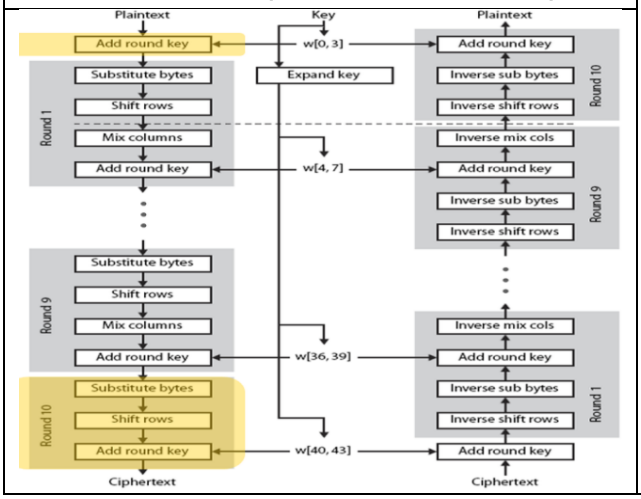
VLSI System Design (prof. Jinsang Kim) Term Project Final Report (18a)

Subject : Advanced Encryption Standard(AES) Algorithm

RTL Simulation Result

AES Structure (암호화 & 복호화 과정)



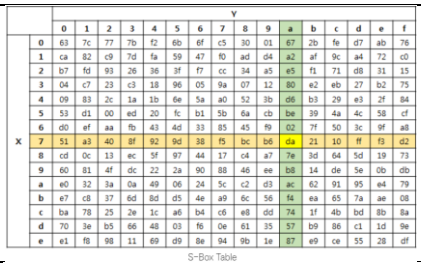
AES 알고리즘은 128비트 단위로 이루어 지며, Add Round Key , Sub Byte, Shift Row, Mix Column 이 반복 되어 이루어진다.

우리 팀은 이번에 AES 알고리즘이 실제로 구현이 될 수 있도록 총 4단계의 암호화 과정 그리고 그 reverse 의 복호화 과정을 수행할 수 있는 AES 알고리즘을 구현하고자 한다.

1. Substitute Bytes

-Encryption : input data를 byte 단위로 쪼개어 S-box의 Matrix를 이용해 mapping

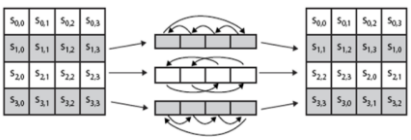
-Decryption : inverse S-box로 복원



S-Box Table

2. Shift Rows

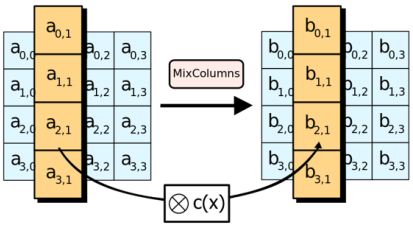
-1byte씩 쪼개어 4x4 행렬로 구성하여 행마다 다른 shifting



3. Mix Columns

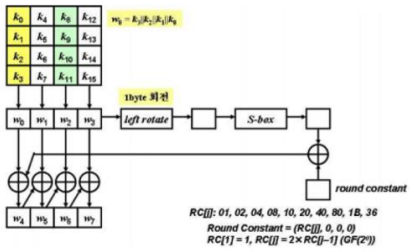
-1byte씩 쪼개어 4x4 행렬로 구성하여 각 열에 대해 predefined 행렬을 곱해준다.

-이 때 더하기와 곱하기는 XOR, Shift 이용



4. Add Round Key

-생성되는 Round Key는 이전 round 에서의 round key와 결합되어 생성된다.(XOR연산)



Hierarchy structure of Verilog Code.

<table>
<tr><td colspan="8">AES_ERC_PAD.v</td></tr>
<tr><td colspan="8">AES_ERC.v (TOP CELL)</td></tr>
<tr><td colspan="3">Subkeys.v</td><td colspan="5">AES_pipe.v</td></tr>
<tr><td colspan="3">Columns.v</td><td rowspan="4">Shift_rows.v</td><td colspan="4">AES_col.v</td></tr>
<tr><td rowspan="3">Xor_tree.v</td><td colspan="2">Prod_gen.v</td><td rowspan="3">Sbox_mi.v</td><td colspan="3">Columns.v</td></tr>
<tr><td colspan="2">Multiply_by_2_pow_n.v</td><td rowspan="2">Xor_tree.v</td><td colspan="2">Prod_gen.v</td></tr>
<tr><td>Multiply_by_2.v</td><td>Switch_gates.v</td><td colspan="2">Multiply_by_2_pow_n.v</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Multiply_by_2.v</td><td>Switch_gates.v</td></tr>
</table>

Verilog Code List

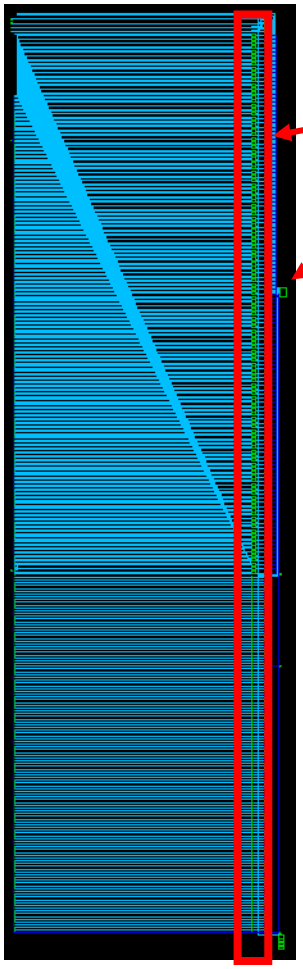
AES_ERC_PADS.v	: Top cell 에 붙는 PAD 를 연결하기 위한 cell.
AES_ERC.v	: TOP cell (out,out_valid,out_ready,in,in_valid,in_ready,dec,clk,rst,size)
Subkey.v	: 암호화와 복호화를 위한 Subkey를 load. 입력된 data의 Mix column 작업 또한 수행한다.
AES_pipe.v	: 1번의 round 를 수행하는 cell.
Shift_row.v	: 입력된 data 를 1byte 단위로 쪼개어 행 별로 1번씩 shift 시켜줌.
AES_col.v	: 각각의 column 에 대해 sbox 에 매핑하여 변환하고, Mix column 작업 수행
Sbox_mi.v	: S-box 의 look up table 이 있으며, 1개 column 에 대해 매핑 및 변환 작업 수행.
Columns.v	: Mix column 작업 수행.
Xor_tree.v	: 입력된 1byte씩의 4개 data 에 대해 XOR 연산을 수행하여 1개의 1byte 출력 data 생성하는 cell.
Prod_gen.v	: Columns.v cell 과 해당 작업을 수행하기 위한 하위 cell 간의 연결 cell. (key, data) 및 다음 작업을 위한 새로운 round key 생성.
Multiply_by_2_pow_n.v	: 입력된 1byte의 data를 총 8배 곱셈 연산하는 cell.
Multiply_by_2.v	: 입력된 1byte의 data를 2배 시켜줌.
Switch_gates.v	: 입력된 data 를 inverter를 통과시켜 data를 flip 시킴.

I/O description.

[out, out_valid, out_ready, in, in_valid ,in_ready ,dec, clk, rst, size]

Pin	Direction	Description
In[0:127]	INPUT	Data Input
Dec	INPUT	Decryption (복호화) flag (encryption : 0, decryption : 1)
Size[0:1]	INPUT	Key length flag (128bits : 0, 192bits : 1, 256bits: 2, don't use : 3)
Out[0:127]	OUTPUT	Data Output
In_valid	INPUT	Data Input is valid
In_ready	INPUT	Input is ready for Data (when it falling 1 -> 0. Last input is input data.)
Out_valid	OUTPUT	Data Output is valid
Out_ready	OUTPUT	Output is ready for Data
Clk	INPUT	Clock
Rst	INPUT	Reset

RTL Synthesis Result

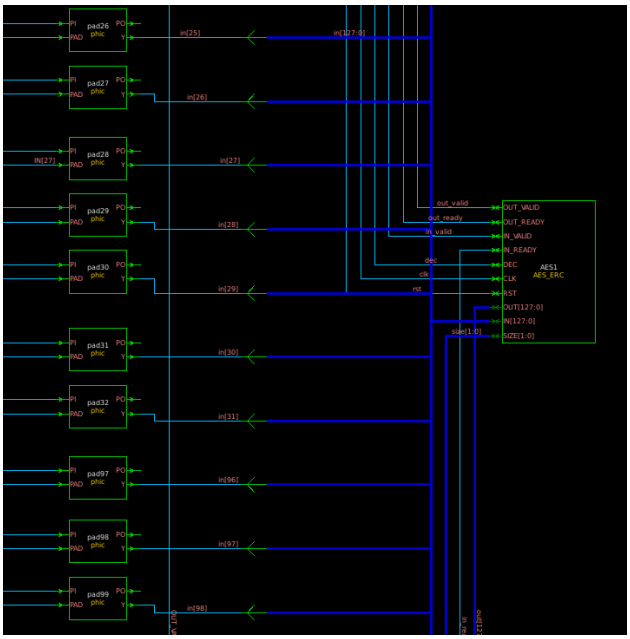


Design Vision 을 이용해 AES 128bits Core module 과 PADS 를 합성한 결과.

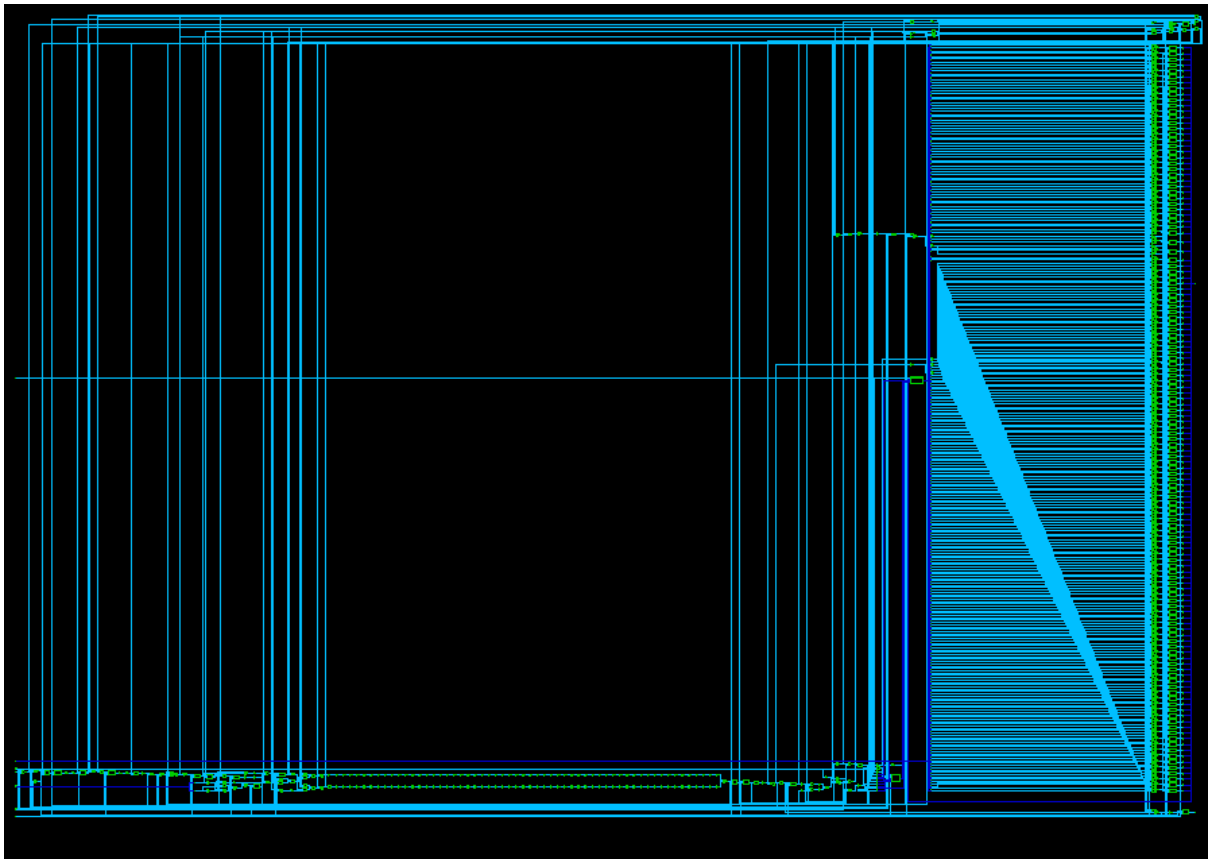
PADS....

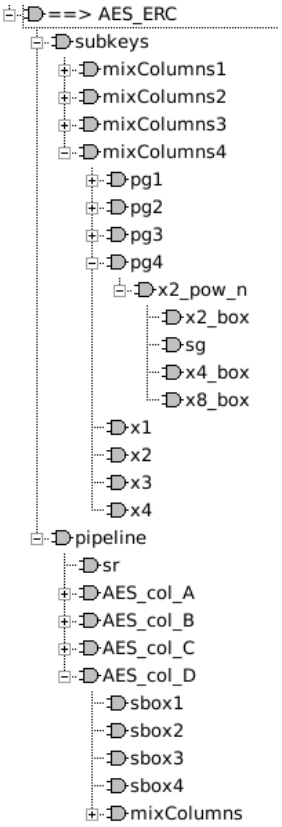
Core AES 128bits

Core 부분 확대



Core Module (AES_ERC) 내부 Schematic





Synthesis 가 완료되었을 때, 전체 Module 의 Hierarchy 구조.

Synthesis Report

- Area Report

<table>
<tr>
<td>

```
Report : area
Design : NAND
Version: F-2011.09-SP5-3
Date   : Tue Jun  5 14:49:57 2018
****************************************

Library(s) Used:

    std150e_typ_120_p025 (File: /Tools/Library/

Number of ports:                          3
Number of nets:                           3
Number of cells:                          1
Number of combinational cells:            1
Number of sequential cells:               0
Number of macros:                         0
Number of buf/inv:                        0
Number of references:                     1

Combinational area:          3.666670
Buf/Inv area:                0.000000
Noncombinational area:       0.000000
Net Interconnect area:       0.022050

Total cell area:             3.666670
Total area:                  3.688720
```

</td>
<td>

사용된 Gate 수를 Estimate 하기 위해서 간단한 AND gate를 synthesis 하여 단일 cell 이 차지하는 Area를 확인함.

➔ 3.68872um^2

</td>
</tr>
<tr>
<td>

```
Report : area
Design : AES_ERC
Version: F-2011.09-SP5-3
Date   : Tue Jun  5 14:13:18 2018
****************************************

Library(s) Used:

    std150e_typ_120_p025 (File: /Tools/Library/samsung013/se

Number of ports:                        265
Number of nets:                         881
Number of cells:                        488
Number of combinational cells:          348
Number of sequential cells:             138
Number of macros:                         0
Number of buf/inv:                      151
Number of references:                    33

Combinational area:       178816.807381
Buf/Inv area:             25684.674480
Noncombinational area:    22575.659727
Net Interconnect area:      942.222430

Total cell area:          201632.467108
Total area:               202334.689538
```

</td>
<td>

Total Area: 202,334 um^2

The Number of Gate = $\frac{202334.689538}{3.68872}$

=54,852.27

약 54,850 개의 Gate 사용됨.

</td>
</tr>
</table>

- Timing Report

```
  pipeline/AES_col_C/mixColumns/pg1/x2_pow_n/x8_box/__tmp100/Y (xo2d4_hd)
                                                    0.27      11.12 r
  pipeline/AES_col_C/mixColumns/pg1/x2_pow_n/x8_box/A_prime[4] (multiply_by_2_21)
                                                    0.00      11.12 r
  pipeline/AES_col_C/mixColumns/pg1/x2_pow_n/x08[4] (multiply_by_2_pow_n_7)
                                                    0.00      11.12 r
  pipeline/AES_col_C/mixColumns/pg1/x1[4]/Y (xo2d4_hd)
                                                    0.20      11.32 f
  pipeline/AES_col_C/mixColumns/pg1/x3[4]/Y (xo2d4_hd)
                                                    0.17      11.48 f
  pipeline/AES_col_C/mixColumns/pg1/x01_0D[4] (prod_gen_7)
                                                    0.00      11.48 f
  pipeline/AES_col_C/mixColumns/x3/A[4] (xor_tree_5)      0.00      11.48 f
  pipeline/AES_col_C/mixColumns/x3/x1[4]/Y (xo2d4_hd)     0.16      11.64 f
  pipeline/AES_col_C/mixColumns/x3/x3[4]/Y (xo2d4_hd)     0.15      11.79 f
  pipeline/AES_col_C/mixColumns/x3/E[4] (xor_tree_5)      0.00      11.79 f
  pipeline/AES_col_C/mixColumns/W_prime[12] (columns_1)
                                                    0.00      11.79 f
  pipeline/AES_col_C/U34/Y (scg5d1_hd)              0.18      11.96 f
  pipeline/AES_col_C/rdXOR[12]/Y (xo2d4_hd)         0.20      12.17 f
  pipeline/AES_col_C/New_State[12] (AES_col_1)      0.00      12.17 f
  pipeline/New_State[44] (AES_pipe)                 0.00      12.17 f
  U93/Y (scg2d2_hd)                                 0.21      12.38 f
  buffer_reg[44]/D (fd1eqd4_hd)                     0.00      12.38 f
  data arrival time                                           12.38

  clock clk (rise edge)                            15.00      15.00
  clock network delay (ideal)                       0.00      15.00
  clock uncertainty                                -0.50      14.50
  buffer_reg[44]/CK (fd1eqd4_hd)                    0.00      14.50 r
  library setup time                               -0.10      14.40
  data required time                                          14.40
  -------------------------------------------------------------------------
  data required time                                          14.40
  data arrival time                                          -12.38
  -------------------------------------------------------------------------
  slack (MET)                                                  2.01

"AES_ERC.report_timing_max" 178L, 11760C
```

```
*****************************************

 # A fanout number of 1000 was used for high fanout net computat

Operating Conditions: V120TTP0250   Library: std150e_typ_120_p02
Wire Load Model Mode: enclosed

  Startpoint: mode_reg[0]
              (rising edge-triggered flip-flop clocked by clk)
  Endpoint: in_ready_reg
            (rising edge-triggered flip-flop clocked by clk)
  Path Group: clk
  Path Type: min

  Des/Clust/Port     Wire Load Model       Library
  ------------------------------------------------
  AES_ERC            113_e_300k_41m        std150e_typ_120_p025

  Point                                    Incr       Path
  -----------------------------------------------------------
  clock clk (rise edge)                    0.00       0.00
  clock network delay (ideal)              0.00       0.00
  mode_reg[0]/CK (fd1eqd4_hd)              0.00 #     0.00 r
  mode_reg[0]/Q (fd1eqd4_hd)               0.27       0.27 f
  in_ready_reg/D (fd1eqd4_hd)              0.00       0.27 f
  data arrival time                                   0.27

  clock clk (rise edge)                    0.00       0.00
  clock network delay (ideal)              0.00       0.00
  in_ready_reg/CK (fd1eqd4_hd)             0.00       0.00 r
  library hold time                        0.01       0.01
  data required time                                  0.01
  -----------------------------------------------------------
  data required time                                  0.01
  data arrival time                                  -0.27
  -----------------------------------------------------------
  slack (MET)                                         0.26
```

- Max Timing report Clock setting = 15ns. Slack time = 2.01ns. (낭비된 시간.)	- Min Timing report Clock setting = 15ns. Slack time = 0.26ns.

- Power Report

```
Global Operating Voltage = 1.2
Power-specific unit information :
    Voltage Units = 1V
    Capacitance Units = 1.000000pf
    Time Units = 1ns
    Dynamic Power Units = 1mW    (derived from V,C,T units)
    Leakage Power Units = 1mW


  Cell Internal Power  =   4.4287 mW   (67%)
  Net Switching Power  =   2.2215 mW   (33%)
                       ---------
Total Dynamic Power    =   6.6503 mW  (100%)

Cell Leakage Power     = 145.8688 uW


                 Internal         Switching           Leakage            Total
Power Group      Power            Power               Power              Power   (   %    )  Attrs
--------------------------------------------------------------------------------------------------
io_pad             0.0000           0.0000            0.0000            0.0000  (   0.00%)
memory             0.0000           0.0000            0.0000            0.0000  (   0.00%)
black_box          0.0000           0.0000            0.0000            0.0000  (   0.00%)
clock_network      0.0000           0.0000            0.0000            0.0000  (   0.00%)
register           0.3969        2.0920e-02        5.7607e-03           0.4235  (   6.23%)
sequential         0.0000           0.0000            0.0000            0.0000  (   0.00%)
combinational      4.0319           2.2006            0.1401            6.3725  (  93.77%)
                                                                      ----------------------
Total              4.4287 mW        2.2215 mW         0.1459 mW         6.7960 mW
```

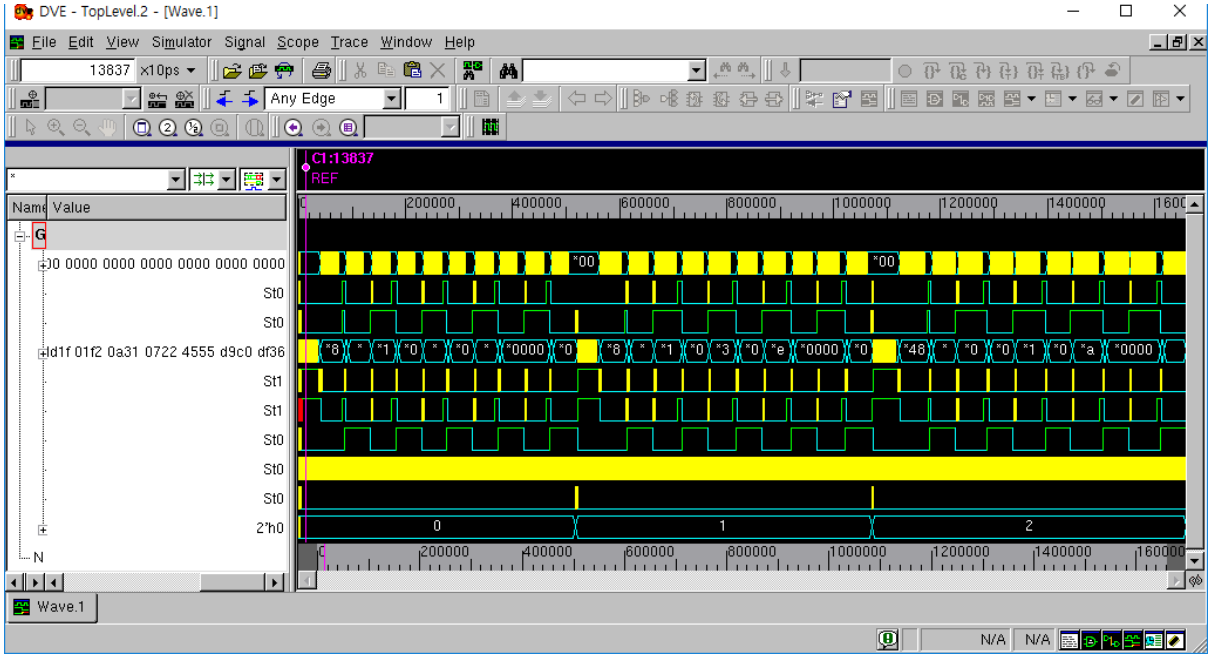
VDD = 1.2V

Dynamic Power
= 6.65 mW

Cell Leakage Power
= 145.8688 uW

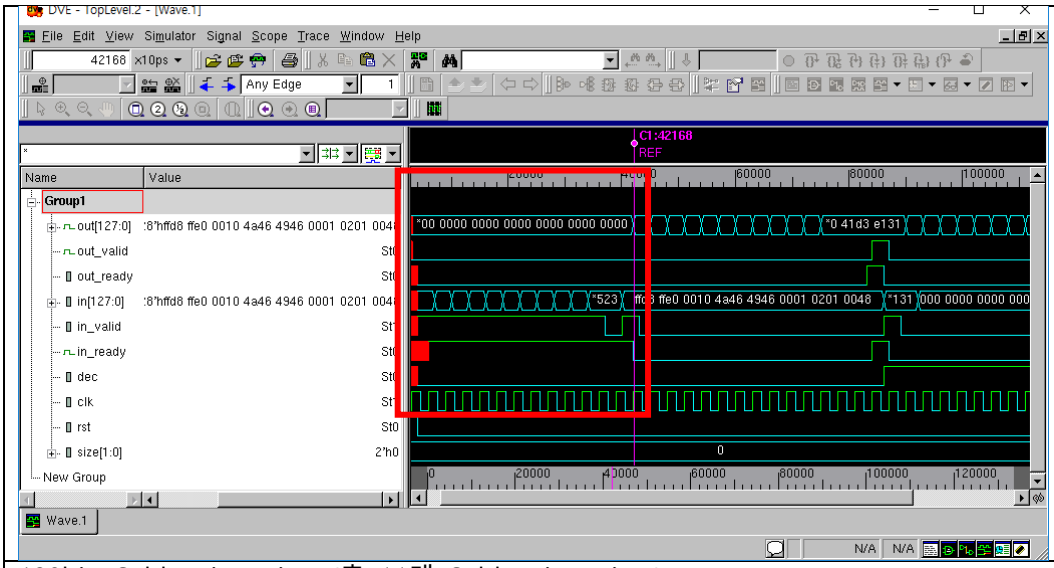
Total power consumption.
= 6.796 mW

- DVE Functional Simulation Result



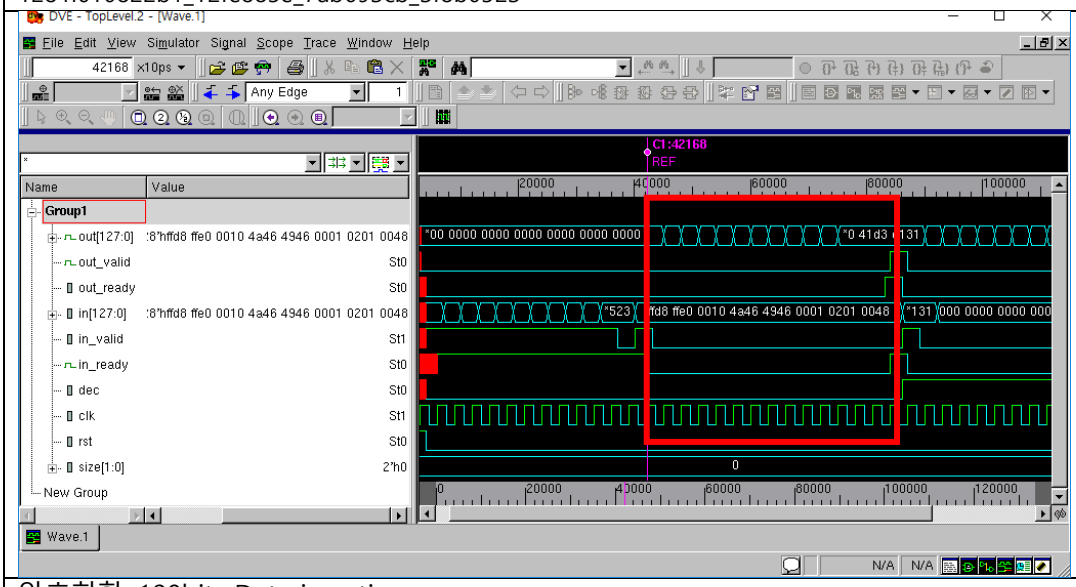
Testbench를 이용하여, 각각의 경우에 대해 (Size = 0, 1, 2), functional simulation 진행.

Size = 0, 128bits Key.



128bits Subkey insertion. (총 11개 Subkey insertion.)

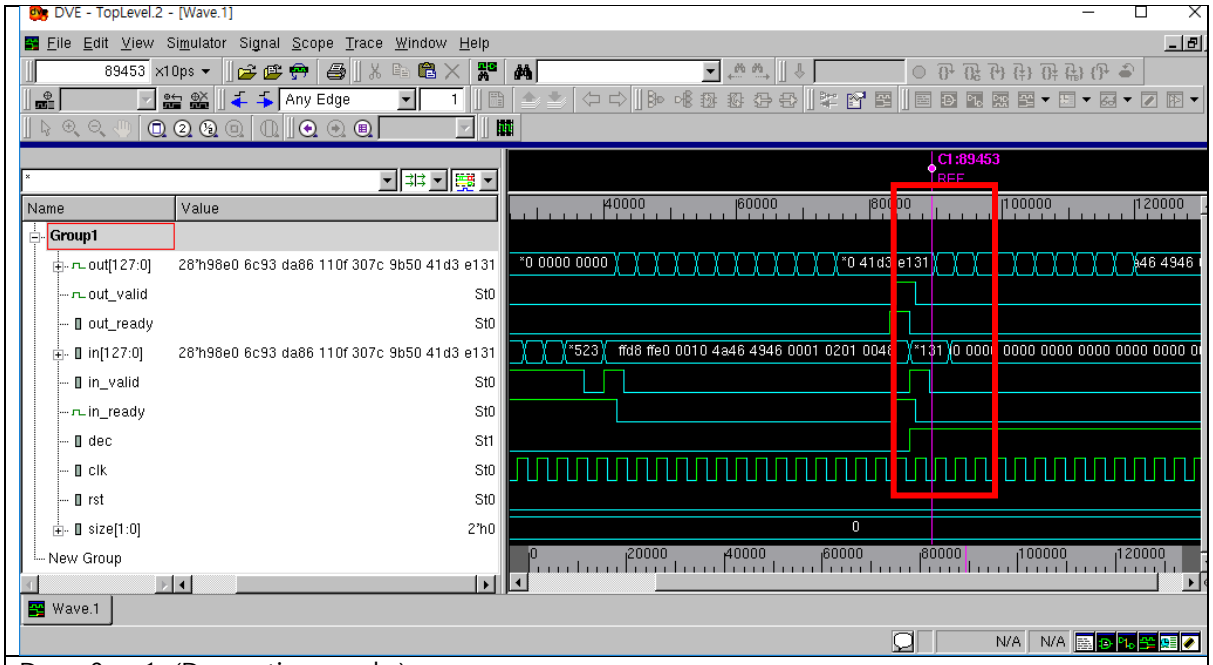
128'h00480000_ffe1124f_45786966_00004d4d
128'h62abe363_9d4af12c_d832984a_d832d507
128'h43a82602_dee2d72e_06d04f64_dee29a63
128'hdf10dd1f_01f20a31_07224555_d9c0df36
128'h6d8ed82a_6c7cd21b_6b5e974e_b29e4878
128'h76dc641d_1aa0b606_71fe2148_c3606930
128'h86256033_9c85d635_ed7bf77d_2e1b9e4d
128'h692e8302_f5ab5537_18d0a24a_36cb3c07
128'hf6c54607_036e1330_1bbeb17a_2d758d7d
128'h7098b9df_73f6aaef_68481b95_453d96e8
128'h610822b1_12fe885e_7ab693cb_3f8b0523



암호화할 128bits Data insertion.

128'hffd8ffe0_00104a46_49460001_02010048

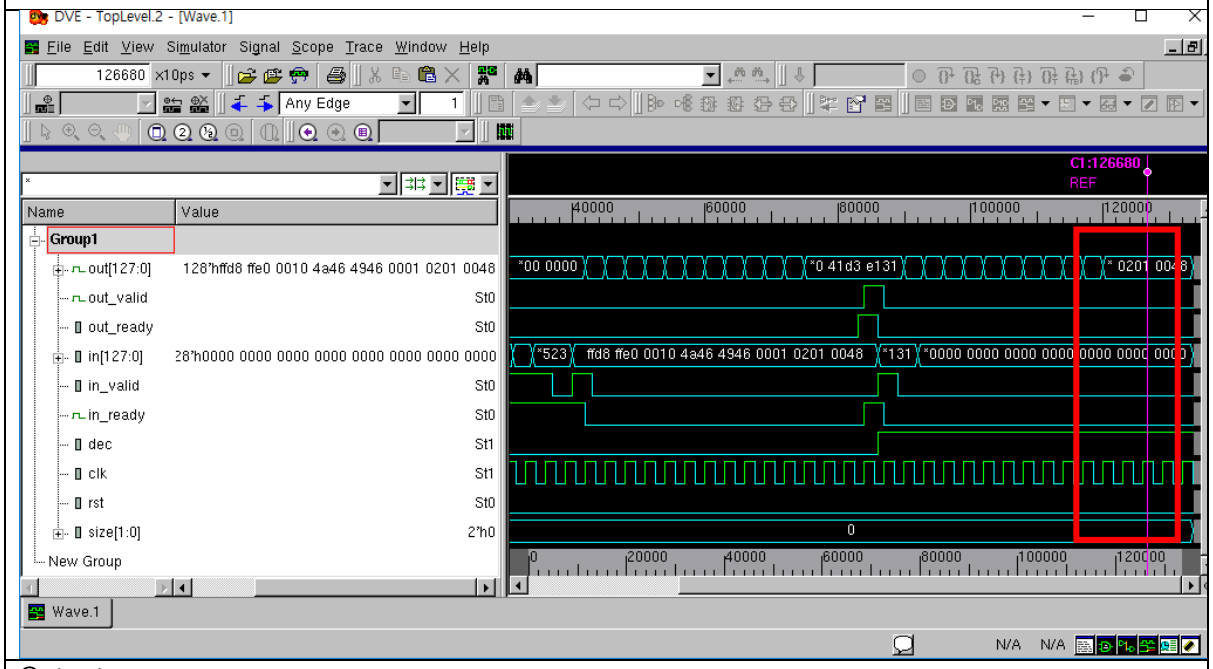
Output :
128'h98e06c93_da86110f_307c9b50_41d3e131



Dec : 0-> 1. (Decryption mode.)

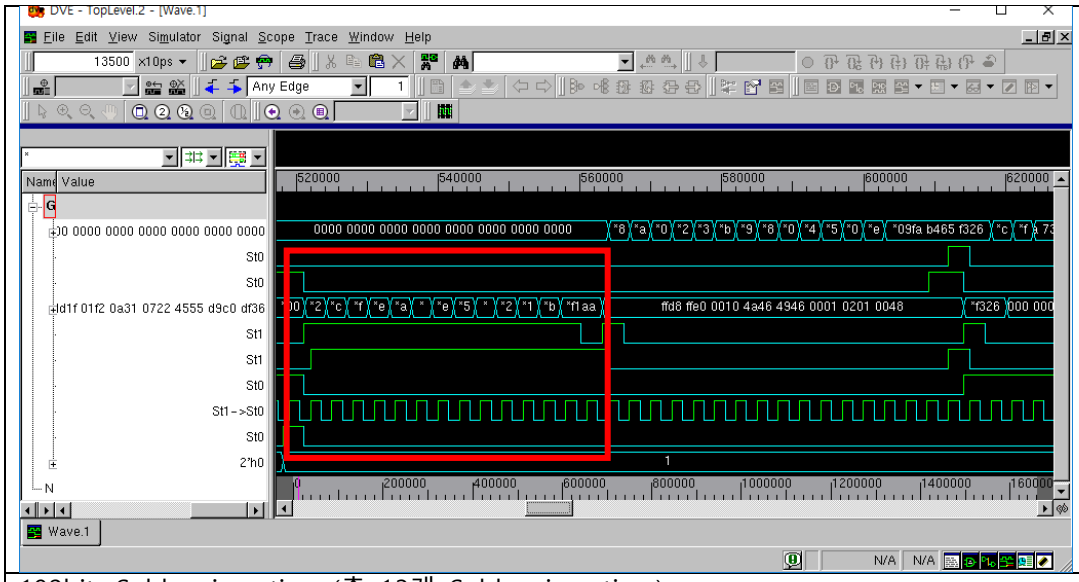
input으로 방금 나왔던 output 을 입력.

Input :
128'h98e06c93_da86110f_307c9b50_41d3e131



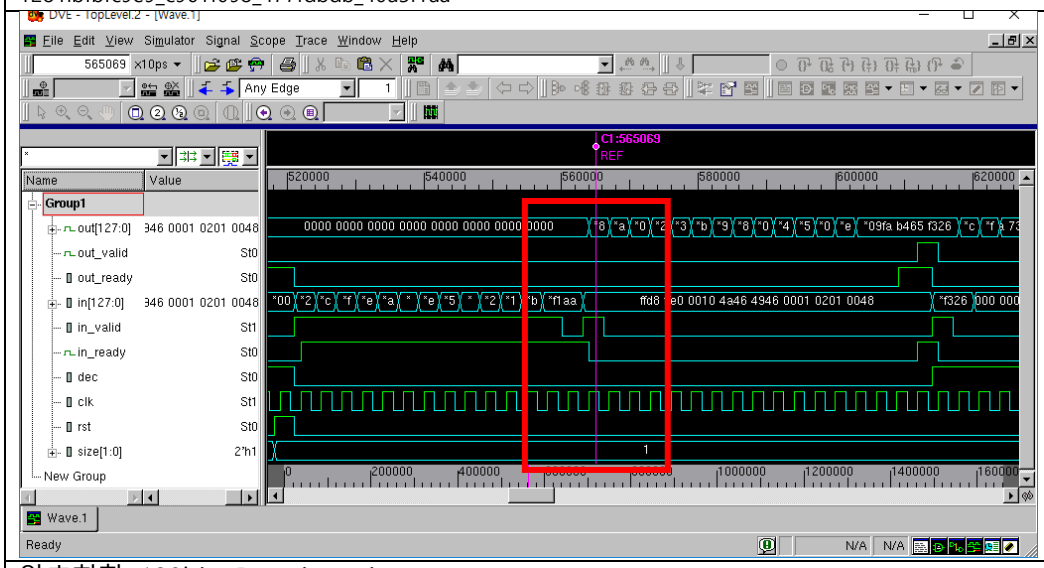
Output :
128'hffd8ffe0_00104a46_49460001_02010048

Size = 1, 192 bits key.



192bits Subkey insertion. (총 13개 Subkey insertion.)

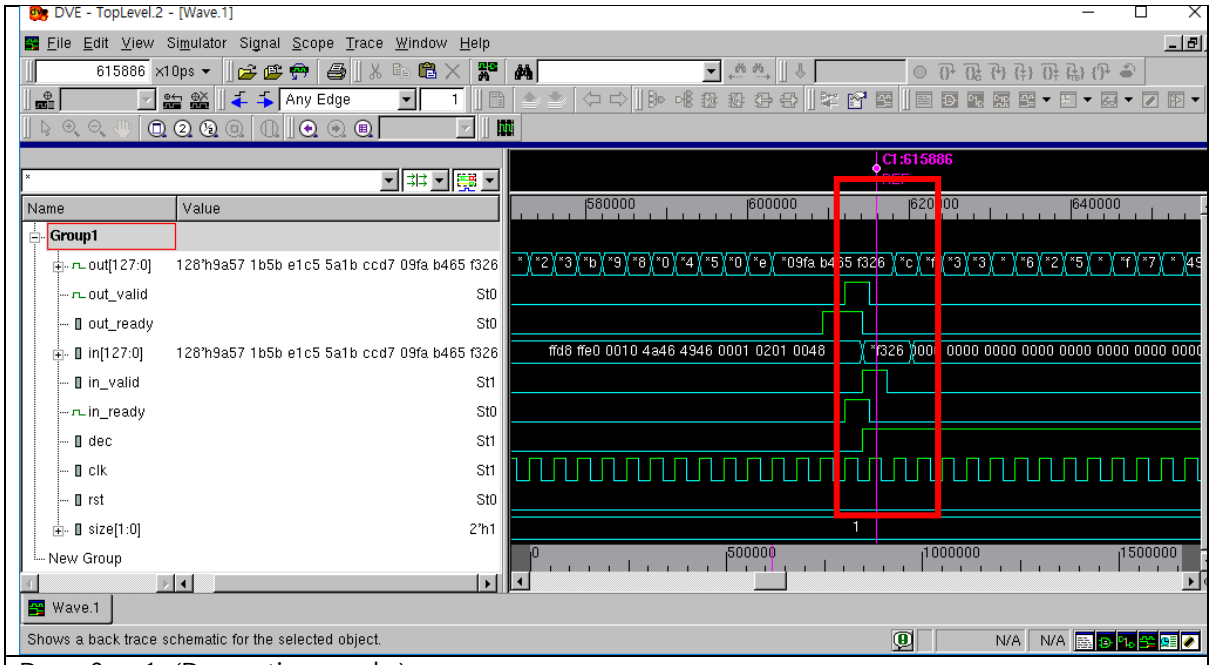
128'h00010000_011a0005_00000001_00000062
128'h00000000_69010000_7d6263f9_7c7863fc
128'h7c7863fd_7c78639f_7c78639f_1579639f
128'hc999b8a0_b5e1db5c_c999b8a1_b5e1db3e
128'hc999b8a1_dce0db3e_2c200a26_99c1d17a
128'h505869db_e5b9b2e5_2c200a44_f0c0d17a
128'h9e1ed0aa_07df01d0_5787680b_b23edaee
128'h9e1ed0aa_6ede01d0_9362a035_94bda1e5
128'hc33ac9ee_71041300_ef1ac3aa_81c4c27a
128'haf477a39_3bfadbdc_f8c01232_89c40132
128'h66dec298_e71a00e2_4d24e2ad_76de3971
128'h8e1e2b43_07da2a71_6104e8e9_861ee80b
128'hbfbfc9e9_c961f098_477fdbdb_40a5f1aa



암호화할 128bits Data insertion.

128'hffd8ffe0_00104a46_49460001_02010048

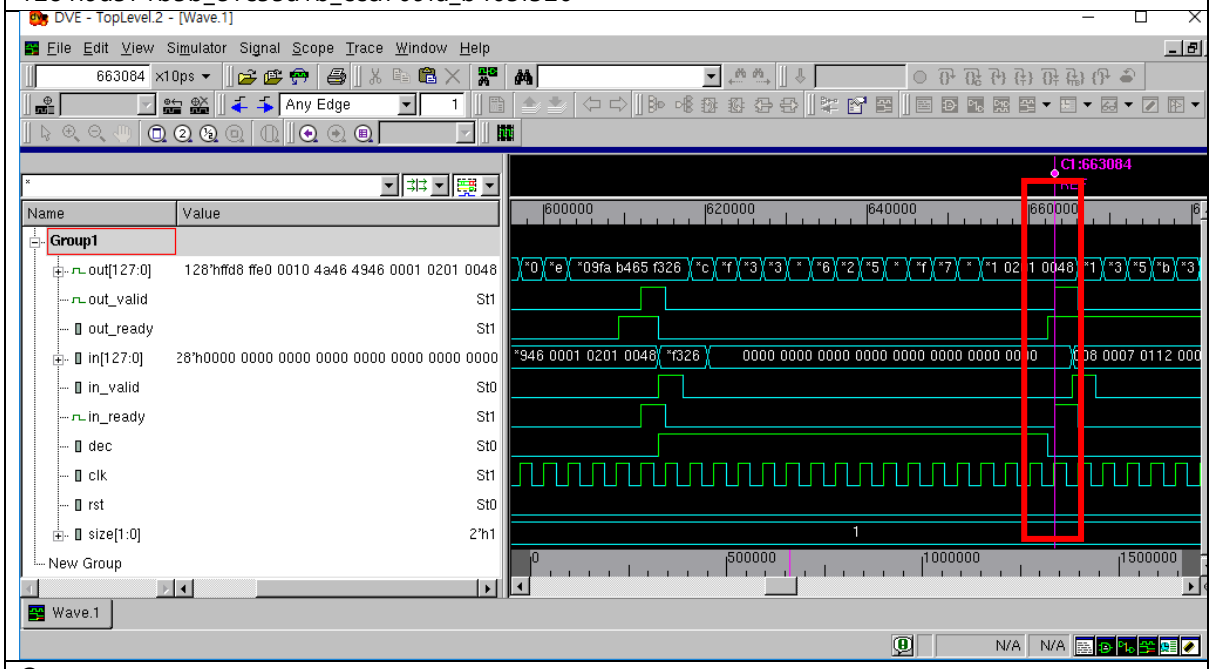
Output :
128'h9a571b5b_e1c55a1b_ccd709fa_b465f326



Dec : 0-> 1. (Decryption mode.)

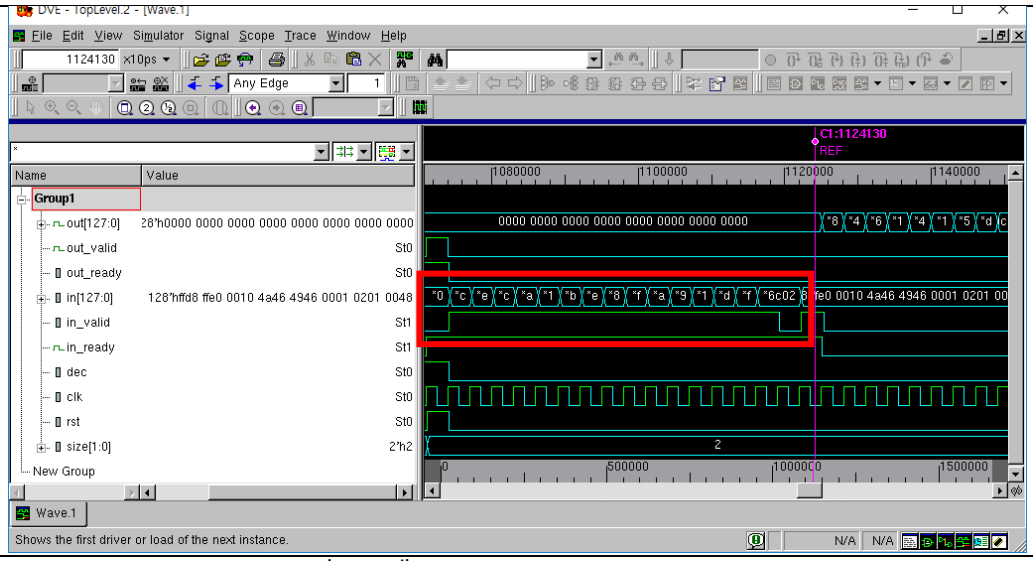
input으로 방금 나왔던 output 을 입력.

Input :
128'h9a571b5b_e1c55a1b_ccd709fa_b465f326



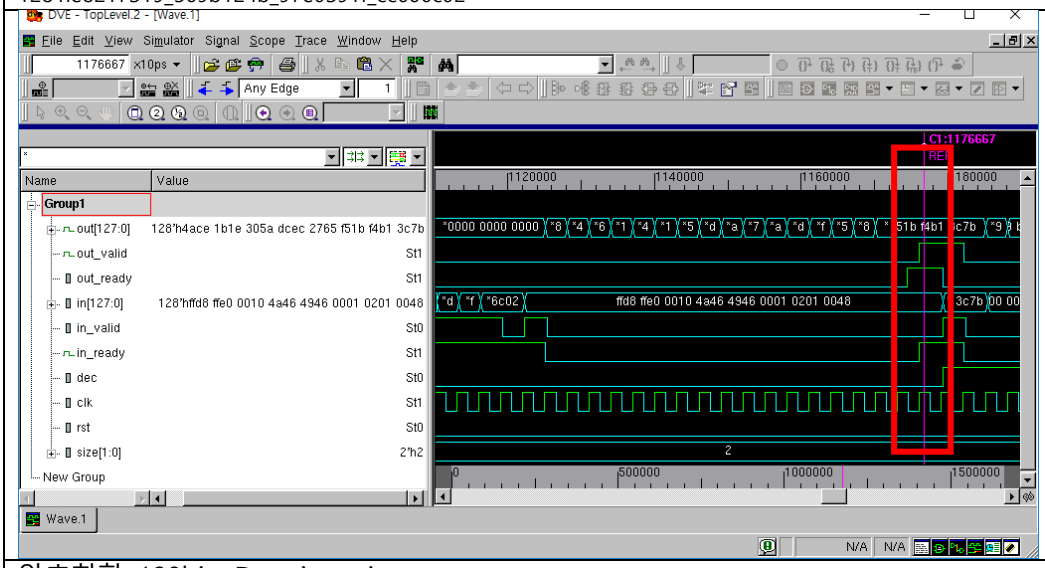
Output :
128'hffd8ffe0_00104a46_49460001_02010048

Size = 2, 256 bits key.



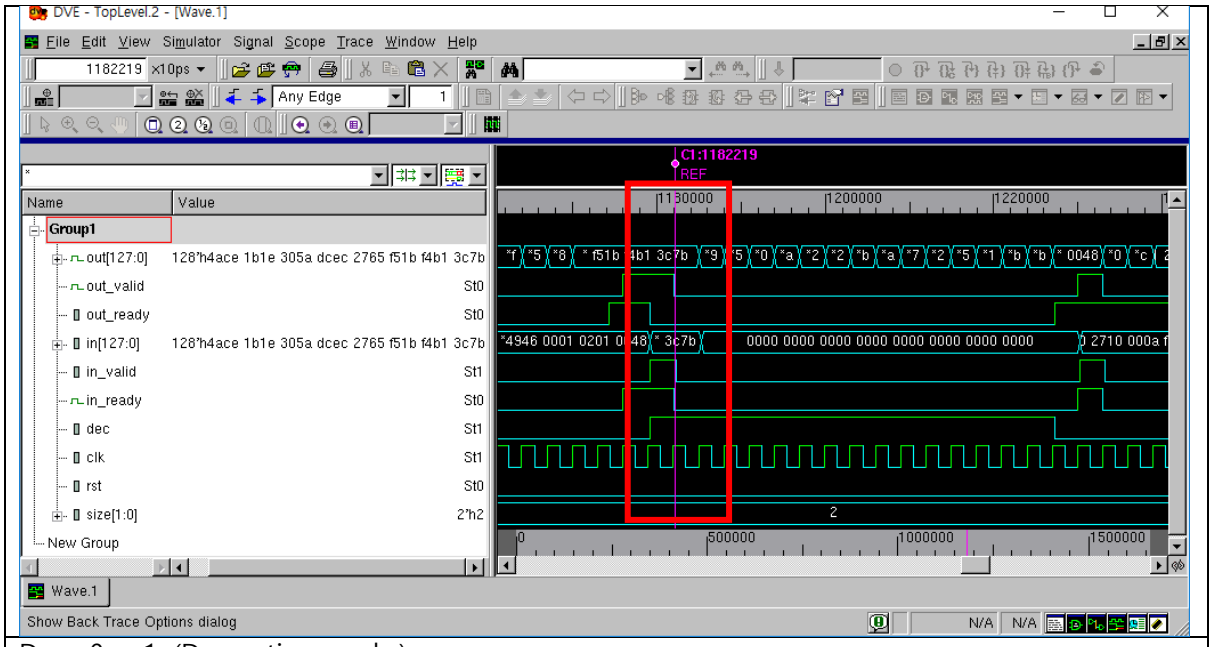
256bits Subkey insertion. (총 15개 Subkey insertion.)

128'h00000001_00020000_01310002_0000001c
128'h00000072_01320002_00000014_0000008e
128'h62631962_62611962_63501960_6350197c
128'hfb53d462_fa61d460_fa61d474_fa61d4fa
128'h8f2b344f_ed4a2d2d_8e1a344d_ed4a2d31
128'hae850ca5_54e4d8c5_ae850cb1_54e4d84b
128'he24a876f_0f00aa42_811a9e0f_6c50b33e
128'hfed66117_aa32b9d2_04b7b563_50536d28
128'h0776b33c_0876197e_896c8771_e53c344f
128'h273d7993_8d0fc041_89b87522_d9eb180a
128'hfedbd409_f6adcd77_7fc14a06_9afd7e49
128'h9f698aa8_12664ae9_9bde3fcb_423527c1
128'h4817ac25_beba6152_c17b2b54_5b86551d
128'ha62d760c_b44b3ce5_2f95032e_6da024ef
128'he8217319_569b124b_97e0391f_cc666c02



암호화할 128bits Data insertion.
128'hffd8ffe0_00104a46_49460001_02010048

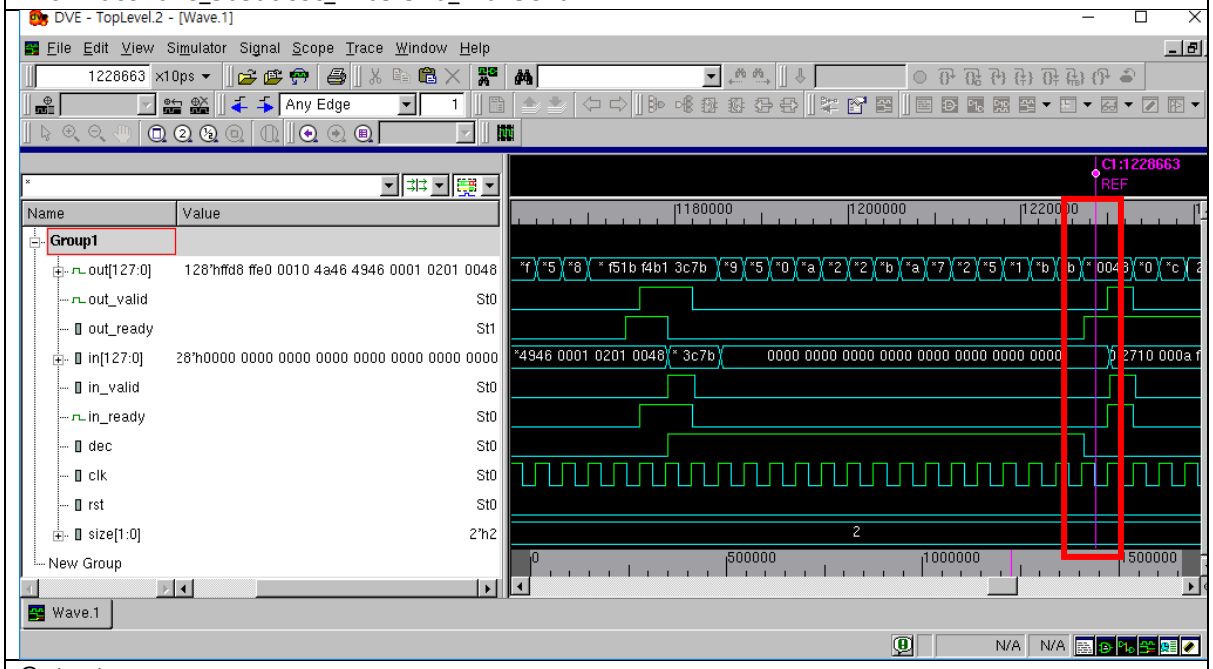
Output :
128'h4ace1b1e_305adcec_2765f51b_f4b13c7b



Dec : 0-> 1. (Decryption mode.)

input으로 방금 나왔던 output 을 입력.

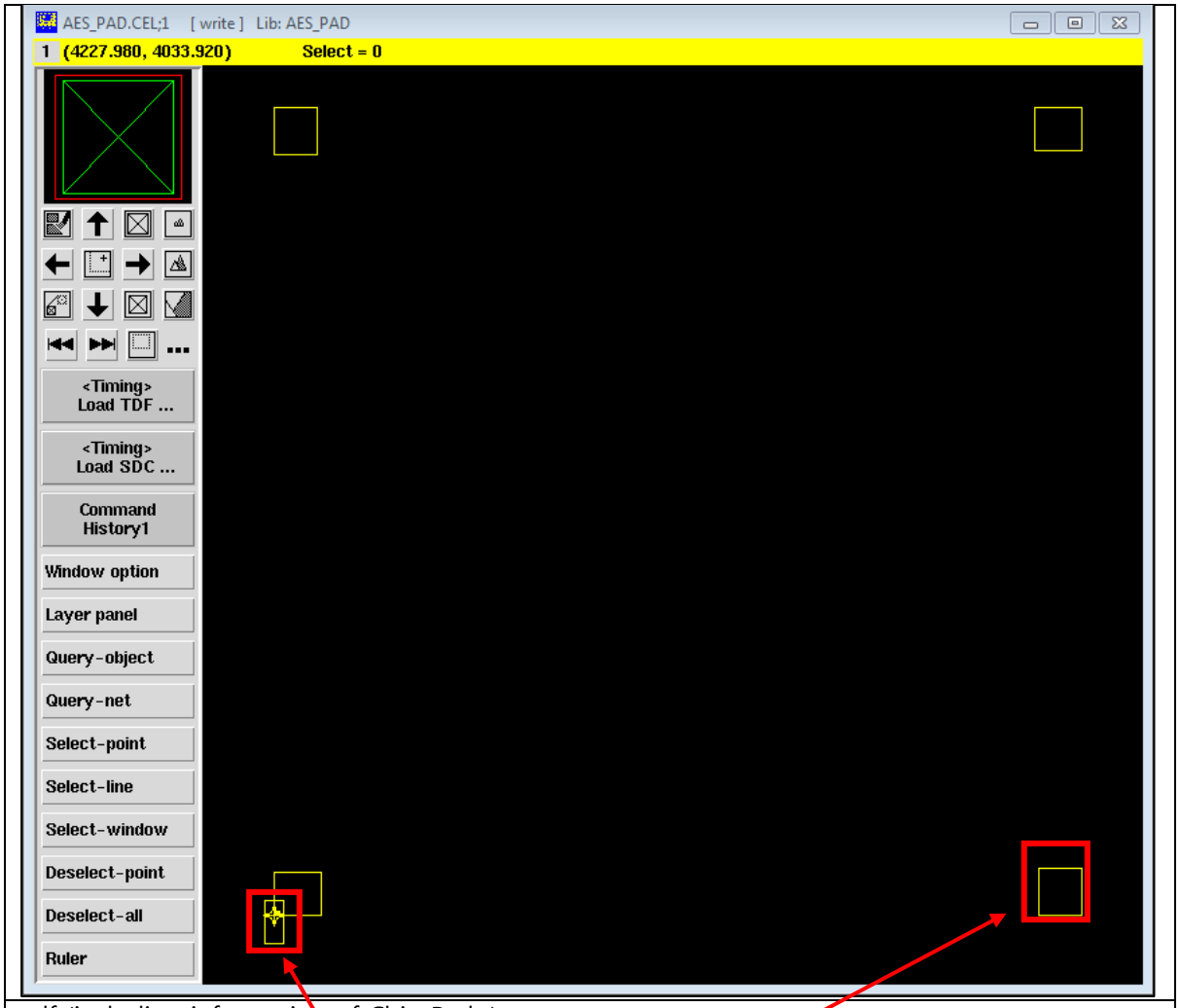
Input :
128'h4ace1b1e_305adcec_2765f51b_f4b13c7b



Output :
128'hffd8ffe0_00104a46_49460001_02010048

- Astro(Place & Route)

ASTRO Tool 을 이용하여 cell을 Place 하고 Routing 한다.



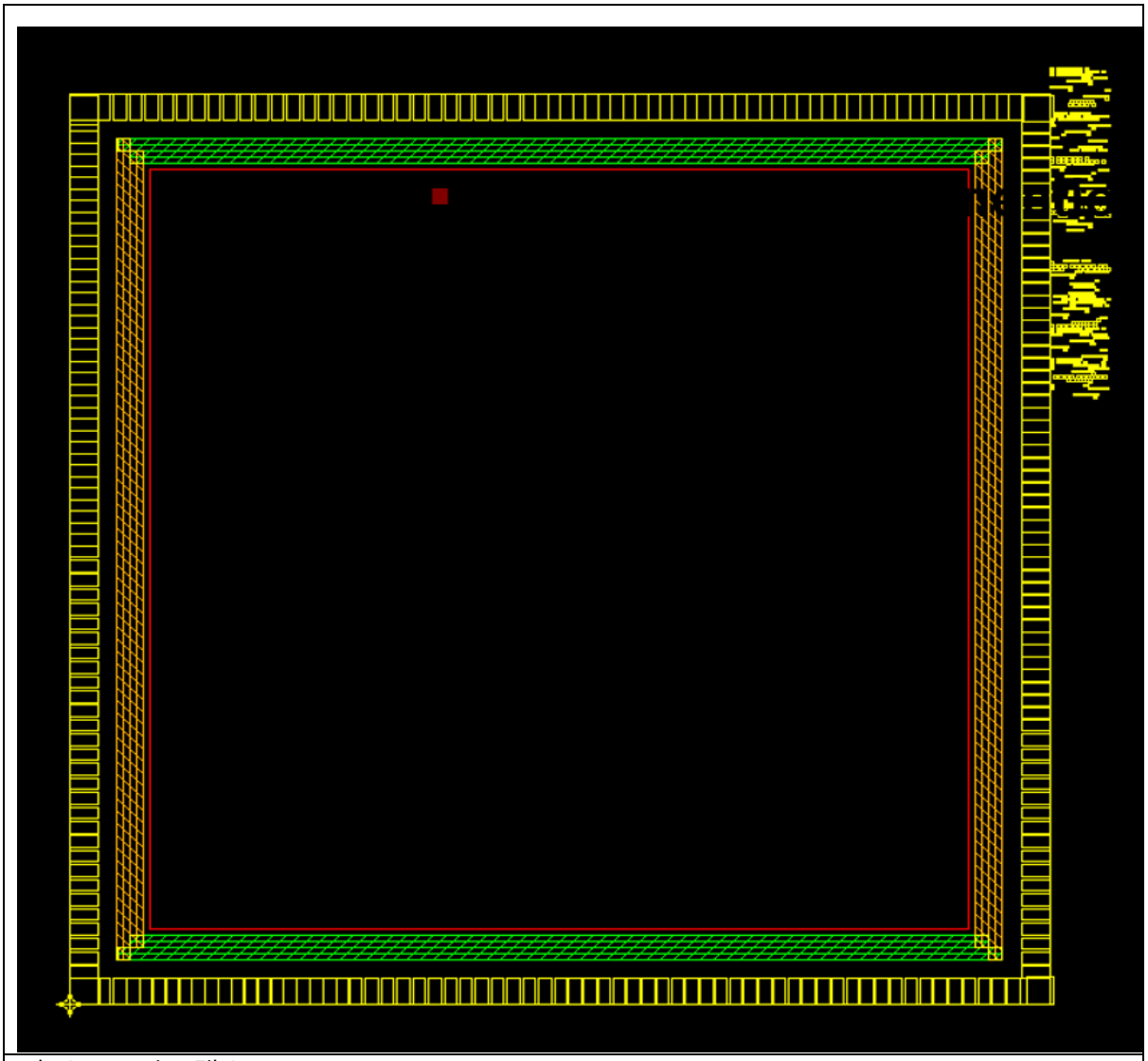
.tdf (including information of Chip Pads.)
[/Tools/Library/Samsung013/Astro_PHA_lib/TECH/padplace_090803_L13_68um.tdf]

➔ 삼성 0.13um 공정에서 제공하는 208pin chip pad 정보.

위 SDC, TDF 파일을 모두 Load 한 이후에 출력되는 화면이다.

사각형으로 배치된 4개는 Chip Pad의 꼭지점을 나타내며,
원점 근처에 직사각형 폴리곤은 Cell 을 나타낸다.

- Floor Planning

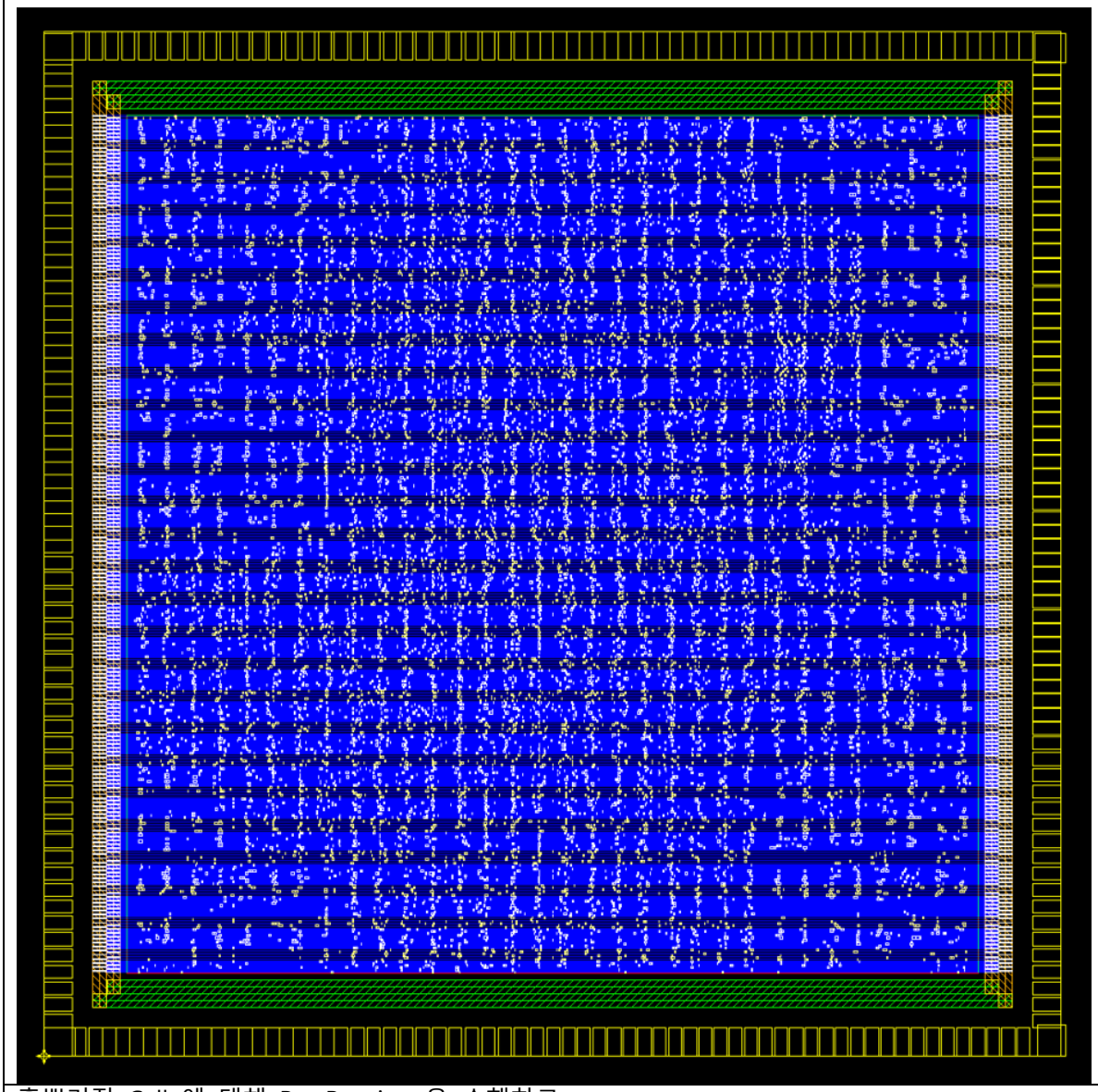


sdc (constraint File)
[AES_ERC_PAD.sdc]
➔ RTL Synthesis 이후에 함께 출력되는 파일.
SDC 파일을 통해 생성된 Cell을 chip Area에 흩뿌린다.
Floor Planner 를 통해 Chip Space 생성.
총 208 pin 의 PADS 가 chip 가장 자리에 잡았으며,
흩뿌려진 전체 Cell의 크기는 Chip 내부에 붉은색 사각형으로 나타난다.

위와 같이 붉은색 사각형이 Chip 내부 영역에 형성되어 있다.

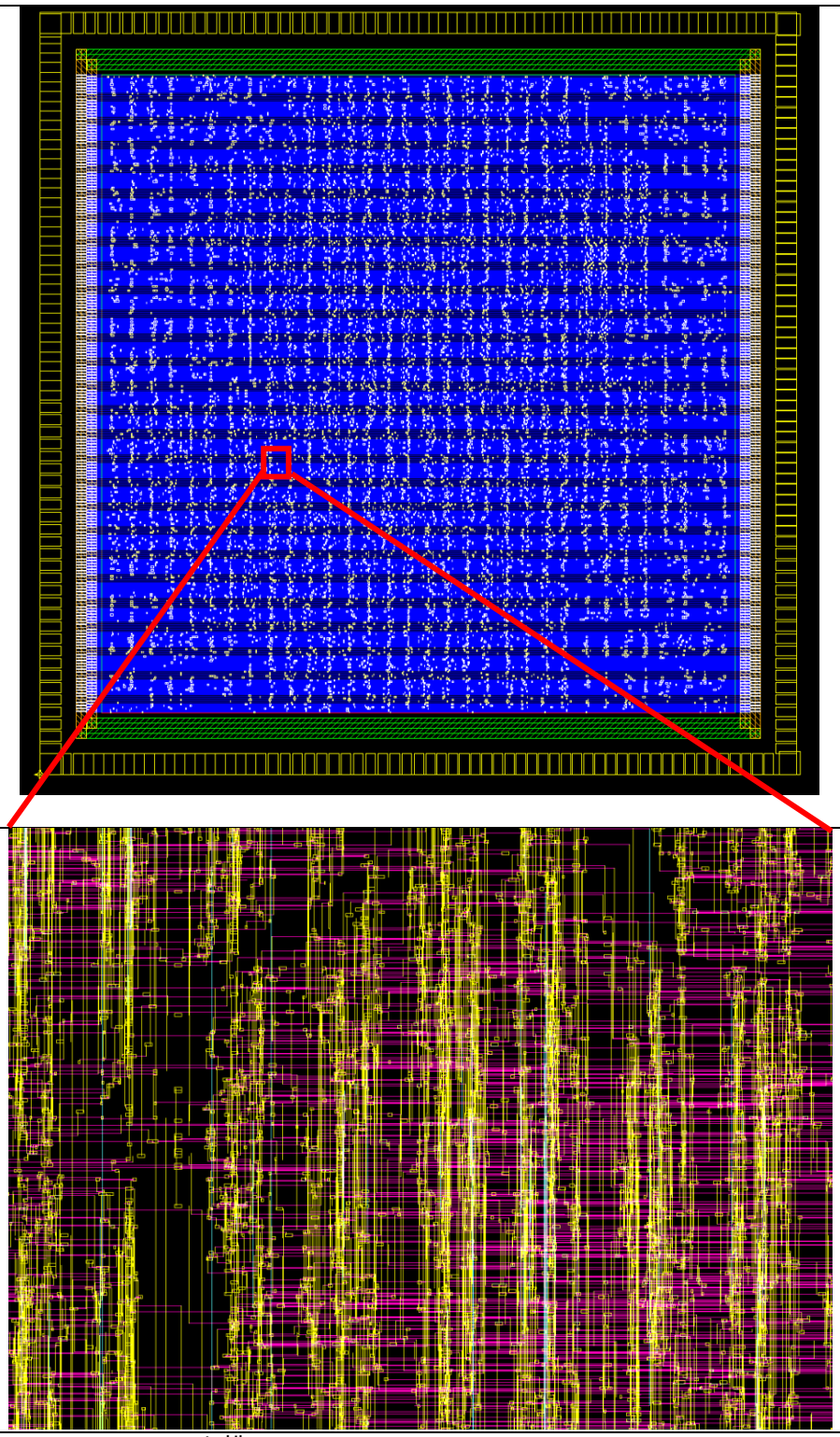
이후 GND, VDD 를 위한 Power Ring을 형성한다.

- Pre-Routing & Standard Cell



흩뿌려진 Cell 에 대해 Pre-Routing 을 수행하고,
Standard Cell 을 mapping 함.

- Global / Detail Routing



이후 Global, Detail Routing 수행.

아래 사진은 Routing 과정 수행 뒤에 특정 부분을 확대한 것이다.