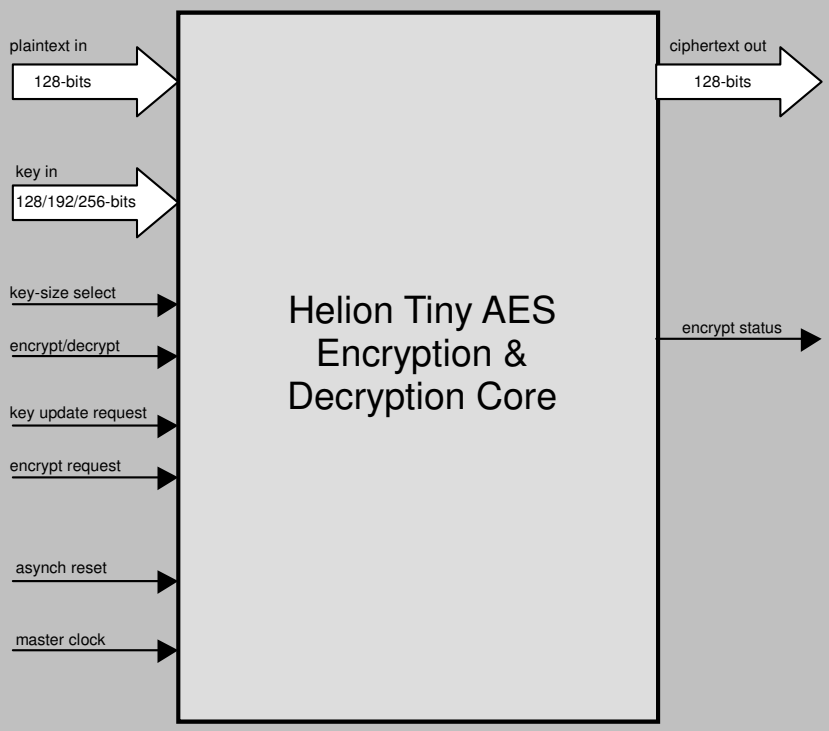
Helion Technology

OVERVIEW DATASHEET – Ultra-Low Resource AES (Rijndael) cores for Actel 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 Actel 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 Actel 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 Actel devices featuring embedded RAM; ProASICPlus, Axcelerator, ProASIC3 and the latest Fusion and Igloo technologies.

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.

 Rev 1.2.1

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 keysizes (128, 192 and 256-bit keys), at data rates up to 25Mbps. 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 a similar AES key as was used for encryption.

The Helion Tiny AES core is available in several versions depending on the exact requirements; the full version handles both encryption and decryption using any keysize, but area-reduced versions are also available for encryption-only, decryption-only, plus single keysize support. Full details of these options are available on request.

The interface provided is very straightforward, and will integrate into any existing system with ease. All the interfaces (plaintext, ciphertext and key) are 8-bits wide, and the interface signal timing has been designed so that the plaintext, ciphertext and AES key ports will talk seamlessly with registers, Actel 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

	Tiny encryptor		Tiny encryptor/decryptor	
options	128-bit AES key encrypt-only version	128-bit AES key encrypt-only version	128-bit AES key encrypt/decrypt version	128-bit AES key encrypt/decrypt version
technology	Actel ProASIC3	Actel Axcelerator	Actel ProASIC3	Actel Axcelerator
typical % utilisation	test device = A3P250-2 12.0% utilised	test device = AX250-2 16.2% utilised	test device = A3P250-2 13.5% utilised	test device = AX250-2 18.3% utilised
typical core logic resource	734 tiles 2 RAMs	306 C-cells 378 R-cells 3 RAMs	829 tiles 3 RAMs	390 C-cells 383 R-cells 3 RAMs
max master clock	>126MHz	>156MHz	>104MHz	>111MHz
max data rate 128-bit key-size, ECB mode	**>26 Mbps**	**>32 Mbps**	**>21 Mbps**	**>23 Mbps**

Example performance and logic utilisation figures are shown above, targeting our popular 128-bit key size encrypt-only and encrypt/decrypt versions, at Actel ProASIC3 and Axcelerator families. If you need support for longer keys or for different Actel technologies, please feel free to 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.

Actel CompanionCore

Helion is very proud to be a founder member of Actel's CompanionCore IP providers program, and aim to ensure that users of Actel technology have easy access to the very highest quality security solutions

HELION

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

tel +44 (0)1223 500 924 fax +44 (0)1223 500 923
email info@heliontech.com web www.heliontech.com