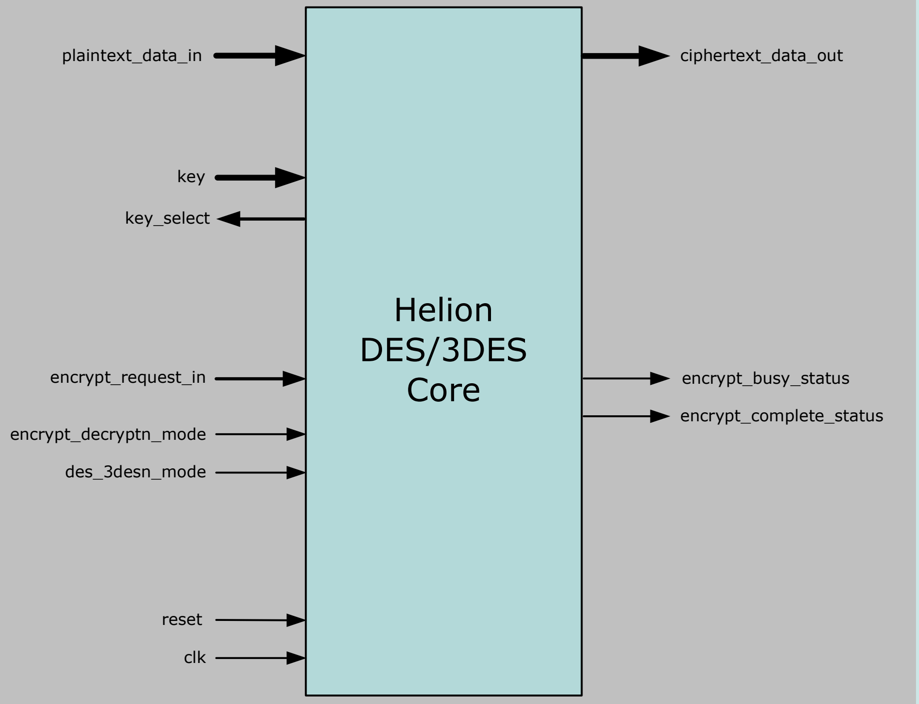
Helion Technology

PRODUCT BRIEF | **DES & 3DES IP cores for FPGA**



Features

- Implements DES and Triple-DES to NIST FIPS publication 46-3
- Two versions available; user can choose best balance between speed and area for application
- Single DES Encryption/Decryption takes only 9-clock cycles in fastest version
- Same core offers dynamically selectable single DES/3DES and encrypt/decrypt modes
- Two and three key 3DES supported
- All classic 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 source code
- VHDL/Verilog simulation model and testbench
- User documentation

Overview

These high performance cores from Helion have been highly optimised for use in FPGA, and implement the DES and Triple-DES (3DES) 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 or low-latency is essential or space is limited, these cores may be the perfect solution.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

Functional Description

Background

The Helion DES cores implement the NIST FIPS 46-3 DES and 3DES algorithms. In encryption mode, 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. Decryption mode reverses this process, when supplied with the same key.

The cores offer selectable DES and 3DES operation, both in encrypt and decrypt modes. When 3DES is selected, both two and three key variants are easily supported. Keys are stored externally to the cores for maximum system flexibility.

Encryption Operation

A block encryption operation using single DES may be performed as follows. The plaintext data block should be presented to the *plaintext_data_in* port on the core, and the 64-bit DES key should be made valid on the *key* input port. Once these two inputs are present, the operation may be initiated by strobing the *encrypt_request_in* input to the core.

During this initial clock cycle, the two control inputs *encrypt_decryptn_mode* and *des_3desn_mode* need to be valid to tell the core what kind of operation is required – encryption or decryption, and single or triple DES. This starts the encryption process, indicated by the core asserting its *encrypt_busy_status* output flag.

Once the core is busy, the input data and input operation controls need not remain valid. In single DES mode the key also need not remain valid – see below for required key behaviour in 3DES mode.

End of the Operation

After the requisite number of clock cycles, the core will complete its encryption operation, and the resulting encrypted data will appear on the *ciphertext_data_out* output port. To indicate this, the *encrypt_complete_status* flag will be asserted for a single clock cycle, and the *encrypt_busy_status* output will be deasserted, ready for the next operation. When *encrypt_busy_status* is low, the core is indicating that it is ready for another operation.

Decryption?

Decryption is the same as above, but with the ciphertext data going into the core on the same *plaintext_data_in* port, and the resulting plaintext data emerging on the *ciphertext_data_out* output port. As you can see, the port naming convention is simply taken from an encryption viewpoint. All other operation is identical to encryption.

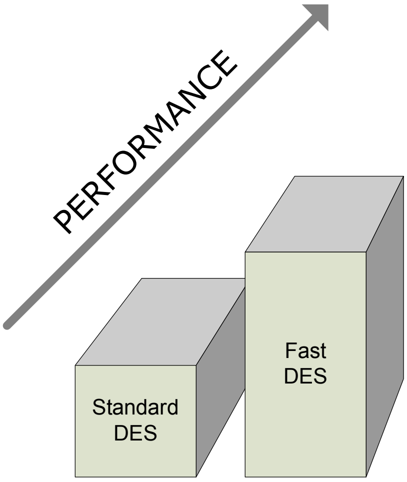
What about 3DES?

For 3DES operation, the same scheme applies, but there is a subtle difference with the way the key works. Triple-DES uses a 3 x 64-bit key to increase security over single-DES. The three 64-bit sections of the key are required one after the other during the lengthened 3DES encryption or decryption process. The section of key required at any one time is indicated by a two-bit select signal generated by the core, called *key_select*. The user must simply supply the appropriate key segment indicated by *key_select* on a cycle-by-cycle basis – easily arranged via use of a simple 3:1 multiplexor or via addressing if the key is being stored in an attached RAM. Other than that, (and the number of cycles used – see below), operation in 3DES mode is identical to DES.

Mode Support

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 Choice



Helion always offer a range of solutions so that the throughput requirements for any application can be closely matched with optimum area efficiency. In this case, Helion have two levels of performance available; the Helion **Standard** DES core and the Helion **Fast** DES core.

The Single-DES algorithm requires 16 rounds for a complete encryption or decryption, and 3DES requires 48 rounds. The **Standard** Helion DES core executes one round for every master clock cycle, so a DES encryption is completed in 16 clock cycles (and 3DES 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 clock cycles (and 3DES 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 choice of core between these two is therefore typically driven by the data throughput required. Please see the next section for more details.

Core Throughput

The tables below show the number of cycles and the maximum data throughput as a function of core clock frequency, for each version of the DES core, for single- and triple-DES operation.

version	Standard DES		Fast DES	
operation	DES	3DES	DES	3DES
clock cycles used per 8-byte block	17	49	9	25
data throughput (Mbps per MHz)	3.76	1.30	7.11	2.56

For any specific application, a core version should be chosen that will achieve the required throughput, with an appropriate and achievable core clock frequency

Logic Utilisation and Performance

Helion cores are fully characterised in all supported FPGA types (please see overleaf for supported FPGA technologies), with specific results available for each device type and speed grade. This yields a huge amount of data, so we don’t include it in this Product Brief. Please contact Helion with your vendor requirements, and we will be delighted to send the appropriate information.

For general guidance however, the typical maximum achievable clock rates in the latest fast FPGA silicon might be ~500MHz in a mid speed grade part for the Standard DES core or ~380MHz for the Fast DES core, whilst in lower cost FPGA devices these rates may be closer to ~250MHz and ~180MHz respectively. These figures can be used as a starting point to determine which version of the core could be suitable for your requirements. A selection of the most popular combinations are also shown on our DES core web pages, at http://www.heliontech.com/des.htm.

Looking for Higher Rates?

The DES algorithm (and 3DES in particular) does have certain inherent limitations in terms of the throughput it can support, due mainly to the number of internal processing rounds it requires. This makes increasing performance difficult.

It may be possible to use multiple engines in parallel to achieve higher rates, however if you have flexibility in terms of the encryption algorithm you are using, it may be worth looking at one of the more modern AES based options. These offer more performance scalability, improved security and highly efficient implementations. Please take a look at our AES webpage at http://www.heliontech.com/aes.htm, or contact Helion for more information on faster AES based solutions.

Ordering Information

Before ordering it is necessary to decide which of our family of DES cores will best fit your application. Simply decide between the **Standard** and **Fast** cores according to the data throughput required and logic resources available.

If any of the choices are unclear, or you would just like to go over the options available, we are always happy to discuss the alternatives and help select the best solution for your application.

FPGA Technology Support

Helion has a long history in high-end FPGA design, and takes a great deal of care when implementing IP cores. As a result, these cores 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. Helion cores always make use of the architectural features available in each FPGA technology to achieve the highest performance combined with the most efficient logic resource utilisation.

Helion is an accredited IP partner with **Altera, Lattice, Microsemi (Actel)** and **Xilinx**, and supports all current and many legacy FPGA technologies from these vendors. Please feel free to contact Helion if your FPGA technology of choice is not listed here.

About Helion

Founded in 1992, Helion is a long established British company based in Cambridge, England. We offer a range of product-proven Data Security and Lossless Compression IP cores, backed by a team of highly experienced engineers, proudly developing and supporting a world-class portfolio.

Our aim is to offer our customers…

Innovation
Helion works hard to anticipate, understand and then deliver great solutions for its customers. As an example, Helion offered the world's first commercial AES core back in 2001, even before the industry had fully adopted the algorithm. This process continues unabated today, with new products in development that will lead the field.

High Performance
Helion IP is specially designed and optimised for each target technology. This means lots of work for us, but this approach yields amazing results for our customers. We always aim for the best in class performance and lowest utilisation in any given ASIC or FPGA target.

High Quality
IP should be problem free, so we always go the extra mile to ensure a smooth and trouble free integration phase for our products. We realise that our customers are putting their faith in us, and want to repay that with an outstandingly easy deployment.

Ease of Use
Helion engineers have many years of real product development experience, and so our IP is designed to be used in realistic situations. It is flexible and well thought through - the result being that it is simple to drop into your system.

See how we achieve all this by visiting our Clients page at http://www.heliontech.com/clients.htm

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