AES Core Modules

Jerzy Gbur

June 24, 2006

This page has been intentionally left blank.

Revision History

Rev.	Date	Author	Description
0.1	24/06/2006	Jerzy Gbur	First draft - Working encoder and decoder

Contents

1

Introduction

In this document I describe components designated to encoding and decoding using AES.

Advanced Encryption Standard has detailed description on this site:
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf
I divide design in some components, you can use them in different configuration.

Best Regards for opencores users.

2

Architecture

There is no strictly top component in this design. They can be used independently.

- aes_enc — parametrizable component which can encrypt input data, using 128, 192 and 256 bit key,
- aes_dec — parametrizable component which can decrypt input data, using 128, 192 and 256 bit key,
- key_expansion — parametrizable component which can produce key expansion, using 128, 192 and 256 bit key,

3

Operation

0	**4**	**8**	**12**
1	**5**	**9**	**13**
2	**6**	**10**	**14**
3	**7**	**11**	**15**

Table 3.1: Order input data in State Table

First thing is to build key expansion. In this time you can not try to read from the key_expansion component. Time of building key expansion depend of key lenght "KEY_SIZE".

- key lenght 128 — 133 clock taps *("B" in figure 3.1)*,
- key lenght 192 — 123 clock taps *("B" in figure 3.1)*,
- key lenght 256 — 157 clock taps *("B" in figure 3.1)*,

Next you can, start encoding/decoding. Philisophy is the same, you put 16 bytes to aes_enc/aes_dec and wait for response block. Time of producing encoded/decoded data depend of key lenght "KEY_SIZE".

- key lenght 128 — 99 clock taps *("D" in figure 3.1)*,
- key lenght 192 — 119 clock taps *("D" in figure 3.1)*,
- key lenght 256 — 139 clock taps *("D" in figure 3.1)*,

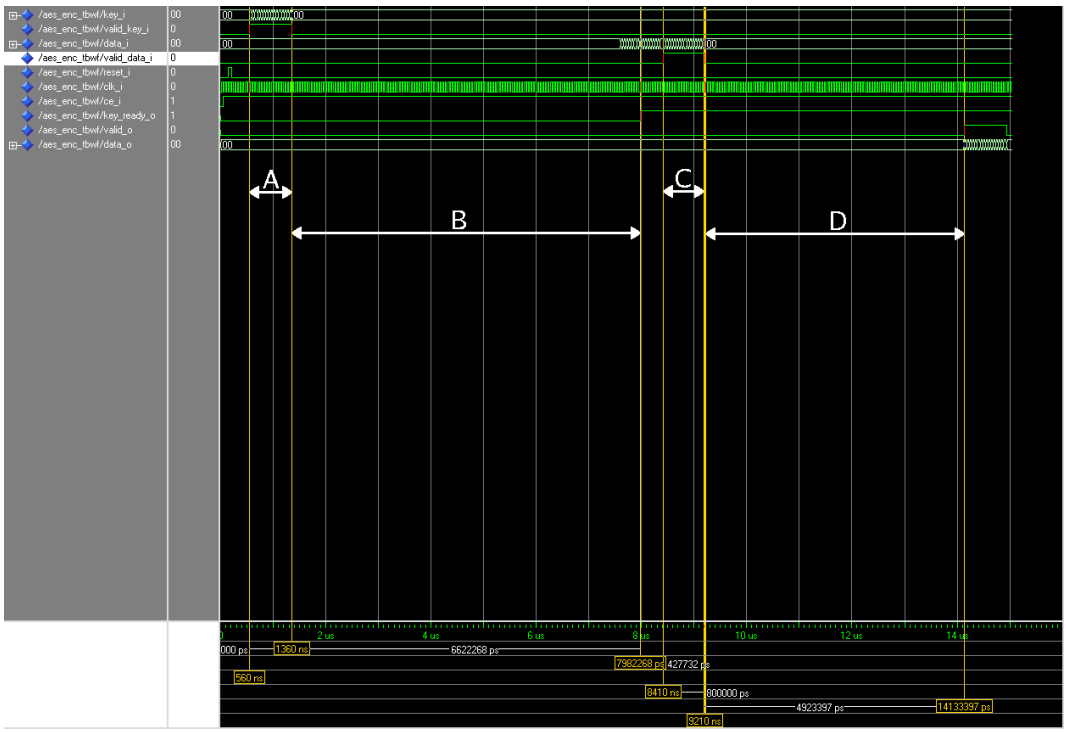

Figure 3.1: Waveform of encoding/decoding process

4

Registers

There is only one generic parameter "KEY_SIZE" which define key lenght we want use.

- key lenght 128 — KEY_SIZE = 0,
- key lenght 192 — KEY_SIZE = 1,
- key lenght 256 — KEY_SIZE = 2,

5

Clocks

Name	Source	Rates [MHz]			Remarks	Description
		Max	Min	Resolution		
CLK_I	external	50MHz	—			

Table 5.1: Clocks

6

IO Ports

Port	Width	Direction	Description
DATA_I	8	in	Data input *(Order showed in table 3.1)*
VALID_DATA_I	1	in	Strob input data
KEY_I	8	in	Key input *(Order showed in table 3.1)*
VALID_KEY_I	1	in	Strob input key
CLK_I	1	in	Clock input
RESET_I	1	in	Reset all internal counters — active "1"
CE_I	1	in	Clock enable — active "1"
KEY_READY_O	1	out	After this output goes "1" you can read Expanded Key
VALID_O	1	out	Strobes output data
DATA_O	8	out	Data output

Table 6.1: List of IO ports