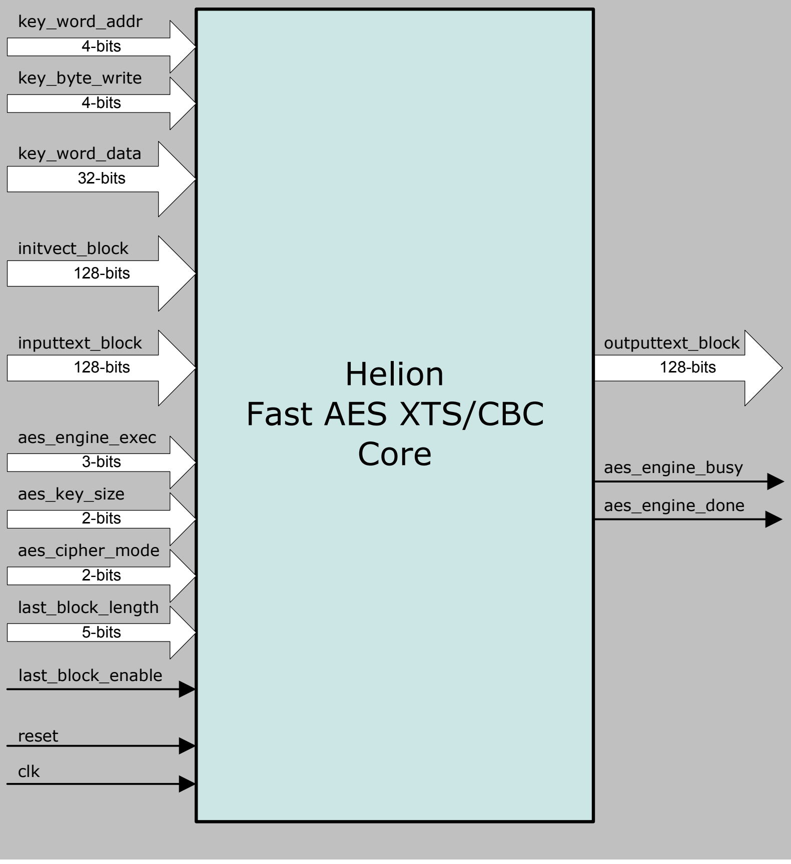
Helion Technology

FULL DATASHEET - Fast AES XTS/CBC Core for Altera FPGA



Features

- Implements AES-XTS mode as specified by IEEE 1619 standards
- Supports AES-CBC mode for legacy storage applications
- Automatically performs XTS tweak computation and ciphertext stealing
- Available in full encrypt-decrypt or encrypt-only configurations
- XTS mode support for both 256 and 512-bit key sizes (optional)
- CBC mode support for 128 and 256-bit key sizes (optional)
- Simple 128-bit external interface
- Highly optimised for use in Altera FPGA technologies

Deliverables

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

Overview

The Helion Fast AES XTS/CBC core implements the AES “XEX-based Tweaked Codebook with Ciphertext Stealing” cipher mode (abbreviated to XTS) specified in IEEE 1619 to provide Narrow-Block Encryption as part of its Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. XTS is also specified in IEEE 1619.1 for use in tape storage applications. In addition, and with very little logic cost, it implements the popular AES Cipher Block Chaining (AES-CBC) mode of operation which is also commonly used to provide data security in storage applications.

Within IEEE 1619 storage applications, AES-XTS is used to encrypt data at the disk sector level, where it addresses threats such as copy-and-paste and dictionary attacks whilst allowing the option of parallel processing to enhance performance. AES-XTS encrypts and decrypts data using a "tweak" value derived from the logical position of the block on the disk. This fulfils the fundamental requirements for disk encryption that data can be independently encrypted and decrypted at the sector level as it arrives in arbitrary order, whilst not changing the data size.

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

Functional Description

The Helion Fast AES XTS/CBC core implements two of the most commonly employed encryption algorithms used for securing data in hard disk and tape storage media applications. The core has a dedicated 32-bit input port which allows the key to be written as either 8, 16 or 32-bit words using individual byte enables. Once the key has been written to the core, the cipher mode and key size are selected by driving the *aes_cipher_mode* and *aes_key_size* inputs respectively, and key loading finalised by issuing an EXEC_KEY command on the *aes_engine_exec* input.

Once the *aes_engine_busy* output indicates the core is ready for the next operation, the *initvect_block* input is used to load either the XTS mode “tweak” or CBC mode IV value into the core, by issuing an EXEC_INIT command on the *aes_engine_exec* input. Following initialisation, when the *aes_engine_busy* output is once again de-asserted, the core is primed and ready for data block processing.

Data for encryption/decryption is input to the core an AES block at a time on the *inputtext_block* input port, and the resulting ciphertext/plaintext is output from the core on the out*puttext_block* output port. Data block processing is initiated by issuing an EXEC_DATA command on the *aes_engine_exec* input, with the resulting output data block being valid when the *aes_engine_done* output is asserted by the core. Special signalling is required to handle the penultimate and final data blocks where the length of the data being processed is not a block multiple. This is provided by the *last_block_enable* and *last_block_length* inputs.

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 in Altera FPGA technology - they are not simply based on a synthesised generic RTL ASIC design like much of the competition.

The Helion Fast AES XTS/CBC core makes use of Altera-specific architectural features in order to achieve high performance combined with efficient logic resource utilisation. It is available in versions with standard or fast key initialisation, full encrypt/decrypt or encrypt-only support, and with or without ciphertext-stealing for arbitrary data lengths, for all current Altera FPGA technologies. The tables below show typical logic area and performance figures for some popular variants using fast key initialisation:

	Full Enc/Dec		**Full Enc/Dec without stealing**		**Enc-only**	
technology	Arria II GX C4	Stratix IV C2	Arria II GX C4	Stratix IV C2	Arria II GX C4	Stratix IV C2
logic resource	5767 ALUTs 1549 DFFs	5759 ALUTs 1542 DFFs	5185 ALUTs 1522 DFFs	5183 ALUTs 1518 DFFs	3278 ALUTs 1377 DFFs	3277 ALUTs 1377 DFFs
max clock	219 MHz	259 MHz	218 MHz	264 MHz	240 MHz	274 MHz
max throughput (256-bit XTS key)	2.3 Gbps	2.7 Gbps	2.3 Gbps	2.8 Gbps	2.5 Gbps	2.9 Gbps

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