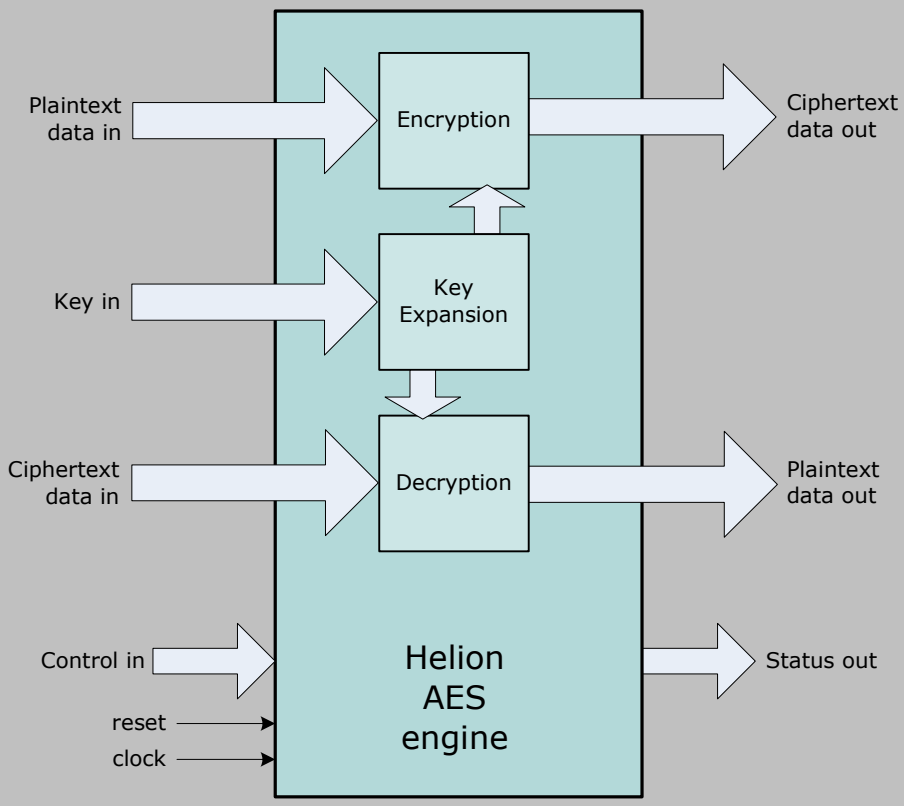
Helion Technology

PRODUCT BRIEF | **AES IP cores for ASIC**



Features

- Implements AES (Rijndael) to NIST FIPS PUB 197
- Full dynamic support for all AES key sizes (128, 192 and 256-bits)
- Multiple versions available; user can choose best balance of speed and area for application
- Separate cores available for encryption and decryption
- Roundkey expansion can be split out for additional flexibility
- All NIST SP800-38A AES operating modes easily implemented (eg. ECB, CBC, OFB, CFB, CTR)
- Simple external interface
- Highly optimised for use in ASIC targets

Deliverables

- Fully synthesisable RTL source code
- VHDL/Verilog testbench with test vectors
- User documentation

Overview

These highly developed cores from Helion implement the Advanced Encryption Standard (AES), as described in the NIST Federal Information Processing Standard (FIPS) Publication 197 document. Designed with ultimate flexibility in mind, the cores offer both encryption and decryption functions, plus they can support any or all of the available key-sizes (128/192/256-bit).

This latest range of solutions comes as part of a long line of AES cores from Helion. Being the very first company in the world to offer commercial AES solutions in FPGA and ASIC back in 2001, our cores are now extremely well proven in thousands of real products. All our cores are very simple to use, and highly versatile; they can be integrated into any AES design requirement with minimum effort.

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

Helion AES core range

Helion was first to market with a set of commercial AES IP cores back in the summer of 2001, so by now we offer the most comprehensive set of mature and product proven AES solutions available anywhere for use in ASIC and FPGA.

The Helion AES cores implement the 128-bit block-size NIST FIPS AES algorithm. The encryptor core accepts a 128-bit plaintext input word, and generates a corresponding 128-bit ciphertext output word using a supplied 128, 192 or 256-bit AES key. The decryptor core provides the reverse function, re-generating plaintext from supplied ciphertext, using the same AES key as was used for encryption.

Which AES core should I choose?

Since AES is being used in so many varied end products, we offer four AES core "families", each with different area/performance combinations, so that you can choose the most efficient for your application. We are proud to say that our solutions are class leading in each category.

The first step is to choose from our four AES core families detailed in the table below. This is usually driven by the throughput levels you require, remembering that older ASIC geometries may not support the rates shown. Then choose from within the families, the direction, mode and key support required, as described below.

Core Family?

TINY AES
STANDARD AES
FAST AES
GIGA AES

Direction Support?

Encryption-only
Decryption-only
Encryption/Decryption

Mode Support?

For example;
ECB, CBC
CFB, OFB, CTR

Key Size Support?

128-bits
192-bits
256-bits
Combinations of above

				
CORE FAMILY	**TINY**	**STANDARD**	**FAST**	**GIGA**
Attributes	Ultra low area	High efficiency	High speed, low latency	Ultra high speed
Typical max throughput	Up to 200Mbps	Up to 1000Mbps	Up to 5.0Gbps	Up to 100Gbps

This product brief covers **TINY, STANDARD** and **FAST AES** cores in some more detail. If you are more interested in the Helion **GIGA AES** cores, please contact Helion for specific literature.

Direction Support

This is simply a question of what AES functions your application requires. With Helion you can have encryption-only, decryption-only or a single engine supporting both encryption and decryption.

Mode Support

The AES cores natively support ECB mode, and then the basic NIST SP800-38A Block Cipher Modes, such as CBC, CFB, OFB and CTR, can be simply implemented using Helion supplied source-code wrappers. More complex modes like AES-CCM, AES-GCM and AES-XTS, plus other functions like KeyWrap and PRNG, are covered by dedicated Helion IP cores, since this allows them to be better tailored for their typical applications. Please refer to the Helion website for information on these products.

If you are not familiar with the concept of "Modes" of AES, then this is fully described in our "AES Basics" document, which can be downloaded from the Helion website; http://www.heliontech.com/downloads/Helion_AES_Primer.pdf.

Key Size Support

The AES algorithm is defined for 128, 192 and 256-bit keys, with the amount of security essentially increasing as the key gets longer. Throughput is unavoidably reduced for the longer keys, since the AES algorithm has more processing rounds. Your application will usually determine which of these key sizes you need to support; Helion AES cores can support single sizes or a combination as required.

Helion Tiny AES cores

The Helion Tiny AES cores have been carefully designed for absolute minimum logic utilisation and power consumption, when lower data rates are the requirement. They are ideal for throughputs up to 200Mbps in ASIC.

These cores use an 8-bit internal datapath to trade off the number of clock cycles against logic area, required to implement the AES algorithm. This internal datapath is matched to external 8-bit plaintext, ciphertext and key ports, which fit well with many applications running at these kinds of data rates. Of course, if you do need to interface with wider or narrower data widths in your system, then the additional glue logic needed is trivial, and the core provides useful control signal "hooks" to make this width translation very simple.

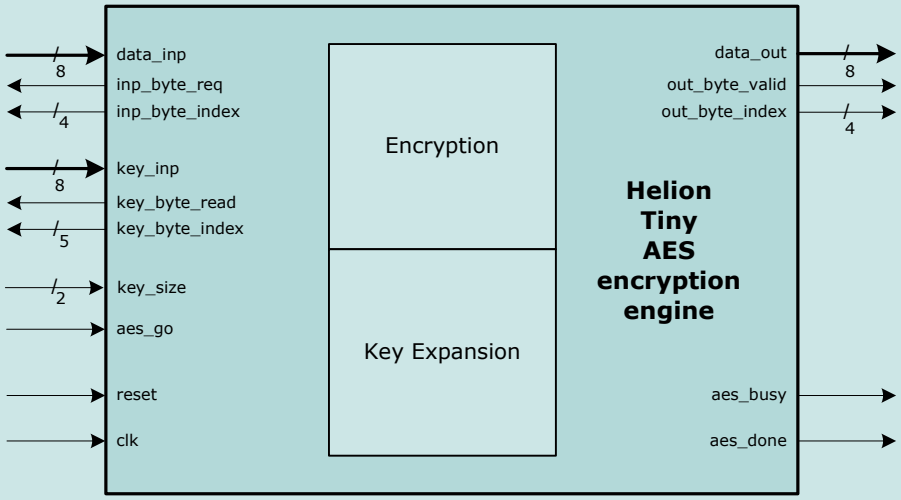
Operation

Operation of these cores is very straightforward; once a block of plaintext and the AES key are available, the *aes_go* input can be asserted. The core will assert *aes_busy*, and pulls in the plaintext and the key bytes as it requires them into *data_inp* and *key_inp* respectively. This is signalled via *inp_byte_index* and *inp_byte_req (for the plaintext),* and *key_byte_index* and *key_byte_read* (for the key). The index outputs may form the LS address bits into buffer RAMs in many designs, or the *byte_req/read* signals could be used to read from FIFOs. When the encryption process has completed, the ciphertext bytes will emerge from the core on *data_out*, validated by *out_byte_index* and *out_byte_valid*. Again, these may be used to drive the LS address bits and write enable into a RAM, or *out_byte_valid* could drive a FIFO write control. When the process is complete, the *aes_done* status flag strobes for a clock cycle, and the *aes_busy* flag is deasserted indicating that the core is ready to start the next encryption process.

Core Ports

The diagram alongside shows the I/O ports for a Tiny AES engine set up for Encryption-only with hardware Key Expansion. A Decryption engine is identical externally, and a combined Encryption/Decryption core simply adds an "enc/dec" input select.

Note how *byte_index* status signals plus *byte_req, byte_read* and *byte_valid* flags for each interface indicate exactly which byte is active on a cycle-by-cycle basis.
These signals make external interfacing and width changing extremely simple.



Core Throughput

The Tiny AES core is the perfect choice for lower rate applications, though it will support any data rates up to ~200Mbps in ASIC silicon. It's throughput vs. clock speed is 0.58 Mbps/MHz for encryption or decryption with a 128-bit key – similarly 0.46 Mbps/MHz for 192-bit keys and 0.43 Mbps/MHz for 256-bit keys. If your target throughput is close to its limit then the required clock rate will be high, so unless absolute minimum logic area is a requirement, it may also be worth considering the Standard AES core family overleaf.

Core Options

The Helion Tiny AES core is fully modular, and therefore configurable to closely match the end application's requirements, minimising logic utilisation in the ASIC. All the options detailed on page 2 of this Product Brief are available, as are some special options which may be discussed if your requirements are complex.

Logic Utilisation and Performance

	Tiny AES, enc-only		Tiny AES, enc/dec	
key support	128-only	128/192/256 selectable	128-only	128/192/256 selectable
typical gatecount	<4k gates	<5k gates	<5k gates	<6k gates
typical max clock rate (65nm)	400MHz	400MHz	400MHz	400Mhz

The tables show typical gatecounts and maximum clock rates for popular configurations of the Helion Tiny AES IP cores.

Note that exact figures will depend significantly on the target library used, as well as the synthesis method and options, so these numbers should be treated as preliminary guidance only.

Helion Standard AES cores

The Helion Standard AES cores have been carefully designed to require the absolute minimum of logic resource, whilst still maintaining high data throughput capabilities, squarely within the most widely used 100Mbps to 1Gbps band.

These cores use a 32-bit internal datapath to trade off the number of clock cycles against logic area, required to implement the AES algorithm. This internal datapath is matched to external 32-bit plaintext, ciphertext and key ports, which fit well with many applications running at these kinds of data rates. Of course, if you do need to interface with wider or narrower data widths in your system, then the additional glue logic needed is trivial, and the core provides useful control signal "hooks" to make this width translation very simple.

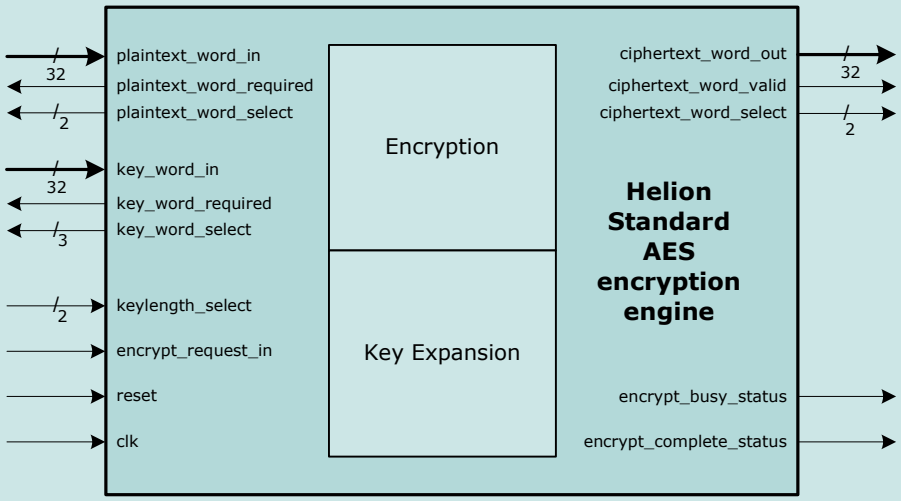
Operation

Operation of these cores is very straightforward; once a block of plaintext and the AES key are available, the encrypt *request* can be asserted. The core will assert the *busy* status output, and pull in the plaintext and the key words as it requires them, using its plaintext and key *word_select* and *word_required* outputs. The *word_selects* form the LS address bits into buffer RAMs in many designs, or the *word_required* signals could be used to read from FIFOs. When the encryption process has completed, the ciphertext words will emerge from the core, validated by the ciphertext *word_select* and *word_valid* outputs. Again, these may be used to drive the LS address bits and write enable into a RAM, or *word_valid* could drive a FIFO write control. When the process is complete, the *complete* status flag strobes for a clock cycle, and the *busy* flag is deasserted indicating that the core is ready to start the next encryption process.

Core Ports

The diagram alongside shows the I/O ports for a Standard AES engine set up for Encryption with hardware Key Expansion. A Decryption engine is correspondingly similar, but would have Ciphertext input and Plaintext output ports.

Note how *word_select* status signals plus *word_required* and *word_valid* flags for each interface indicate exactly which word is active on a cycle-by-cycle basis. These signals make external interfacing and width changing extremely simple



Core Throughput

The Standard AES core is the perfect choice for mid rate applications, though it will support any data rates up to ~1Gbps in ASIC silicon. It's throughput vs. clock speed is 2.66 Mbps/MHz for encryption or decryption with a 128-bit key – similarly 2.28 Mbps/MHz for 192-bit keys and 2.00 Mbps/MHz for 256-bit keys. If your target throughput is close to its limit then the required clock rate will be high, so unless absolute minimum logic area is a requirement, it may also be worth considering the Fast AES core family overleaf.

Core Options

The Helion Standard AES core is fully modular, and therefore configurable to closely match the end application's requirements, minimising logic utilisation in the ASIC. All the options detailed on page 2 of this Product Brief are available, as are some special options which may be discussed if your requirements are complex.

Logic Utilisation and Performance

	Std AES, enc-only		Std AES, enc/dec	
key support	128-only	128/192/256 selectable	128-only	128/192/256 selectable
typical gatecount	<10k gates	<11k gates	<15k gates	<16k gates
typical max clock rate (65nm)	400MHz	400MHz	400MHz	400Mhz

The tables show typical gatecounts and maximum clock rates for popular configurations of the Helion Standard AES IP cores.

Note that exact figures will depend significantly on the target library used, as well as the synthesis method and options, so these numbers should be treated as preliminary guidance only.

Helion Fast AES cores

The Helion Fast AES cores have been carefully designed for applications requiring high throughput coupled with minimum latency. This makes them ideal for data rates in the region 500Mbps to 5Gbps.

These cores use a 128-bit datapath to minimise the number of clock cycles required to implement the AES algorithm. By reducing the path delays to an absolute minimum with careful hand optimisation, these cores represent the fastest possible solution without resorting to pipelining. This internal datapath is matched to external 128-bit plaintext and ciphertext ports, which are ideal where high performance is required. Of course, if you do need to interface with narrower data widths in your system, then the additional glue logic needed is trivial.

Operation

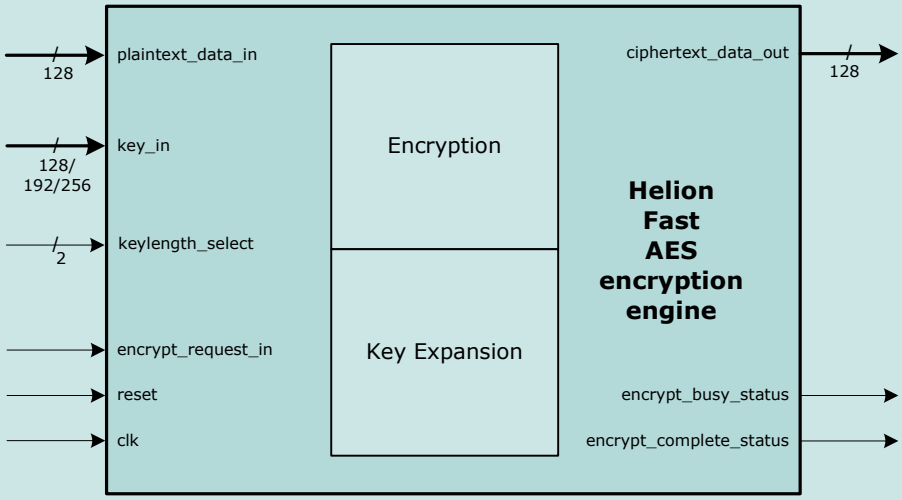
To use encryption as an example, you simply present the plaintext data and the AES key to the core in the same clock cycle, and assert the core encrypt *request*. The core will respond by asserting the *busy* status output, and will begin the encryption operation internally. When the process is complete, the *complete* status flag strobes for a clock cycle indicating the output data is valid, and the *busy* flag is deasserted indicating that the core is ready to start the next encryption process.

Interfacing is therefore easy, with the encrypt *request* and the *complete* status signals typically used to drive FIFO read and write enables, or to manage data pointers and provide write enables for other I/O storage methods.

Core Ports

The diagram alongside shows the I/O ports for a Fast AES engine set up for Encryption with hardware Key Expansion. A Decryption engine is correspondingly similar, but would have Ciphertext input and Plaintext output ports.

With the Helion Fast AES cores, the inputs need only be valid during the clock cycle when the *request* signal is asserted. The results is then valid once the processing has finished, as indicated by the *complete* flag.



Core Throughput

The Fast AES core is the perfect choice for high rate applications, though it will support any data rates up to ~5Gbps in ASIC silicon. It's throughput vs. clock speed is 11.6 Mbps/MHz for encryption or decryption with a 128-bit key – similarly 9.8 Mbps/MHz for 192-bit keys and 8.5 Mbps/MHz for 256-bit keys. If your target throughput is close to its limit then the required clock rate will be high, so unless absolute minimum logic area is a requirement, it may also be worth considering the faster Giga AES core family. Please contact Helion for more information if this is the case.

Core Options

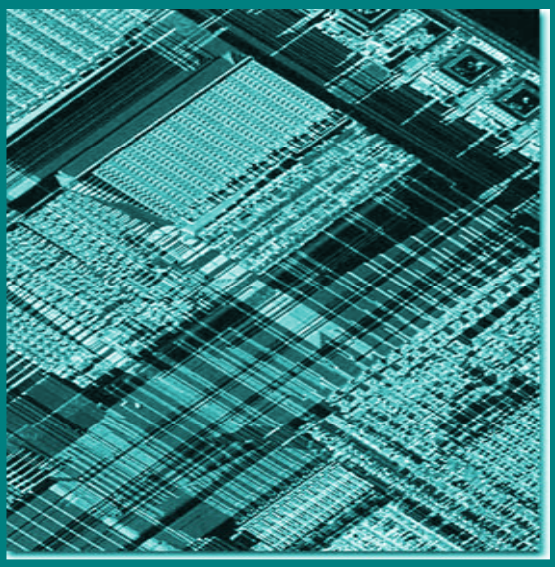
The Helion Fast AES core is fully modular, and therefore configurable to closely match the end application's requirements, minimising logic utilisation in the ASIC. All the options detailed on page 2 of this Product Brief are available, as are some special options which may be discussed if your requirements are complex.

Logic Utilisation and Performance

	Fast AES, enc-only		Fast AES, enc/dec	
key support	128-only	256-only	128-only	256-only
typical gatecount	<27k gates	<31k gates	<57k gates	<60k gates
typical max clock rate (65nm)	400MHz	400MHz	400MHz	400Mhz

The tables show typical gatecounts and maximum clock rates for popular configurations of the Helion Fast AES IP cores.

Note that exact figures will depend significantly on the target library used, as well as the synthesis method and options, so these numbers should be treated as preliminary guidance only.



**"Helion's products and services have consistently fit a variety of our needs.
They are superbly easy to work with, answering questions in clear straightforward terms.
The organization of their deliverables - particularly the concise and sensible documentation - provide for fast successful integration of their IP.
I deal with many vendors, Helion is currently my favorite by every conceivable metric."**

Jeff Harms
IP Procurement Lead
Microchip Technology

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