AES
ASIC-assignment

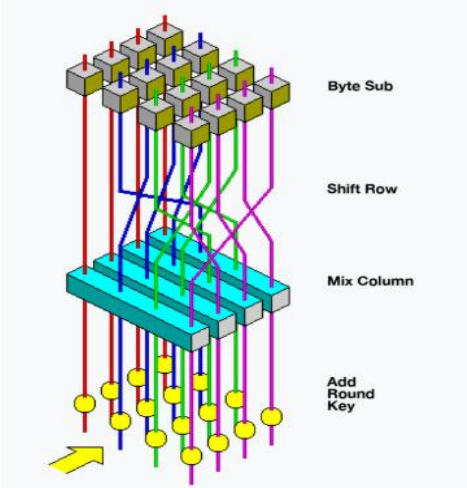
Teams Members:

Youssef Khaled
Youssef Ashraf
Mohamed Adel Abdelrahmen
Marwan Khaled
Mostafa Yousry
Ziad Emad

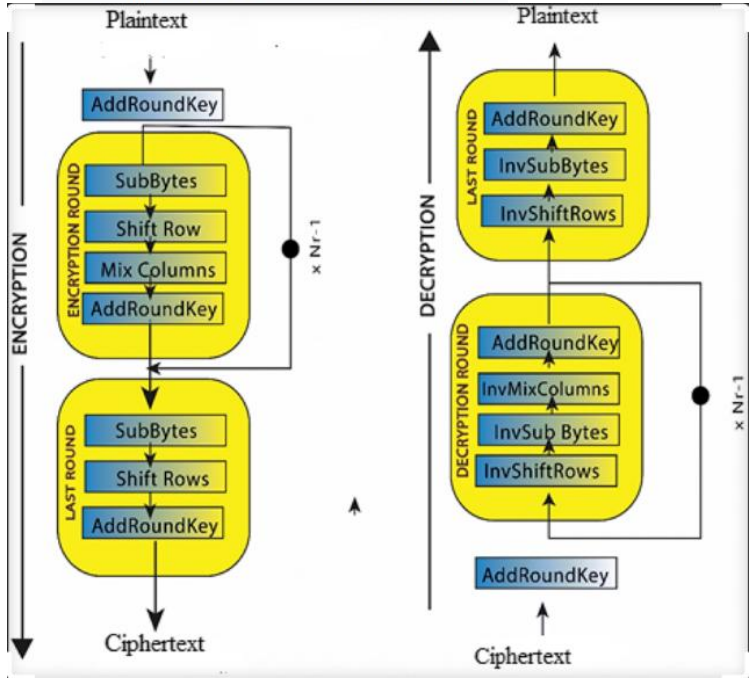
Eng. Mohamed Ewais

AES Encryption Architecture

- AES (Advanced Encryption Standard) is a symmetric-key block cipher.
- Works on 128-bit blocks of plaintext. (could be 192,256)
- Uses a 128-bit cipher key (AES-128).
- Performs 10 rounds of transformation:
  1. SubBytes: byte substitution using an S-box
  2. ShiftRows: circular row shifting in the state matrix.
  3. MixColumns: mixes bytes in each column (except last rount).
  4. AddRoundKey: XOR state with round key.
- First round: only AddRoundKey.
- Last round: no MixColumns.
- Widely used in: SSL/TLS, secure storage, WI_FI encryption.



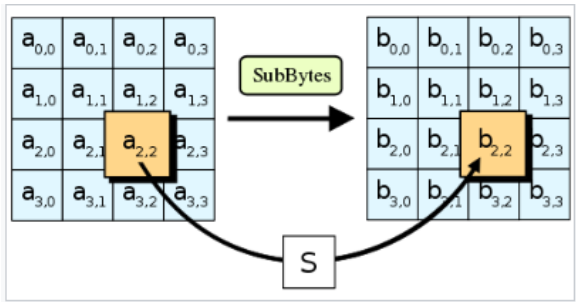
Visualization of the AES round function



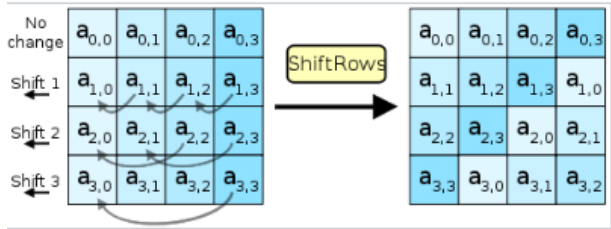
Algorithm

High-level description of the algorithm [edit]

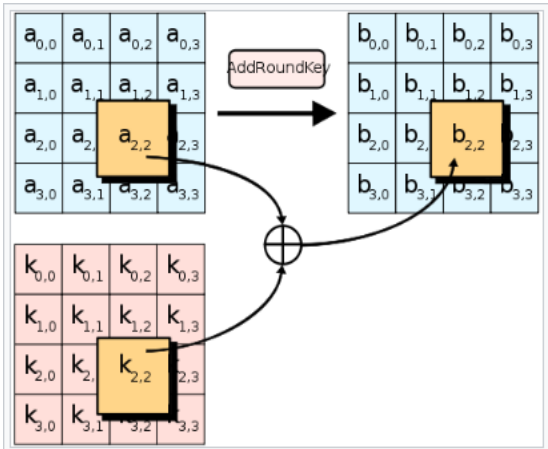
1. `KeyExpansion` – round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial round key addition:
    1. `AddRoundKey` – each byte of the state is combined with a byte of the round key using bitwise xor.
3. 9, 11 or 13 rounds:
    1. `SubBytes` – a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. `ShiftRows` – a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. `MixColumns` – a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. `AddRoundKey`
4. Final round (making 10, 12 or 14 rounds in total):
    1. `SubBytes`
    2. `ShiftRows`
    3. `AddRoundKey`



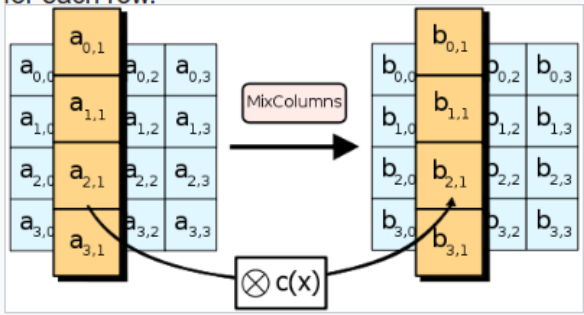
In the `SubBytes` step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.



In the `ShiftRows` step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs incrementally for each row.



In the `AddRoundKey` step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).



In the `MixColumns` step, each column of the state is multiplied with a fixed polynomial $c(x)$.

ASIC implementation overview

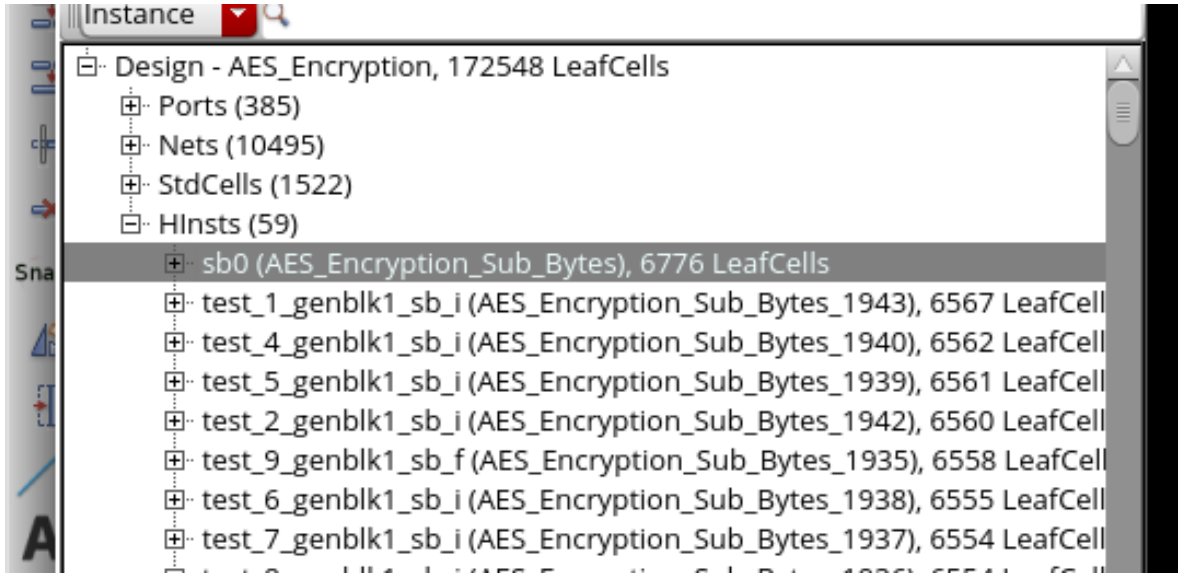
- **Objective:**
- Implement AES-128 encryption as a physical ASIC design.
- Use synthesis, placement, and routing to generate GDSII layout.
- **RTL Design Source:**
- Open-source pipelined AES RTL: https://github.com/aneels3/AES-128/tree/master/AES_Encryption
- **Design Steps:**
- RTL analysis and synthesis.
- Floorplanning and power planning.
- Placement and clock tree synthesis (CTS).
- Routing and DRC/LVS checks.
- Timing and power analysis.
- **Tools Used:**
- ADflow (custom internal flow by Analog)
- Optional: Open-source flow using OpenLane (Yosys, Magic, KLayout, etc.)
- **Design Goal:**
- Generate area-optimized, timing-accurate ASIC layout.
- Analyze physical metrics (area, power, WNS, utilization, etc.)

Post-Syn & Post-Route

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

1- Block dimensions (Width X Height) in um : 280x280 (GUI Missurment)
2- Post-Syn instances count : 91844 (AES_Encryption_instance_count.rep)
3- Post-Syn registers count : 3712 (generate_reports_qor.rep)
4- Post-Route instances count - Phy: 96323 (AES_Encryption_instance_count.rep)
5- Post-Route registers count: 3712 (llength [get_db [get_db [get_db hinsts] .insts] -if .is_flop])
6- Post-Route utilization-Phy : 73.943% (AES_Encryption.main.htm.ascii)

7,8 - module hierarchical instance with the largest leaf cells count , its count , GUI for it : 6776



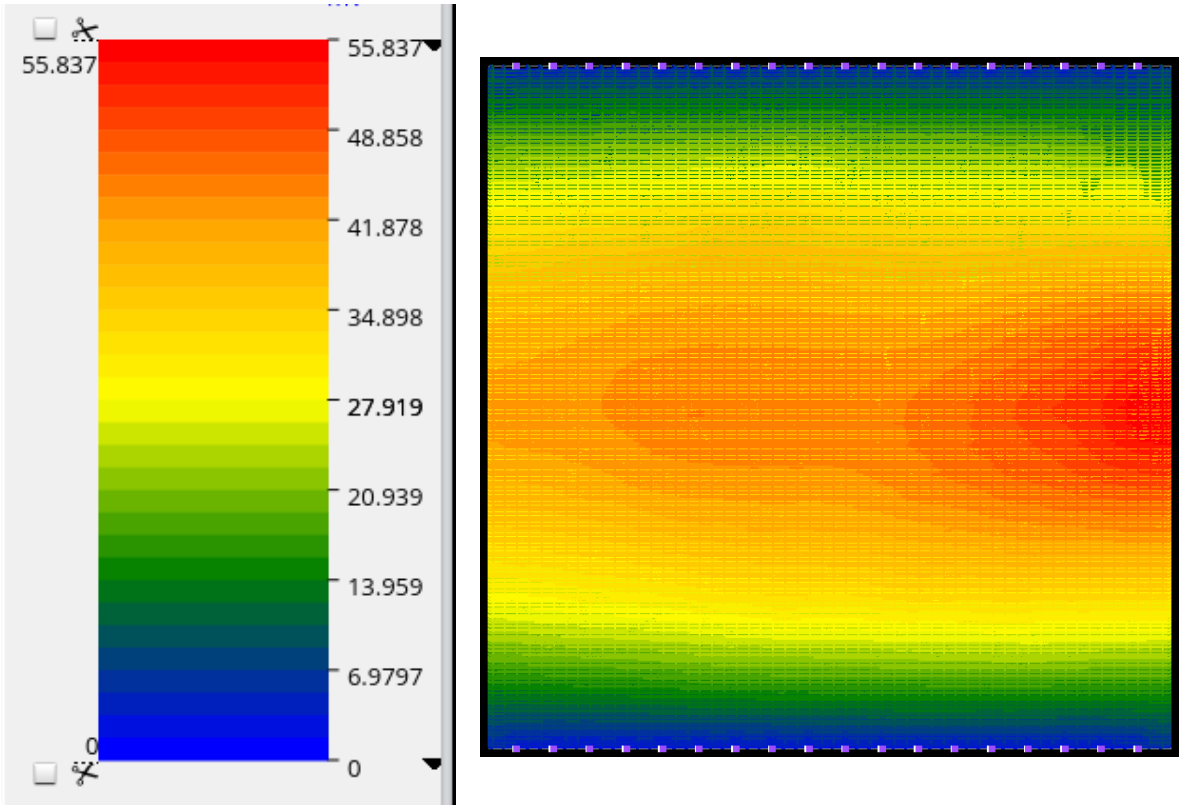
Power and IR drop analysis

9- leakage power using vectorless : 1.22566334 ,1.8309%, (AES_Encryption.vectorless_sdc.summary.power.rep)

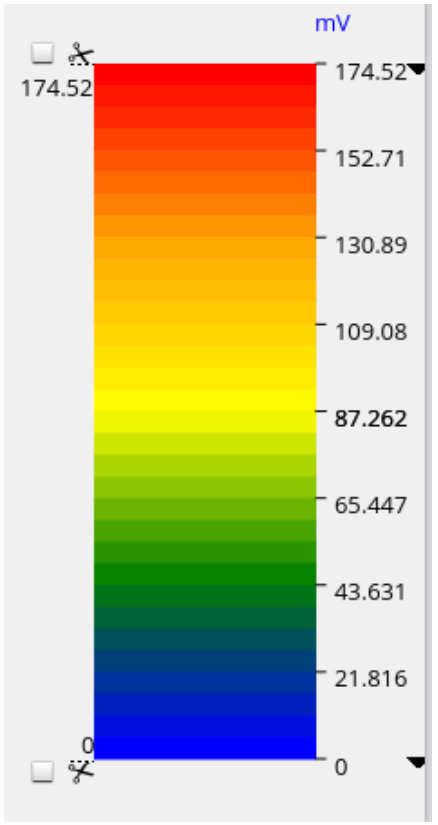
10- dynamic power using vectorbased : 62.9 ,98.3%, (AES_Encryption.Pnr.summary.power.rep)

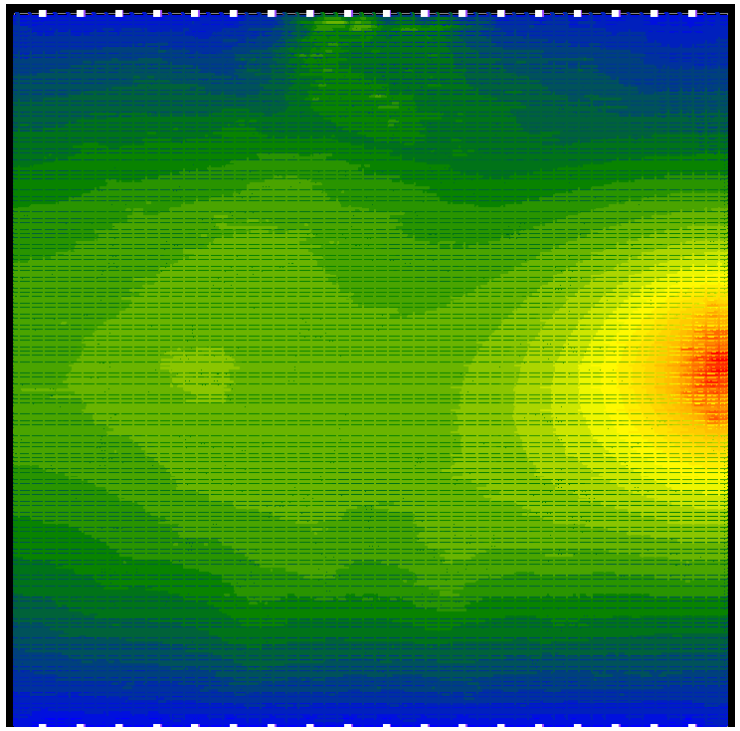
11,12,13,14 - static IR drop in mV, screen shot Hotspot (vectorless)-(vectorbased) :

vectorless



vectorbased





DRC , LVS , formality, STA

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

17-DRC :

```
26038    RULECHECK GRCLC.Cx.DEN.Cy.2_C3 ......... TOTAL Result Count = 16      (16)
26039    RULECHECK GRCLC.Cx.DEN.5_C4 ............ TOTAL Result Count = 22      (22)
26040    RULECHECK GRCLC.Cx.DEN.8_C4 ............ TOTAL Result Count = 1       (1)
26041    RULECHECK GRSPECIAL_GDS_M2_E1_DP_OUT ... TOTAL Result Count = 214363 (214363)
26042    RULECHECK GRSPECIAL_GDS_M2_E2_DP_OUT ... TOTAL Result Count = 205850 (205850)
26043    RULECHECK GRAUX3.C.9 ................... TOTAL Result Count = 729     (729)
26044    RULECHECK GRCxCFILL.W.1_C4 ............. TOTAL Result Count = 98      (98)
```

18- LVS:

```
        #       ###################
      #         #                 #
    #   #       #     CORRECT     #
     # #        #                 #
      #         ###################
```

19-formality status for rtl vs post-syn netlist

```
       Power Grid Comparison |N/A
        Power Intent Compare |N/A
   Supply Power Consistency |N/A
Retention Power Consistency |N/A
     Compare Power Crossing |N/A
             LEC Comparison |PASS
         Flatten Comparison |N/A
    Hierarchical Comparison |PASS
              Logfile Lines |58654
               Logfile Name |beq_rtl_v_syninter.log
```

20-formality status for post-syn vs post-route netlist :

```
        LEC Comparison |PASS
    Flatten Comparison |PASS
```

21- Report post-route STA results showing WNS/TNS for setup/hold analysis:

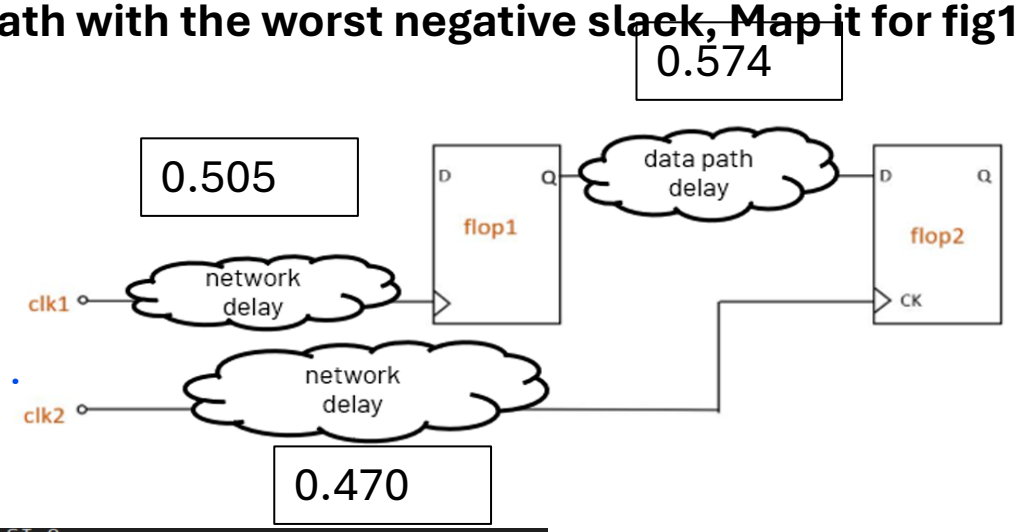
# HOLD	NSIGMA	WNS	TNS	FEP
View : func_tt_typvzb_25_typical_hold	3.000	-0.209	-60.312	384
Group : in2reg	3.000	-0.209	-60.312	384
Group : reg2reg	3.000	0.009	0.0	0
Group : in2out	3.000	N/A	N/A	0
Group : reg2out	3.000	0.782	0.000	0

# SETUP	NSIGMA	WNS	TNS	FEP
View : func_tt_typvzb_25_typical_setup	3.000	-0.143	-16.035	128
Group : in2reg	3.000	0.588	0.0	0
Group : reg2reg	3.000	0.313	0.0	0
Group : in2out	3.000	N/A	N/A	0
Group : reg2out	3.000	-0.143	-16.035	128

STA & DFT

22,23-Report detailed timing path for the reg2reg path with the worst negative slack, Map it for fig1

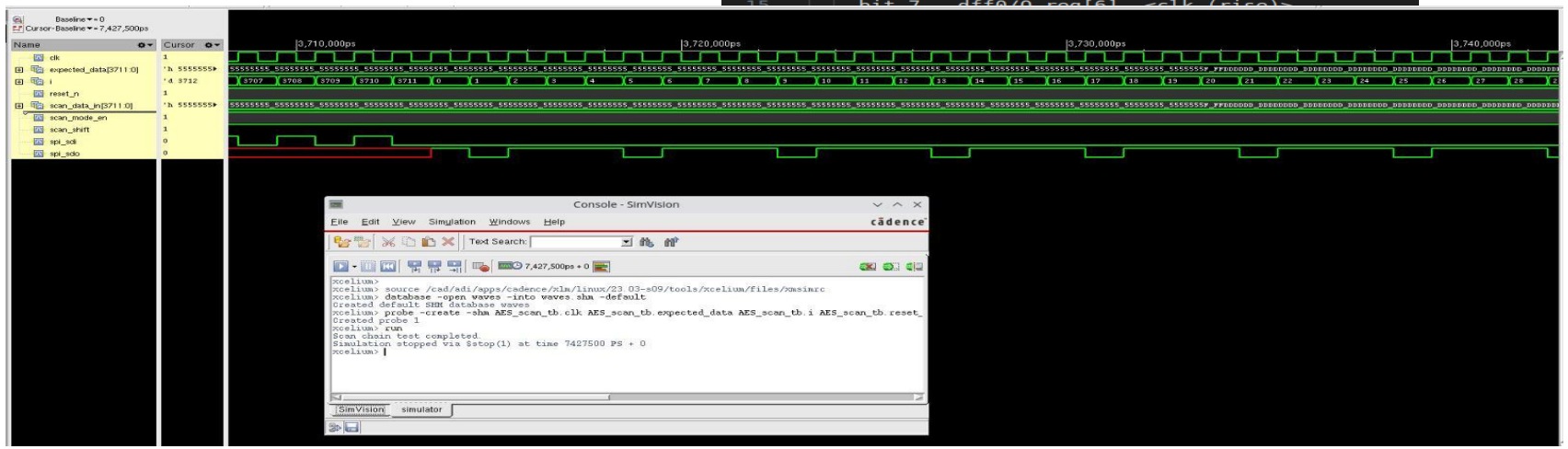
```
        View: func_tt_typvzb_25_typical_setup
       Group: CLK
  Startpoint: (R) test_2_genblk1_r_i/key_out_reg_27_/CK
       Clock: (R) CLK
    Endpoint: (R) test_3_genblk1_r_i/r_out_reg_1_/D
       Clock: (R) CLK
     N-Sigma: 3.000

                Capture                          Launch
  Clock Edge:+    1.000                           0.000
  Src Latency:+   0.038  (0.038,     0.000)       0.038  (0.038, 0.000)
  Net Latency:+   0.432  (0.445,     0.005) (P)   0.467  (0.451, 0.005) (P)
      Arrival:=   1.470  (1.484,     0.005)       0.505  (0.489, 0.005)

        Setup:-   0.011  (0.007,     0.001)
  Uncertainty:-   0.100
  Cppr Adjust:+   0.022  (0.001,     0.007)
Required Time:=   1.393  (1.377, 0.005(-))
 Launch Clock:-   0.505  (0.489,     0.005)
    Data Path:+   0.574  (0.561,     0.004)
        Slack:=   0.313  (0.327,     0.005)
```



24-Report the scan chain length :3712

```
Chain 1: SI_0
  scan_in:       spi_sdi
  scan_out:      spi_sdo
  shift_enable: scan_shift (active high)
  clock_domain: spi_clk (edge: rise)
  length: 3712
    bit 1    dff0/Q_reg[0]   <clk (rise)>
    bit 2    dff0/Q_reg[1]   <clk (rise)>
    bit 3    dff0/Q_reg[2]   <clk (rise)>
    bit 4    dff0/Q_reg[3]   <clk (rise)>
    bit 5    dff0/Q_reg[4]   <clk (rise)>
    bit 6    dff0/Q_reg[5]   <clk (rise)>
```

25-



OpenLane

- Technology and std cell used skywater 130nm , sky130_fd_sc_hd

1) **DIE AREA 2225.135 µm × 2235.855 µm**

```
1 VERSION 5.8 ;
2 DIVIDERCHAR "/" ;
3 BUSBITCHARS "[]" ;
4 DESIGN AES_Encryption ;
5 UNITS DISTANCE MICRONS 1000 ;
6 DIEAREA ( 0 0 ) ( 2225135 2235855 ) ;
7 ROW ROW_0 unithd 5520 10880 N DO 4813 BY 1 STEP 460 0 ;
```

2) **Post syn instances count**

```
Number of cells:                141332
```

from 1-synthesis.AREA 0.stat.rpt

3) **Post-syn registers count**

```
Number of cells:                262104
```

from 1-synthesis_dff.stat

4) **post-route instances count (excluding physical cells)**

```
#scanned instances     = 129438
#unique  instances     = 584
```

From 21-detailed.log

```
[INFO GRT-0111] Final number of vias: 128360
```

5) **post-route registers count**

717,017

```
#scanned instances     = 717017
#unique  instances     = 247
#stdCellGenAp          = 6598
```

6) **post-route utilization (excluding physical cells)**

```
2147 ===========================================
2148 Design area 1508826 u^2 33% utilization.
2149 area report end
```

OpenLane

9,10) Power report

Leakage and dynamic power

```
 report_power
=======================================================================
Group                  Internal  Switching    Leakage      Total
                          Power      Power      Power      Power (Watts)
-----------------------------------------------------------------------
Sequential             7.74e-03   1.67e-03   3.15e-08   9.41e-03  20.8%
Combinational          1.59e-02   2.00e-02   4.16e-07   3.58e-02  79.2%
Macro                  0.00e+00   0.00e+00   0.00e+00   0.00e+00   0.0%
Pad                    0.00e+00   0.00e+00   0.00e+00   0.00e+00   0.0%
-----------------------------------------------------------------------
Total                  2.36e-02   2.16e-02   4.48e-07   4.53e-02 100.0%
                          52.2%      47.8%       0.0%
power_report_end
```

17) DRC violations

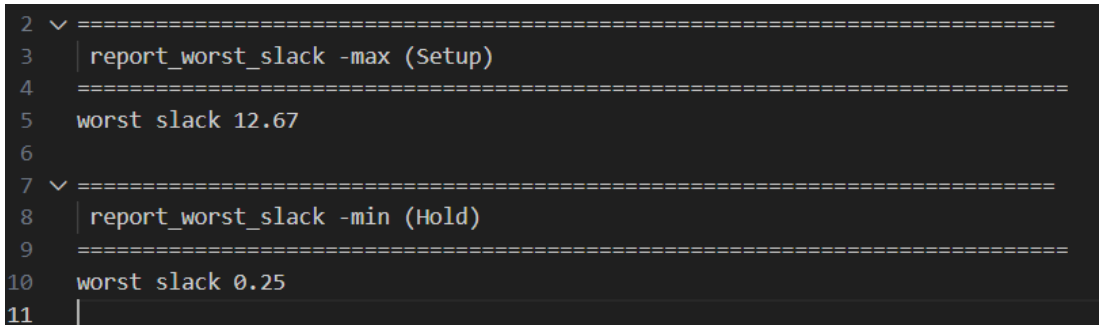
There are a lot of antenna violation after the global routing (filler will solve most of them)

21) post-route STA result showing WNS/TNS for setup/hold analysis

```
-----------------------------------------------------------------------
 report_tns
=======================================================================
tns -2.24
tns_report_end
wns_report

=======================================================================
 report_wns
=======================================================================
wns -2.24
wns_report_end
worst_slack
```

```
=================================================
 report_worst_slack -min (Hold)
=================================================
worst slack 0.24
worst_slack_end
clock_skew
```

OpenLane



ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Results Comparison

	Commercial metrics	ADFLOW
Block Dimensions	2225.135 µm × 2235.855 µm	280x280
- Post-Syn instances count.	141332	91844
- Post-Syn registers count.	262104	3712
- Post-Route instances count.	129438	96323
- Post-Route registers count.	717017	3712
Post-Route utilization- Phy	33%	73.943%
LEAKGE AND DYNAMIC POWER	report_power Group Internal Power Switching Power Leakage Power Total Power (Watts) Sequential 7.74e-03 1.67e-03 3.15e-08 9.41e-03 20.8% Combinational 1.59e-02 2.00e-02 4.16e-07 3.58e-02 79.2% Macro 0.00e+00 0.00e+00 0.00e+00 0.00e+00 0.0% Pad 0.00e+00 0.00e+00 0.00e+00 0.00e+00 0.0% Total 2.36e-02 2.16e-02 4.48e-07 4.53e-02 100.0% 52.2% 47.8% 0.0% power_report_end	1.22566334 ,1.8309%, 62.9 ,98.3%,
WNS (SETUP)	-2.24	-0.143
WNS (HOLD)	0.24	-0.209