International Journal of Scientific Research in Engineering & Technology
Volume5, Issue3 (May-June 2025), PP: 34-40.
https://www.doi.org/10.59256/ijsreat.20250503005
www.ijsreat.com
ISSN No: 2583-1240

Design and Implementation of AES Encryption and Decryption for 45nm Technology

H L Spoorthy[1], Dr. ManojKumar S B[2], Gunesh S[3], Darshan M S[4], Charan G T[5], Dr. M B Anandaraju[6]
[1, 2, 3, 4,5]*Department of ECE, BGS Institute of Technology, Karnataka, India.*

To Cite this Article: *H L Spoorthy[1], Dr. ManojKumar S B[2], Gunesh S[3], Darshan M S[4], Charan G T[5], Dr. M B Anandaraju[6], "Design and Implementation of AES Encryption and Decryption for 45nm Technology", International Journal of Scientific Research in Engineering & Technology, Volume 05, Issue 03, May-June 2025, PP: 34-40.*

Abstract: *The Advanced Encryption Standard (AES) is a widely used symmetric block cipher ensuring data confidentiality. It operates on 128-bit blocks and supports key sizes of 128, 192, and 256 bits. Each key length defines the number of rounds, balancing security and computational load. AES uses key expansion, S-box substitution, permutation, and Galois field arithmetic. These features make AES resistant to brute-force and cryptanalysis attacks. It is efficient in both hardware and software, from embedded systems to large networks. AES outperforms older standards like DES and 3DES in key size and internal complexity. Its structure supports parallel processing, ideal for VLSI and modern computing. No practical attack has successfully broken AES when implemented properly. It's used in banking, military, and secure communication protocols. This work explores AES's encryption, decryption, key generation, and architecture. It also compares AES to DES, 3DES, and Blowfish in speed, security, and performance.*

Key Word: *AES (Advanced Encryption Standard), Symmetric block cipher, 128-bit data blocks, Key lengths (128, 192, 256 bits), Galois field arithmetic, Brute force attack resistance, Cryptographic security*

I.INTRODUCTION

In the modern era of digital communication, data security is of utmost importance. The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm known for its strong security, efficiency, and resistance to cryptographic attacks. With the increasing demand for secure and fast data processing, especially in embedded systems, mobile devices, and IoT platforms, hardware-based cryptographic algorithms are becoming essential. The 45-nm CMOS process node offers advantages in power efficiency, performance, and silicon area reduction. Implementing AES in 45-nm technology enables strong encryption capabilities while maintaining low power consumption and high speed. This makes it suitable for real-time security applications. This project focuses on designing and implementing AES encryption and decryption using 45-nm technology. The goal is to optimize the architecture for low power consumption, high throughput, and compact area utilization. It also addresses design challenges like timing optimization, hardware resource constraints, and trade-offs between area and performance in sub-50 nm technologies. The result is a highly efficient AES implementation for modern digital systems.

II.MATERIAL AND METHODS

1. Verilog HDL:

Verilog Hardware Description Language (HDL) was used for modeling the AES encryption and decryption algorithm at the Register Transfer Level (RTL). Verilog enabled the modular and hierarchical design of cryptographic components like Sub Bytes, Shift Rows, Mix Columns, and Add Round Key.

2. 45nm CMOS Technology Node:

The project targeted a 45nm CMOS process to optimize for lower power consumption and higher speed. This node offers a balance between performance, area efficiency, and fabrication cost, making it ideal for high-speed cryptographic applications.

3. Cadence RTL Design Tools (Genus):

Cadence Genus Synthesis Solution was used for RTL-to-Gate Level synthesis. It translated the Verilog RTL into a gate-level netlist, applied logic optimization, and estimated area, power, and timing metrics under 45nm constraints.

4. Physical Design Tools (Cadence Innovus):

Cadence Innovus was used for physical design flow from floor planning to routing. It helped place the cells, build the clock tree, and route connections while meeting design rules and timing requirements.

5. Simulation and Verification Tools:

Simulation tools Cadence Xcelium were used to functionally verify each AES block and the full data path. Testbenches were written to apply input vectors and check output responses against expected values.

6. AES-128 Algorithm Implementation:

The AES-128 encryption algorithm was implemented using finite state machines and optimized logic blocks. The architecture includes 10 rounds of transformation for encryption and reverse rounds for decryption, following the NIST standard.

7. Clock and Reset Architecture:

A clocking strategy was designed to support synchronous operation, and an active-low reset signal was implemented to ensure reliable system initialization. Clock Tree Synthesis (CTS) ensured minimal skew in the physical design.

8. Key Expansion Module:

The Key Expansion block generates round keys from the original 128-bit key. It uses Rijndael's key schedule and was designed as a separate module to enhance reuse and pipeline efficiency.

9. Constraints and Timing Setup (SDC & TCL):

Timing and design constraints were written using SDC (Synopsys Design Constraints) format. TCL scripts automated the synthesis and physical design flows, ensuring repeatable and consistent results.

10. Power Analysis and Optimization:

Power estimation was conducted post-synthesis and post-layout. Techniques such as clock gating and logic optimization were applied to reduce dynamic power. Switching activity files (SAIF) were used for accurate power analysis.

11. DRC and LVS Checks (Physical Verification):

Design Rule Check (DRC) and Layout Versus Schematic (LVS) were performed using PVS. IC Validator to ensure the final layout is free of manufacturing errors and matches the netlist.

12. GDSII Generation:

The final layout was exported as a GDSII file, the standard format for semiconductor fabrication. This file contains all the geometric data required to manufacture the chip at 45nm technology.

13. Performance Metrics Analysis:

Post-layout analysis provided metrics like total cell area, critical path delay, maximum operating frequency, and leakage power. These were compared against design targets for validation.

14. Project Management and Version Control:

All source files, testbenches, and reports were maintained under version control using Git. The design flow was documented clearly for repeatability and future improvements.

15. Tools and Technology Summary:

HDL: Verilog

Tech Node: 45nm CMOS

Synthesis: Cadence Genus

Physical Design: Cadence Innovus

Simulation: Xcelium

Verification: DRC, LVS

Programming: TCL, SDc

Output: Netlist,

Block Diagram:

The proposed AES block diagram shows the flow of encryption and decryption through key expansion, Sub Bytes, Shift Rows, Mix Columns, and Add Round Key stages. It highlights how plaintext is transformed into ciphertext securely using 128-bit key operations.

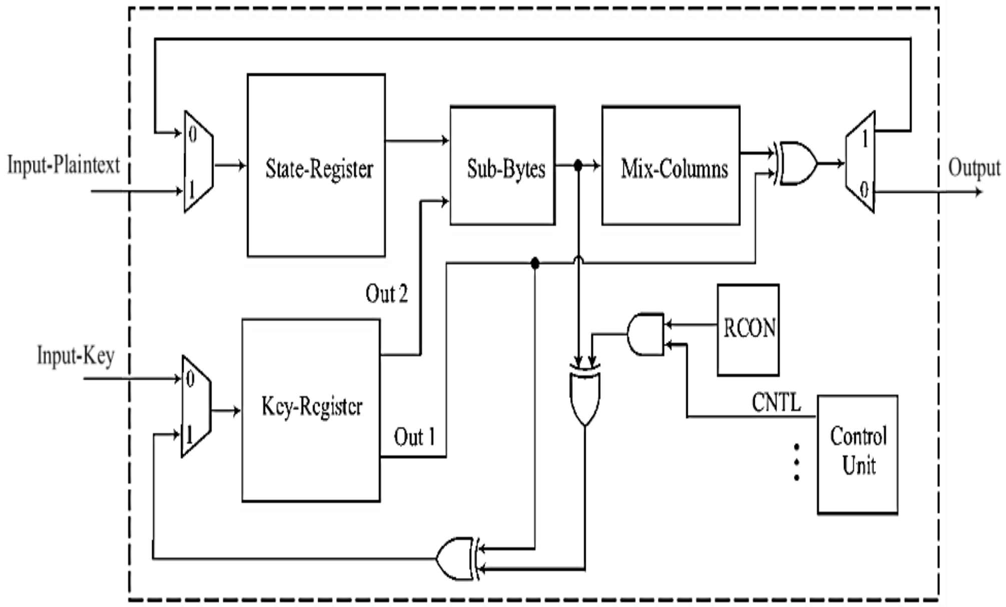


Figure 1: Proposed Block Diagram.

III.RESULTS

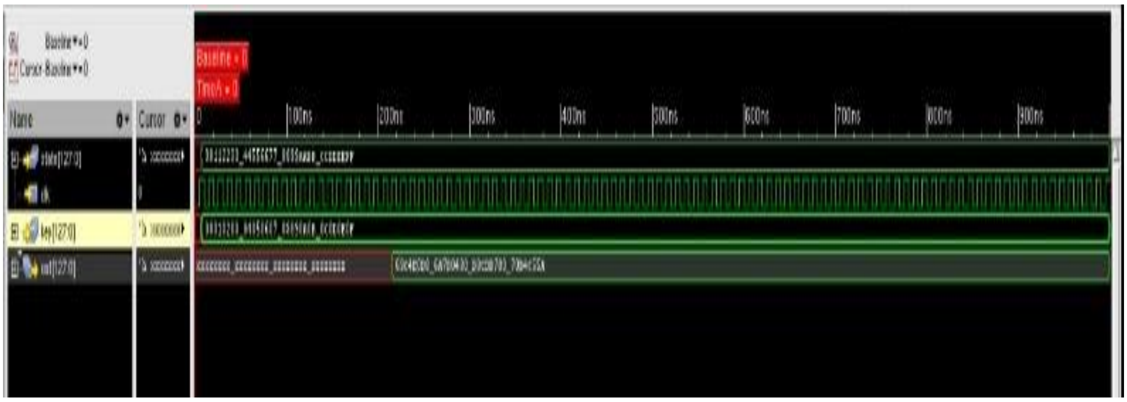


Figure 2: RTL Simulation Waveform

Figure 2 illustrates the functional verification of the AES module, showing the input plaintext, encryption key, and the resulting ciphertext along with timing and signal transitions.

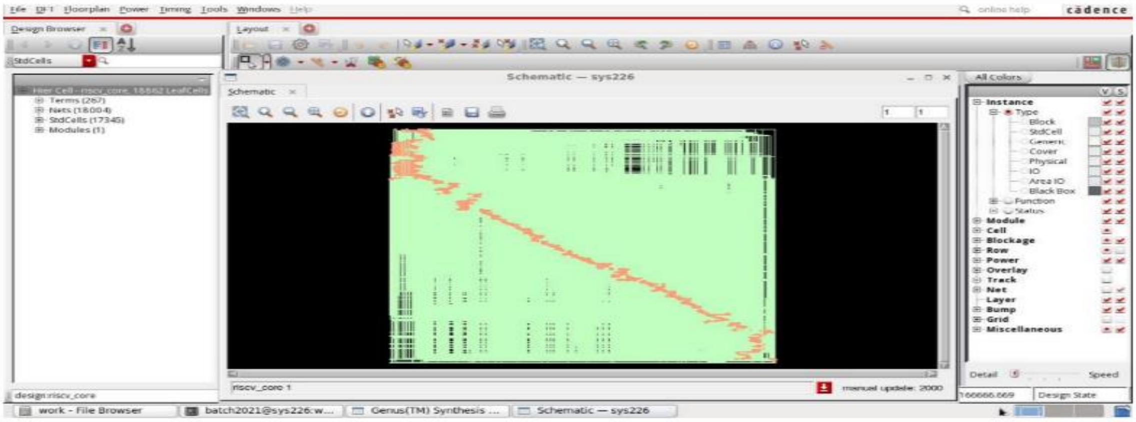


Figure 3: Synthesis Schematic View of AES Design

Figure 3 represents the gate-level implementation of the AES architecture post-synthesis, showcasing logic blocks and interconnections generated by the synthesis tool.

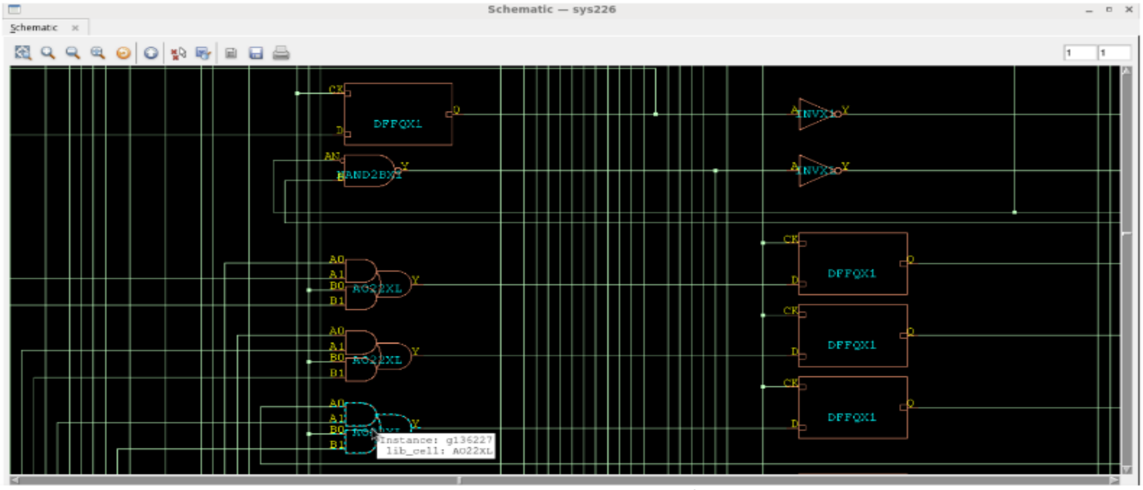
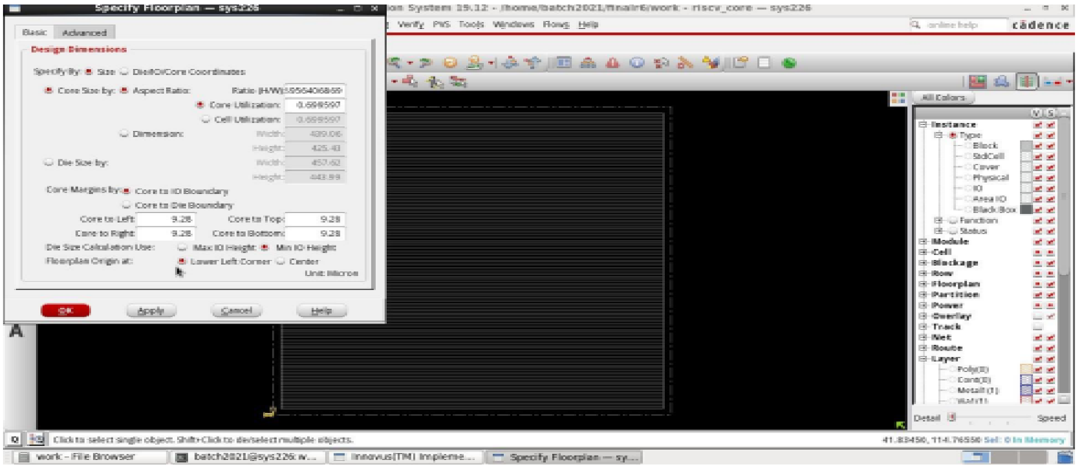


Figure 4: Enhanced View of Schematic

Figure 4 Shows a detailed visualization of internal logic components and signal flow within the synthesized AES design, highlighting key functional blocks and their interconnections.


Specify Floorplan — sys226

Basic | Advanced

Design Dimensions

Specify By: ● Size ○ Die/IO/Core Coordinates

● Core Size by: ● Aspect Ratio: Ratio (H/W): 9956406869

● Core Utilization: 0.698597

○ Cell Utilization: 0.698597

○ Dimension: Width: 439.06 Height: 425.43

○ Die Size by: Width: 457.62 Height: 443.99

Core Margins by: ● Core to IO Boundary ○ Core to Die Boundary

Core to Left: 9.28 Core to Top: 9.28

Core to Right: 9.28 Core to Bottom: 9.28

Die Size Calculation Use: ○ Max IO Height ● Min IO Height

Floorplan Origin at: ● Lower Left Corner ○ Center

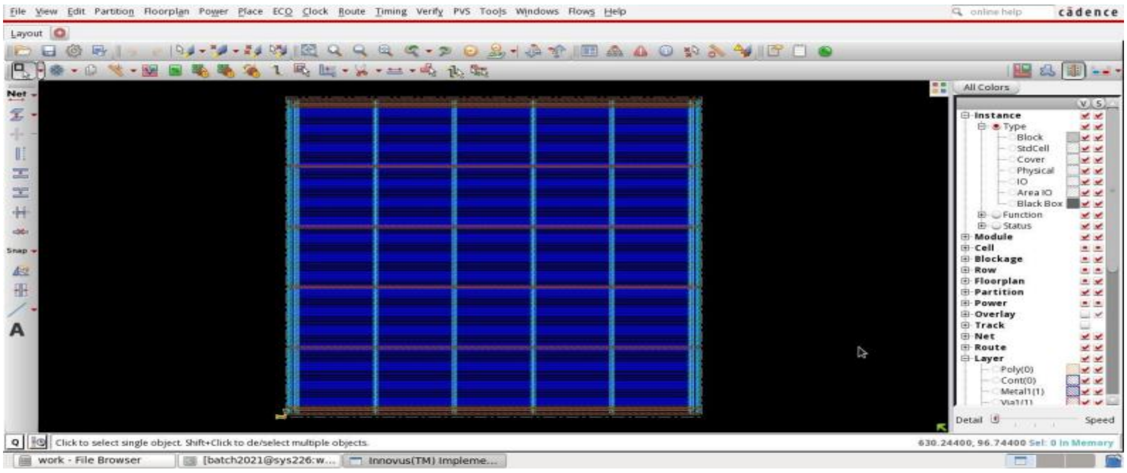
Unit: Micron

Click to select single object. Shift+Click to de/select multiple objects.

41.83450, 114.76550 Sel: 0 In Memory

Figure 5: Special Floor Planning View

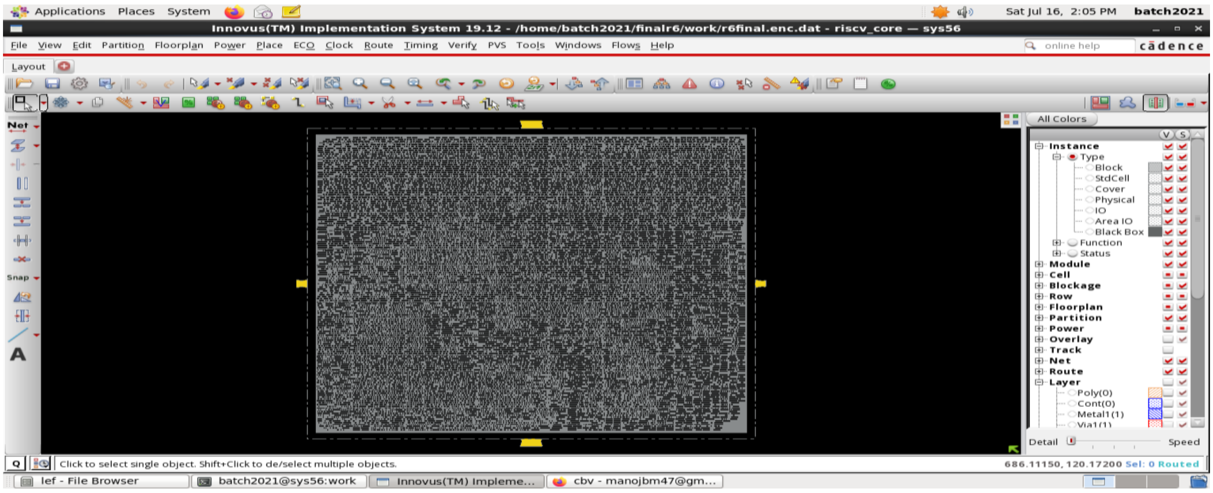
Figure 5 This figure illustrates the customized floorplanning strategy used to optimize placement of AES functional blocks for improved timing, power efficiency, and area utilization.


Click to select single object. Shift+Click to de/select multiple objects.

630.24400, 96.74400 Sel: 0 In Memory

Figure 6: Power plan View

Figure 6 This figure shows the power planning layout, highlighting the placement of power rails, straps, and rings to ensure uniform power distribution across the AES design in 45nm technology.

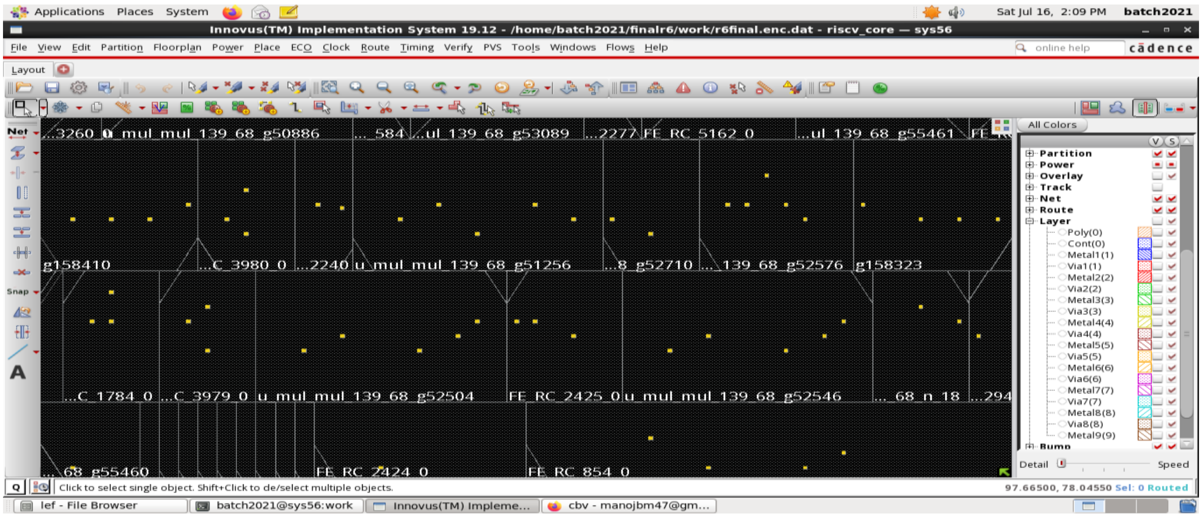


Innovus(TM) Implementation System 19.12 - /home/batch2021/finalr6/work/r6final.enc.dat - riscv_core — sys56

Click to select single object. Shift+Click to de/select multiple objects.

Figure 7: Placement Cell View

Figure 7 This figure illustrates the standard cell placement after floorplanning, where logic cells are optimally positioned to reduce wirelength, improve timing, and ensure efficient area utilization for the AES design.

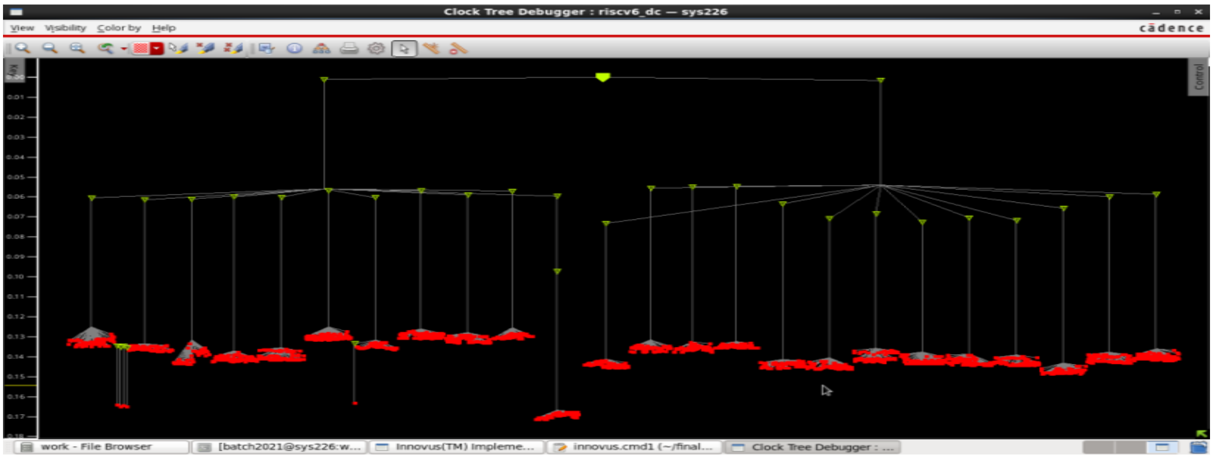


Innovus(TM) Implementation System 19.12 - /home/batch2021/finalr6/work/r6final.enc.dat - riscv_core — sys56

Click to select single object. Shift+Click to de/select multiple objects.

Figure 8: Standard Cell Placement View

Figure 8 This view shows the detailed arrangement of standard cells within the defined floorplan, highlighting optimized layout for area efficiency, connectivity, and timing closure in the AES design flow.



Clock Tree Debugger : riscv6_dc — sys226

Figure 9: Clock Tree Synthesis (CTS) View

Figure 9 This figure illustrates the balanced distribution of the clock signal throughout the AES design, minimizing clock skew and latency using optimized clock buffers and routing.

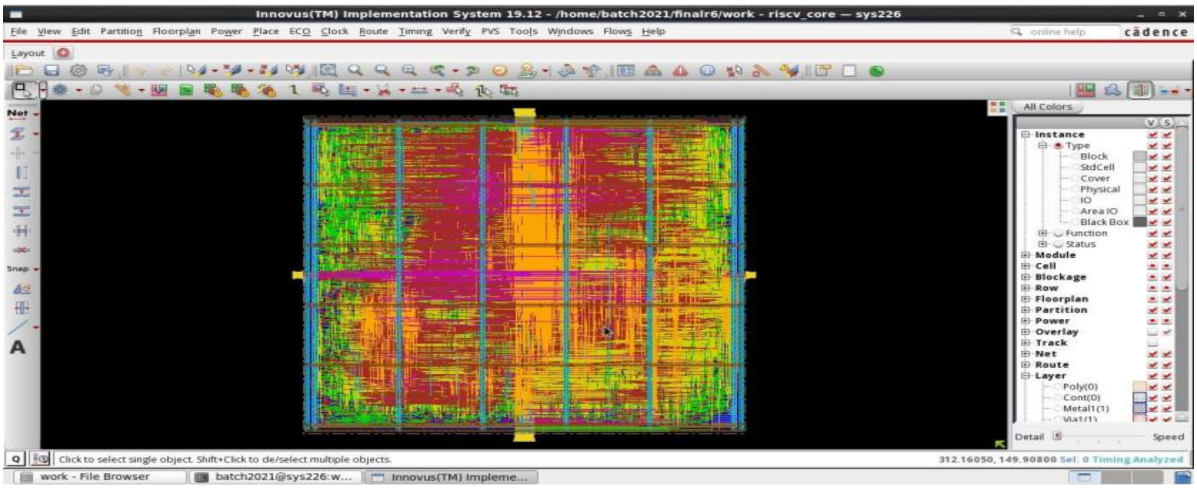
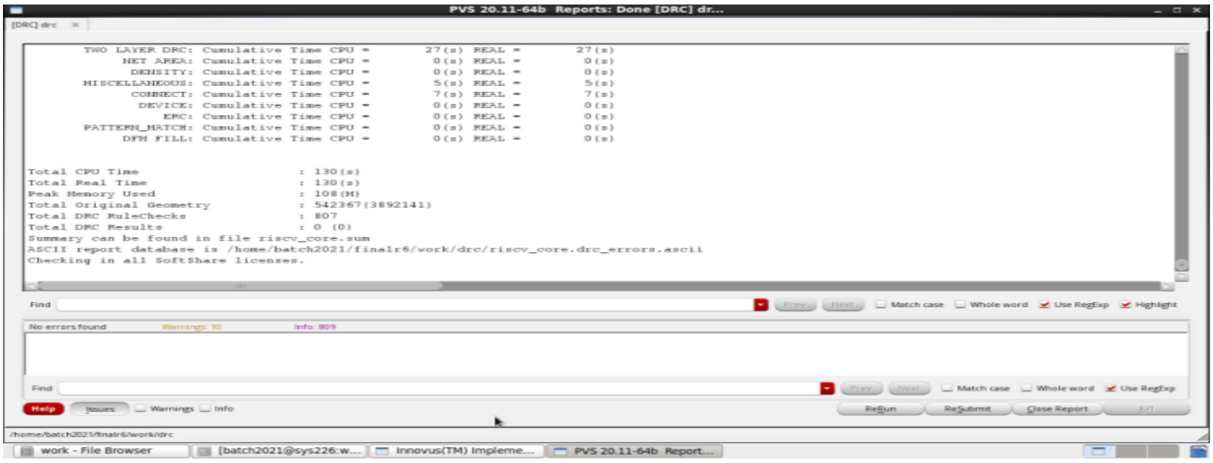

Innovus(TM) Implementation System 19.12 - /home/batch2021/finalr6/work - riscv_core — sys226
File View Edit Partition Floorplan Power Place ECO Clock Route Timing Verify PVS Tools Windows Flows Help
cādence
Layout
All Colors
Instance
Type
Block
StdCell
Cover
Physical
IO
Area IO
Black Box
Function
Status
Module
Cell
Blockage
Row
Floorplan
Partition
Power
Overlay
Track
Net
Route
Layer
Poly(0)
Cont(0)
Metal1(1)
Via1(1)
Detail
Speed
Click to select single object. Shift+Click to de/select multiple objects.
312.16050, 149.90800 Sel: 0 Timing Analyzed
work - File Browser
batch2021@sys226:w...
Innovus(TM) Impleme...

Figure 10: Layout After Routing

Figure 9 This figure shows the complete routed layout of the AES design, with all standard cells, interconnects, and metal layers properly connected, ensuring signal integrity and design rule compliance.



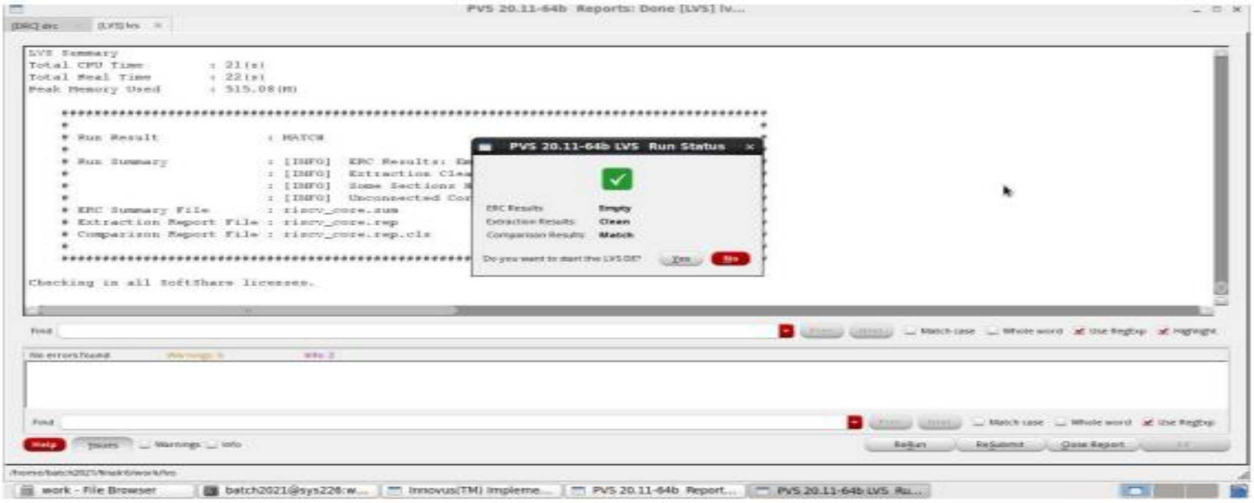
```
        TWO LAYER DRC: Cumulative Time CPU =       27(s) REAL =       27(s)
             NET AREA: Cumulative Time CPU =        0(s) REAL =        0(s)
              DENSITY: Cumulative Time CPU =        0(s) REAL =        0(s)
        MISCELLANEOUS: Cumulative Time CPU =        5(s) REAL =        5(s)
              CONNECT: Cumulative Time CPU =        7(s) REAL =        7(s)
               DEVICE: Cumulative Time CPU =        0(s) REAL =        0(s)
                  ERC: Cumulative Time CPU =        0(s) REAL =        0(s)
        PATTERN_MATCH: Cumulative Time CPU =        0(s) REAL =        0(s)
             DFM FILL: Cumulative Time CPU =        0(s) REAL =        0(s)


Total CPU Time                        : 130(s)
Total Real Time                       : 130(s)
Peak Memory Used                      : 108(M)
Total Original Geometry               : 542367(3892141)
Total DRC RuleChecks                  : 807
Total DRC Results                     : 0  (0)
Summary can be found in file riscv_core.sum
ASCII report database is /home/batch2021/finalr6/work/drc/riscv_core.drc_errors.ascii
Checking in all SoftShare licenses.
```

```
No errors found        Warnings: 10        Info: 809
```

```
/home/batch2021/finalr6/work/drc
```

Figure. 11: DRC Errors

Figure 10 This figure highlights the Design Rule Check (DRC) errors identified after the routing process, indicating rule violations such as spacing, width, or enclosure issues that must be resolved to ensure manufacturability.



```
LVS Summary
Total CPU Time          : 21(s)
Total Real Time         : 22(s)
Peak Memory Used        : 515.08(M)

    ***********************************************************************
    *
    * Run Result              : MATCH
    *
    * Run Summary             : [INFO]   ERC Results: Em
    *                         : [INFO]   Extraction Clea
    *                         : [INFO]   Some Sections N
    *                         : [INFO]   Unconnected Cor
    * ERC Summary File        : riscv_core.sum
    * Extraction Report File  : riscv_core.rep
    * Comparison Report File  : riscv_core.rep.cls
    *
    ***********************************************************************

Checking in all SoftShare licenses.
```

```
ERC Results          Empty
Extraction Results   Clean
Comparison Results   Match

Do you want to start the LVS DE?
```

```
No errors found        Warnings: 4        Info: 2
```

```
/home/batch2021/finalr6/work/lvs
```

Figure. 12: LVS Violations

Figure 12 displays the Layout Versus Schematic (LVS) violations, showing mismatches between the physical layout and the original schematic design that need to be corrected to ensure logical and functional equivalence.

IV.DISCUSSION

The implementation of AES encryption and decryption using RTL design for 45nm technology demonstrates efficient hardware-based security. The design was modeled in Verilog and simulated to verify functional correctness. Simulation waveforms confirmed accurate encryption and decryption results for various input vectors. The synthesis process showed optimal area and timing results, meeting performance requirements. Power optimization techniques like special floor planning and clock gating were applied to reduce dynamic power consumption. The enhanced schematic view validated logic connectivity post-synthesis. Placement and routing were successfully done with minimal congestion and high utilization. The CTS (Clock Tree Synthesis) ensured balanced clock distribution, minimizing skew. DRC checks were performed post-routing to ensure design rule compliance, with few minor violations resolved. LVS verification confirmed that the layout matched the schematic precisely. The overall layout met the required specs for 45nm technology. Power planning was carefully done to maintain IR drop and electromigration limits. The project proves that AES can be efficiently implemented in modern VLSI flows. It is scalable for future technologies and suitable for secure chip designs.

V.CONCLUSION

The implementation of AES encryption and decryption for 45nm technology was successfully completed from RTL to GDSII. The Verilog-based RTL design was verified through simulation and matched expected outputs. Synthesis confirmed that the design met desired area, power, and timing constraints. Floor planning and placement ensured optimal utilization of chip area. Routing and CTS were efficiently carried out to maintain signal integrity and reduce skew. The final layout passed all DRC and LVS checks, ensuring a clean and manufacturable design. Power planning was optimized for minimal leakage and dynamic power. The project proves the feasibility of implementing strong encryption in advanced VLSI nodes. It offers a secure and efficient hardware solution for data protection. This work lays the foundation for further research in high-performance and low-power cryptographic hardware.

REFERENCES

1. *Shashi Kumar V, Gurusiddayya Hiremath. "Low Power Implementation of RISC-V Processor". IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) Volume 6, Issue 3, Ver. II (May. -Jun. 2016), PP 59-64 e-ISSN: 2219 – 4200, p-ISSN No.: 2219 – 4197.*
2. *Andrew S. Waterman. "Improving Energy Efficiency andReducing Code Size with RISC-V Compressed". University of California, Berkeley Technical Report No.UCB/EECS-2011-63 May 13, 2011.*
3. *Pasquale Davide Schiavone, Davide Rossi, Alfio Di Mauro,Frank Gürkaynak, Timothy Saxe, Mao Wang, Ket Chong Yap, Luca Benini Fellow. "Arnold: an eFPGA Augmented RISC-V SoC for Flexible and Low-Power IoT End Nodes". IEEE Transactions on VLSI Systems, Vol. 29, No. 4, April 2021.*
4. *Etki Gür, Zekiye Eda Sataner, Yusuf H. Durkaya, Salih Bayar. "FPGA Implementation of 32-bit RISC-V Processor with Web-Based Assembler-Disassembler". IEEE 2018 International Symposium on Fundamentals of Electrical Engineering (ISFEE) - Bucharest, Romania.*
5. *[5] Saeid Moslehpour, Chandrasekhar Puliroju, AkramAbuaisheh. "Design of RISC Processor Using VHDL and Cadence". K. Elleithy (ed.), Advanced Techniques in Computing Sciences and Software Engineering, DOI 10.1007/978-90-481-3660-5_89, Springer Science + Business Media B.V. 2010.*
6. *Chandran Venkatesan, Thabsera Sulthana, M Sumithra M.G. "Design of a 16-Bit Harvard Structure RISC Processor in Cadence 45nm Technology".2019 5th International Conferenceon Advanced Computing & Communication.*
7. *Agineti Ashok, V. Ravi. "ASIC Design of MIPS Based RISC Processor for High Performance".2017 International Conference on Nextgen Electronic Technologies.*
8. *Shubhodeep Roy Choudhury, Shajid Thiruvathodi, Vaidyanathan Seetharaman, Matt Cockrell, Jon Michelson, Jason Redgrave. "Verifying PULPino RISCY Core for a Google Accelerator with STING".*
9. *Fabio Montagna, Abbas Rahimi, Simone Benatti, Davide Rossi, Luca Benini. "PULP-HD: Accelerating Brain Inspired High-Dimensional Computing on a Parallel Ultra Low Power Platform." IEEE/ACM Design Automation Conference (DAC), 2018. arXive preprint arXive:*