AES Core V2.0

Product Brief (October 2015 - Rev A)

Features

- Implements AES (Rijndael) to latest NIST FIPS PUB 197
- Drop-in module for Spartan®-6, Virtex®-6, Artix™-7, Kintex™-7 and Virtex®-7 FPGAs
- Single clock
- Supports 128/192/256-bits key size
- Same core can be used for encryption and decryption
- Automatic Roundkey generation inside the core
- Update Key is allowed if an encryption or decryption process is running
- ECB (Electronic Code Book) and CBC (Cipher Block Chaining) are supported
- > 200Mbps @ 125MHz (AES-128)
  > 170Mbps @ 125MHz (AES-192)
  > 150Mbps @ 125MHz (AES-256)
- Full synthesizable RTL VHDL design (not delivered) for easy customization
- Design delivered as Netlist

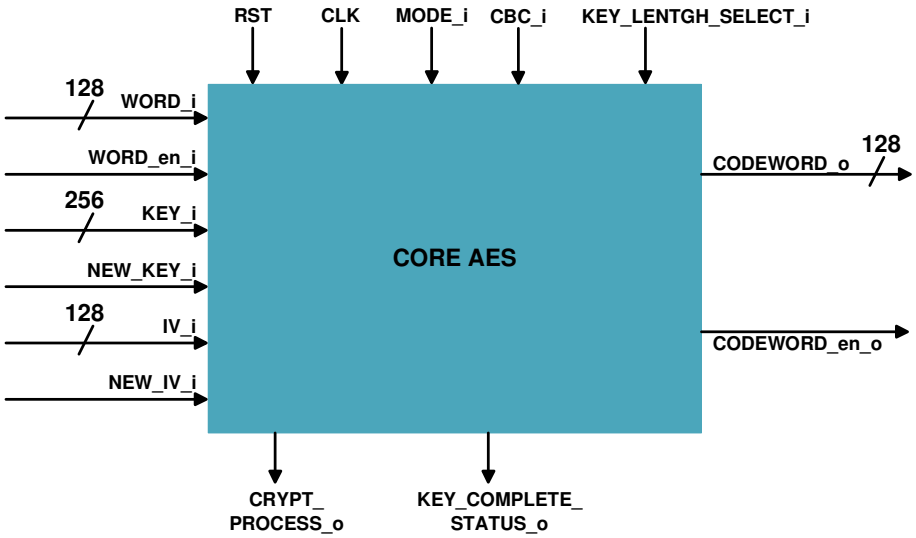
Applications

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

Description

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

- 128/192/256-bits key size
- Automatic Roundkey calculation
- Encryption or decryption functions are implemented in the core



Resource Utilization (Encryption or decryption mode)

	Slices	LUTs	BRAMs (18k)	DSP48	BUFG	Deliverables :
6-Series	440	1700	0	0	1	- Datasheet - Netlist for core generation
7-Series	440	1700	0	0	1	

Ordering information and related cores

Designation
MVD_AES_NET

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

www.mvd-fpga.com
+33 (0) 5 36 47 12 12
Sales information & Technical support:
info_cores@mvd-fpga.com

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*