MW_AES Core

General Description

The MW_AES core performs the digital baseband function that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
Encryption converts data to an unintelligible form called ciphertext, decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.
AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192 or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys; a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

Key length can be changed frame by frame independently. The core can be used for encryption side, but also for decryption side.

Features

- Fully compliant with FIPS PUB 197: Advanced Encryption Standard (AES)
- Fully compliant with ISO/IEC 18033-3: Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers
- Keys length : 128, 192, 256 bits
- Input/Output length : 128 bits
- Encryption or Decryption function
- Synchronous design using single clock
- Low complexity design
- Very fast AES encrypts/decrypts function
- Small resource utilization :

Slices	Slice Reg	LUTs	LUTRAM	BRAM/FIFO	DSP48E1
1398	872	5179	0	0	0

- Zynq/Artix7 technology and ISE Xilinx 14.7/ Vivado tool

MindWay s.r.l. - Via Pordoi 8, 20019 Settimo Milanese (Mi) – Italy
Phone: +39 02 33549098 – Fax: +39 02 3350 3438 – http://www.mindway-design.com – info@mindway-design.com

Typical Application

Support

The core, delivered as is, is warranted against defects for two years from the date of purchase. Sixty days of phone and email technical support are included, starting from the delivery date.

Verification

The core has been verified through extensive simulation and physical implementation on Xilinx Artix™ 7 and Xilinx Zynq™ FPGA technology.

Deliverables

The following deliverables are available:

- FPGA netlist and Xilinx ISE constraint files
- User guide
- Block level design document
- VHDL test bench and test vectors

Optional deliverables:

- Fully synthesizable VHDL source code
- Synthesis script for XST

Please feel free to require any further information. Other MindWay Core Solutions are available, for standard or custom design applications, please visit our web site:

http://www.mindway-design.com

or send an e-mail at:

info@mindway-design.com