3DES Core V1.0

Product Brief (January 2016 - Rev A)

Features

- **Implements Triple DES to latest FIPS PUB 46-3**
- **Drop-in module for Spartan-6™, Virtex-6™, Artix-7™, Kintex-7™, Virtex-7™ FPGAs and Zynq™**
- **Single clock**
- **Supports 192-bit key size (168-bit cipher key with 24 additional parity bits)**
- **Supports Single DES**
- **Key Parity Checking**
- **Same core can be used for encryption and decryption**
- **ECB (Electronic Code Book) implementation per FIPS PUB 81**
- **DES > 470Mbps @ 125MHz**
- **3DES > 150Mbps @ 125MHz**
- **Full synthesizable RTL VHDL design (not delivered) for easy customization**
- **Design delivered as Netlist**

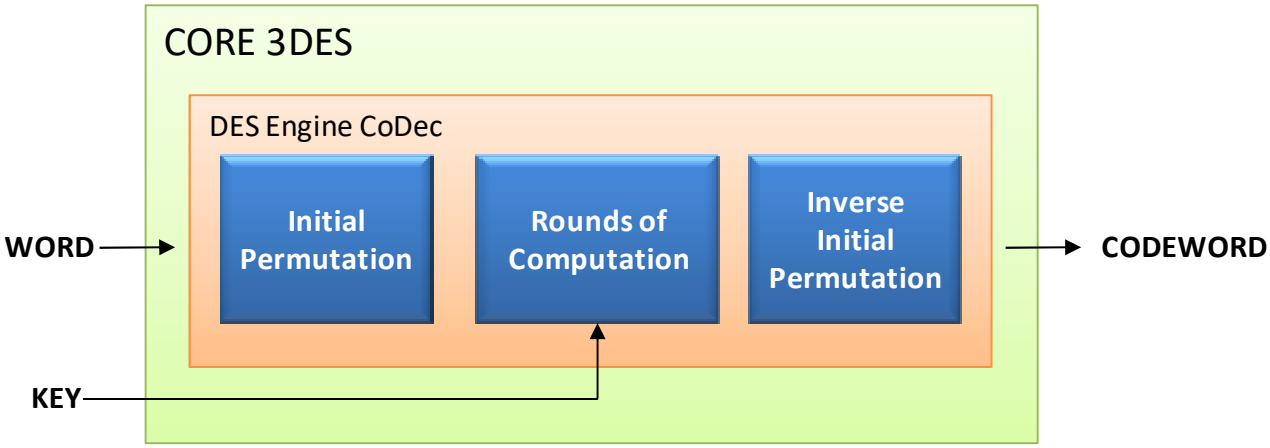
Applications

3DES core may be used in applications related to MPEG-TS stream encryption, or any other encryption applications.

Description

The 3DES core is a drop-in module that includes the following functions :

• 192-bit key size
• Single or Triple Data Encryption Standard
• Encryption or decryption functions are implemented in the core



Resource Utilization (Encryption or decryption mode)

	Slices	LUTs	BRAMs (18k)	DSP48	BUFG	Deliverables :
6-Series	120	440	0	0	1	- Datasheet - Netlist for core generation
7-Series	120	440	0	0	1	

Ordering information and related cores

Designation
MVD_3DES_NET

VHDL source code : can be delivered as an option under NDA and other specific clauses

Related cores : UDP/IP stack, RX RTP, TX RTP, Cable Modulator J83B, DVB-C, DVB-S, DVB-T/H, DVB Remultiplexer, ATSC modulator and/or ASI Receiver cores, contact us at *info_cores@mvd-fpga.com*