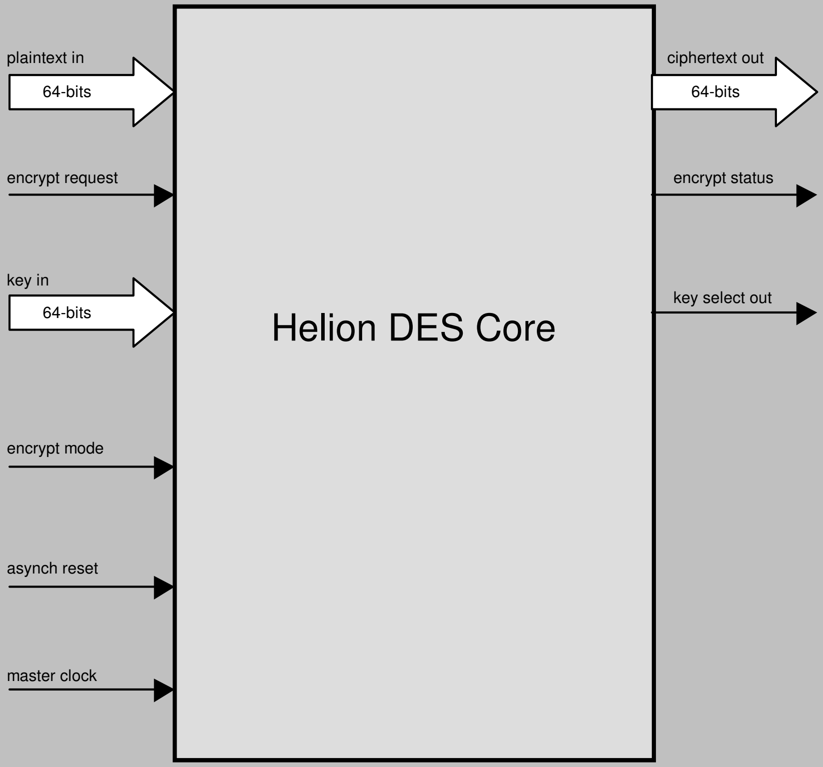
Helion Technology

DATASHEET – High Performance DES and Triple-DES cores for FPGA



Features

- Implements DES and Triple-DES to NIST FIPS publication 46-3
- Two versions available; user can choose best balance of speed and size for application
- Very fast operation – Single DES Encryption/Decryption takes only 9-clock cycles in fastest version
- Same core offers dynamically selectable single DES/triple DES and encrypt/decrypt modes
- All DES operating modes easily implemented (eg. ECB, CBC, OFB, CFB, CTR, CBC-MAC)
- 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

These high performance cores from Helion have been highly optimised for use in FPGA, and implement the DES and triple-DES encryption standards, as described in NIST Federal Information Processing Standard (FIPS) publication 46-3.

Two versions are available, each offering different trade-offs between area and speed. The smallest solution is a one-round-per-clock solution, which has been very carefully designed for minimum area in FPGA. The faster variant is somewhat different to most others commercially available in that it operates at a rate of two-rounds-per-clock. This results in a core which will run significantly faster for a given gate-count, so for high performance designs, where either speed is essential or space is limited, these cores may be the perfect solution.

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

Rev 1.0.0

Functional Description

The Helion DES cores implement the NIST FIPS 46-3 DES and triple-DES algorithms. They accept a 64-bit plaintext input word, and generate a corresponding 64-bit ciphertext output word using a supplied 64- or 192-bit key. The cores offer dynamically selectable DES and triple-DES operation, both in encrypt and decrypt modes. When triple-DES is selected, both two and three key variants are supported. Keys are stored externally to the cores for maximum system flexibility, and a key-select control from the core tells external logic which of these keys is required at any time.

The DES algorithm as described requires 16 rounds for a complete encryption, and triple-DES requires 48 rounds. The Standard Helion DES core executes one round for every master clock cycle, so a DES encryption is completed in 16 master clock cycles (and triple-DES in 48 cycles). The Fast Helion DES core executes two rounds for every master clock cycle, so for this core a DES encryption is completed in 8 master clock cycles (and triple-DES in 24 cycles). For the Standard and Fast cores, one additional cycle is required to unload the resulting ciphertext, and simultaneously load in the next plaintext.

The Helion cores implement DES in basic Electronic Code Book (ECB) mode. This is an ideal building block on which to base any of the more commonly used operational modes, and 'wrapper' logic is available which offers users several alternative modes (CBC, OFB ,CFB, CTR); other modes are very easy to add.

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 DES 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 DES cores in a range of different technologies are available at http://www.heliontech.com/des.htm. Please feel free to contact us should you require 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

Helion Technology Limited
Ash House, Breckenwood Road, 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