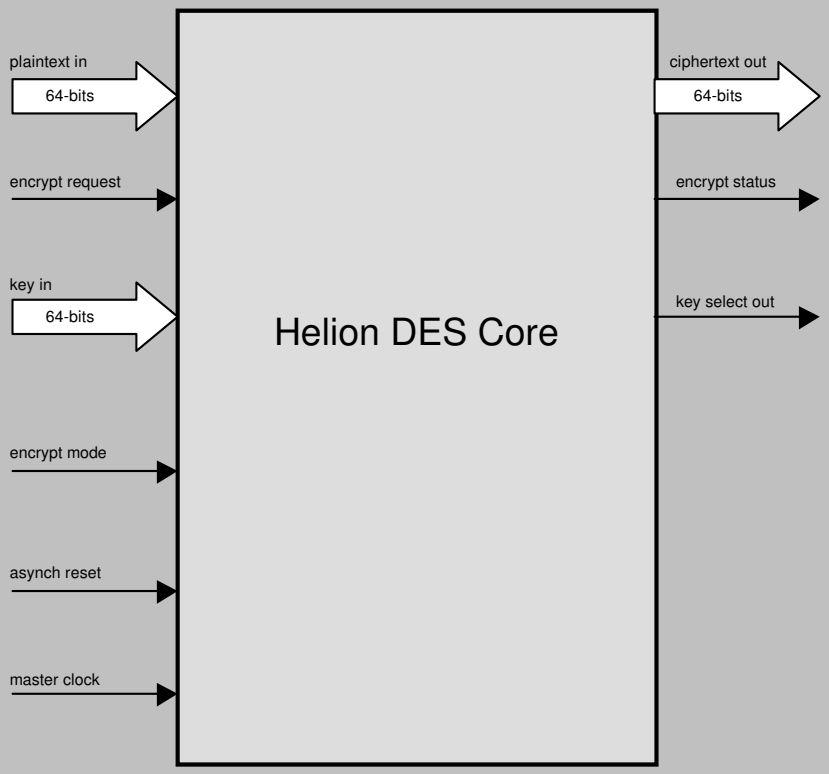
Helion Technology

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

These high performance cores from Helion are intended exclusively for use in Actel 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 Actel 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 2.1.1

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.

Core Performance

Helion also has a long history in high-end FPGA design, and we therefore take our FPGA implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Actel FPGA technology; they are not simply based on a synthesised generic ASIC design like much of the competition.

The Helion DES core makes use of Actel-specific architectural features in order to achieve high performance and efficient logic resource utilisation. It is available for any of the current families including ProASIC3, Fusion, Igloo and Axcelerator, as well as the Rad-Hard RTAX and RTSX families.

Example performance and logic utilisation figures are shown below, targeting Actel Axcelerator and ProASIC3 devices. Obviously, different device families will yield different performance results; we would be pleased to provide details specific to your own applications on request.

	Standard DES	**Fast DES**	**Fast DES**
technology	ProASIC3 –2	ProASIC3 –2	Axcelerator –3
typical core gate count	1118 tiles	2100 tiles	583 C-cells, 142 R-cells
max master clock	91MHz	59MHz	112MHz
max data rate single-DES, ECB mode	**342Mbps**	**419Mbps**	**796Mbps**
max data rate triple-DES, ECB mode	**118Mbps**	**151Mbps**	**286Mbps**

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, England

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