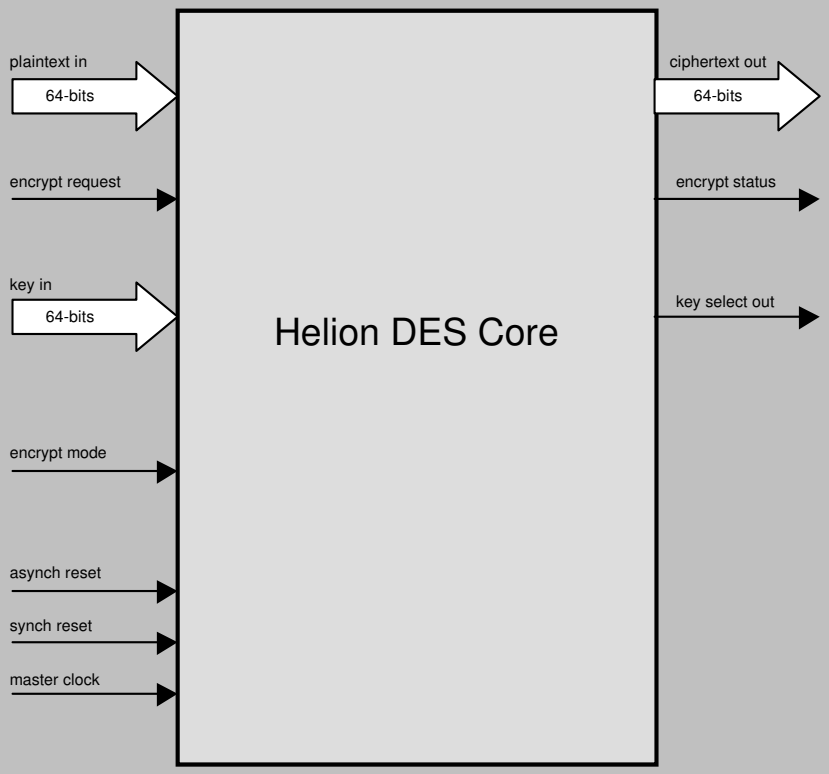
Helion Technology

DATASHEET – High Performance DES and Triple-DES core for ASIC



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, MAC)
- Simple 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

Overview

These high performance cores from Helion are intended for use in ASIC and fine-grain FPGA technologies, 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 ASIC. 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 1.1.1

Functional Description

The Helion DES cores consist of synthesisable VHDL or Verilog which implement the NIST FIPS 46-3 DES algorithm. They accept a 64-bit plaintext input word, and generate a corresponding 64-bit ciphertext output word using a supplied 64-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 core 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 core actually implements 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, MAC); other modes are very easy to add.

Core Performance

These cores have been designed to be used efficiently in both ASIC and fine-grain FPGA designs.

For ASIC applications, example gate count and speed figures for the two cores have been generated in synthesis with Synopsys Design Compiler, and are based on a generic 0.18um CMOS technology. Different end technology may obviously have a large impact on these figures.

For fine-grain FPGA applications, performance and gate count will be very much dependant on the specific technology targeted; hence figures are not quoted here, but we would be more than happy to supply specific details on request.

	Standard DES	Fast DES
technology	0.18um CMOS	0.18um CMOS
typical core gate count	<4k gates	<6k gates
max master clock	>280MHz	>180MHz
max data rate - single-DES	>1.05Gbps	>1.25Gbps
max data rate - triple-DES	>365Mbps	>460Mbps

Other variants

This datasheet covers our Standard and Fast DES cores, as these are good solutions for the majority of applications. However, we also have other variants available for very high throughput applications. We can offer a **non-pipelined 1Gbps triple-DES** solution, suitable for use in all block cipher modes (including CBC). Please contact Helion if this sounds appropriate for your requirements.

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 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