

An Efficient AES-128 CMOS Architecture with Round Reuse and Composite Field S-Box to Secure IoT Devices

S. Ahmed^{1,2}, N. Ahmad^{1,3*}, C. Uttrapphan¹, A. Wijayanto^{1,4} and A. Hirsi^{1,5}

¹*Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Parit Raja, Johor 86400, Malaysia*

²*Department of Electrical Engineering, Sukkur IBA University, Sukkur, 65200, Sindh, Pakistan*

³*VLSI and Embedded Technology (VEST) Focus Group, Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Parit Raja, Johor 86400, Malaysia*

⁴*Informatics Department, Universitas Sebelass Maret, Surakarta, Indonesia*

⁵*Faculty of Engineering, Jamhuriya University of Science and Technology, Mogadishu, Somalia*

The rapid growth of the Internet of Things (IoT) has intensified the demand for lightweight cryptographic solutions that deliver high security without compromising energy and area constraints. This paper presents a highly efficient AES-128 hardware architecture specifically optimised for resource-constrained IoT devices. The proposed design employs reusing a 128-bit AES framework resource, enabling an extensive reduction in functional units across all transformation stages. Additionally, the elimination of intermediate registers and the reuse of a single round computation block for all encryption rounds significantly reduce area while balancing the trade-offs between throughput, frequency and power. A key innovation in this work is the implementation of a compact S-box using composite Galois Field GF_{2^8} arithmetic to enhance the substitution efficiency while maintaining cryptographic strength. The physical layout implemented on 32 nm technology reveals that the proposed architecture achieves a core area of only 0.015 mm^2 , an operating frequency of 200 MHz, with 0.014 Gbps throughput, and a low power consumption of 1.4 mW, offering a well-balanced trade-off among performance, security, and hardware efficiency. A comparative analysis with state-of-the-art designs demonstrates the superiority of this approach for achieving low-cost, energy-aware cryptographic protection. The proposed solution is highly suitable for secure resource constrained IoT deployments.

Keywords: Advanced encryption standard (AES); Application Specific Integrated Circuits (ASIC); Physical Layout Design; Galois field (GF); Internet of Things (IoT); lightweight cryptography; Substitution box (S-box)

I. INTRODUCTION

As the world moves toward greater digitalisation, the paradigm of information exchange is rapidly shifting from conventional communication methods to interconnected, intelligent systems (Bharathi Madavarapu *et al.*, 2024). The Internet of Things (IoT) has enabled widespread connectivity among digital devices and sensors across various

applications, including smart healthcare, agriculture, industrial automation, smart cities, and smart houses (Kohli, Aman and Sikdar, 2024). By 2030, the number of connected IoT devices is projected to surpass one trillion (Schiller *et al.*, 2022). Most IoT nodes are battery-powered and therefore constrained by limited computational resources, memory, and energy availability. The proliferation of interconnected

*Corresponding author's e-mail: nabihah@uthm.edu.my

devices, each employing diverse communication protocols, has significantly increased the attack surface, with studies indicating that approximately 70% of IoT devices are vulnerable to security threats (Ahmed *et al.*, 2025). Although lightweight cryptographic algorithms have been developed, many are insufficient in addressing the growing and evolving security challenges of these heterogeneous environments (Litoussi *et al.*, 2020). Figure 1, discusses the infrastructure for a complete secure IoT environment, having secure data transfer among the connected devices but involving data security element. Encryption remains a fundamental mechanism for ensuring the confidentiality, integrity, and authenticity of data in IoT systems (Cheng *et al.*, 2023). Among available encryption standards, the Advanced Encryption Standard (AES) is widely adopted due to its proven resistance to cryptanalytic attacks (Ghosal, Sardar and Chowdhury, 2024). It supports three key lengths 128, 192, and 256 bits offering varying levels of security, with AES-256 regarded as sufficiently robust even against potential quantum-era threats (Alhayani *et al.*, 2023).

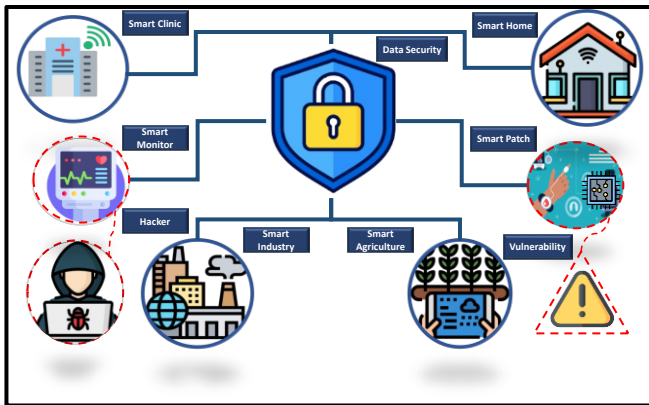


Figure 1. IoT applications with attacks and vulnerabilities.

AES is utilised in a wide array of hardware and software security applications, including data storage, wireless communication, cloud storage, and IoT edge devices (Abebe, 2023). Due to the extensive resource consumption of AES, it is challenging to integrate it directly into constrained IoT devices (Fadhil *et al.*, 2020; Ahmed *et al.*, 2026). Consequently, many researchers have focused on optimising AES for lightweight applications because of its strong shield against cryptanalysis (Singha, Palathinkal and Ahamed, 2023). These optimisations include reducing key sizes, simplifying encryption and decryption, and enhancing key agility to enable frequent, secure key updates. Among these

optimisations, such as reducing the key size, may compromise the security of AES (Ahmed *et al.*, 2025). Hardware AES implementations are also optimised using techniques such as data-path optimisation, algorithm simplification, intermediate-register reduction, resource sharing, and power-saving methods such as clock gating (Abdi *et al.*, 2024). These modifications affect the hardware resource utilisation for IoT resource-constrained devices without compromising the security level of AES (Hirsi *et al.*, 2024). Furthermore, these hardware implementations are considered stronger against cryptanalysis than the software implementations (Hirsi *et al.*, 2025).

This work presents an optimised AES-128 implementation that leverages architectural reuse. While the main data path possesses a 128-bit input, the internal computation within each transformation stage is performed using a 32-bit segmented architecture. The technique of reusing the same 32-bit logic blocks iteratively to complete 128-bit operations reduces the overall hardware complexity. Additionally, intermediate registers between stages are removed, helping minimise storage overhead and dynamic power consumption. A single-round architecture is reused across all 10 AES rounds, improving area and resource efficiency. Furthermore, a resource-optimised S-box based on composite Galois Field arithmetic GF 28 is proposed, specifically tailored for AES-128 to achieve a balanced trade-off among area, power consumption, and throughput. The resulting design is highly suitable for resource-constrained IoT environments where hardware efficiency is critical.

This research presents a highly efficient AES-128 hardware architecture tailored for resource-constrained IoT applications. A key innovation is reusing a single computational round across all 10 encryption iterations, significantly reducing logic duplication and conserving silicon area. Secondly, eliminating intermediate registers between transformation stages minimises switching activity, thereby contributing to both area and power savings. In addition, A notable highlight of this work is the implementation of a Galois Field arithmetic-based S-box, which enhances substitution efficiency while ensuring minimal resource overhead. The proposed architecture was synthesised using Synopsys IC Compiler II at 32 nm, achieving a compact physical design with an optimised trade-

off among area, power, operating frequency, and throughput, making it a robust and scalable solution for secure, low-power IoT systems.

The remainder of this research article is organised as follows. Section II discusses the structure and organisation of AES. In Section III, the proposed optimised AES model, along with the S-box, is discussed in detail. Section IV discusses simulation results, comparisons with related work, and the layout implementation of the proposed model. Lastly, Section V discusses the conclusion and future work of the studies.

II. RELATED WORK

Table 1 provides a comparative novelty positioning of the proposed AES-128 architecture with representative lightweight AES implementations reported in the literature. As observed, individual optimisation techniques such as round reuse, register minimisation, composite Galois Field (GF)-based S-box implementation, and datapath optimisation have previously been explored in different studies. For instance, (Lu *et al.*, 2018) incorporates round reuse and register optimisation techniques to reduce hardware resources, whereas (Shreedhar *et al.*, 2019) employs a composite GF-based S-box together with a segmented datapath architecture. Similarly, (Bui *et al.*, 2017) focuses on datapath optimisation and hardware simplification for lightweight AES realisation.

However, existing work primarily emphasises specific optimisation strategies rather than integrating multiple lightweight design techniques within a single implementation framework. In contrast, the proposed architecture combines round reuse, complete elimination of intermediate registers, a composite GF-based S-box, and a 32-bit datapath organisation within a unified AES-128 design. Furthermore, unlike some prior studies that report only synthesis-level results, the proposed work includes ASIC implementation and physical layout realisation using 32 nm CMOS technology.

Therefore, the novelty of the proposed work lies not in introducing an entirely new cryptographic algorithm or a standalone optimisation technique, but in the effective integration and ASIC implementation of multiple complementary architectural optimisations. This combined optimisation strategy enables substantial reductions in

hardware complexity, area utilisation, and power consumption while maintaining compliance with the AES standard and meeting the requirements of resource-constrained IoT applications.

Table 1. Novelty positioning of the proposed AES-128 architecture compared with representative lightweight AES implementations.

Features	(Lu <i>et al.</i> , 2018)	(Shreedhar <i>et al.</i> , 2019)	(Bui <i>et al.</i> , 2017)	This Work
Round Reuse	✓	✗	✗	✓
Register Elimination	✓	Partial	✓	✓
Composite GF S-box	✗	✓	✗	✓
32-bit Datapath	✗	✓	✓	✓
ASIC Physical Layout	✗	✓	✗	✓
Combined Optimisation Strategy	✗	✗	✗	✓

III. BACKGROUND OF AES

AES is a symmetric block cipher standardised by NIST in 2001, superseding the Data Encryption Standard (DES) due to its increasing vulnerability to brute-force attacks and its limited key length. AES was introduced to provide a secure, flexible, and high-performance encryption method, suitable for modern software and hardware platforms. AES operates on fixed 128-bit data blocks and supports key lengths of 128, 192, and 256 bits, corresponding to 10, 12, or 14 encryption rounds (Daemen and Rijmen, 2002). Among these, AES-128 is the most widely used due to its balanced trade-off between security, performance, and hardware resource utilisation. The AES encryption process is built around a series of iterative transformation stages to ensure strong diffusion and confusion properties, which are essential for cryptographic security (Wang *et al.*, 2016). Each round of AES-128 consists of the following four transformations: Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round-Key, except for the final

round, which excludes Mix-Columns, as shown in Figure 2. A nonlinear substitution is applied to each byte of the 128-bit state using an S-box, which introduces nonlinearity in the Sub-Bytes stage. Shift-Rows is a transposition step that cyclically shifts the rows of the 4×4 state matrix that contribute to inter-byte diffusion. Mix-Columns is a column-wise mixing operation involving matrix multiplication over GF28; this stage disperses byte influence across columns. Add-Round-Key is a bitwise XOR operation between the current state and the round key generated by the key expansion process (Ahmad and Rezaul Hasan, 2013). The Key expansion unit derives a unique round key for each round from the original cipher key using word rotation, sub-Word, and the addition of round constants operations. This process ensures that each round has a distinct key, which enhances cryptographic strength. Among all transformations, the Sub-Bytes stage is considered the most resource-intensive, which is primarily due to the complexity of the S-box operation. The S-box can be implemented using a Look-Up Table (LUT), which stores precomputed substitution values for all 256 possible byte values. This implementation is quite fast but requires significant memory; for this reason, it is less suited to lightweight environments. Composite GF arithmetic, particularly in GF(2⁴)², which decomposes the inverse operation into more efficient logic using structured algebraic transformations. This approach reduces memory consumption and is preferred for area and power-constrained applications such as IoT devices (Ahmad and Hasan, 2021).

To mitigate hardware vulnerabilities, optimised architectures often employ balanced logic paths, reduced switching activity, and power-aware design practices. Composite field-based S-boxes not only conserve area but can also help reduce power leakage by avoiding memory-intensive accesses. This foundational understanding of AES underpins the architectural optimisations proposed in this work, which aim to deliver a lightweight, secure, and high-performance AES-128 design tailored for resource-constrained IoT environments.

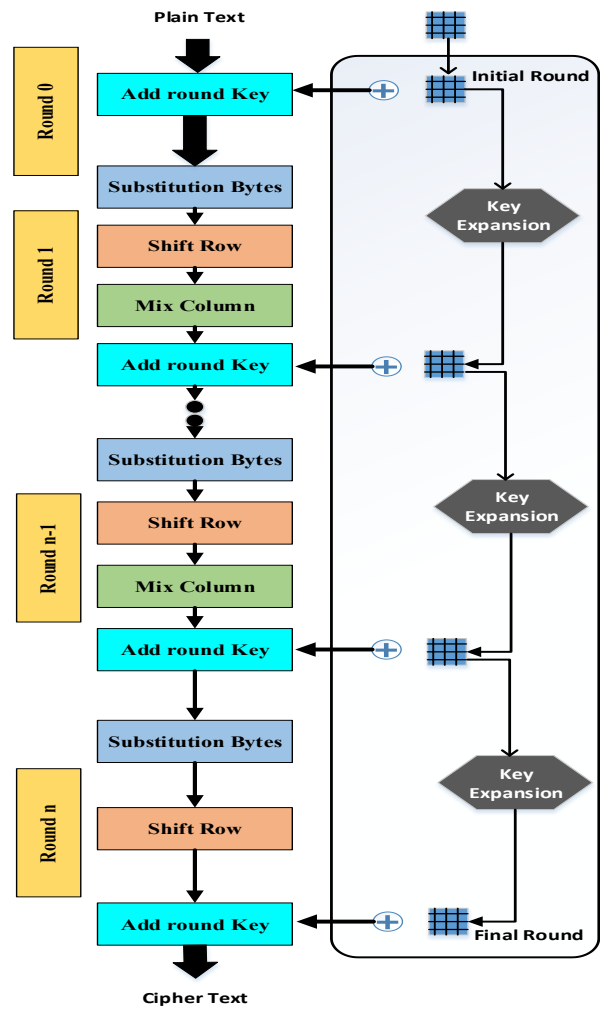


Figure 2. Block diagram of AES encryption cycle.

IV. EFFICIENT AES ARCHITECTURE

The proposed AES hardware architecture is designed to enhance both area efficiency and operational speed by optimising the internal data path and the modular structure of the encryption process. Importantly, the design strictly adheres to the NIST standard's specifications, ensuring that no modifications compromise the functional or cryptographic integrity of the AES algorithm. All transformation stages are preserved as defined. The optimization efforts are confined exclusively to hardware-level resource utilisation, such as data-path segmentation, logic reuse, and register minimisation, without altering the algorithmic operations. This guarantees that the proposed design maintains full compliance with AES standards while achieving improved performance for deployment in resource-constrained environments.

A. Efficient AES Architectural Optimisations

The architecture processes 128-bit data at the input, output, and key, as shown in Figure 3. Inside the main module, the submodules Sub-Bytes, ShiftRows, MixColumns, and AddRoundKey operate on 32-bit data to effectively utilise resources. This bit-width segmentation reduces hardware resource utilisation and enables a more compact, scalable design, particularly suitable for lightweight cryptographic applications. These submodules are chained to maintain the logical flow of the AES round transformation while minimising circuit complexity. The Sub-Bytes module incorporates a Galois Field-based optimised S-box to further reduce power consumption and area overhead, ensuring suitability for resource-constrained environments. It utilises the principle of breaking the S-box into stages to perform the required operation. Rather than replicating the AES round logic for each round, a single round-processing module is iteratively reused under the control of a finite-state machine (FSM). This unit governs the flow of data and control signals, including multiplexer selections, round constant, and key scheduling.

The Key-Generation module is tightly integrated with the data path and reuses existing logic to dynamically derive round keys. A separate round counter module generates the round constants via a controlled incrementing mechanism synchronised with the encryption rounds. Data and key inputs are initially loaded via selection logic and XORed, in alignment with the Add-Round-Key step of the AES algorithm. The outputs from the transformation stages are cyclically routed through the round logic, with the Control Unit managing state transitions and synchronisation across the clock cycles. Such a design is particularly suitable for lightweight cryptographic implementations on ASIC platforms where power, area, and resource efficiency are critical, with some compromise in throughput.

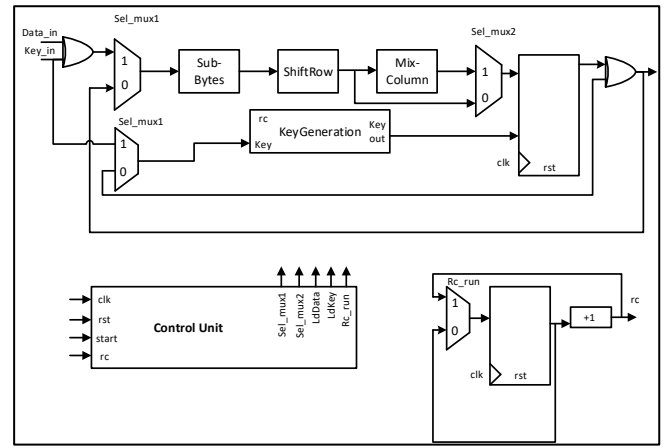


Figure 3. Proposed efficient AES-128 block diagram

B. 8-bit Substitution Box

The internal architecture of the proposed S-box is optimised for AES-128 encryption using composite Galois Field arithmetic. The design meets the standard AES S-box transformation stages: isomorphic mapping, multiplicative inverse, inverse isomorphic mapping, and affine transformation as discussed in Figure 4. The focus of this architecture is to optimise the Sub-Bytes operation by minimising area and power while sustaining balanced throughput and frequency, suitable for lightweight cryptographic implementations.

Isomorphic Mapping transforms the input byte from the standard polynomial basis into an isomorphic basis. This transformation enables more efficient computation in the composite field $GF(2^4)^2$, which simplifies the arithmetic required in the next stage. The Multiplicative Inverse stage computes the inversion of the input element in $GF(2^8)$, excluding the zero inputs. To reduce the logic complexity of inversion, the design employs a composite field representation where $GF(2^8)$ is decomposed into $GF(2^4)^2$. This hierarchical representation allows the inverse to be performed using smaller GF24 blocks and arithmetic circuits to significantly reduce area and switching power. Following inversion, the data is passed through the Inverse Isomorphic Mapping stage, which returns the value from the isomorphic basis back to the standard AES field representation. This ensures consistency and compatibility with the final transformation stage. The Affine Transformation completes the S-box operation by applying a fixed linear transformation followed by a bitwise XOR with a constant vector. This enhances the diffusion properties and provides resistance

against linear and differential cryptanalysis. The internal logic of the multiplicative inverse is further optimised into a three-stage structure comprising Stage 1, Inverse, and Combining Stages. Inter stage data-paths utilise 4-bit and 8-bit buses to enable efficient word-level operations while minimising power dissipation. This optimised S-box design achieves a favourable trade-off between hardware efficiency and cryptographic robustness. It is particularly suitable for resource constrained environments such as IoT edge devices, where low power consumption and small silicon footprint are paramount.

Although the present work focuses on AES-128 due to its widespread adoption in lightweight IoT applications, the proposed architecture is inherently scalable to support AES-192 and AES-256. The core encryption transformations, including Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round-Key, remain unchanged across all AES variants. Therefore, the proposed round-reuse architecture and composite field S-box can be directly reused. Only the key expansion module and the FSM controller require modification to accommodate larger key sizes and more encryption rounds. This architectural compatibility facilitates future extension of the proposed design to higher-security AES variants while preserving the lightweight design philosophy.

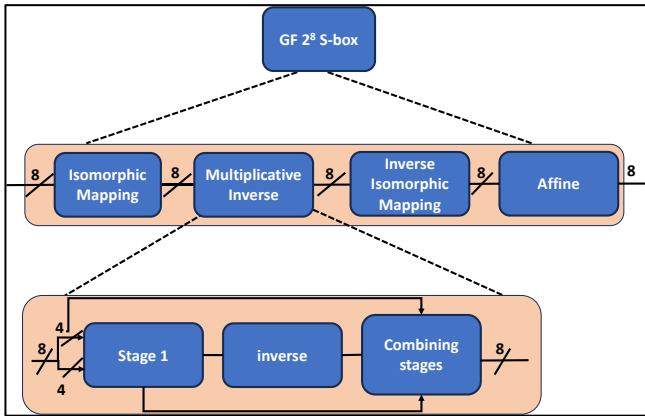


Figure 4. Block diagram of Galois field based 8-bit S-box

V. RESULTS AND DISCUSSION

The section provides an in-depth discussion of the results obtained from simulating the proposed work. In the first stage, the architecture's functionality is checked. In comparative analysis, the results of this research are compared with the previous implementations. Furthermore,

the layout of the proposed architecture is discussed in this section, providing a way forward for researchers.

A. Experimental Setup

The proposed AES-128 architecture was implemented and evaluated using the Synopsys ASIC design flow as shown in Table 1. RTL functionality was verified using Synopsys Verification Compiler Simulator (VCS). Logic synthesis was performed using Synopsys Design Compiler, followed by physical implementation and place-and-route using Synopsys IC Compiler II (ICC-II). The design was mapped to a 32 nm CMOS standard-cell technology library and evaluated under a supply voltage of 0.9 V at the Slow-Slow (SS) process corner with an operating temperature of 125°C. Timing analysis was performed at a target clock frequency of 200 MHz, corresponding to a clock period of 5 ns. Area, timing, and power metrics were extracted following synthesis and physical implementation. All reported results correspond to the specified implementation conditions and ASIC design environment summarised in Table X, ensuring transparency and reproducibility of the proposed architecture.

Table 1. Experimental setup of the proposed AES-128 architecture.

Parameter	Value
Technology Node	32 nm CMOS
RTL Simulator	Synopsys VCS
Synthesis Tool	Synopsys Design Compiler
P&R Tool	Synopsys ICC-II
Supply Voltage	0.9 V
Clock Frequency	200 MHz
Clock Period	5 ns
Process Corner	Slow-Slow
Temperature	125°C
Design Type	ASIC
Cipher Key Length	128-bit

B. Simulations Results

The waveform illustrated in the Figure 5, represents the simulation results of Register Transfer Level (RTL) implementation of the AES-128 encryption algorithm using Synopsys verification compiler suite (VCS). The design operates with a system clock of 10 nanoseconds per cycle. At the beginning of the simulation, a 128-bit plaintext through ports data_in and a 128-bit cipher key using key_in ports are supplied as inputs to the encryption module. Upon assertion of the start signal, the AES core begins its operation. The key expansion unit subsequently derives ten additional round

keys from the initial key, in accordance with the AES-128 specification. These round keys are sequentially applied to each of the round during encryption process.

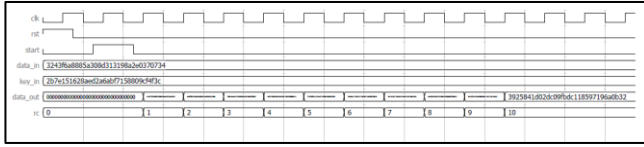


Figure 5. Simulation results of AES-128 design using Synopsys EDA tool

The signal round counter incrementally tracks the current encryption round, progressing from round 0 up to round 10. During each round, intermediate results are processed internally using on the fly concept without using registers for storage. As observed in the waveform, the final encrypted output appears at data_out after tenth round and is correctly achieved. This confirms the correct functionality of the AES-128 RTL design and validates the sequential round-based encryption process.

Table 2 presents a breakdown of the AES-128 encryption simulation outputs, validating the RTL design. It showcases the 128-bit plaintext input, the original key, and the final encrypted output for each AES round. The algorithm conducts 10 main rounds following the initial round, with the key expansion module producing a unique 128-bit round key for each. The output of each round serves as the input for the next, leading to a final ciphertext of “3925841d02dc09fbdc118597196a0b32” at round 10. This result matches NIST’s standard test vectors, confirming the design’s compliance with AES specifications.

Table 2. Details of the AES encryption cycle

Data Input	3243f6a8885a308d313198a2e0370734
Input Key	2b7e151628aed2a6abf7158809cf4f3c
Data Output	3925841d02dc09fbdc118597196a0b32

C. Results Comparison with Previous Works

Numerous research efforts have been undertaken to optimise AES with respect to area utilisation, power consumption, throughput, and operating frequency, particularly for deployment in resource-constrained IoT environments. In (Hocquet *et al.*, 2011), the authors explored ultra-low voltage scaling, increased gate length, and recharacterised standard

cells to reduce area. However, these modifications significantly degraded both throughput and frequency which render the approach unsuitable for real-time IoT applications. In contrast, the work in (Dong, Nguyen and Tran, 2019) focused on achieving high throughput by employing pipelined key expansion and combinational logic across the design, including a pipelined Sub-Bytes operation. Although this design achieved commendable throughput but it incurred excessive area overhead, making it impractical for compact IoT devices. The authors in (Nabihah Ahmad *et al.*, 2024) presented an optimised AES design based on a modified Galois Field S-box, offering a balanced trade-off between area and throughput. Similarly, the study in (Noor and John, 2019) used resource sharing and composite Galois Field arithmetic, introducing row-wise data access rather than conventional byte- or column-wise access. While this technique improved computational structure, it significantly increased silicon area and yielded only marginal throughput gains. Clock gating was applied to mitigate power consumption. In (Lu *et al.*, 2018), the reuse of the S-box and reduction of intermediate registers by up to 67.8% was proposed. This strategy directly inspired the current work, which builds upon that concept to achieve further improvements. The study in (Shreedhar *et al.*, 2019) adopted an 8-bit S-box with a 32-bit data path for AES transformations to reduce data-path complexity. Additionally, (Bui *et al.*, 2017) implemented a 32-bit data path, along with intermediate-register minimisation and on-the-fly key expansion, to reduce overhead. Overall, while each of these prior approaches introduced valuable techniques for AES optimisation, most involved trade-offs between area, power, and performance. The current work advances these ideas by integrating S-box reuse, composite field arithmetic, data-path segmentation, and register elimination, achieving a balanced and scalable solution ideal for lightweight cryptographic applications in IoT.

The proposed design demonstrates significant improvements in core area efficiency when compared to several existing works as given in Table 3. Specifically, it occupies a core area of 0.015 mm², which is notably smaller around 13% and 76% than those reported in references (Hocquet *et al.*, 2011; Lu *et al.*, 2018), whereas, comparing to (Dong, Nguyen and Tran, 2019; Nabihah Ahmad *et al.*, 2024;

Noor and John, 2019) is considered as smallest work, indicating a well-optimised spatial footprint. This reduction in area is particularly important for enhancing integration density, which in turn can lead to lower manufacturing costs and improved suitability for compact, embedded applications. Although reference (Lu *et al.*, 2018) achieves a nominal core area but it suffers from a much lower operating frequency, which may limit its performance in high-speed or real-time scenarios where higher throughput is essential. Similarly, while reference (Shreedhar *et al.*, 2019) presents a smaller area of 0.01 mm², this comes with a significantly higher power consumption of 3.4 mW, which reduces its overall energy efficiency and makes it less suitable for power-constrained environments. In contrast, the proposed design offers a well-balanced trade-off between area, frequency, and power consumption. It maintains a compact area while delivering a high operating frequency of 200 MHz and moderate power consumption of 1.4 mW, thereby offering a more efficient and practical solution.

Beyond area and power efficiency, the proposed architecture also aligns closely with the objectives of lightweight cryptographic design. In such systems,

minimising hardware resources must be carefully balanced with maintaining adequate performance. The proposed AES implementation successfully meets this challenge by achieving a balanced throughput of 0.014 Gbps without sacrificing area or energy efficiency. Many lightweight designs tend to lower frequency or throughput to conserve resources, but this implementation maintains a moderate data rate at a high operating frequency, making it suitable for real-time encryption tasks. This equilibrium of performance and efficiency is essential for resource-constrained IoT applications, including smart sensors, wearable health devices, and secure embedded systems. By combining a compact footprint, low power consumption, and sufficient throughput, the proposed design demonstrates its potential as a robust, lightweight AES solution for next-generation low-power security applications.

Table 2. Comparative analysis of proposed with previous works

Design	Tech (nm)	Block Size (bits)	F (MHz)	Area (mm ²)	Thr (Gbps)	Power (mw)
(Hocquet <i>et al.</i> , 2011)	65	128	0.322	0.018	0.0001	2.45
(Dong, Nguyen and Tran, 2019)	45	128	870	0.13	111.3	56.3
(Nabihah Ahmad <i>et al.</i> , 2024)	90	128	100	0.4324	0.011	-
(Noor and John, 2019)	90	128	100	22.724	0.0256	-
(Lu <i>et al.</i> , 2018)	28	128	50	0.028	0.030	0.45
(Shreedhar <i>et al.</i> , 2019)	65	128	200	0.01	-	3.460
(Bui <i>et al.</i> , 2017)	28	128	10	-	0.028	0.20
This Design	32	128	200	0.0159	0.014	1.4

The optimised AES architectural design is implemented in 32 nm CMOS technology following gate-level simulation using the Synopsys Verification Compiler Suite (VCS). The design includes 128-bit input, 128-bit key, and 128-bit output, while the internal data path within each submodule is 32 bits. This architecture achieves a good balance among

power, area, frequency, and throughput. The simulated RTL code produces a successful gate-level netlist by performing synthesis with the design compiler. The final complete hardware layout for the physical design of the lightweight AES is implemented using the ICC-II shell, as shown in Figure 6. The implemented design achieved 0.0159 mm², a

0.014 Gbps throughput, and a power consumption of 1.4 mW at a supply voltage of 0.9 V. The Lightweight AES achieves a good trade-off between frequency, power, and area, achieving 200 MHz.

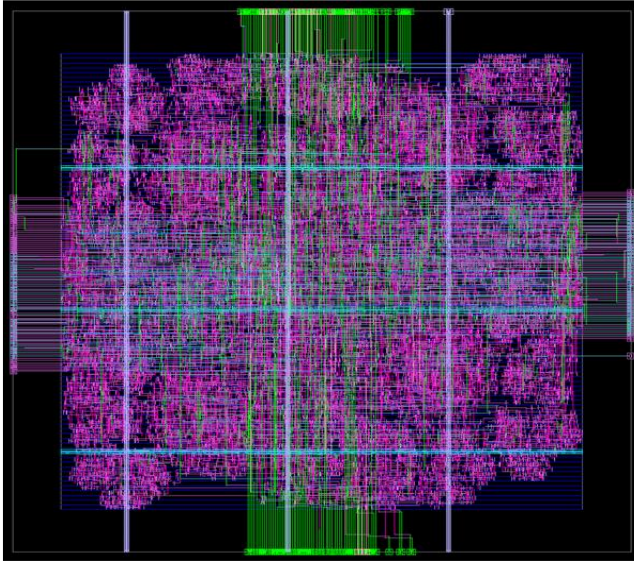


Figure 5. Physical layout of AES core on 32 nm technology.

VI. CONCLUSION

This work presents an optimised and resource-optimised AES-128 architecture tailored for resource-constrained IoT applications. The design enables extensive reuse of computational logic across the 128-bit transformation stages, thereby minimising hardware complexity. The architecture achieves significant reductions in hardware area and power consumption by eliminating intermediate registers between stages and reusing a single round of logic for all rounds. The proposed model integrates a composite GF28-based S-box design, further enhancing substitution efficiency and contributing to overall hardware optimisation. The complete architecture achieves a compact core area of 0.015 mm², an operating frequency of 200 MHz, a throughput of 0.014 Gbps, and a power consumption of 1.4 mW. The proposed solution provides a more balanced trade-off among area, power, and throughput. The physical parameters of layout results validate the proposed design as a highly efficient and secure cryptographic solution for IoT systems where silicon footprint and performance must be co-optimised.

Future work will focus on extending the proposed architecture with additional resource-sharing and datapath-

optimisation techniques to further reduce area and power consumption for ultra-lightweight IoT deployments. In particular, the architecture will be refined toward a fully integrated 8-bit datapath implementation, including optimised Mix-Columns and key expansion modules, to achieve greater hardware efficiency while maintaining cryptographic performance. Furthermore, future research will investigate the integration of established SCA countermeasures, including masking, logic balancing, dual-rail implementations, and power-aware design techniques, and will conduct formal evaluation against Differential Power Analysis (DPA), Electromagnetic Analysis (EMA), and fault-injection attacks. In addition, the proposed architecture will be explored for application-specific deployment in security-sensitive IoT systems such as wearable health monitors, smart medical patches, implantable medical devices, and low-power edge sensing platforms, where stringent constraints on power consumption, silicon area, and real-time operation are critical. The scalability of the architecture toward AES-192 and AES-256 implementations will also be investigated to support higher-security applications requiring extended key lengths.

VII. ACKNOWLEDGEMENT

This work was supported by the Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme under Grant FRGS/1/2022/TK07/UTHM/02/20.

VIII. CONFLICT OF INTEREST

Authors declare that there is no conflict of interests regarding the publication of the paper.

IX. AUTHOR CONTRIBUTION

Salzman **Ahmed:** Writing manuscript & editing, Methodology, Formal analysis. **NorNabihah @ Nabihah Bint Ahmed:** Supervision, Investigation, Formal analysis. **cheesda Uttraphan:** For developing and troubleshooting Verilog code. **Abdinasir Hirsi:** Draft editing and Visualization. **Ardhi Wijayanto:** Proof reading and data collection.

I. REFERENCES

- Abdi, A.H. *et al.* (2024) "Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions," *IEEE Access*, 12, pp. 69941–69980. Available at: <https://doi.org/10.1109/ACCESS.2024.3393548>.
- Abebe, A.T. (2023) "Lightweight and Efficient Architecture for AES Algorithm based on FPGA," *i-ETC : ISEL Academic Journal of Electronics Telecommunications and Computers*, 8(1), p. 3. Available at: <https://doi.org/10.34629/IPL.ISEL.I-ETC.96>.
- Ahmad, N. and Hasan, S.M.R. (2021) "A new ASIC implementation of an advanced encryption standard (AES) crypto-hardware accelerator," *Microelectronics Journal*, 117, p. 105255. Available at: <https://doi.org/10.1016/J.MEJO.2021.105255>.
- Ahmad, N. and Rezaul Hasan, S.M. (2013) "Low-power compact composite field AES S-Box/Inv S-Box design in 65 nm CMOS using Novel XOR Gate," *Integration*, 46(4), pp. 333–344. Available at: <https://doi.org/10.1016/J.VLSI.2012.06.002>.
- Ahmed, S. *et al.* (2025) "Lightweight AES Design for IoT Applications: Optimizations in FPGA and ASIC with DFA Countermeasure Strategies," *IEEE Access* [Preprint]. Available at: <https://doi.org/10.1109/ACCESS.2025.3533611>.
- Ahmed, S. *et al.* (2026) "Area and Power Efficient MixColumns Architecture for Lightweight AES Implementations," *2026 1st International Conference on Innovations in Information and Communication Technologies, IICT 2026* [Preprint]. Available at: <https://doi.org/10.1109/IICT68374.2026.11468724>.
- Alhayani, B.A. *et al.* (2023) "Design of Quantum Communication Protocols in Quantum Cryptography," *Wireless Personal Communications*, pp. 1–18. Available at: <https://doi.org/10.1007/S11277-023-10587-X/FIGURES/5>.
- Bharathi Madavarapu, J. *et al.* (2024) "Heterogeneous Energy Harvesting Techniques for Smart Home IoT Acceleration," *IEEE Access*, 12, pp. 73667–73675. Available at: <https://doi.org/10.1109/ACCESS.2024.3397664>.
- Bui, D.H. *et al.* (2017) "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 25(12), pp. 3281–3290. Available at: <https://doi.org/10.1109/TVLSI.2017.2716386>.
- Cheng, Y. *et al.* (2023) "An Asymmetric Encryption-Based Key Distribution Method for Wireless Sensor Networks," *Sensors* 2023, Vol. 23, Page 6460, 23(14), p. 6460. Available at: <https://doi.org/10.3390/S23146460>.
- Daemen, J. and Rijmen, V. (2002) *The Design of Rijndael*. Berlin, Heidelberg: Springer Berlin Heidelberg (Information Security and Cryptography). Available at: <https://doi.org/10.1007/978-3-662-04722-4>.
- Dong, P.K., Nguyen, H.K. and Tran, X.T. (2019) "A 45nm High-Throughput and Low Latency AES Encryption for Real-Time Applications," *Proceedings - 2019 19th International Symposium on Communications and Information Technologies, ISCIT 2019*, pp. 196–200. Available at: <https://doi.org/10.1109/ISCIT.2019.8905235>.
- Fadhil, M.S. *et al.* (2020) "A New Lightweight AES Using a Combination of Chaotic Systems," *Proceedings of 2020 1st Information Technology to Enhance E-Learning and other Application Conference, IT-ELA 2020*, pp. 82–88. Available at: <https://doi.org/10.1109/IT-ELA50150.2020.9253099>.
- Ghosal, A.K., Sardar, A. and Chowdhury, D.R. (2024) "Differential fault analysis attack-tolerant hardware implementation of AES," *Journal of Supercomputing*, 80(4), pp. 4648–4681. Available at: <https://doi.org/10.1007/S11227-023-05632-2/TABLES/7>.
- Hirsi, A. *et al.* (2024) "Detecting DDoS Threats using Supervised Machine Learning for Traffic Classification in Software Defined Networking," *IEEE Access* [Preprint]. Available at: <https://doi.org/10.1109/ACCESS.2024.3486034>.
- Hirsi, A. *et al.* (2025) "Comprehensive Analysis of DDoS Anomaly Detection in Software-Defined Networks," *IEEE Access* [Preprint]. Available at: <https://doi.org/10.1109/ACCESS.2025.3535943>.
- Hocquet, C. *et al.* (2011) "Harvesting the potential of nano-CMOS for lightweight cryptography: An ultra-low-voltage 65 nm AES coprocessor for passive RFID tags," *Journal of Cryptographic Engineering*, 1(1), pp. 79–86. Available at: <https://doi.org/10.1007/S13389-011-0005-Z/METRICS>.
- Kohli, V., Aman, M.N. and Sikdar, B. (2024) "An Intelligent Fingerprinting Technique for Low-power Embedded IoT

- Devices,” *IEEE Transactions on Artificial Intelligence* [Preprint]. Available at: <https://doi.org/10.1109/TAI.2024.3386498>.
- Litoussi, M. *et al.* (2020) “IoT security: challenges and countermeasures,” *Procedia Computer Science*, 177, pp. 503–508. Available at: <https://doi.org/10.1016/J.PROCS.2020.10.069>.
- Lu, M. *et al.* (2018) “A Compact, Lightweight and Low-Cost 8-Bit Datapath AES Circuit for IoT Applications in 28nm CMOS,” *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 1464–1469. Available at: <https://doi.org/10.1109/TRUSTCOM/BIGDATASE.2018.00204>.
- Nabihah Ahmad *et al.* (2024) *Design of Advanced Encryption System (AES) Algorithm Using ASIC Implementation for Internet of Things (IoT) Devices*. Available at: <https://akademiabaru.com/submit/index.php/ard/article/view/5634/5349> (Accessed: June 2, 2025).
- Noor, S.M. and John, E.B. (2019) “Resource Shared Galois Field Computation for Energy Efficient AES/CRC in IoT Applications,” *IEEE Transactions on Sustainable Computing*, 4(4), pp. 340–348. Available at: <https://doi.org/10.1109/TSUSC.2019.2943878>.
- Schiller, E. *et al.* (2022) “Landscape of IoT security,” *Computer Science Review*, 44, p. 100467. Available at: <https://doi.org/10.1016/J.COSREV.2022.100467>.
- Shreedhar, A. *et al.* (2019) “Low gate-count ultra-small area nano advanced encryption standard (AES) design,” *Proceedings - IEEE International Symposium on Circuits and Systems*, 2019-May. Available at: <https://doi.org/10.1109/ISCAS.2019.8702450>.
- Singha, T.B., Palathinkal, R.P. and Ahamed, S.R. (2023) “Securing AES Designs Against Power Analysis Attacks: A Survey,” *IEEE Internet of Things Journal*, 10(16), pp. 14332–14356. Available at: <https://doi.org/10.1109/JIOT.2023.3265683>.
- Wang, Y. *et al.* (2016) “DW-AES: A Domain-Wall Nanowire-Based AES for High Throughput and Energy-Efficient Data Encryption in Non-Volatile Memory,” *IEEE Transactions on Information Forensics and Security*, 11(11), pp. 2426–2440. Available at: <https://doi.org/10.1109/TIFS.2016.2576903>.