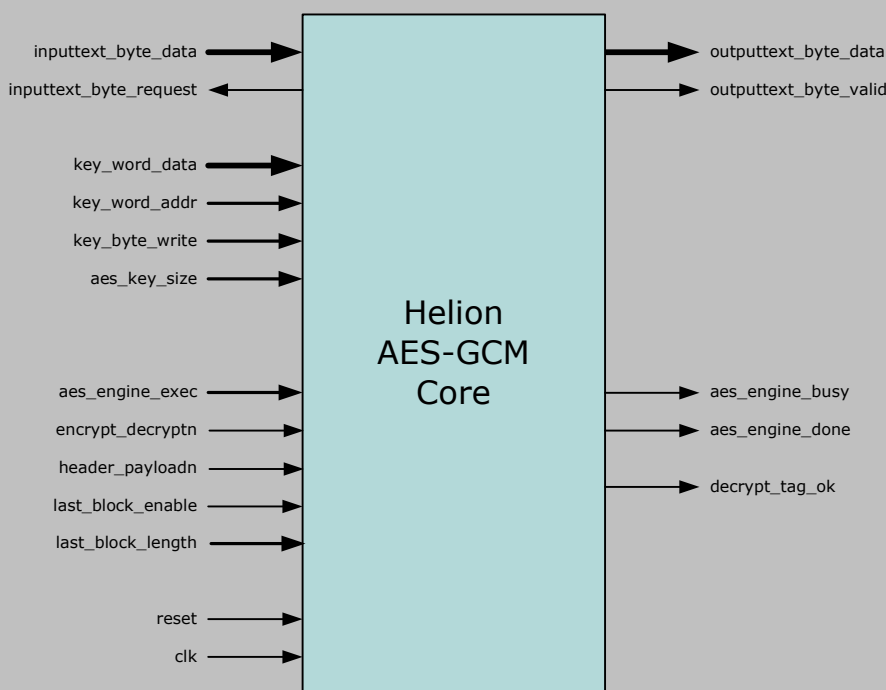
Features

- 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
- Now available in multiple versions providing optimal area/performance AES-GCM solution

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.

Core Choice

Helion always offer a range of solutions so that the throughput requirements of any application can be closely matched with optimum area efficiency. In this case, Helion have three levels of performance available; we name them to reflect the minimum number of clock cycles taken to process each 16-byte data block. NOTE. The actual number of cycles taken by the core to process this block varies with exact core choice and the keysize selected.

The smallest member of the family is the **"218-cycle" AES-GCM** core which takes a minimum 218 clock cycles to encrypt or decrypt each 16-byte data block using a 128-bit key.

For higher throughputs, the **"48-cycle" AES-GCM** core offers over four times the performance of the 218-cycle core while using less than twice its logic area. It takes a minimum 48 clock cycles to encrypt or decrypt each 16-byte data block using a 128-bit key.

The highest performance member of the family is the **"19-cycle" AES-GCM** core, which offers over twice the performance of the 48-cycle core while using approximately twice its logic area. It takes a minimum 19 clock cycles to encrypt or decrypt each 16-byte data block using any key size.

Each version of the core is available with support for one, two and (in most cases) all three AES key sizes (128, 192 and 256-bit).
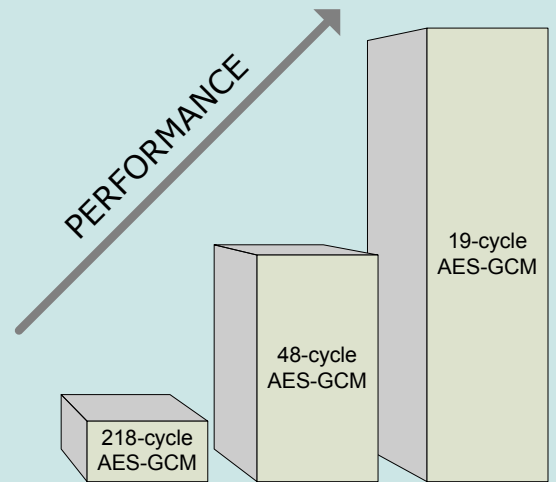
The tables below show the number of cycles and the maximum data throughput for each version of the AES-GCM core, for each supported key size.

	AES-GCM 218-cycle			AES-GCM 48-cycle			AES-GCM 19-cycle		
key size	128	192	256	128	192	256	128	192	256
clock cycles used per 16-byte block	218	n/a	298	48	56	64	19	19	19
max throughput (Mbps per MHz)	0.58	n/a	0.43	2.6	2.2	2.0	6.7	6.7	6.7

The 19-cycle version is available with a choice of standard or fast key expansion, which affects the overhead time of setting up a new key. The standard expansion is preferred in FPGA, especially when support for all three key sizes is required, as considerable area savings can be made.

For even higher data throughput requirements, Helion also have faster AES-GCM core families which have wider data ports to ensure the throughput is not constrained by the I/O bandwidth. Please contact Helion for more information on these faster AES-GCM solutions.

Logic Utilisation and Performance

The data throughput capability of the cores is proportional to the frequency of master clock used, and the maximum value of this depends on the type of device and the speed grade chosen.

	AES-GCM 218-cycle core					
	128-bit key version			Two-sizes key version		
technology	Spartan6 -3	Virtex5 -3	Virtex6 -3	Spartan6 -3	Virtex5 -3	Virtex6 -3
logic resource	209 slices	247 slices	217 slices	220 slices	256 slices	220 slices
max clock	252 MHz	393 MHz	475 MHz	231 MHz	410 MHz	461 MHz
max throughput 128-bit AES key	147 Mbps	230 Mbps	278 Mbps	135 Mbps	240 Mbps	270 Mbps
max throughput 256-bit AES key	-	-	-	99 Mbps	176 Mbps	198 Mbps

The tables on this page show the range of Helion AES-GCM solutions in a selection of common Xilinx device families and speed grades. The table above shows the 218-cycle core for both 128-bit and two-sizes key support. The tables below show the 48-cycle and 19-cycle AES-GCM cores, for 128-bit key and all-sizes key support.

	AES-GCM 48-cycle core					
	128-bit key version			All-sizes key version		
technology	Spartan6 -3	Virtex5 -3	Virtex6 -3	Spartan6 -3	Virtex5 -3	Virtex6 -3
logic resource	340 slices	415 slices	356 slices	362 slices	443 slices	376 slices
max clock	199 MHz	303 MHz	359 MHz	194 MHz	307 MHz	356 MHz
max throughput 128-bit AES key	530 Mbps	808 Mbps	957 Mbps	517 Mbps	818 Mbps	949 Mbps
max throughput 192-bit AES key	-	-	-	443 Mbps	701 Mbps	813 Mbps
max throughput 256-bit AES key	-	-	-	388 Mbps	614 Mbps	712 Mbps

	AES-GCM 19-cycle core					
	128-bit key version			All-sizes key version		
technology	Spartan6 -3	Virtex5 -3	Virtex6 -3	Spartan6 -3	Virtex5 -3	Virtex6 -3
logic resource	639 slices	678 slices	635 slices	672 slices	694 slices	669 slices
max clock	205 MHz	335 MHz	364 MHz	178 MHz	282 MHz	332 MHz
max throughput 128-bit AES key	1.38 Gbps	2.25 Gbps	2.45 Gbps	1.20 Mbps	1.90 Gbps	2.23 Gbps
max throughput 192-bit AES key	-	-	-	1.20 Mbps	1.90 Gbps	2.23 Gbps
max throughput 256-bit AES key	-	-	-	1.20 Mbps	1.90 Gbps	2.23 Gbps

Note that full support is available for all Xilinx families (both old and new). For logic resource and performance figures for other device and speed grade combinations, please feel free to contact Helion for details.

Ordering Information

Before ordering it is necessary to decide which of our family of AES-GCM cores will best fit your application. First decide between the 218-cycle, 48-cycle, and 19-cycle cores according to the data throughput required and logic resources available. Then determine which AES key sizes you would like to support as well as any other special requirements your application may have.

If some of these choices are unclear, or you would just like to go over the options available, we are always happy to discuss the alternatives and help select the best solution for your application.

AES-GCM core	Logic Area	Throughput	Encryption/ Decryption	Authentication	128-bit keys	192-bit keys	256-bit keys
218-cycle	lowest	low	✓	✓	✓	✗	✓
48-cycle	low	mid	✓	✓	✓	✓	✓
19-cycle	mid-high	highest	✓	✓	✓	✓	✓

About Helion

Founded in 1992, Helion is a well established British company based in Cambridge, England, offering a range of product-proven Data Security IP cores backed up by 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 broadline IP vendors who try to supply a very diverse range of solutions, being specialists we can offer much more than just the IP core.

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.

In addition, our Design Services team have an impressive track record in the development of real security products for our customers; we are proud to have been involved in the design of numerous highly acclaimed security products. This knowledge and experience is fed back into our IP cores, to ensure that they are easy to integrate into real systems, and perform appropriately for real engineering applications.

Helion is also a member of the Xilinx AllianceCORE IP program, and a certified Xilinx Alliance Partner. We therefore take our Xilinx implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Xilinx FPGA; they are not simply based on a generic ASIC design like much of the competition.

Most Helion IP cores make use of Xilinx-specific architectural features; in fact in many cases we build-up custom internal logic structures by hand, in order to achieve the very highest performance and most efficient logic resource utilisation. The benefits of this dedicated approach can be clearly demonstrated by direct comparison between Helion data security IP cores and the equivalents from other vendors.

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