



Tiny AES Encryption and Decryption Cores

May 29, 2008

Product Specification



Helion Technology Limited

Ash House, Breckenwood Road, Fulbourn, Cambridge CB21 5DQ, England

Phone: +44 1223 500 924

Fax: +44 1223 500 923

E-mail: helioncores@heliontech.com

URL: www.heliontech.com

Features

- Implements AES (Advanced Encryption Standard) to latest NIST FIPS PUB 197
- Optimised for use with all Xilinx FPGA families
- Full dynamic support for all AES key sizes (128, 192 and 256-bits)
- Low speed/ultra-low area solution
 - the smallest full hardware AES solution available anywhere
 - other core families available from Helion so that user can choose the best balance between speed and size for any application
- Fully integrated encryptor and decryptor
 - high degree of resource sharing between functions results in super-efficient implementation
- All AES operating modes fully supported; eg. ECB, CBC, OFB, CFB, CTR
- Available under terms of the SignOnce IP License

AllianceCORE™ Facts	
Provided with Core	
Documentation	User Guide
Design File Formats	NGC netlist; VHDL or Verilog source code also available
Constraints Files	.ucf
Verification	VHDL or Verilog test bench with NIST FIPS test vectors (including full Monte Carlo tests); VHDL or Verilog Simulation models
Instantiation templates	VHDL, Verilog
Reference designs & application notes	Reference designs for all the common Block Cipher Modes (including CBC, OFB, CFB, CTR)
Additional Items	Example ModelSim scripts
Simulation Tool Used	
ModelSim PE 6.1e	
Support	
Support provided by Helion Technology Limited	

Table 1: Example Implementation Statistics for Xilinx® FPGAs – Encryptor/Decryptor with all keysize support (full support for 128-bit, 192-bit and 256-bit keys)

Family	Example Device	Fmax (MHz) ²	Slices	IOB ¹	GCLK	BRAM	MULT	DCM/DLL	MGT	Design Tools
Spartan®-3E	XC3S250E-5	146	175	49	1	1	0	0	N/A	ISE® 10.1.01i
Spartan®-3	XC3S200-5	159	175	49	1	1	0	0	N/A	ISE® 10.1.01i
Virtex®-4	XC4VLX25-11	226	175	49	1	1	0	0	0	ISE® 10.1.01i
Virtex®-5	XC5VLX30-3	376	97	49	1	0	0	0	0	ISE® 10.1.01i

Notes:

- 1) Assuming all core I/Os and clocks are routed off-chip
- 2) Fmax is quoted assuming all core inputs are sourced from flip-flops, and all core outputs drive flip-flops; this has been done to best represent real applications, where data and key interfaces would usually utilise Xilinx SelectRAM for buffering purposes, in which case these flip-flops are already effectively included. All signal timing and functionality has been designed to accommodate this kind of interface seamlessly.

5.0

May 29, 2008

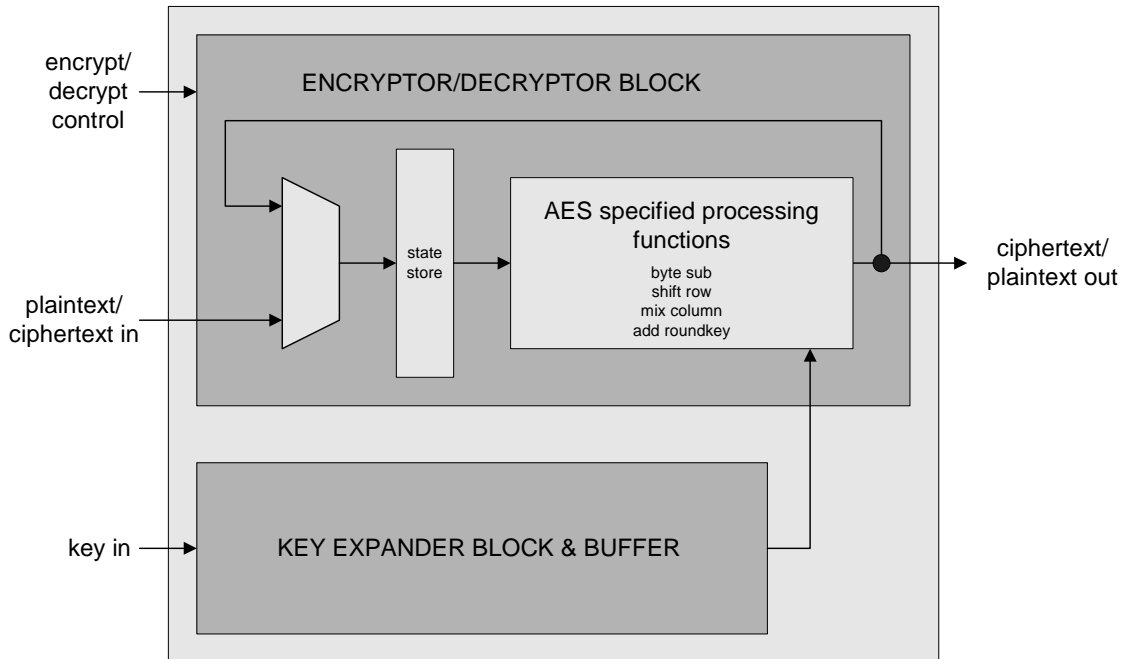


Figure 1: Tiny AES Encryptor/Decryptor Block Diagram

Features (continued)

- Internal support for separate encryption and decryption keys
- Simple external interface
- Mature and product proven IP

Applications

Security in wireless applications

- 802.11 WLAN
- 802.15 PAN
- 802.16 MAN
- Satellite communications

Security in networked environments

- IPsec and Virtual Private Networks (VPN)
- Storage Area Networks (SAN)
- Voice over IP (VoIP)

Securing program content

Securing financial transactions

Secure telemetry and remote monitoring

General Description

The Helion AES cores implement the 128-bit block-size NIST Federal Information Processing Standard AES algorithm. The Tiny AES cores offer support for both encryption and decryption; in encrypt mode the cores accept a 128-bit plaintext input block, and generate a corresponding 128-bit ciphertext output block using a supplied 128, 192, or 256-bit AES key. In decrypt mode, the cores provide the reverse function, generating plaintext from supplied ciphertext, using a similar AES key as was used for encryption.

The Helion Tiny family of AES cores have been specifically designed to target low speed applications up to a few tens of Mbps, whilst at the same time being ultra resource and power efficient. Other families of AES cores are available from Helion if this ultra small solution is not appropriate; for example where the requirement is for a much higher throughput, the Helion “Fast” AES cores might be more appropriate, or for medium-rate/low-resource applications, the Helion “Standard” cores might be a better fit.

All Helion cores are designed for maximum flexibility and efficiency in Xilinx FPGA. They have been carefully crafted at the Xilinx primitive level in critical areas so that performance is maximised, and logic area minimised; these product-proven cores are not re-targeted ASIC cores, but designed from the ground up to achieve class-leading results in Xilinx technology.

Functional Description

Figure 1. shows the internal structure of the Helion Tiny Encryptor/Decryptor. The AES algorithm consists of a complex non-linear core function; a sequence of permutations, nonlinear substitutions and Galois field additions and multiplications; which is iterated multiple times on the incoming plaintext data block. The number of times this iteration is needed, or more correctly, the number of “rounds” required, depends on the selected key size. For 128-bit key AES, there are 10 rounds, for 192-bit key AES there are 12 rounds, and for 256-bit key AES there are 14 rounds. Note that the round function is slightly different for the final round, and that an initial pre-processing function is also required at the start.

To handle the required processing, the Helion Tiny AES cores split the 128-bit AES data block into a sequence of sixteen 8-bit values; each AES round then takes multiple master clock cycles to process, and all the interfaces (plaintext, ciphertext and key) are 8-bits wide. The result is the smallest full hardware implementation of AES available anywhere, covering typical applications up to a few tens of Mbps, and using the absolute minimum of logic resource.

Each round of AES also requires a unique 128-bit Roundkey to be fed in to the complex round function mentioned above. This series of 128-bit Roundkeys is generated from the supplied 128-bit, 192-bit or 256-bit AES key using a specified AES key expansion algorithm. This expansion process yields exactly the right number of Roundkeys to feed the single initialisation step and the multiple rounds. So for 128-bit keysize AES there are 11 Roundkeys, for 192-bit there are 13 Roundkeys, and for 256-bit there are 15 Roundkeys.

Generating these expanded Roundkeys is really easy using the Helion Key Expander block as shown in Figure 1., this being an integral part of the Helion Tiny AES core. This takes in the AES key, and generates the sequence of Roundkeys for use in the Encryptor/Decryptor, storing them for subsequent use. Since this key expansion and subsequent storage is internal to the core, its operation becomes transparent to the user. It should be viewed as a simple one-time process, required only when the keys are changed. To further simplify operation, internal support is provided as standard for separate encryption and decryption keys, permitting rapid mode switching when the core is used to process bi-directional flows.

Core Data Throughput Capability

The maximum data throughput capability of the cores is directly proportional to the master clock frequency used in the implementation. For 128-bit keys, the maximum data throughput is as follows;

$$\text{Max Throughput (Mbps)} = (128 / 615) \times \text{Master Clock Frequency (MHz)}$$

The highest Master Clock Frequency which may be used is technology dependent; typical maximum frequencies for some of the Xilinx families are shown in Table 1 the Tiny Encryptor/Decryptor. Figures for other key sizes, core versions and device families and speed grades can be supplied on request; please feel free to contact Helion for this additional information.

Core Modifications

The Helion Tiny core is supplied as standard as a combined Encryptor/Decryptor supporting all the AES key sizes (128-, 192- and 256-bits). This can be viewed as a “super-set” of features, and versions of the core can be supplied which implement encryption-only or decryption-only, or maybe supporting a subset of the key sizes (for example 128-bit only is a common requirement). Versions can also be supplied which do not handle the key expansion in hardware, and rely on external generation of the roundkeys. These are all ways in which the already minimal resource requirements may be reduced even further for specific applications. Please contact Helion directly to discuss these options in more detail.

In addition, a suite of Block Cipher Mode wrapper designs is available for the user to implement all the common modes of operation (eg. CBC, CFB, OFB, CTR), plus a number of the more recent complex ones (eg. CCM, GCM); please request the appropriate mode wrappers required at time of ordering.

Core I/O Signals

The core signal I/O have not been fixed to specific device pins to provide flexibility for interfacing with user logic. Descriptions of all signal I/O are provided in Table 2.

Please note that signal naming was derived in encrypt mode, and so in decrypt mode, incoming ciphertext should still be put into the “plaintext” input; similarly, the resulting plaintext will still be output from the “ciphertext” port. Please also note that in the Helion Tiny AES cores, all data and key interfaces are based on multiple 8-bit values, and select lines are provided to indicate which byte from the 128-bit block, or 128-, 192-, or 256-bit key is being addressed; the timing of these select lines is fully Xilinx Blockram compatible.

Table 2: Core I/O Signals.

Signal	Width	Signal Direction	Description
clk	1	Input	Master Clock Input
reset	1	Input	Master asynchronous reset; 1 = reset
key_byte_in	8	Input	Incoming AES key byte
key_byte_required	1	Output	Control to indicate that key is being read
key_byte_select	5	Output	Control to select next key byte (1 of 16, 24 or 32)
plaintext_byte_in	8	Input	Plaintext data byte input
plaintext_byte_required	1	Output	Control to indicate that Plaintext is being read
plaintext_byte_select	4	Output	Control to select next Plaintext byte (1 of 16)
ciphertext_byte_out	8	Output	Resulting ciphertext byte
ciphertext_byte_select	4	Output	Control to indicate which ciphertext byte is being output (1 of 16)
ciphertext_byte_valid	1	Output	Indication that the current ciphertext byte is valid
keylength_select	2	Input	Select key size to use '00' = 128 bits '01' = 192 bits '1X' = 256 bits
enc_decn	1	Input	Mode select input; Encrypt = '1', Decrypt = '0'
encrypt_request_in	1	Input	Encrypt request input; '1' = start encryption
key_schedule_request_in	1	Input	Key schedule request input; '1' = start key schedule
engine_busy_status	1	Output	Engine busy status flag output; '1' = busy
engine_complete_status	1	Output	Engine completed status flag output; '1' = completed

Verification Methods

The Helion Tiny AES cores have been thoroughly verified under simulation using the NIST FIPS submission test vectors, including the full Monte Carlo tests; these tests are also supplied as part of the core deliverables to demonstrate operation. In addition, the cores have been carefully tested in real Xilinx devices, and have all been successfully used many times over in real products shipping in volume.

Recommended Design Experience

Users should be familiar with HDL methodology and Xilinx design flows including VHDL/Verilog component instantiation, synthesis, implementation and simulation.

Ordering Information

This product is available directly from Xilinx AllianceCORE member Helion Technology Limited under the terms of the SignOnce IP License. Please contact Helion Technology for pricing and additional information about this product. Contact information for them is on the front page of this datasheet. To learn more about the SignOnce IP License program, contact Helion Technology or visit the web:

Email: commonlicense@xilinx.com
 URL: www.xilinx.com/ipcenter/signonce

Export

Strong encryption technology such as AES is governed internationally by export regulations. Immediate export is permitted to the following countries;

Austria	Australia	Belgium
Bulgaria	Canada	Cyprus
Czech Republic	Denmark	Estonia
Finland	France	Germany
Greece	Hungary	Ireland
Italy	Japan	Latvia
Lithuania	Luxembourg	Malta
New Zealand	The Netherlands	Norway
Poland	Portugal	Romania
Slovakia	Slovenia	Spain
Sweden	Switzerland	United Kingdom
United States		

Please contact Helion to discuss delivery to other destinations; approval is subject to the applicable export licenses being granted. Please note that licensees are responsible for complying with the applicable requirements for re-export of electronics containing AES technology.

Related Information

Advanced Encryption Standard specification

For more detailed information on the Advanced Encryption Standard algorithm, the original specification for AES (NIST FIPS Publication 197) may be downloaded from the NIST website at;

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Xilinx Programmable Logic

For information on Xilinx programmable logic or development system software, contact your local Xilinx sales office, or:

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
Phone: +1 408-559-7778
Fax: +1 408-559-7114
URL: www.xilinx.com