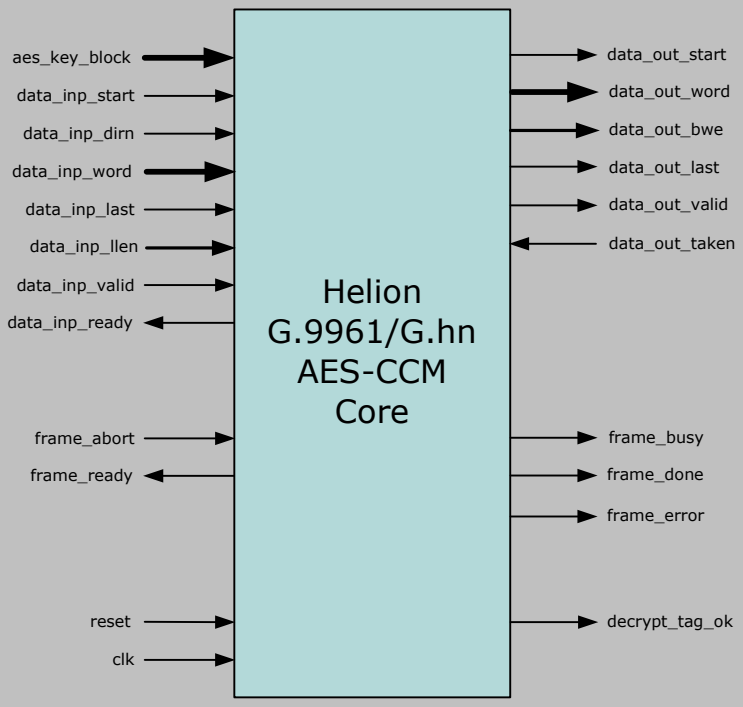
Helion Technology

FULL DATASHEET – G.9961 AES-CCM Frame Encryption Core for ASIC



Features

- Suitable for use in G.hn applications
- Capable of supporting 3x 1GbE links
- Implements Counter with CBC-MAC (CCM) authenticated encryption for the G.9961 standard
- Parses header fields and constructs CCM nonce and header (AAD) blocks automatically
- Performs all CCM counter management, block chaining, block masking, tag appending and checking
- Simple 64-bit data interface for easy system integration
- Available in two versions providing optimal area/performance AES-CCM solutions for G.9961

Deliverables

- Fully synthesisable Verilog RTL
- Verilog testbench
- User documentation

Overview

G.hn is a standard for home networking over power, coaxial, or telephone cable, or a combination of the three. The Data Link Layer is specified in ITU-T recommendation G.9961. The encryption requirement for G.9961 is based on AES-CCM; 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 Helion G.9961 AES-CCM ("AES-G.hn") core is designed to sit near the top of the LLC sublayer and provide the security functionality described in Section 9.1 of ITU-T G.9961. The core integrates all of the underlying functions required to implement AES in CCM mode for G.9961 including nonce and header formation, round-key expansion, counter management, block chaining, final block masking, and tag appending and checking features. The only external logic required is to insert the CCMP header field for frames that are to be encrypted.

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

Functional Description

The Helion "AES-G.hn" 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 128-bit key which is loaded into the core when a frame is started.

Once the start of a frame has been indicated to the core the frame can be input over the data interface using standard valid/ready handshaking. The core will parse the header fields and assemble the nonce and CCM header blocks in the format described in the G.9961 standard. A short time after the start of the frame the output interface will indicate that output can commence and the processed frame can be read out using the same handshaking method as the input interface.

The last data word may be less than 64 bits, and so its presence and length in bytes is indicated to the core using the last block control inputs. If the indicated length is inconsistent with the LFH FLEN field, a frame error is indicated. 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.

Depending on the core variant, the input interface may be ready to accept the next frame almost immediately, or it may be necessary to wait until the output of the current frame has completed before beginning the next.

Core Performance and Resource Requirements

There are two levels of performance available for this core. Both core versions have nominally the same throughput performance on long frames, but differ in the maximum frame rate for short frames.

	AES-G.9961 Frame Processor	
	Overlapped	Non-Overlapped
technology	0.13um	0.13um
logic resource	< 82k gates	< 72k gates
max clock	> 300 MHz	> 300 MHz
max throughput	> 3.5 Gbps	> 3.5 Gbps
max frame-rate 49-byte encrypted payload	> 4.4 Mfps	> 3.2 Mfps

The **overlapped** core allows the user to begin processing a new frame before the current one has finished. This yields the maximum possible frame-rate as frames can be input back-to-back. It is possible to support 3x 1GbE links (each with ~1.4 Mfps max frame-rate) with this core.

The **non-overlapped** core offers an area saving for applications where frame-rate is not critical. Frames are processed independently and each must be read from the output in its entirety before the next can be started. This core cannot meet the frame-rate required for 3x 1GbE links.

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.

Unlike many broadline IP core vendors, Helion also spends a great deal of effort designing its cores at the very lowest level. We strongly believe that if you are buying IP, it should have been designed with the ultimate in care, and crafted to achieve the desired performance; not just put together at a high level to get the job done quickly. We find that this approach pushes the results much closer to the intended performance envelope.

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