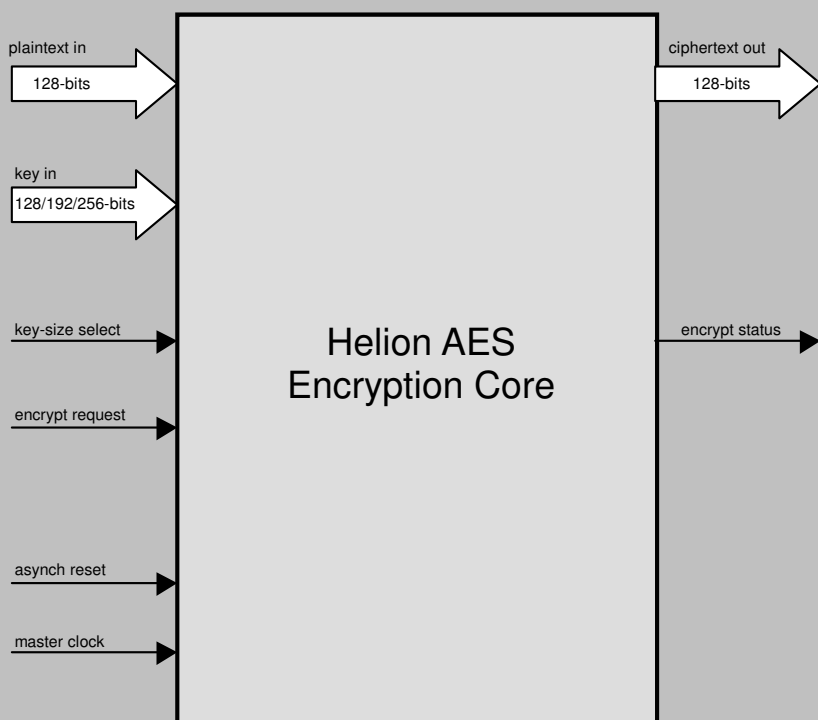


Helion Technology

OVERVIEW DATASHEET – High Performance AES (Rijndael) cores for Xilinx FPGA



Helion AES solution block diagram

Features

- Implements AES (Rijndael) to latest NIST FIPS PUB 197
- Full dynamic support for all AES key sizes (128, 192 and 256-bits)
- Four versions available; user can choose best balance of speed and size for application
- Fastest version supports data rates well in excess of 40Gbps
- Separate cores provided for encryption and decryption
- Roundkey generation can be split out for ultra low gatecount implementations
- All AES operating modes easily implemented (eg. ECB, CBC, OFB, CFB, CTR, CCM, GCM, XTS, OCB)
- Simple external interface
- Highly optimised for use in Xilinx FPGA technologies

Deliverables

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

Overview

These high performance cores from Helion are intended exclusively for use in Xilinx FPGA, and implement the AES (Rijndael) encryption standard, 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 support any or all of the available key-sizes (128/192/256-bit). Helion was the very first company in the world to offer commercial AES solutions in hardware back in 2001, and given this head start, our cores are by now extremely well proven in numerous real products. These cores are extremely simple to use, and highly versatile; they can be integrated into any AES design requirement with minimum effort.

Helion Technology Limited

Ash House, Breckenwood Rd, Fulbourn,
Cambridge CB21 5DQ, England.



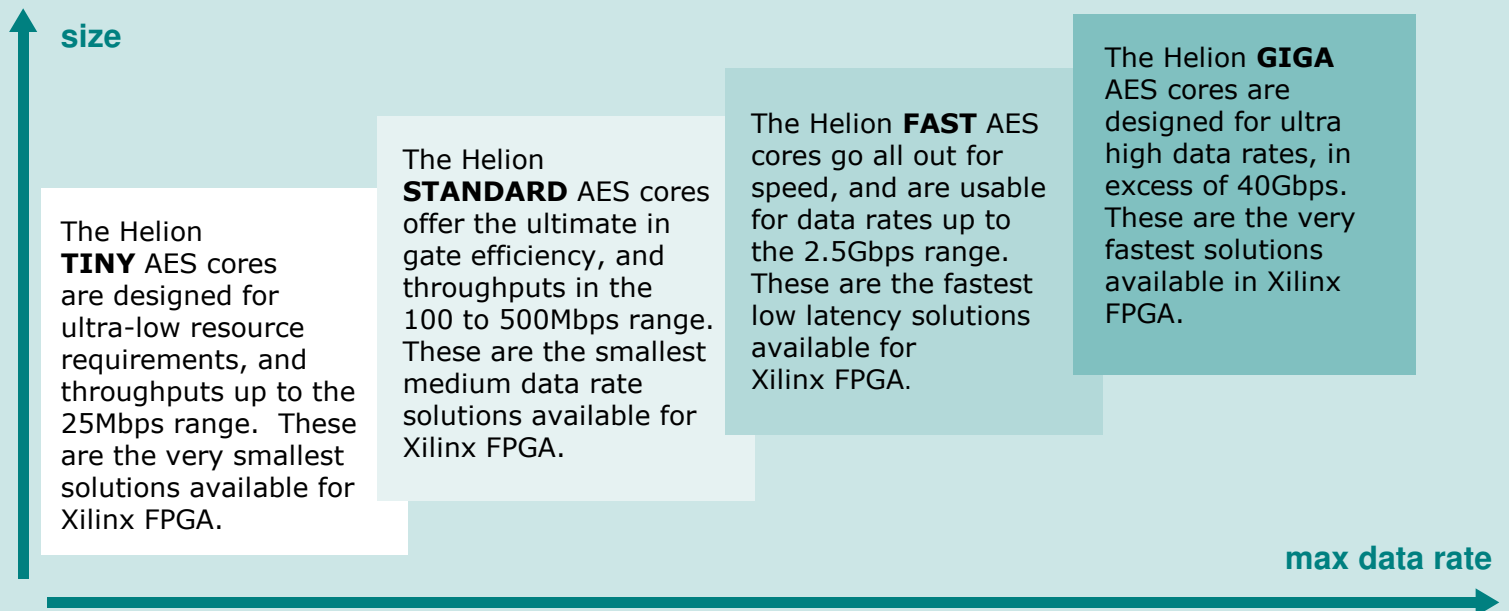
The Helion AES core range

Functional Description

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, generating plaintext from supplied ciphertext, using the same AES key as was used for encryption.

The encryption and decryption cores are supplied as standard with hardware roundkey expansion logic included, so that they form a complete stand-alone AES solution, as described above. However, Helion has designed the roundkey expansion logic as a discrete building block; and taking this approach opens up a number of interesting possibilities. For instance, the user can choose to dispense with the hardware roundkey expansion completely, in situations where it is preferable to generate the expanded roundkeys off-line in software, to save both logic resource and power. Or alternatively, roundkey expansion hardware can be shared between multiple encryption/decryption cores, again to lower the required logic real-estate requirements, where this approach is appropriate. These options are unique to Helion; if you would like to learn more about this, or need some background on the AES algorithm and roundkeys, please request our "Full" AES datasheet.

Since AES is being used in so many varied end products, we offer a range of four AES core families, each with different gatecount/speed 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.



Core Choice

The choice of core family is very application specific, driven mainly by the data throughput required, and also by the space available in the target FPGA.

The Helion **TINY** AES core is an ideal solution when your data throughput requirements fall below 25Mbps, and your application is highly sensitive to resource utilisation; perfect for high volume consumer applications.

For higher data rates, the Helion **STANDARD** AES core suits a large number of modern applications, where it offers higher throughput capabilities in the hundreds of Mbps region, coupled with the advantage of its incredibly small size.

However, if your application data rate is measured in low Gbps, the Helion **FAST** AES cores offer a combination of low latency and high throughput; ideal for situations which make use of feedback modes at higher data rates.

And if this still is not enough throughput for your application, the Helion **GIGA** AES cores should fit the bill, with encryption capabilities up to more than 40Gbps available.

The following pages cover our most popular solutions, the STANDARD and FAST cores, in some more detail. If you are more interested in the Helion TINY or GIGA AES cores, please contact Helion for specific literature.



The 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 100 to 500Mbps band.

The implementation approach taken was to split the 128-bit AES data block into four 32-bit words; each AES round then takes four master clock cycles to process, and all the interfaces (plaintext, ciphertext and key) are a manageable 32-bit width.

The interface provided is very straightforward, and will integrate into any existing system with ease. The core interface signal timing has been designed so that plaintext, ciphertext and AES key ports will talk seamlessly with registers, Xilinx CLB-based RAMS, Xilinx Blockrams, or FIFOs. Once started, the Helion core handles all of the data and key word access timing without any further user intervention.

Example performance and logic utilisation figures are shown below, targeting low cost Spartan-3E and Spartan-6 devices. Note that these cores are fully available in any current (plus most of the older) Xilinx device types, including all Spartan-3 types, plus the faster Virtex-4, Virtex-5 and Virtex-6; please feel free to contact us for full details.

If you would like additional information on the Helion STANDARD AES cores, we have a much more detailed datasheet available. This includes specific core interfacing information, additional performance and utilisation figures including decryption, plus some essential background information. If this sounds of interest, we are more than happy to email this out on request.

The Helion FAST AES cores

The Helion FAST AES cores have been carefully designed to achieve the ultimate in data throughput, along with minimum latency. This makes them ideal for applications requiring data rates in the region 500Mbps to 3Gbps, and where feedback is necessary, for example in many of the common Block Cipher modes.

The implementation approach taken was to handle the 128-bit AES data block in one go; each AES round then takes just one master clock cycle to process, and all the interfaces (plaintext, ciphertext and key) are 128-bits wide, which is ideal where high performance is required. Of course, if you do need to interface with narrower data widths in your system, then the additional logic required is trivial.

The interface to the core has been designed to be extremely simple to use, and will integrate seamlessly into any kind of system. The plaintext, ciphertext, and AES keys may be stored in registers, Xilinx CLB or Blockram, or FIFOs, and the core can be used with the absolute minimum of effort and additional logic.

Example performance and logic utilisation figures are shown below, targeting a low cost Spartan-6 device, and higher performance Virtex-5 and Virtex-6 parts. Note that these cores are fully available in any current (plus most of the older) Xilinx device types, including Spartan-3, -3E, -3A and Virtex-4; please feel free to contact us for full details.

If you would like additional details on the Helion FAST AES cores, we have a much more detailed datasheet available. This includes specific core interfacing information, additional performance and utilisation figures including those for the option to expand roundkeys off-line, plus some essential background information. If this sounds of interest, we are more than happy to email this out on request.

Standard and Fast AES core performance and resource requirements

options	Standard encryptor			Fast encryptor		
	off-line roundkey expansion (128-bit key)	hardware roundkey expansion (128-bit key)	hardware roundkey expansion (128-bit key)	hardware roundkey expansion (128-bit key)	hardware roundkey expansion (128-bit key)	hardware roundkey expansion (128-bit key)
technology	Xilinx Spartan 3E -5	Xilinx Spartan 3E -5	Xilinx Spartan 6 -2	Xilinx Spartan 6 -2	Xilinx Virtex 5 -3	Xilinx Virtex 6 -3
typical core logic resource	103 slices 3 blockrams	234 slices 3 blockrams	133 slices 0 blockram	332 slices 0 blockrams	342 slices 0 blockrams	331 slices 0 blockrams
max master clock	161MHz	161MHz	154MHz	162MHz	363MHz	450MHz
max data rate 128-bit key-size, ECB mode	429Mbps	429Mbps	410Mbps	1885Mbps	4224Mbps	5236Mbps

For our figures above, we have targeted our most popular core combinations at the most popular target devices. Note that we fully support all current (and most older) Xilinx FPGA types. Please feel free to contact us for figures specific to your target application.



Ordering Information

Before ordering it is necessary to decide which of our range of AES cores will best fit your application. Decide between the TINY, STANDARD, FAST and GIGA families, according to data throughput required and logic resource available. Then, determine whether you require encryption cores, decryption cores, or both; this will be determined by your application, as well as the block cipher mode you are planning to use. And finally, decide if you require the Roundkey expansion to be handled by the hardware, and if so, which AES key sizes you would like to use.

If some of these choices are unclear, or you would just like to go over the options, we are always happy to discuss the alternatives and suggest the most viable solutions. More information is also available in our family specific AES datasheets, which are available on request.

Base core family	encrypt only	decrypt only	encrypt & decrypt	hardware roundkey expansion	offline roundkey expansion	128-bit keys	192-bit keys	256-bit keys
TINY	✓	✓	✓	✓	✓	✓	✓	✓
STANDARD	✓	✓	✓	✓	✓	✓	✓	✓
FAST	✓	✓	✓	✓	✓	✓	✓	✓
GIGA	✓	✓	✓	✓	✓	✓	✓	✓

About Helion

Helion is a small well established British company based in Cambridge, England, offering a range of product-proven Data Security silicon IP cores backed up by our 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 is also a member of the Xilinx AllianceCORE IP program, and a certified Xilinx Xpert consultancy. We therefore take our Xilinx implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Xilinx FPGA designs; they are not simply based on a generic ASIC design like much of the competition.

The Helion AES cores make use of Xilinx-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 AES 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 Rd, 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