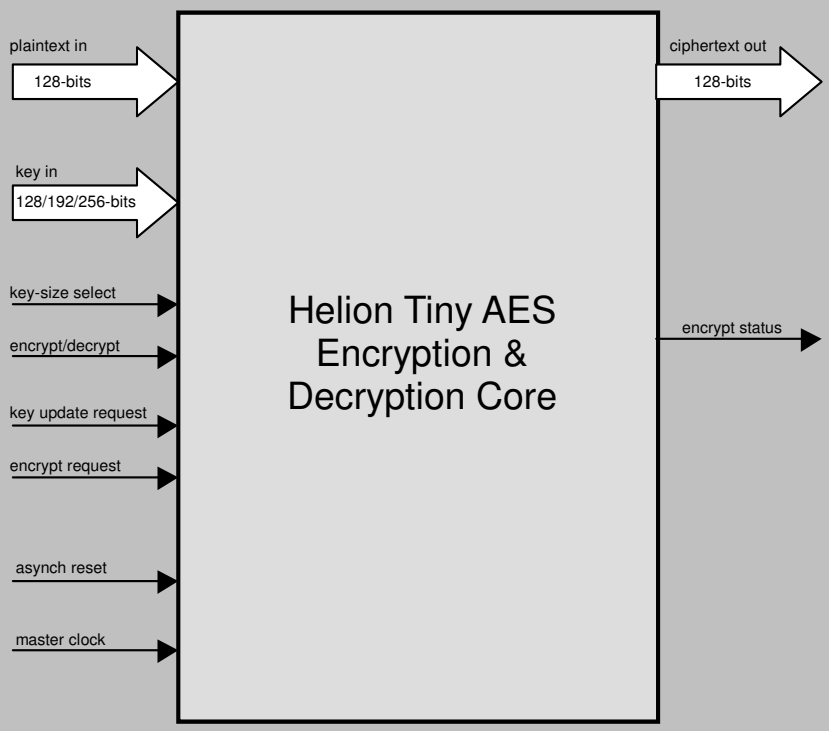
Helion Technology

OVERVIEW DATASHEET – Ultra-Low Resource AES (Rijndael) cores for 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 75Mbps
- 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 each individual FPGA technology

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 highly optimised for use in FPGA, and implements the AES (Rijndael) encryption standard, as described in the NIST Federal Information Processing Standard (FIPS) Publication 197 document.

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 1.0.0

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 in the tens of Mbps. 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, and popular FPGA style RAMs or FIFOs. Once started, the Helion core handles all of the data and key word access timing without any further user intervention.

Logic Utilisation and Performance

Helion has a long history in high-end FPGA design, and we therefore take great care when implementing our IP cores. As a result they have been designed from the ground up to be highly optimal for each individual FPGA technology - they are not simply based on a synthesised generic RTL ASIC design. The Helion Tiny AES cores make use of the architectural features available in each FPGA technology to achieve the highest performance combined with the most efficient logic resource utilisation.

The latest logic area, performance figures, and datasheets for the Helion Tiny AES cores in a range of different technologies are available at http://www.heliontech.com/aes_tiny.htm. Please feel free to contact us for further details.

About Helion

Helion is a long 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 itself.

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.

The quality of our IP is however the main reason our customers keep coming back for more. We passionately believe that if you are buying IP, it should have been designed with the ultimate in care, crafted to achieve the ultimate performance in each target technology, and thoroughly tested to ensure compliance with any associated standards. All this comes as standard with IP from Helion.

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