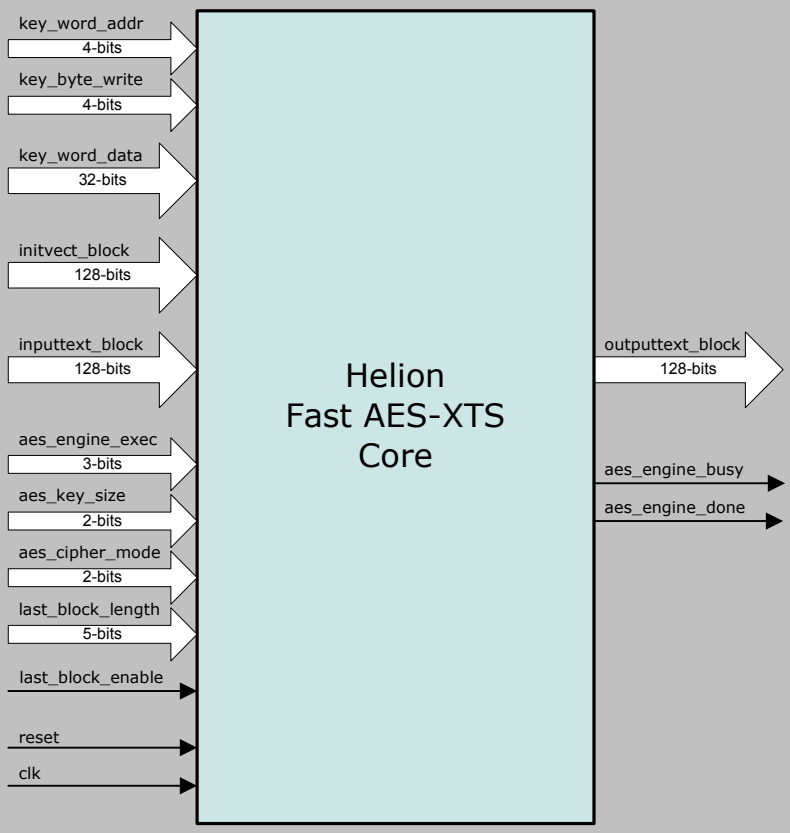
Helion Technology

PRODUCT BRIEF | **AES-XTS IP cores for FPGA**



Features

- Implements AES-XTS mode as specified by IEEE 1619 standards and NIST SP800-38E
- Supports AES-CBC mode for legacy storage applications
- Automatically performs XTS tweak computation and ciphertext stealing
- Available in full encrypt-decrypt or separate encrypt-only & decrypt-only configurations
- XTS mode support for both 256 and 512-bit key sizes (optional)
- CBC mode support for 128, 192 and 256-bit key sizes (optional)
- Simple parallel external interface
- Available in multiple versions providing optimal area/performance AES-XTS solution in FPGA

Deliverables

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

Overview

The Helion Fast AES XTS core implements the AES "XEX-based Tweaked Codebook with Ciphertext Stealing" cipher mode (abbreviated to XTS) specified by NIST SP800-38E and 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, some versions optionally implement the AES Cipher Block Chaining (AES-CBC) mode of operation which is sometimes used in legacy 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 core implements the most commonly employed encryption algorithm used for securing data in hard disk storage applications. Optional version-specific support is also available for AES-CBC mode (useful in legacy applications), or AES-ECB mode (useful for certification purposes). Please see "Core Choice – More Options" below for details.

Whilst processing hard disk sector data, the user drives the core by issuing a sequence of commands via the *aes_engine_exec* port, and the core's status is indicated at each stage by the *aes_engine_busy* and *aes_engine_done* flags.

Keying the core
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.

Starting each sector
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.

Processing the data
Data for encryption/decryption is input to the core one 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. Please see "Core Choice" section for information on the size of the block processed during each operation.

At the end of the sector
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.
Once the final block has been completed, the process can then be repeated for the next sector by loading a new key (if required) or the next tweak value.

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, there are two performance levels available. The baseline product is the **Fast AES-XTS core**, offering high data rates suitable for many applications, and is typically able to support the needs of a single SATA 2.0 Hard disk in high performance FPGA silicon. However, if you require more throughput, the **Twin Fast AES-XTS core** offers 2x the data rate of the Fast core, at less than twice the logic area. It may therefore be the better solution to support a single SATA 3.0 SSD, or to achieve higher throughput in slower, low cost FPGA silicon.

The two cores have exactly the same method of operation; they essentially only differ in the width of their data I/O ports and therefore how much data they process per encryption/decryption operation. The Fast XTS core has 128-bit I/O, and processes 128-bit blocks of data per operation. The Twin Fast XTS core has 256-bit I/O, and therefore processes 256-bit blocks of data per operation. Appropriate signalling is provided in both versions to flag the last valid byte in a block, at the end of a sector.

More Options
A wider key port (128-bit with 32-bit write enables) is available as an option for quicker key loading in those applications where fast switching between multiple key scopes is needed.

The Fast AES-XTS core version optionally supports the IEEE 1619 specified ciphertext stealing scheme which allows it to process non-block-multiple payload lengths. This option does affect the area of the core, so should only be specified if it is required. This option is not currently supported by the Twin Fast AES-XTS core – please contact Helion if this is a particular requirement.

In addition, the Fast XTS core can be specified to support CBC mode for one or more AES key sizes with very little logic penalty, providing a complete solution for vendors who must support this legacy mode. Note that this option is not available with the Twin Fast XTS core. However in its place, this core implements ECB mode as standard, to facilitate easier FIPS testing in a final end product.

Core Throughput

The tables below show the number of cycles and the maximum data throughput as a function of core clock frequency, for each version of the AES-XTS core, for each supported key size.

	Fast AES-XTS data block size = 128-bits		**Twin Fast AES-XTS** data block size = 256-bits	
key size	256	512	256	512
clock cycles used per enc/dec block operation	12	16	12	16
max throughput (Mbps per MHz)	10.6	8.0	21.3	16.0

For any specific application, a core version can be chosen that will achieve the required throughput, with an appropriate and achievable core clock frequency, not forgetting to take into account the inevitable per-sector overheads which may be incurred.

Logic Utilisation and Performance

Helion cores are fully characterised in all supported FPGA types (please see overleaf for supported FPGA technologies), with specific results available for each device type and speed grade. This yields a huge amount of data, so we don't include it in this Product Brief. Please contact Helion with your vendor requirements, and we will be delighted to send the appropriate information.

For general guidance however, the typical maximum achievable clock rates in the latest fast FPGA silicon might be ~300MHz to ~350MHz in a mid speed grade part (depending on the exact version and device), whilst in lower cost FPGA devices this range may be closer to ~140MHz to ~190MHz. These figures can be used as a starting point to determine which version of the core could be suitable for your requirements. A selection of the most popular combinations are also shown on our AES-XTS core web pages, at http://www.heliontech.com/aes_xts.htm.

Looking for Higher Rates?

The AES-XTS mode may be accelerated to very high rates based on parallel processing, so as well as the medium/high rate solutions presented here, Helion also have even faster AES-XTS core families aimed at multi-Gigabit data rates. Please take a look at our AES-XTS webpage at http://www.heliontech.com/aes_xts.htm, or contact Helion for more information on these faster AES-XTS solutions.

Ordering Information

Before ordering it is necessary to decide which of our family of AES-XTS cores will best fit your application. First decide between the **Fast AES-XTS** and **Twin Fast AES-XTS** 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 options or requirements your application may have. The main options are detailed on the previous page, under the "Core Choice – More options" section.

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.

FPGA Technology Support

Helion has a long history in high-end FPGA design, and takes a great deal of care when implementing IP cores. As a result, these cores have been designed from the ground up to be highly optimal for each individual FPGA technology - they are not simply based on a synthesised generic RTL ASIC design. Helion cores always make use of the architectural features available in each FPGA technology to achieve the highest performance combined with the most efficient logic resource utilisation.

Helion is an accredited IP partner with **Altera, Lattice, Microsemi (Actel)** and **Xilinx**, and supports all current and many legacy FPGA technologies from these vendors. Please feel free to contact Helion if your FPGA technology of choice is not listed here.

About Helion

Founded in 1992, Helion is a long established British company based in Cambridge, England. We offer a range of product-proven Data Security and Lossless Compression IP cores, backed by a team of highly experienced engineers, proudly developing and supporting a world-class portfolio.

Our aim is to offer our customers…

Innovation
Helion works hard to anticipate, understand and then deliver great solutions for its customers. As an example, Helion offered the world's first commercial AES core back in 2001, even before the industry had fully adopted the algorithm. This process continues unabated today, with new products in development that will lead the field.

High Performance
Helion IP is specially designed and optimised for each target technology. This means lots of work for us, but this approach yields amazing results for our customers. We always aim for the best in class performance and lowest utilisation in any given ASIC or FPGA target.

High Quality
IP should be problem free, so we always go the extra mile to ensure a smooth and trouble free integration phase for our products. We realise that our customers are putting their faith in us, and want to repay that with an outstandingly easy deployment.

Ease of Use
Helion engineers have many years of real product development experience, and so our IP is designed to be used in realistic situations. It is flexible and well thought through - the result being that it is simple to drop into your system.

See how we achieve all this by visiting our Clients page at http://www.heliontech.com/clients.htm

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