Advanced Encryption Standard
AES IP Core

Highlights

- Complete AES implementation to latest NIST FIPS -197
- 128 bit block size and configurable bit key size (128, 192 or 256 bit)
- Technology independent HDL model
- Simple external interface, easy adaptation
- Structured core design, access to internal nodes
- Separate encoder and decoder available
- Implementations for high data rate
- Implementations with – or without key expansion

Overview

AES is one of the latest crypto standards certificated by the National Institute of Standard and Technology (NIST). The AES is a symmetric block cipher algorithm. It provides a high security level for data transmission. The TES Electronic Solutions hardware implementation offers a high level of security and flexibility for the customer.

The AES / Rijndael module is a hardware implementation of the Rijndael algorithm specified by J. Daemen and V. Rijmen and described in NIST Federal Information Processing Standard proposal document (NIST FIPS 197).

Two different decoder and encoder versions are available, optimised for high data rate or low gates quantity. They are also available as implementations with or without key expansion. The block- and key size is configurable (128, 192 or 256 bit). Other specified block- and key sizes can be easily supported.

Function

The AES / Rijndael core can handle input block sizes of 128, 192 or 256 bit. The Encoder needs the key and the plain text as input. The start_en signal signalise the beginning of an encryption. The input data is read and ciphered. After the cipher text is build the cipher data were wrote to the output and the ready_en signal signalised this.

Cores available

- TES Rijndael Slow AES Decoder
- TES Slow AES Encoder
- TES Slow AES De-/Encoder
- TES Rijndael Fast AES Decoder
- TES Fast AES Encoder
- TES Fast AES De-/Encoder

- TES Standard Slow AES Decoder
- TES Standard AES Encoder
- TES Standard AES De-/Encoder
- TES Standard Fast AES Decoder
- TES Standard AES Encoder
- TES Standard AES De-/Encoder

Cores with special requirements are available in a short time upon request (info@tes-dst.com).

Performance

Fast AES

Decoder

Altera (Apex20ke):

- Fmax up to 100 MHz
- 1357 LE and 28 ESB
- throughput 1.15 Gbit / sec

Encoder

Altera (Apex20ke):

- Fmax up to 100 MHz
- 895 LE and 21 ESB
- throughput 1.15 Gbit / sec

Advantage

- One of the fastest AES implementations
- Every AES specified block size can be realised
- Separate implementation for encode and decode
- Every user requirements can be easily implemented

Testing

Known Answer Test and Monte Carlo Tests described from the NIST were successfully done. The tests were done in Electronic Codebook Mode and in Cipher Block Chaining Mode. The TES Electronic Solutions AES Core passed all Tests.

Deliveries

- HDL RTL code or net list for each required technology
- Testbench with functional test vectors
- User-Documentation

Applications

Every application which needs a cryptographic algorithm to protect sensitive (unclassified) information.

Examples:

- Electronic Financial Transactions
- Secure Communication Links
- Secure Video surveillance systems
- Entertainment Systems (Pay-per-view)
- Encrypted Data Storage

Why TES Electronic Solutions AES Solution for Your Business

- High Quality and Efficient Object Codes
- Service offers for: product tuning, hardware, software optimisation and support on final product design
- IC Chip Design Service Provider
- Excellent High Tech Engineering Service References
- Well recognised large B2B Company backed powerful International Holding with 67,000 people

TES related IPs

- **Read Solomon**
  RS(n,K) coding technique for various kind of communication
- **CAN**
  Controller area Network core including transfer and object layer.
- **MPEG-4**: Low Cost MPEG-4 for video coding

Contact

TES Electronic Solutions GmbH
Nikolaus-Otto-Straße 25
70771 Leinfelden-Echterdingen
Tel. +49 (0)711 / 214 74 0
E-mail: info@tes-dst.com
https://www.tes-dst.com