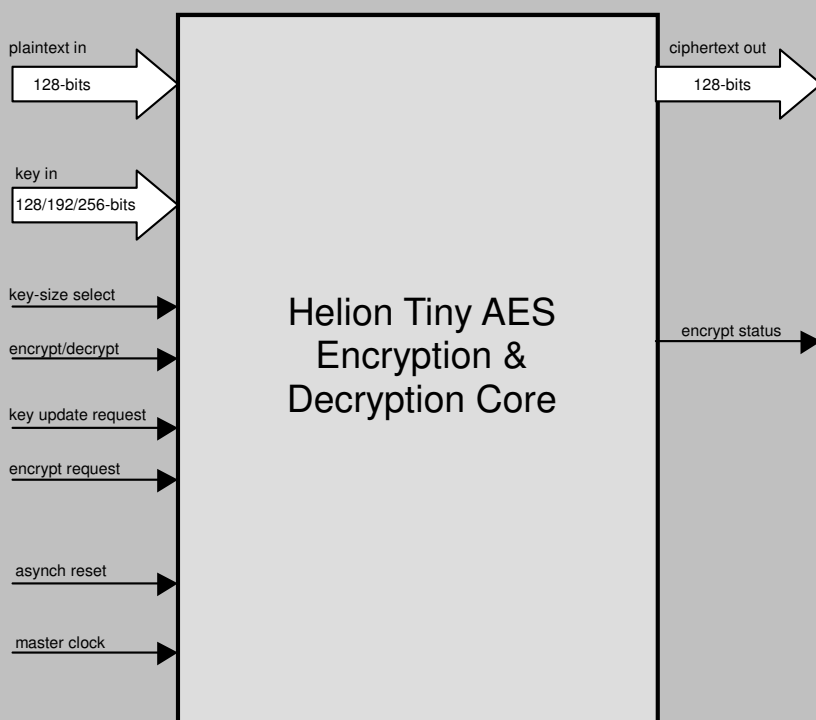


Helion Technology

OVERVIEW DATASHEET – Ultra-Low Resource AES (Rijndael) cores for Altera FPGA



Helion Tiny AES solution block diagram

Features

- Implements AES (Rijndael) to latest NIST FIPS PUB 197
- Designed specifically for ultra low resource applications – this is the very smallest hardware AES solution available
- Data throughput up to 25Mbps
- Full dynamic support for all AES key sizes (128, 192 and 256-bits)
- Single core handles encryption, decryption, and hardware roundkey expansion
- All AES operating modes easily implemented (eg. ECB, CBC, OFB, CFB, CTR)
- Simple 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 FIPS test vectors
- User documentation

Overview

This high performance core from Helion is intended exclusively for use in Altera FPGA, and implements the AES (Rijndael) encryption standard, as described in the NIST Federal Information Processing Standard (FIPS) Publication 197 document. Specific versions of this AES core are available for use in all current Altera technologies including Stratix II, Stratix III, Cyclone II and Cyclone III.

Designed to require the absolute minimum in logic resource, the Tiny AES core from Helion is ideal when silicon area is at a premium, for example in high volume consumer applications. The Tiny AES core comes as part of a long line of AES cores from Helion; being the very first company in the world to offer AES solutions in hardware back in 2001, our cores are now well proven in numerous real products. All our 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 Tiny AES core

Functional Description

The Helion Tiny AES core implements the 128-bit block-size NIST FIPS AES algorithm. It was designed to require the absolute minimum of logic resource, whilst still providing full support for both encryption and decryption, plus roundkey expansion for all the AES specified key sizes (128, 192 and 256-bit keys), at data rates up to 65Mbps. In encryption mode, the 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. In decryption mode, the core provides the reverse function, generating plaintext from supplied ciphertext, using the same AES key as was used for encryption.

The implementation approach taken was to split the 128-bit AES data block into sixteen 8-bit wide elements, and to process each in turn; each AES round then takes multiple master clock cycles to process, and the datapath logic is highly optimal for the algorithm; all the interfaces (plaintext, ciphertext and key) are also a simple 8-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 the plaintext, ciphertext and AES key ports will talk seamlessly with registers, Altera embedded RAMs or FIFOs. Once started, the Helion core handles all of the data and key word access timing without any further user intervention.

Tiny AES core performance and resource requirements

options	Tiny encryptor/decryptor		Tiny encryptor/decryptor	
	128-bit AES key encrypt/decrypt version	128-bit AES key encrypt/decrypt version	All key sizes AES encrypt/decrypt version	All key sizes AES encrypt/decrypt version
technology	Altera Cyclone II	Altera Cyclone III	Altera Stratix II	Altera Stratix III
test device	EP2C5T144C6	EP3C5M164C6	EP2S15F672C3	EP3SL50F484C2
typical core logic resource	404 LEs 3 M4K RAMs	397 LEs 3 M9K RAMs	509 ALUTs 1 M512 RAM 2 M4K RAMs	526 ALUTs 2 M9K RAMs
max master clock	>165MHz	>160MHz	>228MHz	>319MHz
max data rate 128-bit key-size, ECB mode	> 34 Mbps	> 33 Mbps	> 47 Mbps	> 66 Mbps

Example performance and logic utilisation figures are shown above, targeting our popular 128-bit only and our "all-sizes" encrypt/decrypt versions (the "all-sizes" version supports 128, 192 and 256-bit keys with dynamic selection), at some current Altera Stratix and Cyclone families. Please contact us for figures specific to your target application.

About Helion

Helion is a 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. As veteran programmable logic designers, we take our FPGA solutions extremely seriously; they are not merely retargeted ASIC cores, but handcrafted designs aimed specifically at the technology; the value of this approach can be clearly appreciated by direct comparison with solutions offered by the more broadline IP 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.

