3DES Triple DES Crypto-processor Core

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.

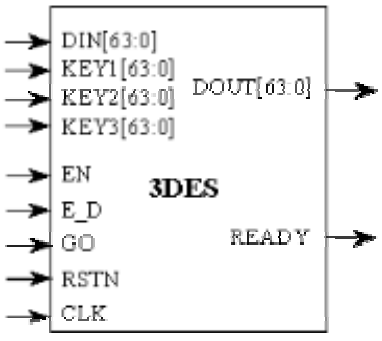
Features

- Implemented according to the X9.52 standard
- Implementation based on NIST certified DES core
- 112- or 168-bit 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
- High clock speed (160 MHz in .25 um) and low gate count achieved (10500 gates)
- Fully synchronous design
- Available as fully functional and synthesizable VHDL or Verilog soft-core
- Test benches provided

Applications: 3DES is used in a variety of applications, including:

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

Symbol



Functional Description

The 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: O = EK3(DK2(EK1(I)))

Where the EK(I) and DK(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 = DK1(EK2(DK3(I)))

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

1. Key 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.

Intelop Corporation 4800 Great America Pkwy. Ste-201 Santa Clara CA. 95054. www.intelop.com
Ph: 408-496-0333. Fax: 408-496-0444 Email: sales@intelop.com