Architectural Evaluation of Iterative and Unrolled AES-128 in 45 nm Using an Open-Source Flow

Dinis Santos
DEEC, NOVA FCT
2829-516 Caparica, Portugal
dj.santos@campus.fct.unl.pt

Joao Cabacinho
DCM, NOVA FCT
CENIMAT | I3N
2829-516 Caparica, Portugal

Joao Casaleiro
DEETC, ISEL
CTS-UNINOVA & LASI
1959-007 Lisbon, Portugal

Luis Bica Oliveira
DEEC, NOVA FCT
CTS-UNINOVA & LASI
2829-516 Caparica, Portugal

***Abstract*—This paper presents a systematic architectural evaluation of iterative, partially unrolled and fully pipelined AES-128 cores synthesized using a fully open-source ASIC flow in 45 nm technology. Three design points are explored under identical synthesis conditions: a 10-cycle iterative architecture reusing a single round block, a 2-round partially unrolled implementation and a fully unrolled 10-stage 128-bit pipeline producing one block per clock cycle after pipeline fill. All designs were synthesized with Yosys and analysed using OpenSTA and the Nangate 45 nm standard-cell library. The fully pipelined architecture achieves up to 881 MHz and 113 Gbps in post-synthesis timing analysis. To enable fair comparison with prior literature, silicon area was additionally normalized to 65 nm, allowing consistent throughput-per-area evaluation across technology nodes. A composite-field $GF((2^4)^2)$ S-Box variant is also implemented to quantify the impact of arithmetic structure on frequency, area and efficiency. All architectures were validated against NIST reference vectors, demonstrating reproducible open-source AES evaluation.**

***Keywords*—AES; hardware implementation; pipeline; loop unrolling; Composite-field S-Box; open-source; ASIC synthesis; Yosys; OpenSTA; Nangate 45.**

I. Introduction

The Advanced Encryption Standard (AES) is widely deployed in secure embedded and high-performance systems, where the trade-off between silicon area and throughput is critical. Compact iterative implementations minimize area by reusing a single round block, but require multiple cycles per block, limiting throughput. In contrast, fully unrolled and pipelined architectures replicate round logic to achieve one block per cycle after pipeline fill, at increased area cost. This work presents a controlled architectural evaluation of iterative, partially unrolled, and fully pipelined AES-128 implementations synthesized using a fully open-source 45 nm ASIC flow (Yosys + OpenSTA with the Nangate 45 nm library). All architectures share a 128-bit datapath and are evaluated under identical synthesis conditions to isolate architectural trade-offs. Post-synthesis results show that the fully unrolled pipeline reaches 113 Gb/s at 881 MHz with competitive throughput-per-area relative to reported 45 nm implementations.

II. Architecture and Methodology

Three AES-128 architectural variants were implemented in synthesizable Verilog: a 10-cycle iterative core reusing a single round block, a 2-round partially unrolled architecture processing two rounds per cycle and a fully unrolled 10-stage pipeline instantiating one round per stage. All designs operate on a 128-bit datapath and share identical round and key-expansion modules to ensure controlled comparison. In the fully pipelined configuration, 128-bit register boundaries are inserted between consecutive rounds, reducing combinational depth and enabling one ciphertext block per clock cycle after an initial 10-cycle pipeline fill. All architectures were synthesized using Yosys and analysed with OpenSTA targeting the Nangate 45 nm standard-cell library. Maximum frequency and silicon area were extracted from post-synthesis static timing analysis and reported in mm².

TABLE I.
Simulation based evaluation at 45 nm.

AES-128 Core Comparison at 45 nm								
Datapath With	Design	Area (mm^2)	CLK (MHz)	Throughput (Gbps)	Throughput (bits/cycle)	Cycles /Round	Latency (Cycles)	Area Efficiency ($Gbps/mm^2$)
128	Mathew et al.[1]	0.150	2100	53	64	2	20	353
	Sayilar and D. Chiou [2]	6.320	1000	128	64	2	20	20
	Dong et al [3]	0.13	870	111	116	1.1	11	854
	This work							
	Pipe Line	0.109	881	113	128	1	10	1035
	Pipe Line GF	0.052	671	86	128	1	10	1652
	Iterative	0.032	293	3.8	12.8	1	10	117
	Iterative GF	0.019	320	4.1	12.8	1	10	216
	P Unrolled	0.040	284	7.3	25.6	0.5	5	182
	P Unrolled GF	0.022	220	5.6	25.6	0.5	5	256

III. Results and Comparison

The fully pipelined architecture achieves 881 MHz, while the composite-field (GF) variant reaches 671 MHz. The iterative and 2-round unrolled designs operate between 220-320 MHz. These frequencies correspond to steady-state throughputs of 113 Gb/s (pipeline), 86 Gb/s (pipeline GF), 3.8-4.1 Gb/s (iterative LUT-GF) and 7.3-5.6 Gb/s (2-round unrolled LUT-GF). At 45 nm, the LUT-based pipeline occupies 0.109 mm², yielding 1035 Gbps/mm², while the GF variant reduces area to 0.052 mm² and increases efficiency to 1652 Gbps/mm². Compared with reported 45 nm implementations [1-3], the proposed pipeline achieves comparable throughput and competitive or higher throughput-per-area. The iterative and partially unrolled variants illustrate the expected trade-off between round replication, silicon area and performance.

IV. Conclusions

The fully unrolled pipeline reaches 113 Gb/s at 881 MHz with 0.109 mm² area. The results demonstrate that an open-source 45 nm flow enables reproducible and competitive AES evaluation.

This work was supported by the national funds through the Fundação para a Ciência e a Tecnologia (FCT) under the CTS multiannual funding program UID/00066/2025, the Lisbon 2030 Program under the code LISBOA2030-FEDER-00816400, and by the European Union through the European Regional Development Fund (ERDF), with DOI: 10.54499/2023.16583.ICDT.

References

[1] S. K. Mathew et al., "53 Gb/s GF(2^4)^2 AES accelerator in 45 nm," IEEE J. Solid-State Circuits, vol. 46, no. 4, 2011.

[2] G. Sayilar and D. Chiou, "Cryptoraptor: High-throughput cryptographic processor," in Proc. IEEE/ACM ICCAD, 2015.

[3] P. K. Dong et al., "45 nm high-throughput AES for real-time applications," in Proc. ISCIT, 2019.