128 bit AES Pipelined Cipher

Amr Salah

Version 0.0
07.07.2013

Revision History

Revision	Date	Author(s)	Description
0.0	07.07.2013	Amr Salah	Initial document

Chapter 1

Module description

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES-128 pipelined cipher module uses AES algorithm which is a symmetric block cipher to encrypt (encipher) information. Encryption converts data to an unintelligible form called ciphertext .Here the AES algorithm is capable of using cryptographic keys of 128bit to do this conversion .This module is optimized for speed as it pipeline hardware to perform repeated sequence called round

Chapter 2

Module interface

```
module Top_PipelinedCipher
#
(
parameter DATA_W = 128,   //data width
parameter KEY_L = 128,       //key length
parameter NO_ROUNDS = 10   //no of rounds
)
(
input clk,                          //system clock
input reset,                        //async reset
input data_valid_in,              //data valid  bit
input cipherkey_valid_in,      //key valid bit
input [KEY_L-1:0] cipher_key,          //cipher   key
input [DATA_W-1:0] plain_text,         //plain    text
output valid_out,
output [DATA_W-1:0] cipher_text         //cipher text
);
```

Chapter 3

RTL design and implementation

3.1 **Pipelined Cipher**

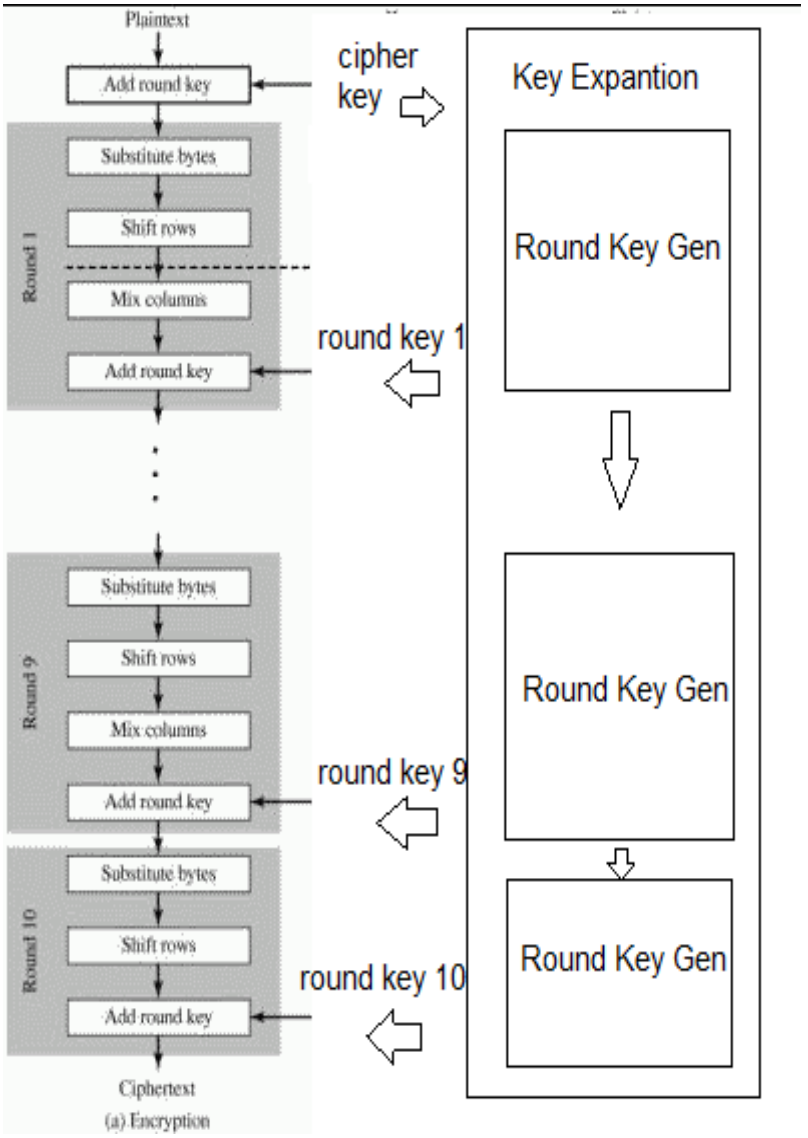

Fig .1.3

- All modules are controlled using one clock , asynchronous reset, inputs valid signal ,outputs valid signal

- **Sub Bytes:**
  - uses SBox LUT to substitute every byte in the 128 bit data
- **Shift Rows:**
  - this module is used to arrange data in the state array and shifting rows of this array as declared on the standard document
- **Mix Columns:**
  - This Module is used to perform Mix Columns calculations (finite field multiplication) declared in standard document
- **Add Round Key:**
  - This module is used for xoring data and round key
- **Round:**
  - This module is used to connect SubBytes-ShiftRows-MixColumns-AddRoundKey modules
- **Round Key Gen:**
  - This module is used to perform the process of round key generation from input key . This module is the basic block of key expantion module
  - The key generation stages should be balanced with the 4 round stages (SuBytes-ShiftRows-MixColumns-AddRoundKey)in order to let the round key and the data meet at the AddRound Key module
  - Round key generation includes RotWord, SubBytes,Xor operations using RCON which are declared in fips197 document
- **Key Expantion:**
  - The key Expantion Module is used to generate round key from cipher key using

Pipelined architecture

- Instantiate number RounkeyGen modules = number of rounds to get number of roundkeys = number of rounds

- **Top Pipelined Cipher:**
  - The top module of the design which forms rounds and connects KeyExpantion using pipelined architecture
  - Instantiate KeyExpantion which will feed every round with round key
  - due to algorithm, first cipher key will be xored with plain text
  - Instantiate all rounds , connect them with key expantion
  - this is the final round it doesn't contain mixcolumns as declared in fips197 standard document
  - as the final round has only three stages a delay register should be introduced to be balanced with key expantion

Chapter 4

Verification

4.1 Functional verification

- Every module is verified using self-checking test bench
- Test vectors and expected output vectors are stored in files and called using $readmemh
- Top module testbench (Top_PopelinedCipher_tb) covered 284 test pattern included in AES validation suit document(AESVS)
- Compilation and simulation of files is automated using do files

4.2 Gate level simulation

- After synthesis and implementation first step for gate simulation is to generate post place and route
- simulation model to generate Verilog netlist and sdf file
- Compilation of Xilinx libraries in model sim
- Using ISE model sim is invoked to apply gate level
- simulaton using the net list , sdf file and top module test bench

Chapter 5

Synthesis-Place and Route

5.1 **FPGA**

•Synthesis, Place and route were done on Xilinx virtex 6 6vcx240tff784-2 board using ISE

- Max Frequency: 639.391Mhz
- Constrain Frequency : 200 Mhz

5.2 Synthesis-Place and Route results

```
Device Utilization Summary:
Slice Logic Utilization:
  Number of Slice Registers:                10,769 out of 301,440    3%
    Number used as Flip Flops:              10,769
    Number used as Latches:                      0
    Number used as Latch-thrus:                  0
    Number used as AND/OR logics:                0
  Number of Slice LUTs:                     12,475 out of 150,720    8%
    Number used as logic:                    9,842 out of 150,720    6%
      Number using O6 output only:           9,081
      Number using O5 output only:               0
      Number using O5 and O6:                  761
      Number used as ROM:                        0
    Number used as Memory:                       0 out of  58,400    0%
    Number used exclusively as route-thrus:  2,633
      Number with same-slice register load:  2,633
      Number with same-slice carry load:         0
      Number with other load:                    0
Slice Logic Distribution:
  Number of occupied Slices:                 3,214 out of  37,680    8%
  Number of LUT Flip Flop pairs used:       12,527
    Number with an unused Flip Flop:         5,031 out of  12,527   40%
    Number with an unused LUT:                  52 out of  12,527    1%
    Number of fully used LUT-FF pairs:       7,444 out of  12,527   59%
```

```
    Number of slice register sites lost
      to control set restrictions:              0 out of 301,440    0%
  A LUT Flip Flop pair for this architecture represents one LUT paired
with
  one Flip Flop within a slice.  A control set is a unique combination
of
  clock, reset, set, and enable signals for a registered element.
  The Slice Logic Distribution report is not meaningful if the design is
  over-mapped for a non-slice resource or if Placement fails.
  OVERMAPPING of BRAM resources should be ignored if the design is
  over-mapped for a non-BRAM resource or if placement fails.
IO Utilization:
  Number of bonded IOBs:                        389 out of     400   97%
Specific Feature Utilization:
  Number of RAMB36E1/FIFO36E1s:                   0 out of     416    0%
  Number of RAMB18E1/FIFO18E1s:                   0 out of     832    0%
  Number of BUFG/BUFGCTRLs:                       2 out of      32    6%
    Number used as BUFGs:                         2
    Number used as BUFGCTRLs:                     0
  Number of ILOGICE1/ISERDESE1s:                  0 out of     720    0%
  Number of OLOGICE1/OSERDESE1s:                  0 out of     720    0%
  Number of BSCANs:                               0 out of       4    0%
  Number of BUFHCEs:                              0 out of     144    0%
  Number of BUFIODQSs:                            0 out of      72    0%
  Number of BUFRs:                                0 out of      36    0%
  Number of CAPTUREs:                             0 out of       1    0%
  Number of DSP48E1s:                             0 out of     768    0%
  Number of EFUSE_USRs:                           0 out of       1    0%
  Number of GTXE1s:                               0 out of      12    0%
  Number of IBUFDS_GTXE1s:                        0 out of       8    0%
  Number of ICAPs:                                0 out of       2    0%
  Number of IDELAYCTRLs:                          0 out of      18    0%
  Number of IODELAYE1s:                           0 out of     720    0%
  Number of MMCM_ADVs:                            0 out of      12    0%
  Number of PCIE_2_0s:                            0 out of       2    0%
  Number of STARTUPs:                             1 out of       1  100%
  Number of SYSMONs:                              0 out of       1    0%
  Number of TEMAC_SINGLEs:                        0 out of       1    0%
Overall effort level (-ol):   High
Router effort level (-rl):    High
Starting initial Timing Analysis.  REAL time: 35 secs
Finished initial Timing Analysis.  REAL time: 36 secs
Starting Router
Phase  1  : 77964 unrouted;      REAL time: 42 secs
Phase  2  : 70512 unrouted;      REAL time: 54 secs
Phase  3  : 26862 unrouted;      REAL time: 1 mins 44 secs
Phase  4  : 26860 unrouted; (Setup:0, Hold:1, Component Switching
Limit:0)     REAL time: 1 mins 56 secs
Updating file: Top_PipelinedCipher.ncd with current fully routed design.
Phase  5  : 0 unrouted; (Setup:0, Hold:0, Component Switching Limit:0)
REAL time: 2 mins 30 secs
Phase  6  : 0 unrouted; (Setup:0, Hold:0, Component Switching Limit:0)
REAL time: 2 mins 30 secs
Phase  7  : 0 unrouted; (Setup:0, Hold:0, Component Switching Limit:0)
REAL time: 2 mins 30 secs
Phase  8  : 0 unrouted; (Setup:0, Hold:0, Component Switching Limit:0)
REAL time: 2 mins 30 secs
Phase  9  : 0 unrouted; (Setup:0, Hold:0, Component Switching Limit:0)
REAL time: 2 mins 30 secs
```

```
Phase 10  : 0 unrouted; (Setup:0, Hold:0, Component Switching Limit:0)
REAL time: 2 mins 38 secs
Total REAL time to Router completion: 2 mins 38 secs
Total CPU time to Router completion: 2 mins 42 secs
Partition Implementation Status
-------------------------------
  No Partitions were found in this design.
-------------------------------
Generating "PAR" statistics.
**************************
Generating Clock Report
**************************
+---------------------+--------------+------+------+------------+-------
------+
|        Clock Net    |   Resource   |Locked|Fanout|Net Skew(ns)|Max
Delay(ns)|
+---------------------+--------------+------+------+------------+-------
------+
|           clk_BUFGP | BUFGCTRL_X0Y0| No   | 3213 |  0.252     |  1.834
|
+---------------------+--------------+------+------+------------+-------
------+
* Net Skew is the difference between the minimum and maximum routing
only delays for the net. Note this is different from Clock Skew which
is reported in TRCE timing report. Clock Skew is the difference between
the minimum and maximum path delays which includes logic delays.
Timing Score: 0 (Setup: 0, Hold: 0, Component Switching Limit: 0)
Asterisk (*) preceding a constraint indicates it was not met.
   This may be due to a setup or hold violation.
--------------------------------------------------------------------------
  Constraint            |    Check    | Worst Case |  Best Case
                        |             |    Slack   | Achievable
--------------------------------------------------------------------------
TS_clk = PERIOD TIMEGRP | SETUP       |     0.084ns| 4.952ns
"clk" 5  ns HIGH  50%   | HOLD        |     0.006ns|
----------------------
| Timing |   Timing
| Errors |    Score
----------------------
|       0|           0
|       0|           0
----------------------

All constraints were met.
```

5.3 Latency and Throughput

- **Latency:** according to constraint frequency (200Mhz)/Period (5ns)

  Latency = 41clockcycle = 41 X 5 ns= 205 ns

- **Throughput:** according to constraint frequency (200Mhz)/Period (5 ns)

  Throughput = 128 bit / 5 ns = 25.6 bits/ns = 25.6 Gbits/sec

Chapter 6

File archive

- **AES2**
  - **rtl**
    - **Top_PipelinedCipher.v**
    - **KeyExpantion.v**
    - **RoundKeyGen.v**
    - **Round.v**
    - **SubBytes.v**
    - **SBox.v**
    - **ShifRows.v**
    - **MixColumns.v**
    - **AddRoundKey.v**
  - **sim**
    - **Top_PipelinedCipher_tb.v**
    - **topcipher_data_test_inputs.txt**
    - **topcipher_key_test_inputs.txt**
    - **topcipher_test_outputs.txt**
    - **Top_PipelinedCipher.do**
    - **Key_Expantion_tb.v**
    - **keyexpantion_test_inputs.txt**
    - **keyexpantion_test_outputs.txt**
    - **KeyExpantion.do**
    - **Round_tb.v**
    - **round_test_inputs.txt**
    - **round_test_outputs.txt**

- **roundkey_test_inputs.txt**
- **Round.do**
- **SubBytes_tb.v**
- **subbytes_test_inputs.txt**
- **subbytes_test_outputs.txt**
- **Subbytes.do**
- **ShiftRows_tb.v**
- **shiftrows_test_inputs.txt**
- **shiftrows_test_outputs.txt**
- **ShiftRows.do**
- **MixColumns_tb.v**
- **mixcolumns_test_inputs.txt**
- **mixcolumns_test_outputs.txt**
- **MixColumns.do**
- **AddRoundKey_tb.v**
- **addroundkey_data_test_inputs.txt**
- **addroundkey_key_test_inputs.txt**
- **addroundkey_test_outputs**
- **AddRoundKey.do**

- **Syn**
  - **AES.tcl**
  - **Run.tcl**
  - **Top_PipelinedCipher.ucf**
- **reports**
  - **Top_PipelinedCipher.syr**
  - **Top_PipelinedCipher.par**
  - **Top_PipelinedCipher.twr**
  - **Top_PipelinedCipher_map.mrp**
- **doc**
  - **Cipher.pdf**
  - **release_notes.txt**