

Serial Triple Data Encryption / Decryption Standard

Features

- Serial Triple DES Encryption and Decryption core
- Compliant with FIPS PUB 46-3
- Available for all vendors
- Easy to use interface signals
- On the fly encryption decryption changes

Application

The serial Triple DES core can be used to secure all communication systems, data storage, financial transactions, video, etc...

I/O

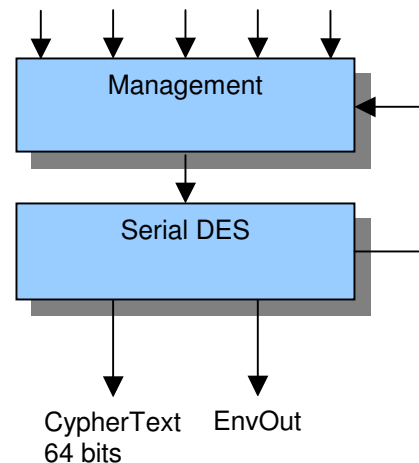
Signal	Direction	Width	Function
Clk	IN	1 bit	Input clock
Reset_n	IN	1 bit	Reset (active Low)
Enable	IN	1 bit	Enable
EnvIn	IN	1 bit	Input envelop
EncryptDecrypt	IN	1 bit	Encryption ('1') or Decryption ('0') selection
PlainText	IN	64 bits	Data to encrypt or decrypt
Key1	IN	64 bits	Encryption or decryption key for the first DES
Key2	IN	64 bits	Encryption or decryption key for the second DES
Key3	IN	64 bits	Encryption or decryption key for the third DES
CypherText	OUT	64 bits	Encrypted or decrypted data
Ready	OUT	1 bit	Module ready
EnvOut	OUT	1 bit	Output envelop

Functional description

The serial Triple DES core encrypts and decrypts block words of 64 bits with the ECB (Electronic Codebook) method.

The architecture is shown below :

Encryption / Key1 Key2 Key3 PlainText
Decryption 64 bits 64 bits 64 bits 64 bits
Start



One word is encrypted or decrypted every 48 clocks.

Performance characteristics

The serial Triple DES occupies 404 slices on Xilinx Virtex 2 Pro and the synthesis frequency is 240 MHz.

The overall throughput is 320 Mbits/s.

Timing

