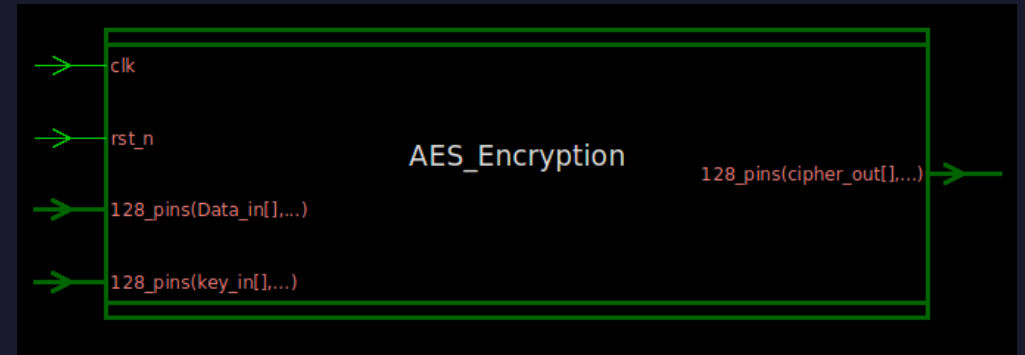


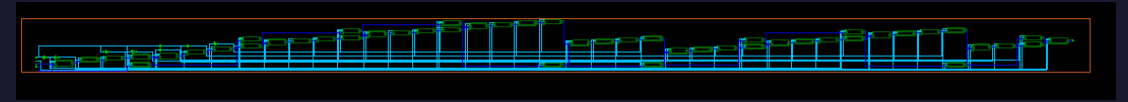
Introduction to AES

- Advanced Encryption Standard (AES) is a symmetric block cipher standardized by NIST
- Operates on 128-bit data blocks using a 128-bit key (AES-128)
- Consists of 10 rounds of transformations: SubBytes, ShiftRows, MixColumns, and AddRoundKey
- Our implementation features a 40-stage pipeline architecture
- Achieves high throughput: 12.8 Gbps on FPGA, 128 Gbps on ASIC
- Operates at 100 MHz on FPGA and 1 GHz on ASIC



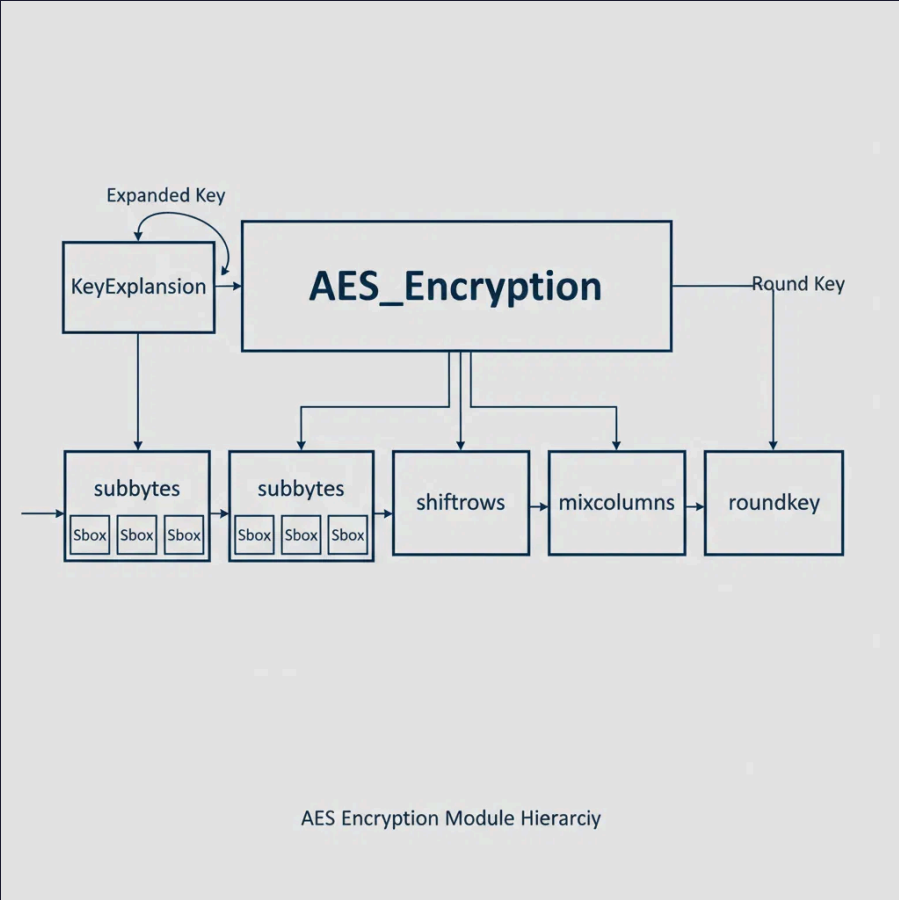
40-Stage Pipelined Architecture

- Design features **40 pipeline stages** for maximum throughput
- Each AES operation (SubBytes, ShiftRows, MixColumns, AddRoundKey) is registered
- Key expansion is also pipelined with unique round constants
- Initial latency: 40 clock cycles
- After pipeline fill, produces one 128-bit output per clock cycle
- DFF_128 modules used throughout for consistent pipeline registers
- Final round omits MixColumns operation per AES standard



RTL Design Modules

Module	Function
AES_Encryption	Top-level module orchestrating the entire encryption process
KeyExpansion	Generates round keys using S-box and round constants
subbytes	Performs byte substitution using S-box lookup tables
shiftrows	Cyclically shifts rows of the state matrix
mixcolumns	Mixes data within each column using GF(2^8) operations
roundkey	XORs the state with the round key
Sbox	Implements the AES substitution box
DFF_128	128-bit register for pipeline stages



Verification Methodology

1. Submodule Verification

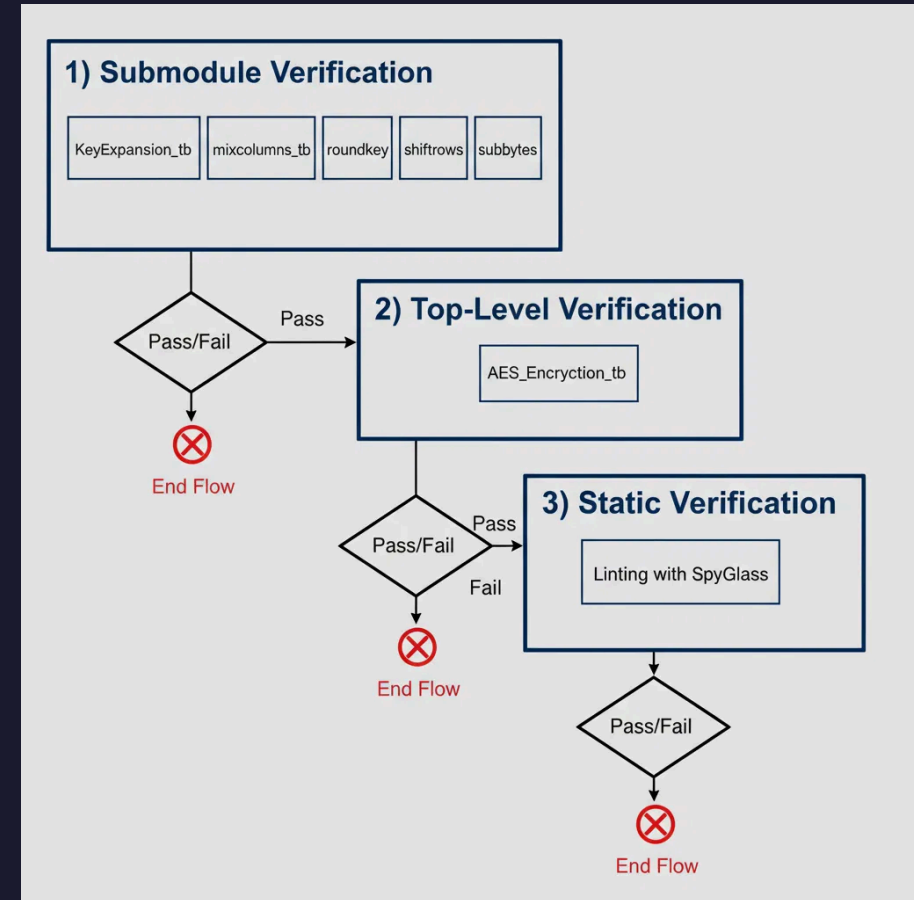
- ✓ Individual testbenches for each functional module (KeyExpansion, mixcolumns, roundkey, shiftrows, subbytes)
- ✓ Verified against known test vectors and expected outputs

2. Top-Level Verification

- ✓ Comprehensive testbench (AES_Encryption_tb.sv) for the integrated design
- ✓ Validated pipeline operation across all 40 stages

3. Static Verification (Linting)

- ✓ SpyGlass tool used to check for coding issues and style violations
- ✓ Passed without violations, confirming synthesis-friendly design








FPGA Implementation Results

Target FPGA: Xilinx Virtex-7

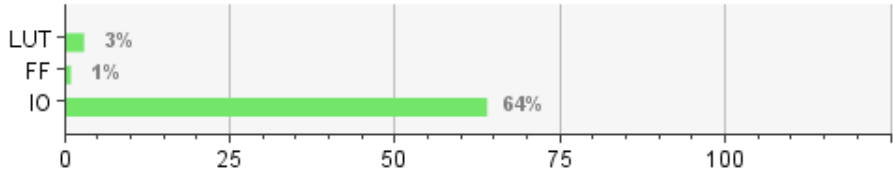
Device: xc7vx485tffg1157-2L

Maximum Frequency: 100 MHz

-  **Timing:** All constraints met with WNS = 0.557 ns
-  **Utilization:** 9,913 LUTs (3.27%), 6,400 FFs (1.05%)
-  **I/O:** 386 pins (64.33% of available)
-  **Power:** Total on-chip power of 0.779 W
-  **Constraints:** 10 ns clock period with 0.1 ns uncertainty

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.					

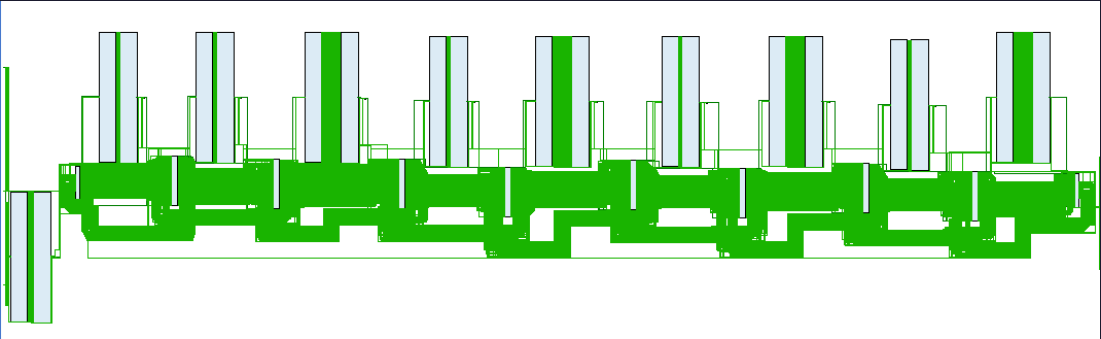
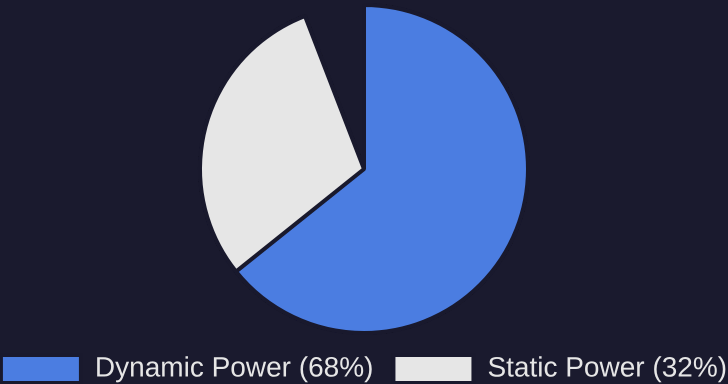
Resource	Utilization	Available	Utilization %
LUT	9913	303600	3.27
FF	6400	607200	1.05
IO	386	600	64.33



FPGA Performance Metrics

Metric	Value
Clock Frequency	100 MHz
Latency	$40 \text{ cycles} \times 10 \text{ ns} = 400 \text{ ns}$
Throughput	$128 \text{ bits} / 10 \text{ ns} = 12.8 \text{ Gbps}$
Total Power	0.779 W

Power Breakdown:



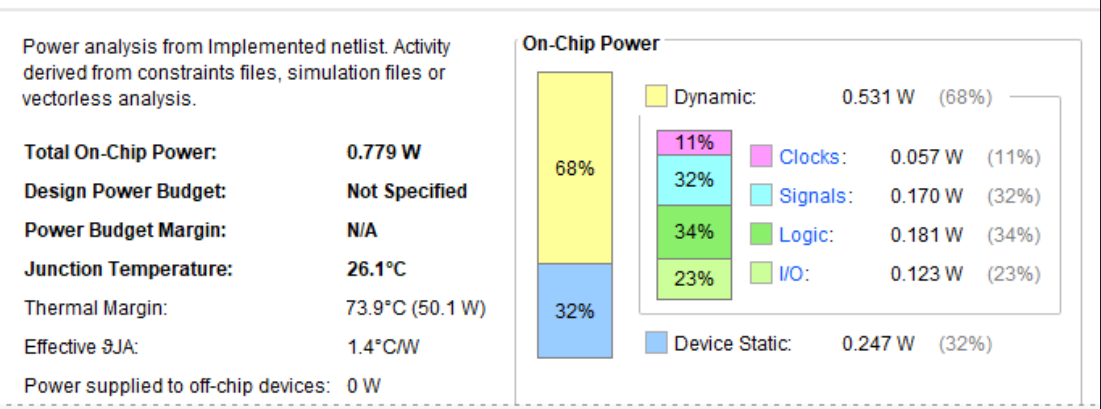
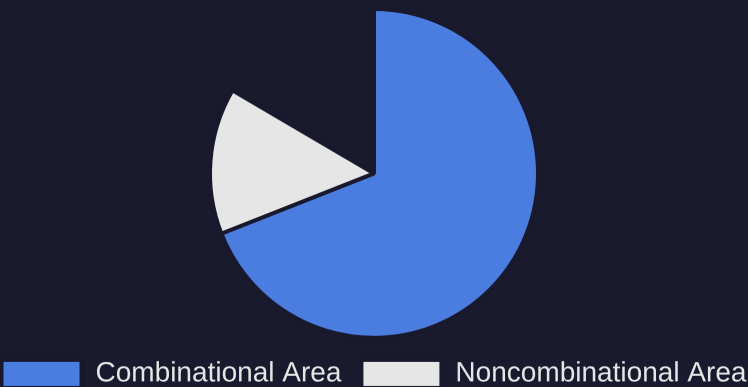
ASIC Synthesis Results

Synthesis Tool: Synopsys Design Compiler 2018

Target Frequency: 1 GHz (1 ns period)

- Total Cell Area:** 39,514.40 μm^2
- Total Power:** 46.45 mW
- Timing:** Setup constraints met (WNS = 0.00 ns)
- Hold Violations:** 4,576 paths (require clock tree synthesis)
- Cell Count:** 116,305 (109,605 combinational, 6,400 sequential)

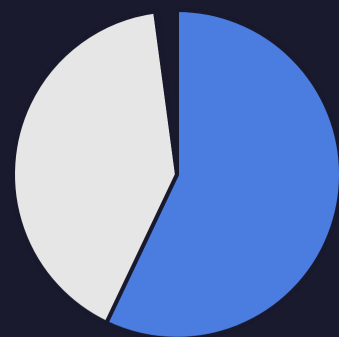
Area Breakdown:



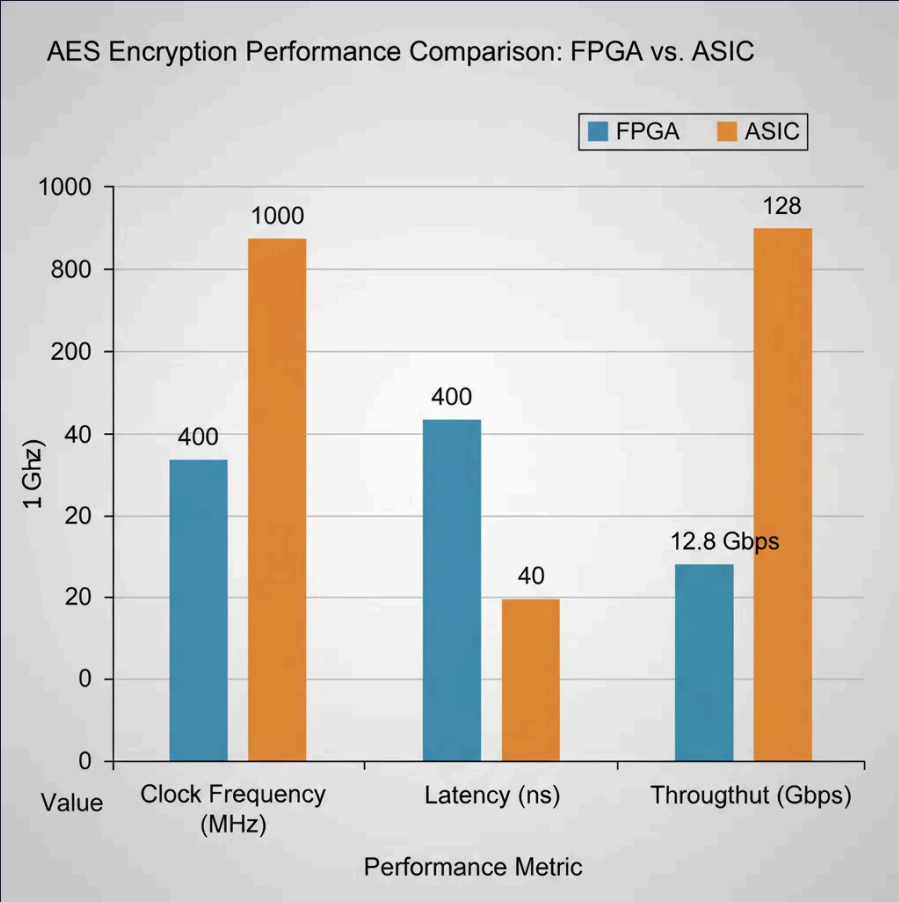
ASIC Performance Metrics

Metric	Value
Clock Frequency	1 GHz
Latency	40 cycles × 1 ns = 40 ns
Throughput	128 bits / 1 ns = 128 Gbps
Area	39,514.40 μm²
Power	46.45 mW

Power Breakdown:



Switching Power Internal Power Leakage Power



Conclusion

Design Success

Successfully implemented a **40-stage pipelined AES encryption core** with modular RTL design

Verification

Comprehensive verification at submodule and top levels
Passed static linting with **zero violations**

FPGA Implementation

Achieved **100 MHz** on Xilinx Virtex-7
Throughput: **12.8 Gbps**

ASIC Synthesis

Achieved **1 GHz** with Synopsys DC 2018
Throughput: **128 Gbps**
Area: 39,514.40 μm^2 , Power: 46.45 mW

