■機能概要

AES-128 暗号化機能搭載モジュールです。

■信号一覧

Top-Level Entity は「aes_top」です。aes_top の入出力信号について以下に示します。

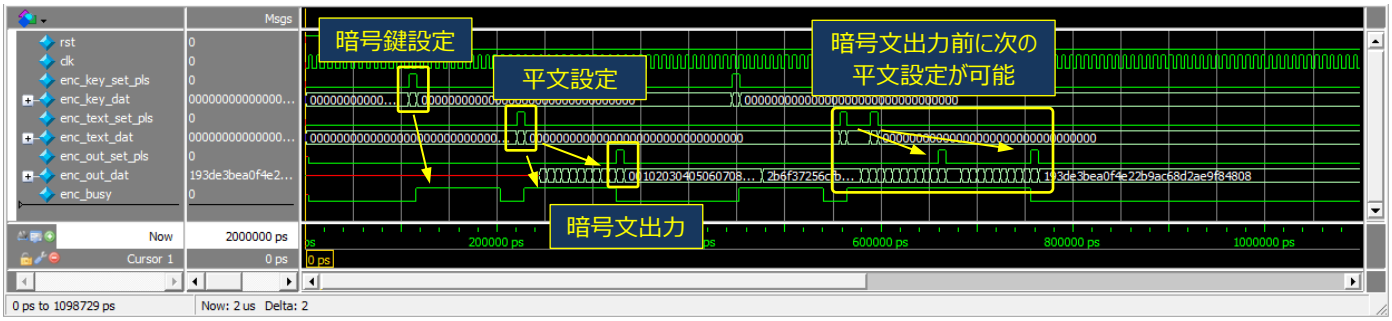
Name	I/O	Description
clk	in	クロックです。
enc_key_set_pls	in	暗号鍵設定信号です。1 クロック幅で入力して下さい。
enc_key_dat[127:0]	in	暗号鍵
enc_text_set_pls	in	平文設定信号です。1 クロック幅で入力して下さい。
enc_text_dat[127:0]	in	平文
enc_out_set_pls	out	暗号文出力信号です。1 クロック幅で出力されます。
enc_out_dat[127:0]	out	暗号文
enc_busy	out	暗号動作実行中を示す信号です。ラウンド鍵算出中もセットされます。
rst	in	clk に同期したリセット(Active-High)入力です。

■機能詳細

暗号鍵設定後、平文を入力すると暗号化されたデータが出力されます。対応している AES 暗号機能を以下に示します。

項目	対応	Description
Cipher Key Length	–	128-bit only
Data blocks	–	128-bit only
Key Expansion	○	
Key Mode	×	ECB mode only
Inverse Cipher (DECRYPT)	×	Cipher (ENCRYPT) only
SubBytes	–	Use LUT (Look-Up-Table)

シミュレーション波形を以下に示します。



暗号鍵設定

暗号鍵を設定するとラウンド鍵を生成します。ラウンド鍵生成による enc_busy が Low になってから平文を入力します。

平文設定

暗号文出力前に次の平文を設定することが出来ます。但し、保持できる平文は一つのみです。

暗号文出力

「enc_out_set_pls」(1 クロック幅)が 1 になった時、「enc_out_dat」に暗号文が出力されます。

■参考情報

Altera (Intel)

項目	Description
Tool	Quartus Prime Version 16.1.0 Lite Edition
Device	Cyclone V [5CEBA7F31C8]

Analysis & Synthesis

項目	Description
Estimate of Logic utilization (ALMs needed)	2,274
Combinational ALUT usage for logic	2,553
Dedicated logic registers	2,075
Total DSP Blocks	0

Fitter

項目	Description
Logic utilization (in ALMs)	1,957
Total registers	2,225
Total block memory bits	0
Total DSP Blocks	0
Fmax	122.84 MHz

Xilinx

クロックに BUFG を追加して確認。

項目	Description
Tool	Vivado v 2016.3 (64-bit)
Device	Kintex-7 [xc7k326tffg676-2]

Synthesis、Implementation (同じ結果)

項目	Description
LUT	1,896
FF	2,083
BRAM	0
DSP	0
Clock	Constraints で 200MHz 設定(timing constraints are met)