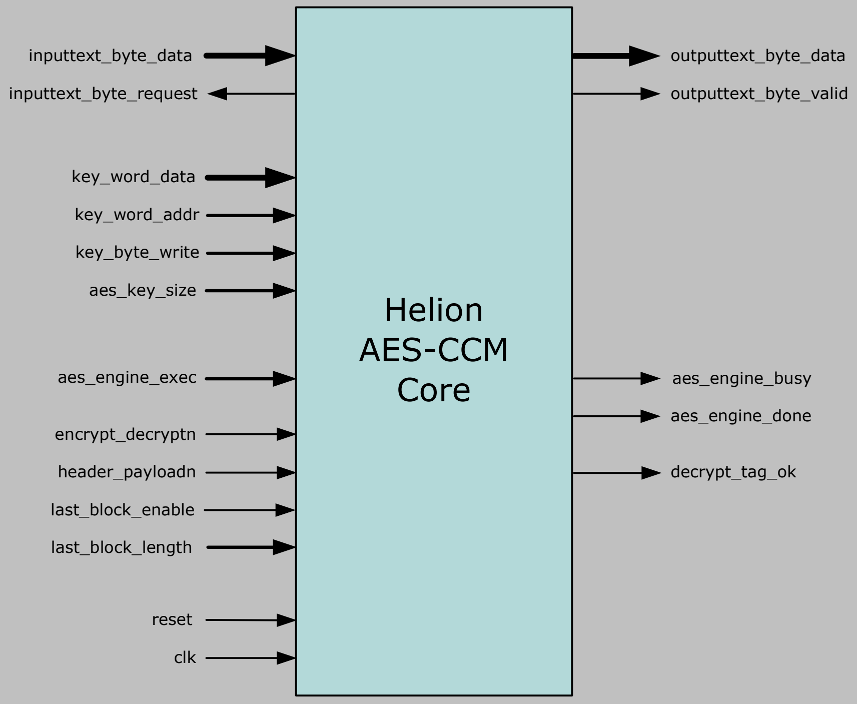
Helion Technology

FULL DATASHEET – AES-CCM Core family for Altera FPGA



Features

- Implements Counter with CBC-MAC (CCM) authenticated encryption mode to NIST 800-38C
- Supports all AES key sizes (128,192, and 256 bits) with integrated key expansion
- Performs all CCM counter management, block chaining, block masking, tag appending and checking
- Simple 8-bit data interface for easy system integration
- Suitable for use in 802.11, 802.15 and 802.16 wireless applications
- Available in multiple versions providing optimal area/performance AES-CCM solution

Deliverables

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

Overview

AES-CCM is an authenticated encryption block cipher mode which was originally conceived to provide data confidentiality, integrity and origin authentication for use in the IEEE 802.11i standard. The original version specified AES with 128-bit key support only and is documented in RFC 3610, although NIST Special Publication 800-38C describes a more general use with multiple key size support.

The Helion AES-CCM core integrates all of the underlying functions required to implement AES in CCM mode including round-key expansion, counter management, block chaining, final block masking, 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, thus supporting all three IEEE wireless standards: 802.11, 802.15 (including 802.15.4 and ZigBee™ with a CCM* variant) and 802.16.

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

Functional Description

The Helion AES-CCM core internally performs two distinct AES operations; AES-CTR mode to provide data encryption or decryption, and AES-CBC-MAC mode to provide message authentication. Both AES operations use the same key which is loaded into the core using the byte-writable 32-bit key interface. Key processing 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 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. Two control inputs are used to indicate the direction (encrypt_decryptn) and data type (header_payloadn) of the incoming CCM data block. 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 message 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

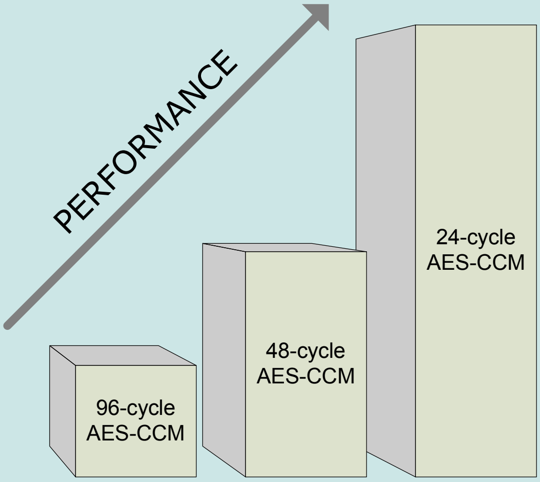
Helion always offer a range of solutions so that the throughput requirements of any application can be closely matched with optimum area efficiency. In this case, Helion have three levels of performance available; we name them to reflect the nominal number of clock cycles taken to process each 16-byte 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 called the **"96-cycle" AES-CCM** core which takes a nominal 96-clock cycles to encrypt or decrypt each 16-byte data block using a 128-bit key.

For higher throughputs, the **"48-cycle" AES-CCM** core offers twice the performance of the 96-cycle core while using less than twice its logic area. It takes a nominal 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 called the **"24-cycle" AES-CCM** core, which offers nominally twice the performance of the 48-cycle core while using less than twice its logic area. It takes a nominal 24-clock cycles to encrypt or decrypt each 16-byte data block using a 128-bit key.

Each version of the core is available with support for either 128-bit only or all sizes (128, 192 and 256-bit) key support.



version	**AES-CCM 24-cycle**		**AES-CCM 48-cycle**		**AES-CCM 96-cycle**	
key option	128 only	Allsizes 128/192/256	128 only	Allsizes 128/192/256	128 only	Allsizes 128/192/256
actual clock cycles	23	28/28/31	48	48/56/64	96	96/112/128
data throughput (Mbps per MHz)	5.5	4.5/4.5/4.1	2.6	2.6/2.2/2.0	1.3	1.3/1.1/1.0

The tables above show the actual number of cycles plus the resulting data throughput (expressed as Megabits per second per MHz) for each version of the AES-CCM core and for each key support option.

Note that the two types of 24-cycle core are individually optimised to minimise logic area, and so have differing cycle counts for 128-bit keys. Other options are available if the listed performance above is not appropriate.

For even higher data throughput requirements, Helion also have faster AES-CCM 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-CCM solutions.

Logic Utilisation and Performance

The tables below show the area and performance of the 96-cycle and 48-cycle AES-CCM cores targeting Altera Stratix2. These cores also support Cyclone1, 2 & 3 and Stratix2 & 3 devices. For logic resource and performance figures for other Altera device and speed grade combinations, or for our faster core variants, please feel free to contact Helion for details.

	AES-CCM 96-cycle core		**AES-CCM 48-cycle core**	
	128-bit key version	**Allsizes key version**	**128-bit key version**	**Allsizes key version**
technology	Stratix2 -3	Stratix2 -3	Stratix2 -3	Stratix2 -3
logic resource	628 ALUTs 3 M4K RAMs	768 ALUTs 3 M4K RAMs	773 ALUTS 5 M4K RAMs	901 ALUTs 5 M4K RAMs
max clock	234 MHz	226 MHz	238 MHz	224 MHz
max throughput 128-bit key	312 Mbps	301 Mbps	634 Mbps	597 Mbps
max throughput 192-bit key	-	258 Mbps	-	512 Mbps
max throughput 256-bit key	-	226 Mbps	-	448 Mbps

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 has a very long history in working with high performance FPGAs, so we take our Altera implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Altera FPGA; they are not simply based on a generic ASIC design like much of the competition.

Most Helion IP cores make use of Altera-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