TES AES Core

V2.0 February 2021

Advanced Encryption Standard (AES / Rijndael) Core

Highlights

- Complete AES implementation to latest NIST FIPS -197
- 128 bit block size and configurable bit key size (128, 192 or 256 bit)
- Complete Rijndael implementation to latest Rijndael specification
- Configurable block- and key size (128, 192 or 256 bit) with potentiality of all other allowed block- and key size
- Simple external interface
- Separate encoder and decoder available
- Implementations for high data rate or low gates quantity
- Implementations with – or without key expansion

Overview

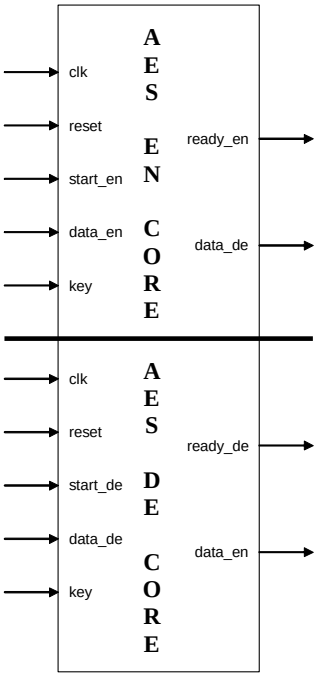
The AES / Rijndael module is a hardware implementation of the Rijndael algorithm specified by J. Daemen and V. Rijmen and described in NIST Federal Information Processing Standard proposal document (NIST FIPS 197).

Decoder and encoder 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

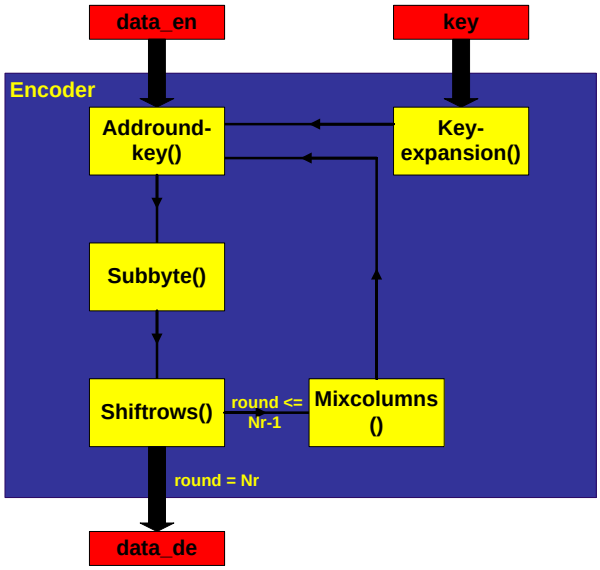
The AES / Rijndael core can handle input block sizes of 128, 192 or 256 bit. The Encoder needs the key and the plain text as input. The start_en signal signalise the beginning of a encryption. The input data is read and ciphered. After the cipher text is build the cipher data were wrote to the output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

Symbol



Block diagram

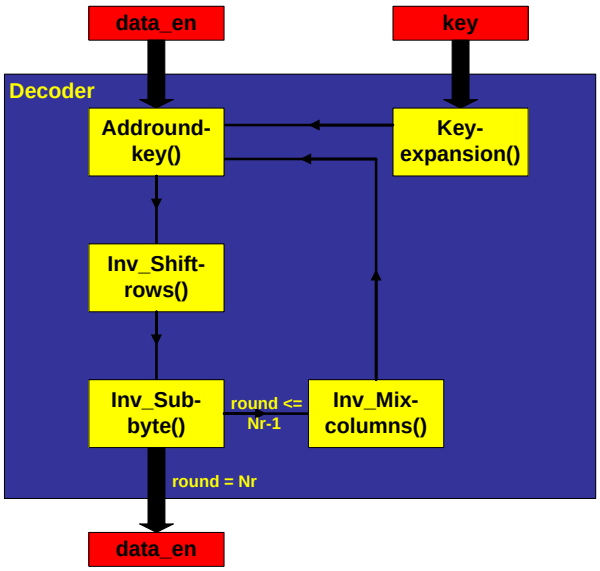
Encoder



TES AES Core

V2.0 February 2021

Decoder



Application Interface

Encoder

Global inputs / outputs

Signal name	Type	Description
clk	IN	System clock
ready_en	OUT	Shows that the encryption is finished
reset	IN	System reset
start_en	IN	Starts the encryption

Data input / output

Signal name	Type	Description
data_de	OUT	Cipher text
data_en	IN	Plain text
key	IN	Key for crypto

Decoder

Global inputs / outputs

Signal name	Type	Description
clk	IN	System clock
ready_de	OUT	Shows that the decryption is finished
reset	IN	System reset
start_de	IN	Starts the decryption

Data input / output

Signal name	Type	Description
data_de	IN	Cipher text
data_en	OUT	Plain text
key	IN	Key for crypto

Advantage

- Free configurable VHDL code
- Every AES specified block size can be realised
- Separate implementation for encode and decode
- Every user requirements can be easily implemented

Testing

The test vectors described in the NIST FIPS 197 and in Rijndael specification were completely tested.

Deliveries

- VHDL RTL code or net list for each required technology
- Testbench
- Graphical user interface