ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

AES Encryption Backend Flow Assignment

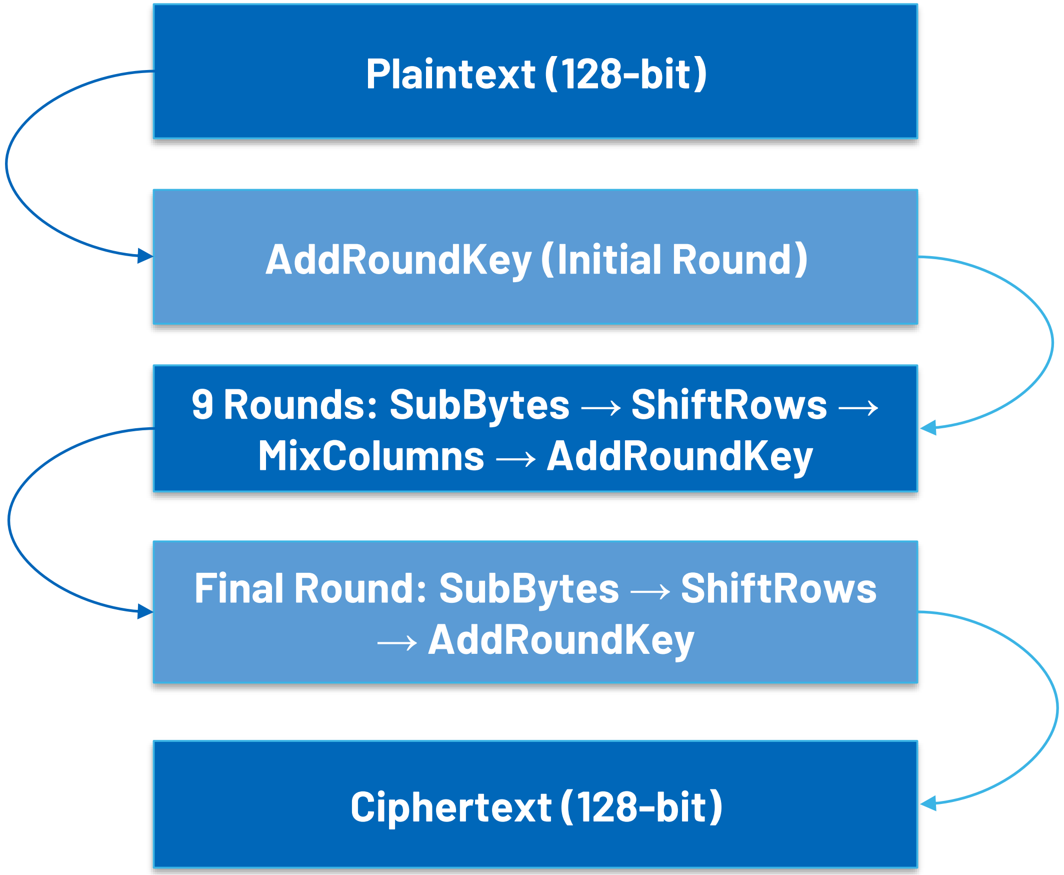
Onsite Part

Team D: Khaled Mohamed, Galal Mohamed, Mohamed Abdel-Hay, Youssef Ahmed, Nadim Abdelrahman, Khaled Ahmed

7 August 2025

AES Encryption Architecture

AES-128 is a symmetric block cipher that encrypts 128-bit plaintext using a 128-bit key over 10 rounds. Each round includes SubBytes, ShiftRows, MixColumns, and AddRoundKey operations. The final round omits MixColumns. Round keys are generated using a separate Key Expansion process.


Plaintext (128-bit)
AddRoundKey (Initial Round)
9 Rounds: SubBytes → ShiftRows → MixColumns → AddRoundKey
Final Round: SubBytes → ShiftRows → AddRoundKey
Ciphertext (128-bit)

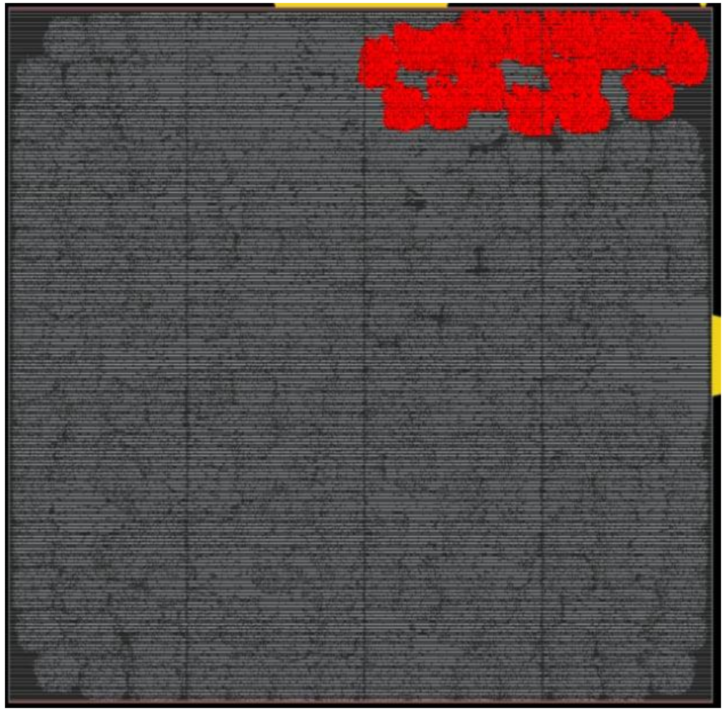
Dimensions & Cells count

Block dimensions= 285 x 285 um^2

	syn	PNR
Library-cells	91844	95991
AND	51279	51677
BUF	81	2818
REGISTERS	3712	3712
INV	17461	18761
NAND	23426	23765
NOR	9515	9653
OR	36483	36629
XNOR	2752	2751
XOR	3968	3839

Post-Route utilization: 73.181%

largest leaf cells count: sb0 (instance of sub bytes) with 6721 leaf cells



Logic cells placement

Power & IR drop

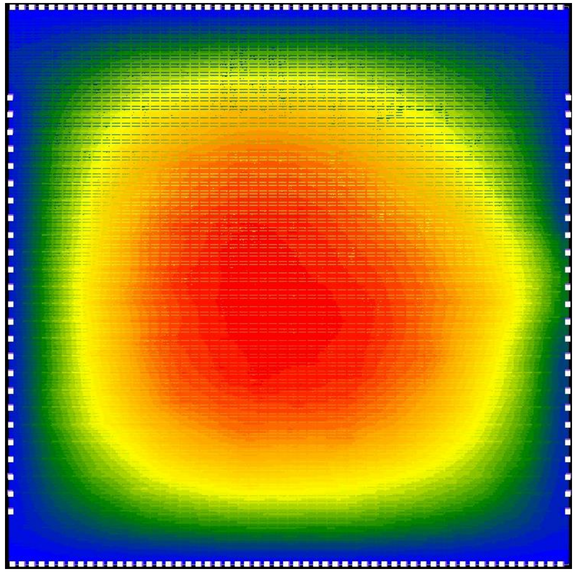
- **Calculate Post-Route leakage power using vectorless analysis**

  Total Leakage Power: 1.21557553 mW 1.8156%

- **Calculate Post-Route dynamic power using vectorbased analysis**

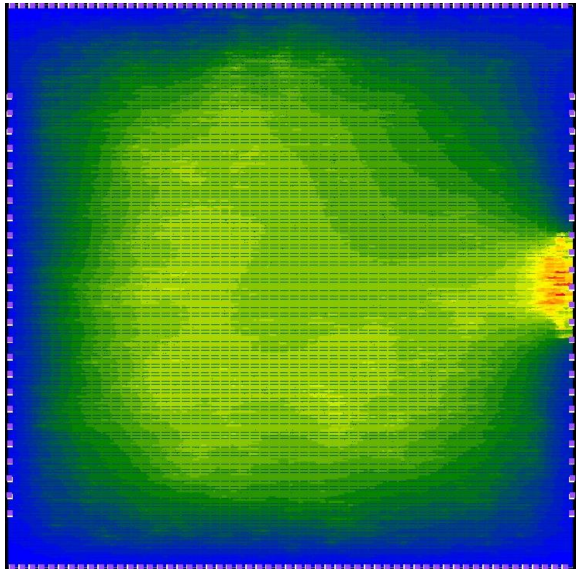
  Total Switching Power: 30.41229120 mW 42.8119%

Static IR drop



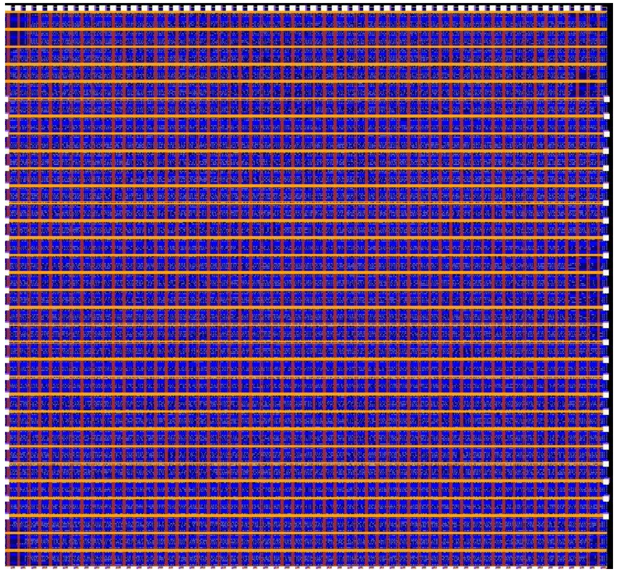
Peak = 22.834 mV

Dynamic IR drop



Peak = 107.58 mV
time window (ns): 192.500 196.500

Voltage sources location



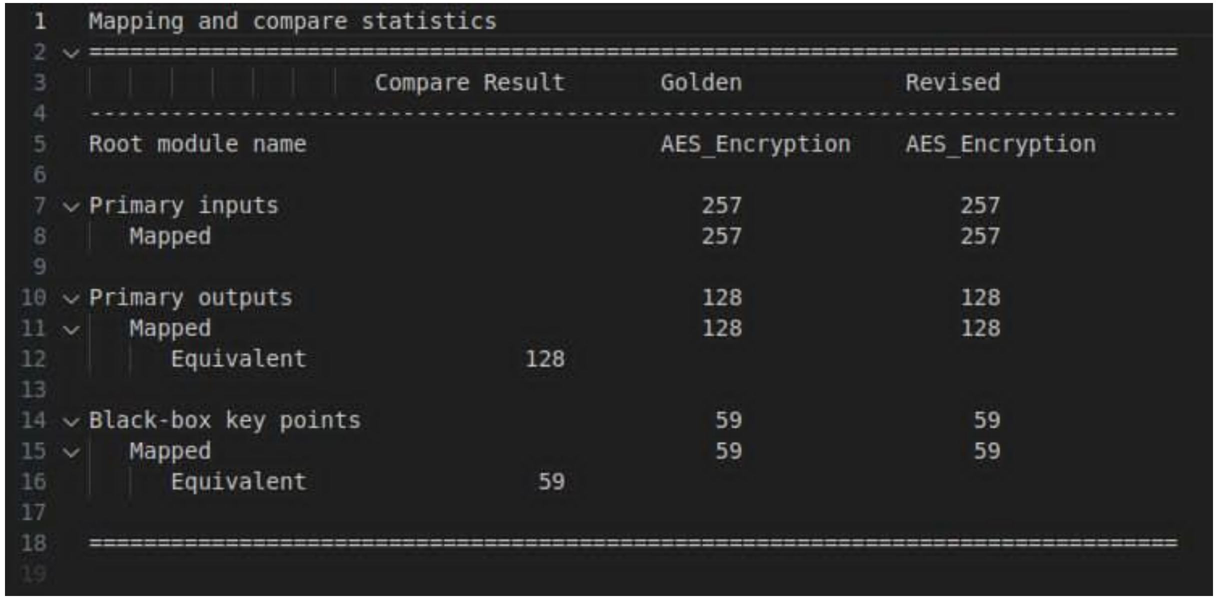
Report formality status

Post-Route Formality check: PASS

DRC violations: RULECHECK GRAUX3.C.9 .... TOTAL Result Count = 980 (980)

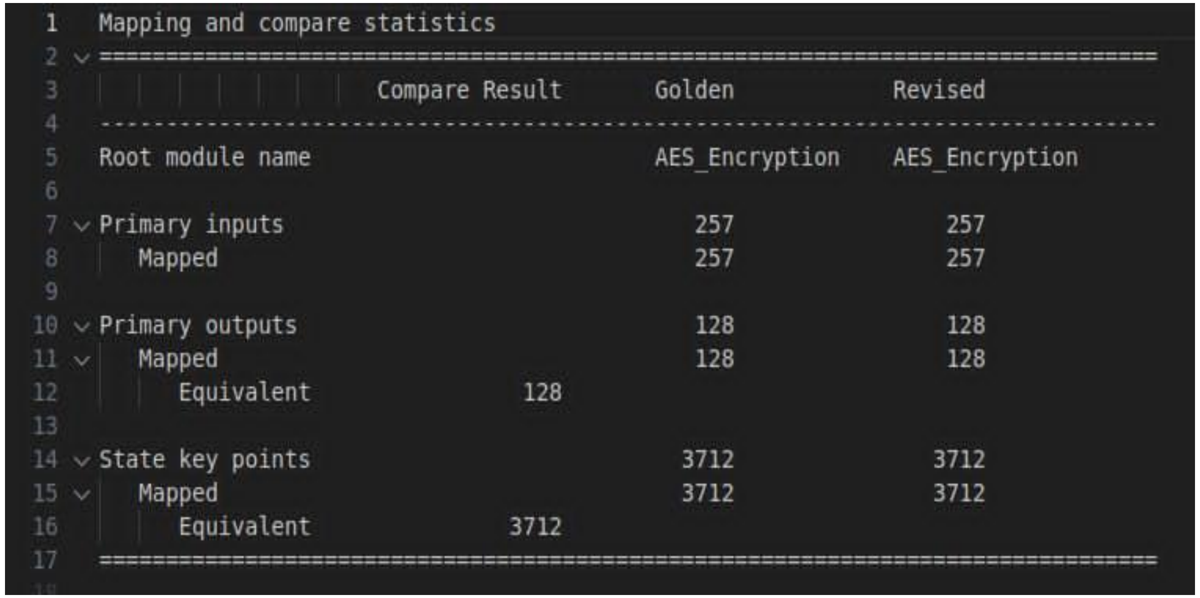
LVS status: PASS

Report formality status for RTL vs post-syn netlist



```
Mapping and compare statistics
=====================================================================================
                    Compare Result        Golden             Revised
-------------------------------------------------------------------------------------
Root module name                          AES_Encryption     AES_Encryption

Primary inputs                               257                257
  Mapped                                     257                257

Primary outputs                              128                128
  Mapped                                     128                128
    Equivalent                128

Black-box key points                          59                 59
  Mapped                                      59                 59
    Equivalent                 59

=====================================================================================
```

Report formality status for post-syn vs post-route netlist.



```
Mapping and compare statistics
=====================================================================================
                    Compare Result        Golden             Revised
-------------------------------------------------------------------------------------
Root module name                          AES_Encryption     AES_Encryption

Primary inputs                               257                257
  Mapped                                     257                257

Primary outputs                              128                128
  Mapped                                     128                128
    Equivalent                128

State key points                            3712               3712
  Mapped                                    3712               3712
    Equivalent               3712
=====================================================================================
```

Report post-route STA results for setup/hold analysis

Setup analysis

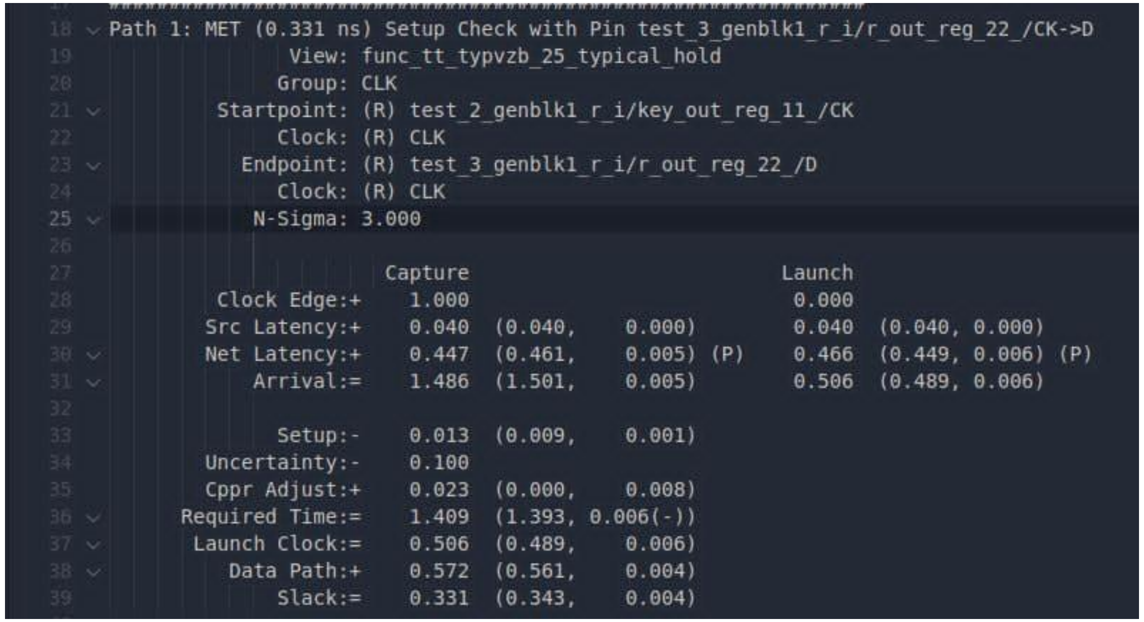
WNS: -0.152 ns, caused by reg2out cipher_out[106],
TNS: -17.279 ns all caused by reg2out

Hold analysis

WNS: -0.214 ns, caused by in2reg r0/key_out_reg_38-/D
TNS: -63.961 ns all caused by in2reg

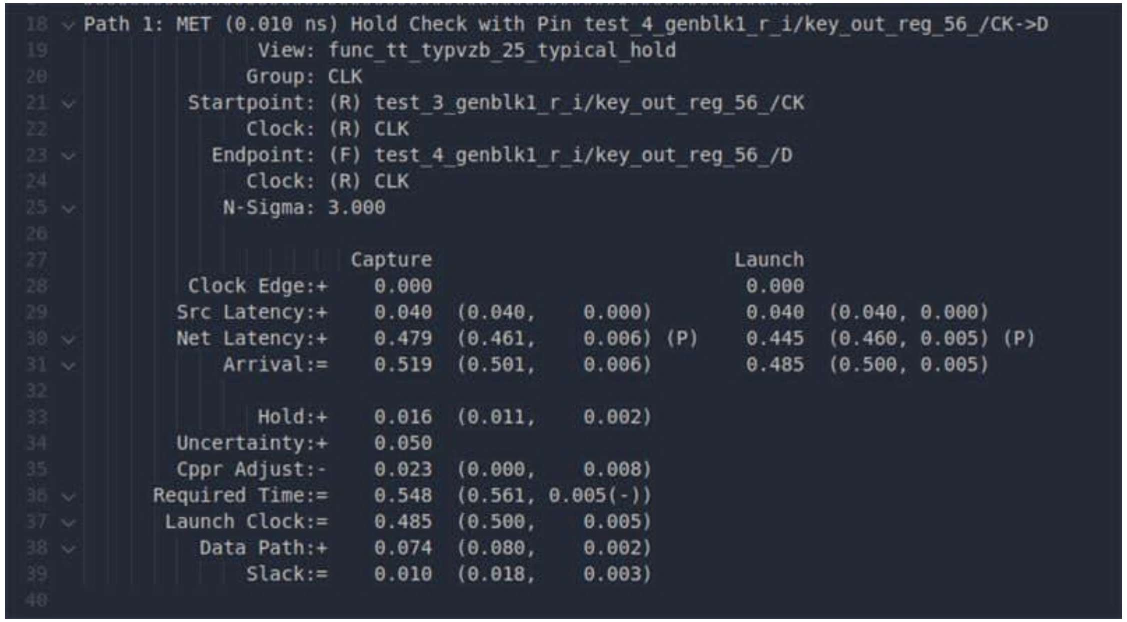
Report detailed timing path for the reg2reg path with the worst negative slack.

Setup analysis



```
Path 1: MET (0.331 ns) Setup Check with Pin test_3_genblk1_r_i/r_out_reg_22_/CK->D
               View: func_tt_typvzb_25_typical_hold
              Group: CLK
         Startpoint: (R) test_2_genblk1_r_i/key_out_reg_11_/CK
              Clock: (R) CLK
           Endpoint: (R) test_3_genblk1_r_i/r_out_reg_22_/D
              Clock: (R) CLK
            N-Sigma: 3.000

                      Capture                         Launch
         Clock Edge:+   1.000                          0.000
        Src Latency:+   0.040  (0.040,    0.000)       0.040  (0.040, 0.000)
        Net Latency:+   0.447  (0.461,    0.005) (P)   0.466  (0.449, 0.006) (P)
            Arrival:=   1.486  (1.501,    0.005)       0.506  (0.489, 0.006)

              Setup:-   0.013  (0.009,    0.001)
        Uncertainty:-   0.100
        Cppr Adjust:+   0.023  (0.000,    0.008)
      Required Time:=   1.409  (1.393, 0.006(-))
       Launch Clock:=   0.506  (0.489,    0.006)
          Data Path:+   0.572  (0.561,    0.004)
              Slack:=   0.331  (0.343,    0.004)
```

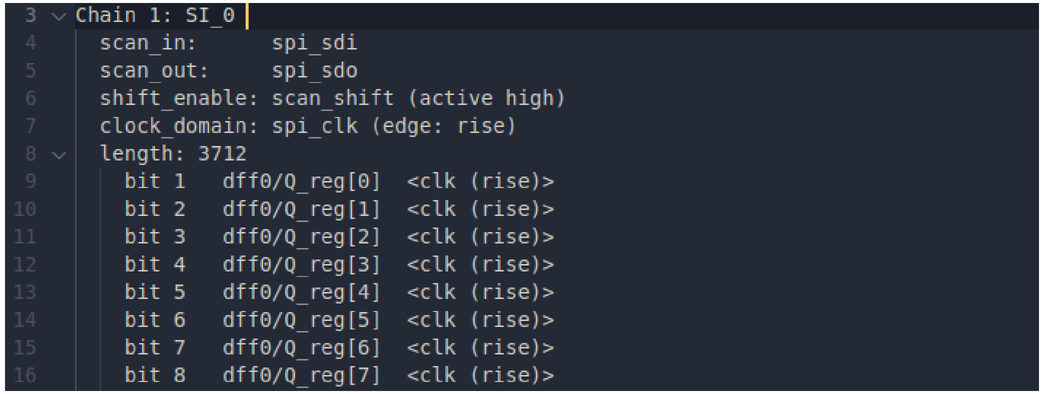
Hold analysis



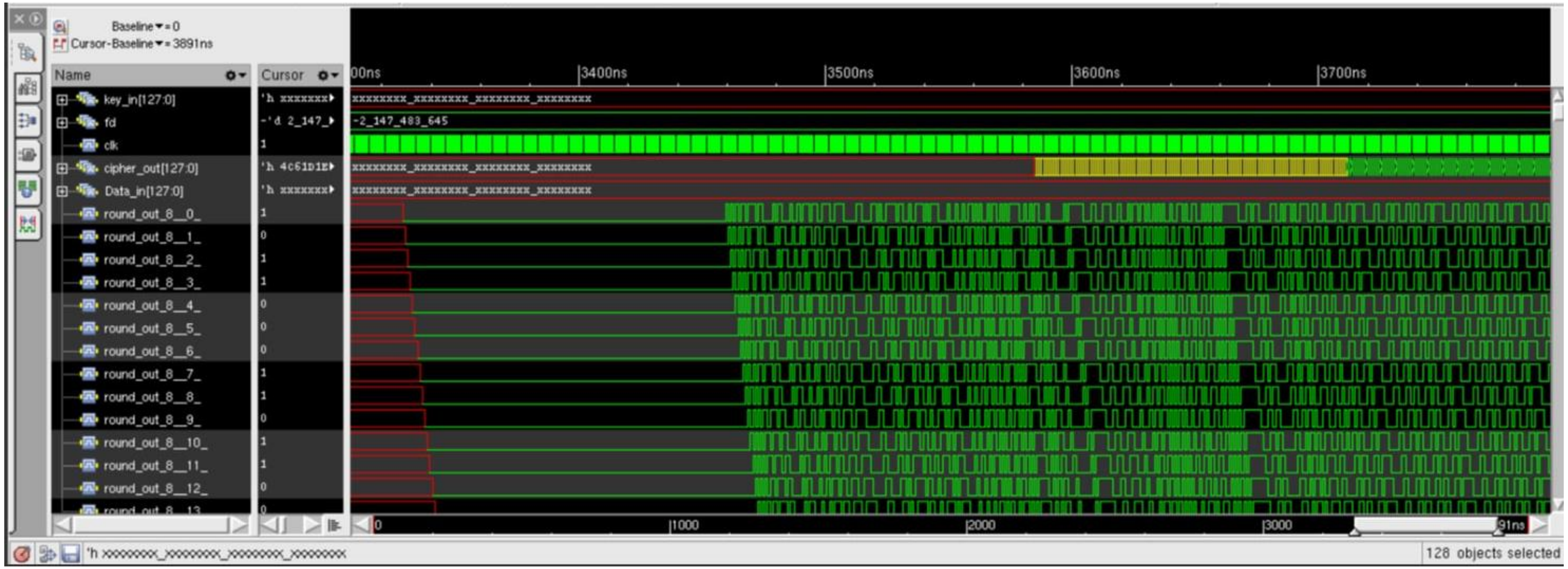
```
Path 1: MET (0.010 ns) Hold Check with Pin test_4_genblk1_r_i/key_out_reg_56_/CK->D
               View: func_tt_typvzb_25_typical_hold
              Group: CLK
         Startpoint: (R) test_3_genblk1_r_i/key_out_reg_56_/CK
              Clock: (R) CLK
           Endpoint: (F) test_4_genblk1_r_i/key_out_reg_56_/D
              Clock: (R) CLK
            N-Sigma: 3.000

                      Capture                         Launch
         Clock Edge:+   0.000                          0.000
        Src Latency:+   0.040  (0.040,    0.000)       0.040  (0.040, 0.000)
        Net Latency:+   0.479  (0.461,    0.006) (P)   0.445  (0.460, 0.005) (P)
            Arrival:=   0.519  (0.501,    0.006)       0.485  (0.500, 0.005)

               Hold:+   0.016  (0.011,    0.002)
        Uncertainty:+   0.050
        Cppr Adjust:-   0.023  (0.000,    0.008)
      Required Time:=   0.548  (0.561, 0.005(-))
       Launch Clock:=   0.485  (0.500,    0.005)
          Data Path:+   0.074  (0.080,    0.002)
              Slack:=   0.010  (0.018,    0.003)
```

Scan Chain

Scan chain length= 3712 FF



```
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)>
    bit 7   dff0/Q_reg[6]  <clk (rise)>
    bit 8   dff0/Q_reg[7]  <clk (rise)>
```



ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Online Part

AES Encryption Backend Flow Assignment

ASIC Design Flow Overview

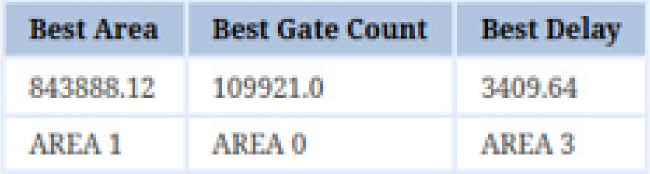
Operation	Tool	Flow Description
RTL-to-Gate-Level	Yosys + ABC	Logic synthesis, technology mapping, and optimization
Floorplanning & Placement	OpenROAD + OpenPDN	Die boundary definition, macro placement, power grid planning
Placement & CTS	OpenROAD	Standard cell placement and clock tree synthesis
Global & Detailed Routing	OpenROAD	Two-phase routing (global → detailed) with DEF/O-DB output
Post-Route Leakage Power	OpenROAD + OpenSTA	Vectorless analysis using SPEF/DEF/Liberty (worst-case conditions)
Post-Route Dynamic Power	OpenROAD + OpenSTA	Vector-based analysis using SAIF activity files + SPEF parasitics
Static Timing Analysis	OpenSTA & Synopsys ICC	Multi-corner setup/hold analysis with Liberty models
Physical Verification	Magic + Netgen	DRC/LVS checks and antenna rule validation
Parasitic Extraction	SPEF-Extractor	Generate .spef netlist for back-annotation
GDSII Generation	KLayout/Magic	Final layout export to manufacturable GDSII format
Static IR Drop Analysis	Synopsys ICC	Vectorless IR analysis using worst-case power profiles
Dynamic IR Drop Analysis	Synopsys ICC	Vector-based IR analysis with switching activity (VCD) + SPEF
Voltage Source Analysis	Synopsys ICC	Identification and optimization of power delivery network sources

AES ASIC Flow Results using OpenLane

We used 45nm technology Synopsys and 130nm technology with OpenLane

Steps to reach out the best synthesis strategies

- Applying **-synth_explore** for the RTL that runs a synthesis strategy exploration and reports the results in a table by trying multiple predefined synthesis strategies.
- we choose AREA3 as it has the most optimum delay



Best Area	Best Gate Count	Best Delay
843888.12	109921.0	3409.64
AREA 1	AREA 0	AREA 3

Block dimension

- Width = 1837.24, height =1836.0.
- Aspect ratio = 1

Post-synthesis instances count: 132808

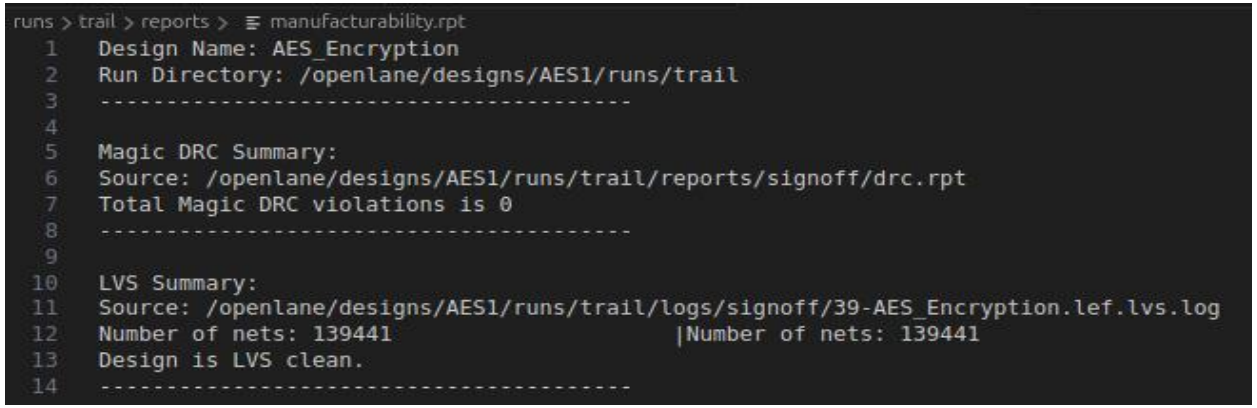
Post-synthesis registers count: 4000

Post-route instance count: 139182

Post-Route registers count: 4000

Post-Route utilization: 33%

DRC Report & LVS Status



```
Design Name: AES_Encryption
Run Directory: /openlane/designs/AES1/runs/trail
----------------------------------------

Magic DRC Summary:
Source: /openlane/designs/AES1/runs/trail/reports/signoff/drc.rpt
Total Magic DRC violations is 0
----------------------------------------

LVS Summary:
Source: /openlane/designs/AES1/runs/trail/logs/signoff/39-AES_Encryption.lef.lvs.log
Number of nets: 139441                      |Number of nets: 139441
Design is LVS clean.
----------------------------------------
```

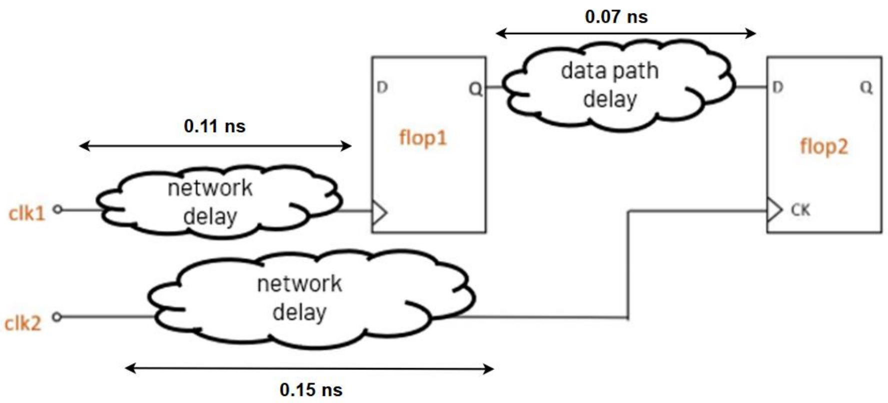
Module Hierarchical Instance using OpenLane

Module	Leaf Cells per Instance	Instances	Submodule	Sub-Instances per Parent	Total Sub-Instances	Notes
AES_Encryption	-	1	-	-	-	Top-level
DFF_128	128	10	-	-	-	Pipeline registers
Key	237	10	Sbox	4	40	Key expansion
MUX2_1	128	10	-	-	-	Data routing
Mix_Column	448	9	Lut2	16	144	GF(2^8) multiplication
			Lut3	16	144	
Round_reg	256	10	-	-	-	Round state storage
Shift_Rows	0	10	-	-	-	Byte permutation
Sub_Bytes	16	10	Sbox	16	160	Non-linear substitution
			Sub_Key	1	10	Key addition
mux	128	10	-	-	-	Operation selection

- **largest leaf cells count**: Mix_Column

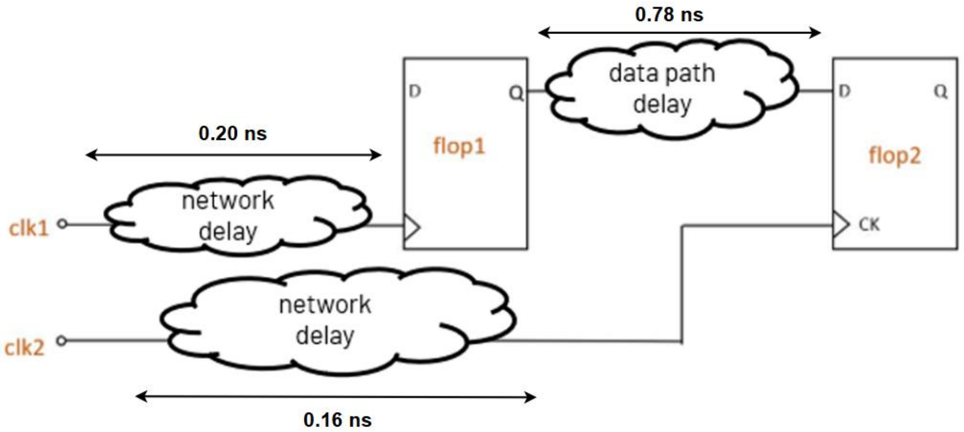
STA & Power using Synopsys ICC

- Hold Analysis



Data required time	1.12
Data arrival time	-0.98
Slack (MET)	0.15

- Setup Analysis



Data required time	0.17
Data Arrival time	-0.18
Slack (MET)	0.02

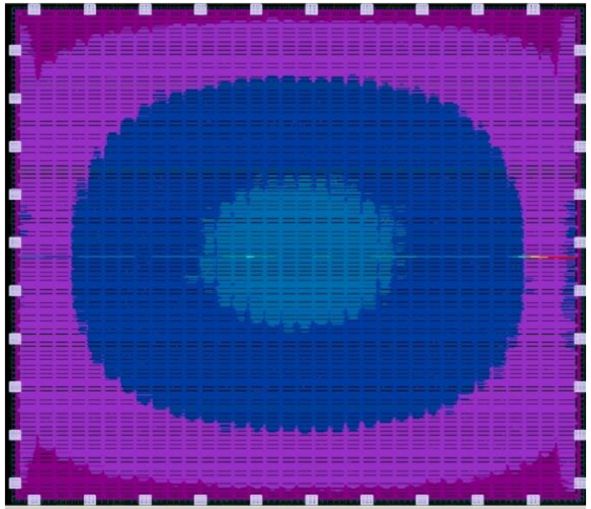
- Power Analysis

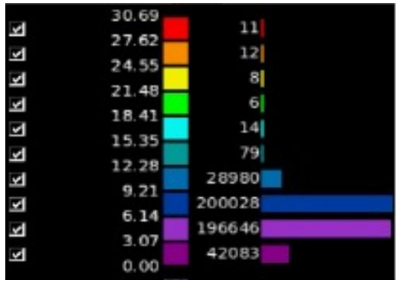
Internal Power	Switching Power	Leakage Power	Total Power
99.200 mW	126.24 mW	13.483 mW	238.92 mW

- For vector-based Analysis we simulated the RTL using an SV TB and generated the VCD file
- Click here for more info: Click Here

Screenshots Results using Synopsys ICC & KLayout

▶ IR Drop

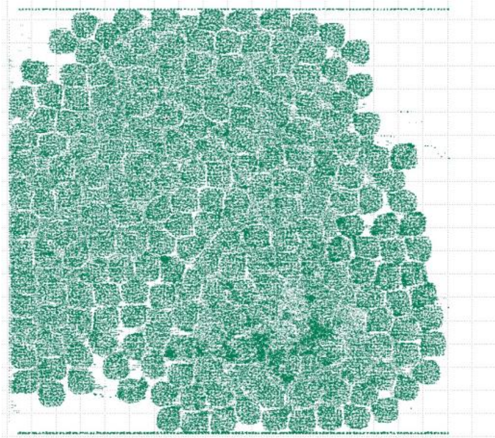




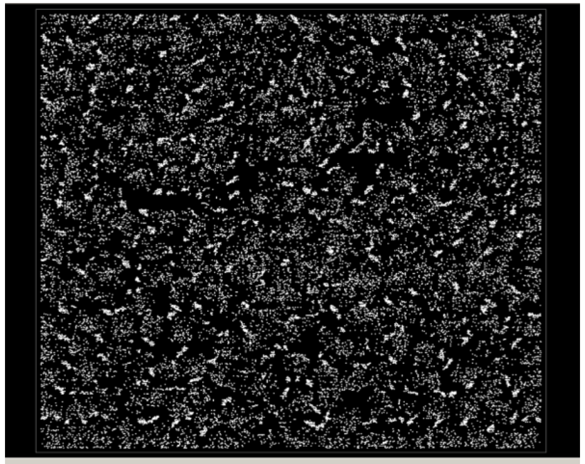
Max: 30 mV,

Supply: 1.25 V

▶ Logic Cells Screenshot

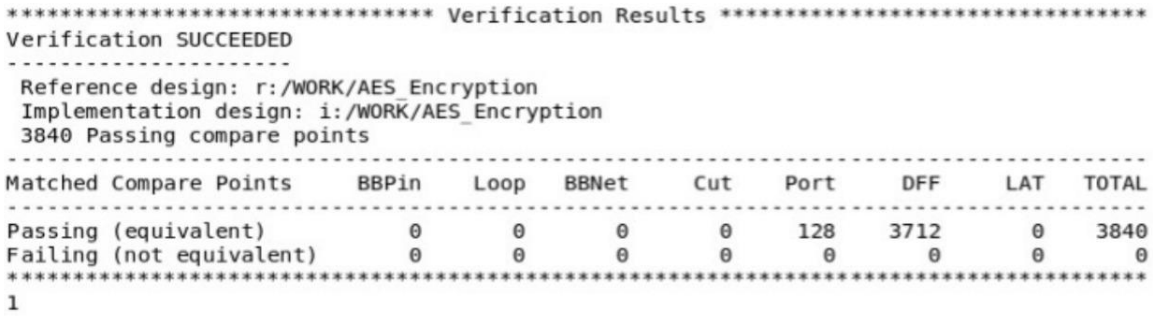


▶ Most Used Logic Cell Screenshot



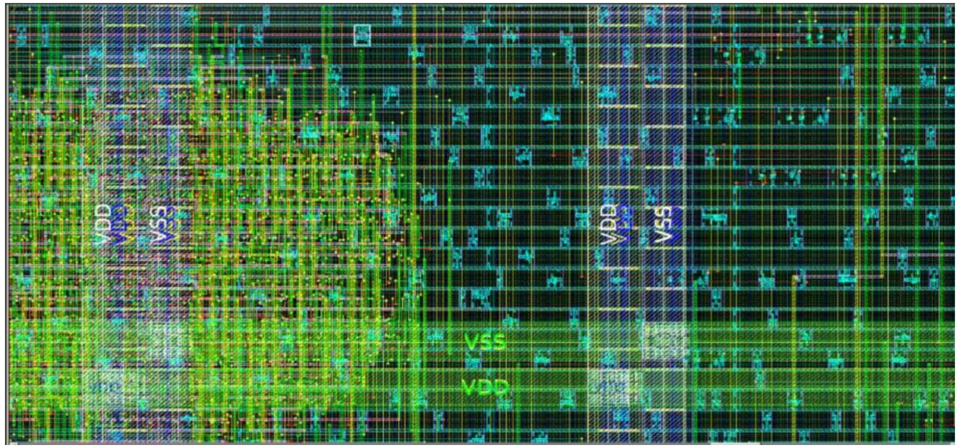
NAND2 with driving strength 1

▶ Formality (rtl vs post synthesis netlist)



```
********************************* Verification Results *********************************
Verification SUCCEEDED
----------------------
 Reference design: r:/WORK/AES_Encryption
 Implementation design: i:/WORK/AES_Encryption
 3840 Passing compare points
------------------------------------------------------------------------------------------
Matched Compare Points     BBPin    Loop   BBNet     Cut    Port     DFF     LAT   TOTAL
------------------------------------------------------------------------------------------
Passing (equivalent)           0       0       0       0     128    3712       0    3840
Failing (not equivalent)       0       0       0       0       0       0       0       0
******************************************************************************************
1
```

▶ GDSII Screenshot



Comparison

Type	ADFlow	OpenLane	Synopsys
Clock period	1 ns	4 ns	1ns
Technology	22 nm	185 nm	45 nm
Area	Lower	Higher	Medium
Instance count	Medium	Higher	Lowest
Cell count	Lower	Higher	Lowest
Register count	Lower	Higher	Lowest
Leakage Power	Lower	Higher	Medium
Dynamic Power	Lower	Higher	Medium
Utilization	Higher	Medium	Lowest
Largest Leaf Cell Count Module	SB0 (6721)	Mix Columns (461327)	NAND2_X1 (25632) **(ungrouped logic)**
WNS	Violated (-ve)	Violated (-ve)	Met (+ve)
IR Drop (Vectorless)	Lower	Higher	Medium

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Thank You