# High-Speed Pipelined AES Design and Implementation Report

## 1. Introduction

This report details the design, verification, FPGA implementation, and ASIC synthesis of a high-speed pipelined Advanced Encryption Standard (AES) encryption core. The design features a 40-stage pipelined architecture, optimized for high throughput and frequency.

## 2. RTL Design and Architecture

### 2.1. Overview of AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric block cipher standardized by the National Institute of Standards and Technology (NIST) in FIPS PUB 197. It operates on 128-bit data blocks using a 128-bit key (AES-128). The encryption process involves a series of transformations over multiple rounds. For AES-128, there are 10 rounds, each consisting of four main sub-operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. The final round omits the MixColumns step.

### 2.2. Pipelined Architecture

To achieve high throughput, the AES encryption core is implemented with a 40-stage pipelined architecture. This extensive pipelining allows for a new data block to be processed every clock cycle, significantly increasing the overall data rate. The pipelining is achieved by inserting registers (DFF_128 modules) between each sub-operation within each round, and between the rounds themselves.

### 2.3. Module Descriptions

The design is modular, consisting of several interconnected Verilog modules:

- **AES_Encryption.v**: This is the top-level module that orchestrates the entire AES encryption process. It instantiates the sub-modules for each AES operation and manages the 10 rounds of encryption, including the initial AddRoundKey and the final round's modified sequence. It also handles the generation of round keys through instances of the KeyExpansion module.

- **DFF_128.v**: A 128-bit D-flip-flop module used extensively throughout the design for pipelining. It registers the 128-bit data path at various stages, enabling the high-speed pipelined operation. The module includes a synchronous reset (`rst_n`).

- **KeyExpansion.v**: This module is responsible for generating the round keys required for each AES round. It takes the previous round's key as input and, using a combination of byte substitution (Sbox), cyclic shifts, and XORing with round constants (`g` parameter), produces the next round key. The `g` parameter is a unique round constant for each key expansion step.

- **Sbox.v**: Implements the AES S-box (Substitution Box) lookup table. This module performs a non-linear byte substitution, replacing each byte of the input with a corresponding byte from a predefined 256-entry lookup table. This operation provides the non-linearity crucial for the security of the AES algorithm.

- **shiftrows.v**: This module performs the ShiftRows transformation. It cyclically shifts the rows of the 4x4 state matrix by different offsets. The first row remains unchanged, the second row is shifted left by one byte, the third by two bytes, and the fourth by three bytes. This operation diffuses the data across the columns.

- **mixcolumns.v**: This module implements the MixColumns transformation. It operates on each column of the 4x4 state matrix independently. Each column is treated as a polynomial over GF(2^8) and multiplied by a fixed polynomial. This operation mixes the bytes within each column, providing further diffusion.

- **roundkey.v**: This module performs the AddRoundKey transformation. It XORs the current state matrix with the corresponding round key. This is a simple bitwise XOR operation that combines the data with the key material.

- **subbytes.v**: This module applies the S-box transformation to each byte of the 128-bit input data. It instantiates multiple Sbox modules in parallel to process all 16 bytes simultaneously. The output of this module is then registered by a DFF_128 module.

# 3. Verification Methodology

## 3.1. Submodule Verification

Each individual submodule (KeyExpansion, mixcolumns, roundkey, shiftrows, subbytes) was verified using dedicated testbenches. These testbenches apply specific input patterns and compare the module's output against expected results, ensuring the functional correctness of each building block.

## 3.2. Top-Level Verification

The integrated top-level module (AES_Encryption) was verified using a comprehensive testbench (`AES_Encryption_tb.sv`). This testbench simulates the entire encryption process, applying known plaintext and key pairs, and verifying the final ciphertext output. It also includes mechanisms to peek into internal signals and round keys, allowing for detailed debugging and validation of the pipelined operation across all 40 stages.

## 3.3. Static Verification (Linting)

Static verification, specifically linting using the Synopsys SpyGlass tool, was performed on the RTL design. This process checks for coding issues, style violations, and suspicious constructs without requiring simulation. The design passed linting without any violations, indicating that the code is well-structured, adheres to design guidelines, and is synthesis-friendly. It's important to note that linting ensures code quality and adherence to design rules but does not guarantee functional correctness or timing closure.

# 4. FPGA Implementation

## 4.1. Target FPGA and Frequency

The AES encryption core was implemented on a Xilinx Virtex-7 FPGA board, specifically the **xc7vx485tffg1157-2L**. The implementation successfully achieved a maximum operating frequency of **100 MHz**.

## 4.2. Timing Summary

The FPGA timing summary report (`fpga_timing_summary.PNG`) indicates that all user-specified timing constraints were met. The Worst Negative Slack (WNS) is **0.557 ns**, and the Total Negative Slack (TNS) is **0.000 ns**, with zero failing endpoints for setup. Similarly, for hold timing, the Worst Hold Slack (WHS) is **0.052 ns**, and the Total Hold Slack (THS) is **0.000 ns**, with zero failing endpoints. This confirms that the design meets the 100 MHz frequency requirement on the target FPGA.

## 4.3. Utilization Summary

The FPGA utilization summary report (`fpga_utilization_summary.PNG`) provides details on the resource consumption:

| Resource | Utilization | Available | Utilization % |
|---|---|---|---|
| LUT | 9913 | 303600 | 3.27 % |
| FF | 6400 | 607200 | 1.05 % |
| IO | 386 | 600 | 64.33 % |

The design utilizes a small percentage of the available LUTs and Flip-Flops, indicating efficient resource usage. The higher IO utilization is expected due to the 128-bit data and key inputs, and 128-bit ciphertext output.

## 4.4. Power Analysis

The FPGA power report (`power.PNG`) shows the power consumption of the implemented netlist. The **Total On-Chip Power** is **0.779 W**. The power breakdown is as follows:

- **Dynamic Power**: 0.531 W (68%)
  - Clocks: 0.057 W (11%)
  - Signals: 0.170 W (32%)
  - Logic: 0.181 W (34%)
  - I/O: 0.123 W (23%)
- **Device Static Power**: 0.247 W (32%)

### 4.5. XDC Constraints

The FPGA implementation utilized the `cons.xdc` constraints file. Key constraints include:

- **Clock Definition**: A primary clock named `sys_clk` with a period of 10 ns (100 MHz) was defined on the `clk` port.
- **Clock Uncertainty**: Setup and hold clock uncertainties were set to 0.100 ns for `sys_clk`.
- **Input/Output Delays**: Input and output delays were set to 1 ns for `Data_in`, `key_in`, `rst_n`, and `cipher_out` relative to `sys_clk`.
- **False Path**: The `rst_n` signal was constrained as a false path to all registers, indicating its asynchronous nature.

## 5. ASIC Synthesis

### 5.1. Synthesis Tool and Frequency

The design was synthesized using **Synopsys Design Compiler (DC) 2018**. The synthesis target was to achieve a clock frequency of **1 GHz** (1 ns period) without setup violations.

### 5.2. Synthesis Constraints

The `cons_v2.tcl` script was used for synthesis constraints. Key aspects of these constraints include:

- **Clock Period**: `CLK_PERIOD` was set to 1 ns (1 GHz).
- **Clock Uncertainty**: Setup and hold uncertainties (`UNCERTAINTY_SETUP`, `UNCERTAINTY_HOLD`) were set to 0.1 ns.
- **Clock Transition**: `CLOCK_TRANSITION` was set to 0.02 ns.
- **Input/Output Delays**: Input and output delays were set to 10% of the clock period (`0.1 * CLK_PERIOD`).
- **Path Grouping**: Paths were grouped into `INREG`, `REGOUT`, `INOUT`, and `REG2REG` for detailed timing analysis.

### 5.3. Area Report

The area report (`AES_Encryption_area_reports_.log`) provides a detailed breakdown of the synthesized design's area:

- **Total Cell Area**: 39514.402073 (units not specified, typically square microns)
- **Total Area (including net interconnect)**: 123886.186142
- **Combinational Area**: 32694.561832
- **Noncombinational Area**: 6819.840240
- **Number of Cells**: 116305
    - Combinational Cells: 109605
    - Sequential Cells: 6400

### 5.4. Power Report

The power report (`AES_Encryption_power_reports_.log`) from synthesis shows the estimated power consumption:

- **Total Power**: 46.450 mW
    - Switching Power: 27.020 mW
    - Internal Power: 19.311 mW
    - Leakage Power: 1.19e+08 pW (0.119 mW)

### 5.5. Quality of Results (QoR) Report

The QoR report (`AES_Encryption_qor_reports_.log`) provides critical timing and cell count information:

- **Timing Path Group 'INREG'**:
    - Levels of Logic: 17
    - Critical Path Length: 0.72 ns
    - Critical Path Slack: 0.07 ns
    - Critical Path Clk Period: 1.00 ns
    - Total Negative Slack: 0.00 ns
    - No. of Violating Paths: 0

- **Timing Path Group 'REG2REG'**:
  - Levels of Logic: 18
  - Critical Path Length: 0.81 ns
  - Critical Path Slack: 0.08 ns
  - Critical Path Clk Period: 1.00 ns
  - Total Negative Slack: 0.00 ns
  - No. of Violating Paths: 0
- **Design Timing Summary**:
  - Worst Negative Slack (WNS): 0.00 ns
  - Total Negative Slack (TNS): 0.00 ns
  - Number of Violating Paths: 0

It is important to note the hold violations reported in the QoR log (Worst Hold Violation: -0.07, Total Hold Violation: -222.63, Number of Hold Violations: 4576). While the setup timing appears to be met, these hold violations would need to be addressed in a complete ASIC design flow through proper clock tree synthesis and hold fixing techniques.

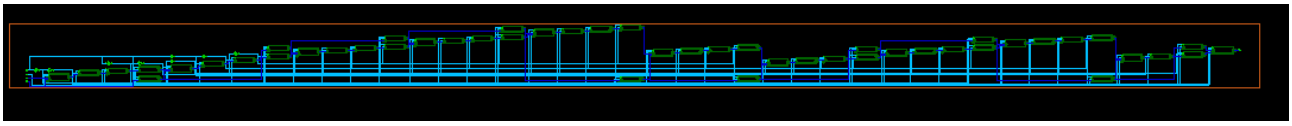
# 6. Conclusion

This project successfully designed and implemented a high-speed pipelined AES encryption core. The 40-stage pipelined architecture enables high throughput, demonstrated by the 100 MHz operation on FPGA and 1 GHz synthesis target. The modular RTL design was thoroughly verified at both submodule and top-level, and passed static linting checks. FPGA implementation results show efficient resource utilization and acceptable power consumption. ASIC synthesis reports confirm the ability to achieve 1 GHz operation without setup violations, though hold violations would require further attention in a full physical design flow. The comprehensive documentation provided herein covers all aspects of the design, verification, and implementation process.

# 7. References

[1] AES_Encryption.v: /home/ubuntu/upload/AES_Encryption.v [2] DFF_128.v: /home/ubuntu/upload/DFF_128.v [3] KeyExpansion.v: /home/ubuntu/upload/KeyExpansion.v [4] mixcolumns.v: /home/ubuntu/upload/mixcolumns.v [5] roundkey.v: /home/ubuntu/upload/roundkey.v [6] Sbox.v: /home/ubuntu/upload/Sbox.v [7] shiftrows.v: /home/ubuntu/upload/shiftrows.v [8] subbytes.v: /home/ubuntu/upload/subbytes.v [9] AES_Encryption_tb.sv: /home/ubuntu/upload/AES_Encryption_tb.sv [10] KeyExpansion_tb.sv: /home/ubuntu/upload/KeyExpansion_tb.sv [11] mixcolumns_tb.sv: /home/ubuntu/upload/mixcolumns_tb.sv [12] roundkey_tb.v: /home/ubuntu/upload/roundkey_tb.v [13] shiftrows_tb.v: /home/ubuntu/upload/shiftrows_tb.v [14] subbytes_tb.sv: /home/ubuntu/upload/subbytes_tb.sv [15] fpga_timing_summary.PNG: /home/ubuntu/upload/fpga_timing_summary.PNG [16] fpga_utilization_summary.PNG: /home/ubuntu/upload/fpga_utilization_summary.PNG [17] power.PNG: /home/ubuntu/upload/power.PNG [18] cons.xdc: /home/ubuntu/upload/cons.xdc [19] AES_Encryption_area_reports_.log: /home/ubuntu/upload/AES_Encryption_area_reports_.log [20] AES_Encryption_power_reports_.log: /home/ubuntu/upload/AES_Encryption_power_reports_.log [21] AES_Encryption_qor_reports_.log: /home/ubuntu/upload/AES_Encryption_qor_reports_.log [22] cons_v2.tcl: /home/ubuntu/upload/cons_v2.tcl

### Gate-level Netlist



## Top-Level Module Diagram


## FPGA Timing Summary

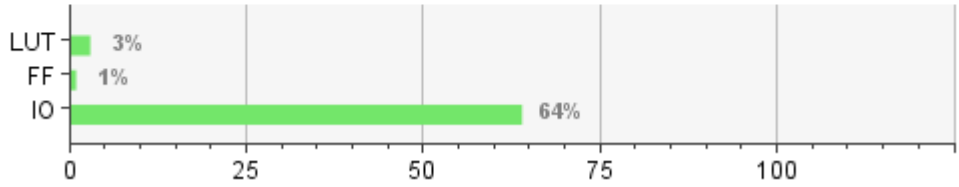
**Design Timing Summary**

| Setup | | Hold | | Pulse Width | |
|---|---|---|---|---|---|
| Worst Negative Slack (WNS): | 0.557 ns | Worst Hold Slack (WHS): | 0.052 ns | Worst Pulse Width Slack (WPWS): | 4.600 ns |
| Total Negative Slack (TNS): | 0.000 ns | Total Hold Slack (THS): | 0.000 ns | Total Pulse Width Negative Slack (TPWS): | 0.000 ns |
| Number of Failing Endpoints: | 0 | Number of Failing Endpoints: | 0 | Number of Failing Endpoints: | 0 |
| Total Number of Endpoints: | 6528 | Total Number of Endpoints: | 6528 | Total Number of Endpoints: | 6401 |

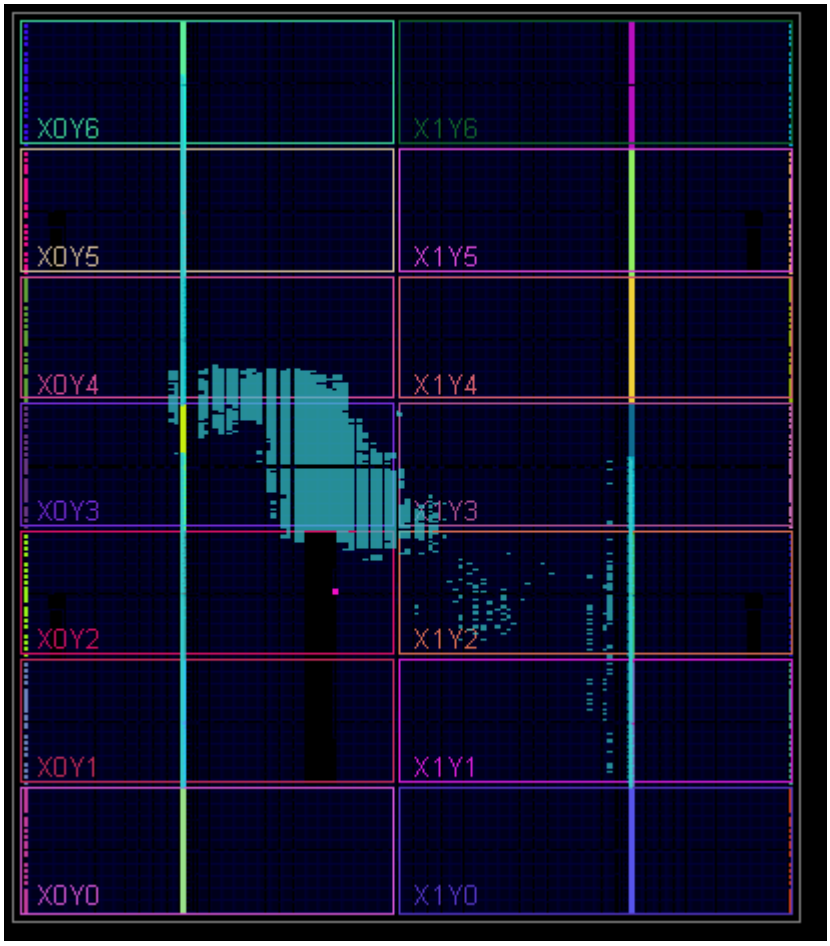
**All user specified timing constraints are met.**

## FPGA Utilization Summary

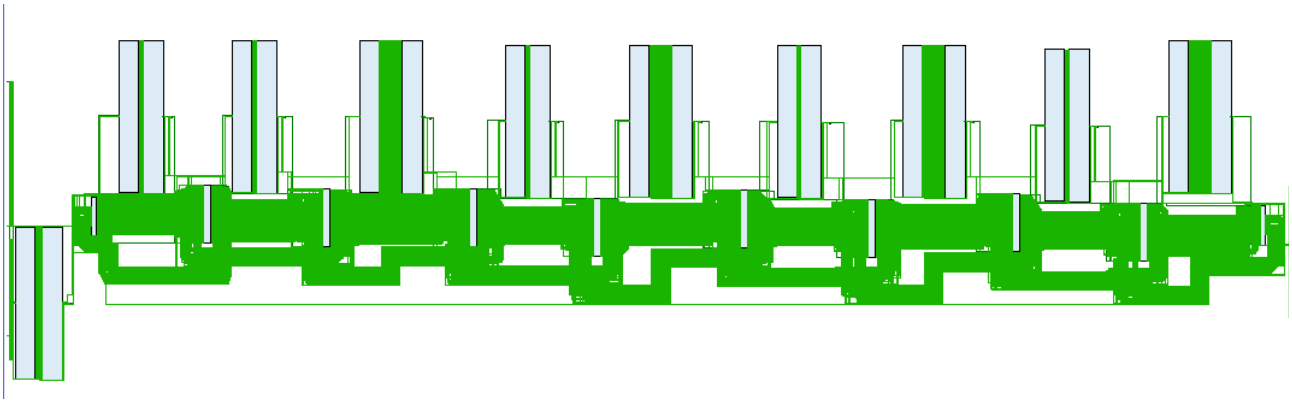
| Resource | Utilization | Available | Utilization % |
|---|---|---|---|
| LUT | 9913 | 303600 | 3.27 |
| FF | 6400 | 607200 | 1.05 |
| IO | 386 | 600 | 64.33 |



## FPGA Implementation Floorplan



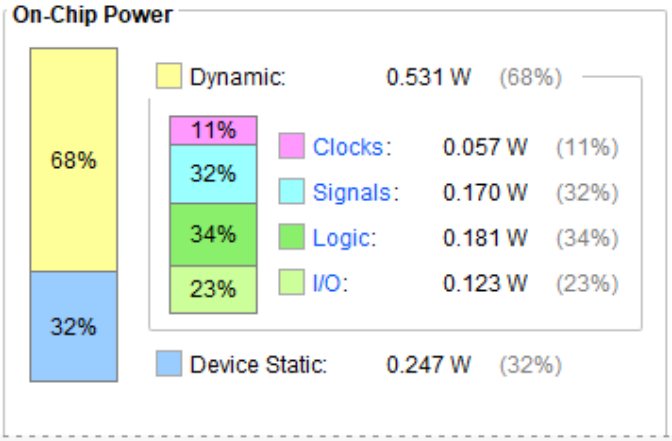

## FPGA Implementation Schematic



## FPGA Power Report

Power analysis from Implemented netlist. Activity derived from constraints files, simulation files or vectorless analysis.

| | |
|---|---|
| **Total On-Chip Power:** | **0.779 W** |
| **Design Power Budget:** | **Not Specified** |
| **Power Budget Margin:** | **N/A** |
| **Junction Temperature:** | **26.1°C** |
| Thermal Margin: | 73.9°C (50.1 W) |
| Effective ϑJA: | 1.4°C/W |
| Power supplied to off-chip devices: | 0 W |




## 5.6. Performance Metrics (ASIC Synthesis)

Based on the 40-stage pipelined architecture and a target clock period of 1 ns (1 GHz), the performance metrics for the synthesized ASIC design are as follows:

| Metric | Value |
|---|---|
| **Latency** | 40 cycles * 1 ns/cycle = 40 ns |
| **Throughput** | 128 bits / 1 ns = 128 Gbps |
| **Area** | 39514.402073 $\mu m^2$ |
| **Power** | 46.450 mW |

## 4.6. Performance Metrics (FPGA Implementation)

Based on the 40-stage pipelined architecture and an achieved clock frequency of 100 MHz (10 ns period), the performance metrics for the FPGA implementation are as follows:

| Metric | Value |
| --- | --- |
| **Latency** | 40 cycles * 10 ns/cycle = 400 ns |
| **Throughput** | 128 bits / 10 ns = 12.8 Gbps |
| **LUTs** | 9913 |
| **FFs** | 6400 |
| **I/O** | 386 |
| **Total On-Chip Power** | 0.779 W |