OL_3DES
Triple DES

Rev 1.45

General Description

This core is a full implementation of the Triple DES encryption algorithm. Both encryption and decryption are supported. Simple, fully synchronous design with low gate count.

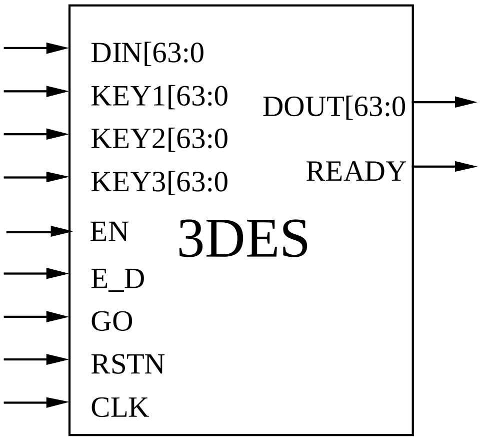
Applications

- Electronic financial transactions.
- Secure communications.
- Secure video surveillance systems.
- Encrypted data storage.

Features

- Implemented according to the X9.52 standard
- Implementation based on NIST certified DES core
- Also available in CBC, CFB and OFB modes.
- 112 or 168 bits keys supported.
- Both encryption and decryption supported.
- Encryption and decryption performed in 48 clock cycles.
- No dead cycles for key loading or mode switching. .
- Encryption or decryption can start every 16 or 48 cycles, depending on the version.
- Fully synchronous design.
- Available as fully functional and synthesizable VHDL or Verilog soft-core.
- Test benches provided.
- Xilinx and Altera netlists available

Symbol



Pin Description

Name	Type	Description
RSTN	Input	Core reset, active low.
CLK	Input	Core clock signal.
GO	Input	Activates encryption or decryption.
EN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored
E_D	Input	Selects encryption or decryption.
KEY1[63:0]	Input	Input key K1.
KEY2[63:0]	Input	Input key K2.
KEY3[63:0]	Input	Input key K3.
DIN[63:0]	Input	Input data.
DOUT[63:0]	Output	Output data.
READY	Output	Ready to operate and output data valid.

General Description

The X_3DES core is a full hardware implementation of the triple DES algorithm as described in the X9.52 standard, suitable for a variety of applications.

The triple DES algorithm was proposed by IBM when it became clear that the security of the DES had been compromised by advances in computer technology.

Compared to the DES algorithm, the triple DES algorithm provides a much higher level of security.

Each triple DES encryption/decryption operation (as specified in ANSI X9.52) is a compound operation of the DES encryption and decryption operations.

A triple DES encryption operation consists in the transformation of a 64-bit block I into a 64-bit block O, defined as follows:

$$O = E_{K3}(D_{K2}(E_{K1}(I)))$$

Where the $E_K(I)$ and $D_K(I)$ represent the DES encryption and decryption of I using DES key K respectively.

Similarly, a triple DES decryption operation consists in the transformation of a 64-bit block I into a 64-bit block O, defined as follows:

$$O = D_{K1}(E_{K2}(D_{K3}(I)))$$

The standard specifies the following keying options for the keys (K1, K2, K3).

1. Keying Option 1: K1, K2, and K3 are independent keys;

2. Keying Option 2: K1 and K2 are independent keys and K3 = K1;

3. Keying Option 3: K1 = K2 = K3

In the last case, the triple DES algorithm coincides with the DES algorithm, providing backward compatibility.

Functional description

Encryption or decryption behavior is selected by the E_D input port. If this input is high, the core performs encryption, otherwise decryption is performed.

Rising the input on the GO port triggers the beginning of a cryptographic operation on the data DIN using the KEY as key.

Only 56 of the 64 bits of each KEY input port are considered by the core, according to the triple DES algorithm. A bit every eight is ignored from each KEY input.

A cryptographic operation takes 48 clock cycles and its completion is indicated by the READY output going high.

Although 48 clock cycles are required to complete a cryptographic operation, a new operation can be started every 16 cycles. As no dead cycles are necessary between two operations, the core can sustain processing 64 bits of data every 16 cycles.
The processing capability of the core is therefore 4 bits/cycle. This means, for example, that, at 100 MHz, 400 Mbit/s can be processed.

The timing diagram below shows a single cryptographic operation. Note that the inputs KEY and DIN need to be valid only for one clock cycle. The valid output, indicated by the READY signal going high, appears after 48 cycles. The GO input remains high during the whole operation.

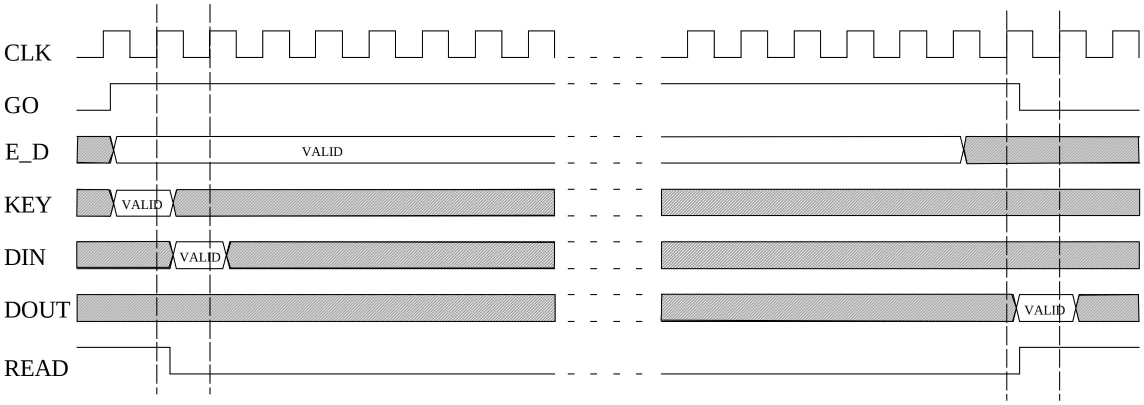


Figure 1. Timing Diagram for the triple-DES

Performance

Performance figures of the core in ECB mode, implemented with some particular technologies, are shown in the table below. Performance in other modes can vary since they might not be parallelizable.

Technology	Area	Speed	Throughput
ASIC 0.18 u	12.2 Kgates	250 MHz	1.0 Gbit/s
Virtex E	790 slices	134 MHz	536 Mbit/s
Virtex II	790 slices	167 MHz	668 Mbit/s

Versions available

Multiple versions of this core, as described in the X9.52 standard, are available.
Customization requests are welcome.

Export Permits

The core is available for export to all the countries of the world with the exception of the following:

Iran North Korea Libya Cuba Sudan
Syria Iraq

It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing this technology.

Deliverables

Netlist available for most Xilinx and Altera devices.
Synthesizable VHDL or Verilog RTL.
Complete HDL testbench.

Ocean Logic Pty Ltd
PO BOX 768 - Manly NSW 1655 - Australia
Tel: +61-2-99054152 Fax: +61-2-99050921
E-Mail: info@ocean-logic.com URL : http://www.ocean-logic.com/