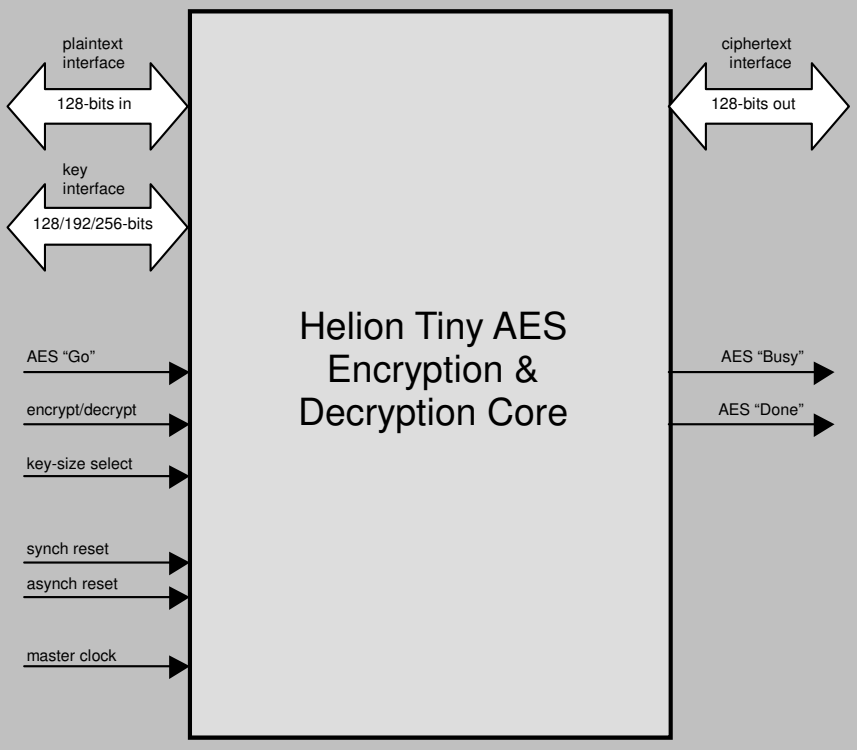
Helion Technology

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



Helion Tiny AES solution block diagram

Features

- Implements AES (Rijndael) to latest NIST FIPS PUB 197
- Designed specifically for ultra low resource low-power applications – this is the very smallest hardware AES solution available
- Data throughput up to >100Mbps
- Full dynamic support for 128-bit 192-bit and 256-bit AES key sizes
- Single core handles encryption, decryption, and hardware key expansion
- All AES operating modes easily implemented (eg. ECB, CBC, OFB, CFB, CTR, CCM, GCM)
- Simple byte-wide external interface
- Suitable for use in ASIC or fine-grain FPGA technologies

Deliverables

- Fully synthesisable RTL VHDL or Verilog source code
- VHDL or Verilog testbench with FIPS test vectors
- Example synthesis scripts
- User documentation

Overview

This high performance core from Helion is intended for use in ASIC and fine-grain FPGA technologies, 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 2.1.0

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 hardware key expansion for 128-bit, 192-bit and 256-bit key sizes, at data rates up to >100Mbps. 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 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 Helion Tiny AES core is available in several versions depending on the exact requirements; the full version handles both encryption and decryption with 128-, 192- and 256-bit keys, but area-reduced versions are also available for encryption-only, decryption-only, plus reduced 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, 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 & decryptor	
options	encrypt-only 128-bit key (HW key expansion)	encrypt & decrypt 128/192/256-bit keys (HW key expansion)
technology	0.13um CMOS	0.13um CMOS
typical core logic resource	<4k gates (No RAM required)	<6k gates (No RAM required)
max master clock	>300MHz	>300MHz
max data rate 128-bit key-size, ECB mode	**>100Mbps**	**>100Mbps**

For our figures here, we have targeted two popular core configurations at a generic 0.13um CMOS library; namely encryption-only with a fixed 128-bit AES key, and then selectable encryption and decryption with dynamic support for 128-bit, 192-bit and 256-bit AES keys. If your requirements are not covered by these examples, then please feel free to contact us for figures specific to your target application.

Note that this core requires **no RAM**, even when supporting decryption, making it especially efficient in ASIC targets.

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.

Unlike many IP core vendors, Helion also spends a great deal of effort designing its cores at the very lowest level. We strongly believe that if you are buying IP, it should have been designed with the ultimate in care, and crafted to achieve the desired performance; not just put together at a high level to get the job done quickly. We find that this approach pushes the results much closer to the intended performance envelope. 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.

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