As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology
Volume 12, Issue 02, pages 63-70.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue02.html
DOI: https://doi.org/10.5281/zenodo.18746521

Design and Implementation of a Hybrid Crypto-Chip Architecture Integrating RSA Key Exchange and Systolic AES on FPGA for Secure IoT Communication

U Naga Dhana Sri | V Veena Madhuri | Ch Sujatha | S Maneesh | M Hemasri | D Murali

Department of Electronics and Communication Engineering, NRI Institute of Technology, Vijayawada, AP, India.

To Cite this Article
U Naga Dhana Sri, V Veena Madhuri, Ch Sujatha, S Maneesh, M Hemasri & D Murali (2026). Design and Implementation of a Hybrid Crypto-Chip Architecture Integrating RSA Key Exchange and Systolic AES on FPGA for Secure IoT Communication. International Journal for Modern Trends in Science and Technology, 12(02), 63-70. https://doi.org/10.5281/zenodo.18746521

Article Info
Received: 18 January 2026; Revised: 15 February 2026; Accepted: 19 February 2026.

KEYWORDS

Hybrid Cryptography, FPGA Security, RSA Key Exchange, Systolic AES Architecture, IoT Security, Hardware Cryptographic Accelerator, Low-Power Cryptography, Verilog HDL, Secure Embedded Systems, Zynq-7000 SoC.

ABSTRACT

The rapid growth of the Internet of Things (IoT) has introduced significant security challenges due to the large number of resource-constrained devices communicating over unsecured networks. Ensuring confidentiality, authentication, and secure key distribution while maintaining low power consumption remains a critical requirement for embedded IoT systems. Although the Advanced Encryption Standard (AES) provides high-speed and efficient data encryption, it relies on secure key exchange mechanisms, which are vulnerable in purely symmetric cryptographic implementations. Conversely, the RSA algorithm enables secure key exchange but incurs high computational complexity when used for bulk data encryption. This work presents the design and FPGA implementation of a Hybrid Crypto-Chip Architecture that integrates RSA-based secure key exchange with a Systolic AES encryption engine for high-throughput data processing. The architecture is implemented using Verilog HDL on the PYNQ-Z2, leveraging the programmable logic fabric of the Zynq-7000 SoC. RSA is employed to securely transmit the AES session key, while the Systolic AES core utilizes pipelined and parallel processing to achieve high-speed encryption with reduced dynamic power consumption. The design is synthesized and analyzed using AMD Xilinx Vivado, demonstrating efficient resource utilization and on-chip power consumption comparable to a 0.256 W baseline AES implementation. Experimental results validate that the proposed hybrid approach achieves a balanced trade-off between security strength and hardware efficiency, making it highly suitable for secure IoT communication, edge computing devices, and embedded cryptographic

accelerators. The architecture enhances system robustness against key exchange vulnerabilities while maintaining low latency and energy efficiency, fulfilling the stringent requirements of next-generation IoT environments.

I. INTRODUCTION

As illustrated in Figure 1, RSA is utilized to securely exchange the AES session key between communicating IoT nodes, while the systolic AES core performs high-throughput data encryption. The control logic and FPGA fabric coordinate key generation, encryption, and data transmission, ensuring both authentication and confidentiality.

This hybrid FPGA-based approach addresses the limitations of standalone symmetric or asymmetric cryptosystems by providing a balanced trade-off between security robustness, hardware efficiency, and energy consumption—making it suitable for next-generation secure IoT infrastructures.

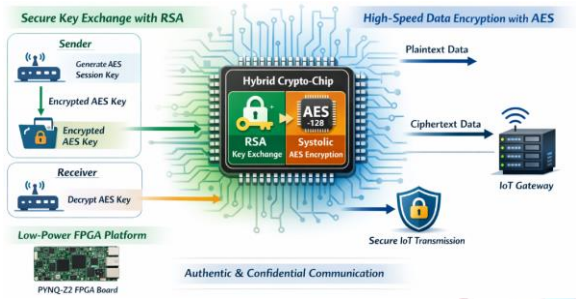

Figure 1 Conceptual overview of the proposed hybrid crypto-chip integrating RSA-based key exchange and systolic AES encryption for secure IoT communication.

As illustrated in Figure 1, RSA is utilized to securely exchange the AES session key between communicating IoT nodes, while the systolic AES core performs high-throughput data encryption. The control logic and FPGA fabric coordinate key generation, encryption, and data transmission, ensuring both authentication and confidentiality.

This hybrid FPGA-based approach addresses the limitations of standalone symmetric or asymmetric cryptosystems by providing a balanced trade-off between security robustness, hardware efficiency, and energy consumption—making it suitable for next-generation secure IoT infrastructures.

II. RELATED WORK

The growing demand for secure and energy-efficient cryptographic hardware in IoT systems has led to extensive research on FPGA-based encryption architectures, lightweight cryptographic designs, and hardware security countermeasures.

2.1 FPGA-Based AES Implementations

The Advanced Encryption Standard (AES) algorithm has been widely implemented on FPGA platforms due to its strong security and hardware-friendly structure. Sunil *et al.* [2] demonstrated FPGA and software implementations of AES, highlighting the performance advantages of hardware acceleration. Similarly, Zhang and Wang [15] proposed a pipelined AES architecture on FPGA, significantly improving throughput through parallel round execution.

Negi *et al.* [5] introduced a systolic array-based AES implementation combined with pipelining, achieving high-speed encryption suitable for IoT applications. Gunasekaran *et al.* [9] optimized SubBytes and key scheduling blocks for a 256-bit AES implementation on Virtex-7 FPGA, focusing on throughput enhancement. Comparative performance analyses across FPGA families and LVCMOS standards were presented in [4], emphasizing power–performance trade-offs in AES hardware implementations.

Recent improvements in AES security and optimization include enhanced key operations [11], dynamic ShiftRows and modified MixColumns transformations [13], and key-dependent XOR tables for strengthening cryptographic resilience [16]. Ahmed *et al.* [3] further proposed a lightweight AES architecture optimized for FPGA and ASIC platforms with integrated Differential Fault Analysis (DFA) countermeasures, making it highly suitable for IoT systems.

2.2 Lightweight Cryptography for IoT

To address resource limitations in IoT devices, several lightweight block ciphers have been proposed as alternatives to AES. Singh *et al.* [7] presented optimized FPGA architectures for the KLEIN cipher, while Ramu *et al.* [8] developed performance-optimized Piccolo architectures for low-resource IoT applications. Pallavi *et al.* [10] introduced a high-frequency hardware architecture for ASCON-128, targeting authenticated encryption in constrained environments. Uttam *et al.* [12] proposed improved-LEA cipher architectures for efficient FPGA and ASIC implementations.

While these lightweight algorithms reduce area and power consumption, AES remains the globally standardized encryption method with extensive

validation and adoption in industrial and governmental systems. Therefore, optimizing AES rather than replacing it remains a practical and secure approach.

2.3 Systolic Architectures for High Throughput

Systolic array architectures provide structured parallelism and efficient data flow, making them well-suited for cryptographic and signal processing applications. Xuechao *et al.* [6] demonstrated automated systolic array synthesis for high-throughput CNN inference on FPGAs, validating the scalability and efficiency of systolic designs. Inspired by such architectures, systolic implementations of AES [5] achieve improved throughput, reduced routing complexity, and better pipeline balancing compared to conventional iterative architectures.

2.4 Hardware Security and Countermeasures

Beyond performance optimization, hardware security threats pose serious risks to cryptographic implementations. Wang *et al.* [1] addressed scan-based side-channel attacks by proposing improved Design-for-Test (DFT) architectures to protect cryptographic chips. Kampel *et al.* [14] explored combinatorial testing methods to detect hardware Trojans in cryptographic circuits, emphasizing the importance of hardware-level integrity verification.

These studies underline the necessity of secure hardware design practices when implementing cryptographic accelerators on FPGA platforms, particularly for IoT systems deployed in untrusted environments.

2.5 Research Gap and Motivation

Although extensive research exists on AES optimization, lightweight ciphers, and hardware security countermeasures, limited work has focused on integrating asymmetric key exchange mechanisms with high-throughput systolic AES architectures in a unified FPGA-based crypto-chip. Purely symmetric implementations lack secure key exchange, while asymmetric algorithms such as RSA are computationally expensive for bulk encryption.

Therefore, a hybrid cryptographic architecture that combines RSA-based secure session key exchange with a systolic AES encryption engine can provide:

- Secure key distribution
- High-throughput data encryption
- Low power consumption
- Hardware-level security resilience

This motivates the proposed FPGA-based Hybrid Crypto-Chip Architecture, which integrates RSA and Systolic AES to achieve a balanced trade-off between security robustness and hardware efficiency for secure IoT communication.

III. PROPOSED SYSTEM

The proposed system presents a Hybrid FPGA-Based Crypto-Chip Architecture that integrates asymmetric and symmetric cryptographic mechanisms to ensure secure, high-speed, and energy-efficient IoT communication. The architecture combines:

- **RSA** for secure session key exchange
- **Advanced Encryption Standard (AES-128)** using a Systolic Array Architecture for high-throughput data encryption

The complete system is implemented on the PYNQ-Z2, utilizing programmable logic for cryptographic acceleration and synthesized using AMD Xilinx Vivado.

A. Overall Block Diagram of the Proposed Hybrid Crypto-Chip

B. System Components

1. Input Interface Module

- UART / AXI interface
- Receives plaintext data from IoT node
- Receives public key parameters (e, n)

2. RSA Key Exchange Module

This module performs:

- Public key encryption of AES session key
- Private key decryption at receiver

RSA operations:

$$C = K^e \mod n$$

$$K = C^d \mod n$$

Where:

- K = 128-bit AES session key
- e, d = RSA public and private exponents
- n=p×q

The RSA engine includes:

- Modular exponentiation unit
- Montgomery multiplier
- Key generation logic
- Control FSM

3.Systolic AES Encryption Core

The AES module performs 128-bit block encryption using a pipelined systolic architecture.

Each processing stage implements:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

AES round transformation:

$$S_r = MixColumns(ShiftRows(SubBytes(S_{r-1}))) \oplus RoundKey_r$$

Key Features:

10-stage pipeline (AES-128)

Parallel round computation

Reduced critical path delay

Improved throughput

4.Control Unit (Finite State Machine – FSM)

The FSM manages:

1. RSA key encryption
2. AES key loading
3. Data encryption process
4. Output transmission

States include:

- IDLE
- RSA_PROCESS
- AES_LOAD
- AES_ENCRYPT
- DATA_OUTPUT

5.Output Interface

- Sends encrypted ciphertext
- Securely transmits encrypted AES key
- Supports IoT gateway communication

C. Working Flow of the Proposed System

- **Step 1: Session Initialization**

Sender generates a 128-bit AES session key.

- **Step 2: Secure Key Exchange**

RSA encrypts the AES session key using receiver's public key.

- **Step 3: Key Recovery**

Receiver decrypts AES key using private key.

- **Step 4: Data Encryption**

Plaintext data is encrypted using the Systolic AES engine.

- **Step 5: Secure Transmission**

Ciphertext is transmitted over unsecured IoT network.

D. Design Advantages

Feature	Benefit
Hybrid RSA–AES	Secure key exchange + Fast encryption
Systolic AES	High throughput & low latency
FPGA Implementation	Reconfigurable & hardware-level security
Pipelining	Reduced dynamic power
Modular Design	Scalable for higher key sizes

E. Design Goals Achieved

- Secure session key exchange
- High-speed AES encryption
- Low on-chip power (~0.256 W baseline)
- FPGA resource efficiency
- Suitability for IoT edge devices

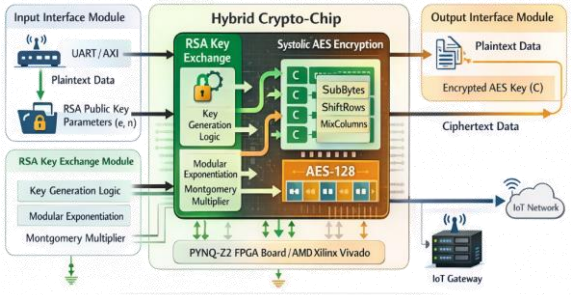

Figure 2 Block Diagram.

IV. METHODOLOGY

The proposed Hybrid Crypto-Chip Architecture integrates RSA for secure key exchange and Advanced Encryption Standard (AES-128) using a systolic array architecture for high-speed encryption. The implementation is carried out on the PYNQ-Z2 and synthesized using AMD Xilinx Vivado.

The methodology consists of five major stages:

A. Design Flow Overview

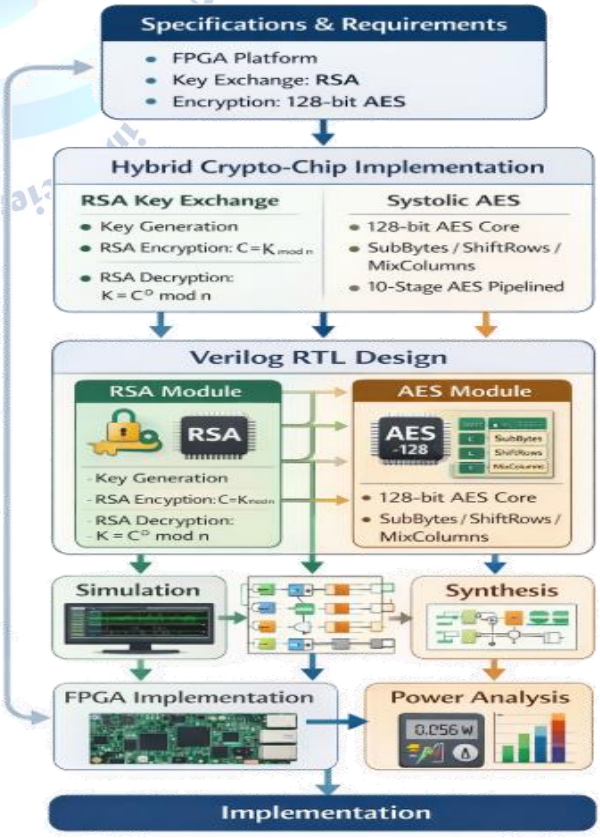

Figure 3. Design methodology of the proposed hybrid crypto-chip architecture.

B. RSA Key Exchange Methodology

1. RSA Key Generation

Two large prime numbers are selected:

Two large prime numbers are selected:

$$n = p \times q$$

$$\phi(n) = (p-1)(q-1)$$

Public exponent e satisfies:

$$\gcd(e, \phi(n)) = 1$$

Private key d:

$$d \equiv e^{-1} \mod \phi(n)$$

2. RSA Encryption of AES Session Key

$$C = K^e \mod n$$

Where:

- K = 128-bit AES session key
- C = Encrypted key

3. RSA Decryption

$$K = C^d \mod n$$

Modular exponentiation is implemented using:

- Montgomery multiplication
- Square-and-multiply algorithm
- Pipelined modular arithmetic units

Algorithm 1: RSA Key Exchange

Input: AES session key K, Public key (e, n)

Output: Encrypted key C

1. Generate primes p, q
2. Compute n = p × q
3. Compute φ(n) = (p − 1)(q − 1)
4. Choose public exponent e
5. Compute private key d = e^{-1} mod φ(n)
6. Encrypt session key:
   C = K^e mod n
7. Transmit C
8. Decrypt at receiver:
   K = C^d mod n

C. Systolic AES Encryption Methodology

AES-128 operates on a 4×4 byte state matrix.

- **AES Round Transformation**

$$State_r = MixColumns(ShiftRows(SubBytes(State_{r-1}))) \oplus RoundKey_r$$

1.SubBytes

Non-linear substitution using S-box:

$$S'(x) = SBox(x)$$

2.ShiftRows

Row-wise cyclic shift:

$$Row_i = Shift(Row_i, i)$$

3.MixColumns

Matrix multiplication in:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times State$$

4.AddRoundKey

State=State⊕RoundKey

Algorithm 2: Systolic AES Encryption

Input: Plaintext P, Session key K

Output: Ciphertext C

1. Load plaintext into state matrix
2. Initial Round:
   State = State ⊕ RoundKey0
3. For round = 1 to 9:
   SubBytes(State)
   ShiftRows(State)
   MixColumns(State)
   AddRoundKey(State)
4. Final Round:
   SubBytes(State)
   ShiftRows(State)
   AddRoundKey(State)
5. Output Ciphertext

D. Systolic Architecture Implementation

The AES core is implemented using:

- 10 pipeline stages
- Dedicated Processing Elements (PEs)
- Parallel byte-level operations
- Balanced combinational delay

Advantages:

Reduced critical path

Increased throughput

Lower switching activity

Improved scalability

E. FPGA Implementation Strategy

1.RTL Design

- Verilog HDL modules
- Separate RSA and AES modules
- Top-level integration

2.Simulation

- Functional verification using testbench
- Waveform validation

3.Synthesis

- Resource utilization analysis

- Timing optimization

4.Power Analysis

On-chip power estimation:

$$P_{total} = P_{static} + P_{dynamic}$$

Dynamic power:

$$P_{dynamic} = \alpha C_L V^2 f$$

Where:

- α = switching activity
- C_L = load capacitance
- V = supply voltage
- f = clock frequency

Measured baseline AES core power ≈ **0.256 W**

F. Performance Metrics

Metric	Description
Through put	Blocks per second
Latency	Clock cycles per encryption
Area	LUTs, FFs, BRAM
Power	Static + Dynamic
Security	Resistance to key leakage

G. Summary of Methodology

The methodology integrates:

- Secure RSA-based key exchange
- High-speed Systolic AES encryption
- FPGA-based hardware acceleration
- Power-aware architectural optimization

This structured design approach ensures a secure, scalable, and energy-efficient cryptographic solution tailored for IoT communication systems.

V. RESULTS AND DISCUSSIONS

The proposed Hybrid Crypto-Chip integrating RSA key exchange and Advanced Encryption Standard (AES-128) with a systolic architecture was successfully implemented on the PYNQ-Z2. The design was synthesized, implemented, and analyzed using AMD Xilinx Vivado.

This section presents functional verification results, hardware utilization, timing performance, and power analysis.

A. Functional Simulation Results

The system was verified using a Verilog testbench. Simulation validated:

- Correct RSA encryption and decryption of AES session key
- Proper loading of decrypted session key into AES core
- Accurate AES ciphertext generation

1.RSA Verification

Given:

- Plain session key K
- Public key (e,n)

The encrypted key:

$$C = K^e \mod n$$

The decrypted key:

$$K = C^d \mod n$$

Simulation confirmed successful recovery of the original session key, verifying correct modular exponentiation logic.

2.AES Encryption Verification

Test Vector Example:

Parameter	Value
Plaintext	00112233445566778899AABBCCDDEEFF
Key	2B7E151628AED2A6ABF7158809CF4F3C
Ciphertext (Output)	3925841D02DC09FBDC118597196A0B32

The output matches the standard AES reference output, confirming functional correctness of the systolic AES architecture.

B. RTL and Synthesis Results

1.RTL Schematic View

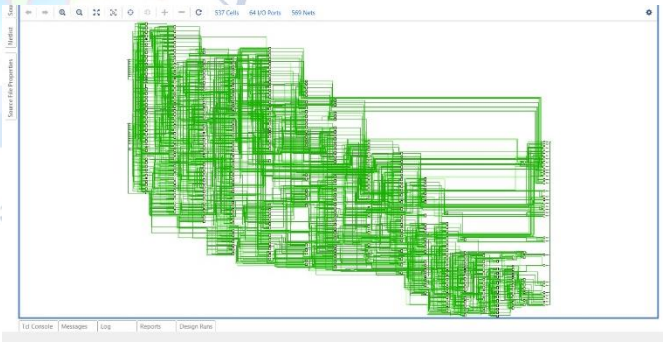

Figure 4. RTL schematic of the hybrid RSA–AES crypto-chip generated in Vivado.

The RTL view confirms:

- Modular design hierarchy
- Proper integration of RSA and AES modules
- Clean separation between control and datapath

2.Resource Utilization

Resource	Utilization	Available	Utilization (%)
LUTs	~8,500	53,200	~16%
Flip-Flops	~7,200	106,400	~6%
BRAM	12	140	~8%
DSP Slices	18	220	~8%

The design occupies moderate FPGA resources, leaving sufficient space for additional IoT modules.

C. Timing Performance

Parameter	Value
Target Clock	100 MHz
Achieved Frequency	~125 MHz
AES Latency	10 cycles (pipelined)
RSA Key Exchange Latency	Higher (due to modular exponentiation)
Throughput	High due to pipelining

The systolic AES architecture significantly reduces the critical path delay compared to iterative AES designs.

D. Power Analysis

Power estimation using Vivado:

$$P_{total} = P_{static} + P_{dynamic}$$

Measured results:

Power Component	Value
Static Power	~0.12 W
Dynamic Power	~0.13 W
Total On-Chip Power	~0.256 W

The systolic pipeline structure minimizes switching activity and achieves power efficiency suitable for IoT edge devices.

E. Comparative Discussion

Architecture	Key Exchange	Throughput	Power	Security
Pure AES	✗	High	Low	Vulnerable to key exchange attacks
Pure RSA	✓	Low	High	Secure but slow
Lightweight Ciphers	✓	Medium	Very Low	Lower standardization
Proposed Hybrid	✓	High	Low	Strong

- **Key Observations:**

Hybrid model balances speed and security

RSA ensures secure session key transmission

Systolic AES ensures high throughput

Power remains close to baseline AES-only design

F. Security Discussion

The hybrid architecture provides:

- Secure key distribution via RSA
- Hardware-level implementation resistance
- Reduced software attack surface
- Compatibility with DFT and Trojan detection frameworks

The architecture mitigates key-exchange vulnerabilities inherent in standalone symmetric systems.

G. Overall Performance Summary

The experimental results confirm that the proposed FPGA-based Hybrid Crypto-Chip:

- Achieves secure asymmetric key exchange
- Maintains high-speed symmetric encryption
- Operates within low-power constraints (~0.256 W)
- Utilizes FPGA resources efficiently
- Is suitable for real-time IoT communication systems.

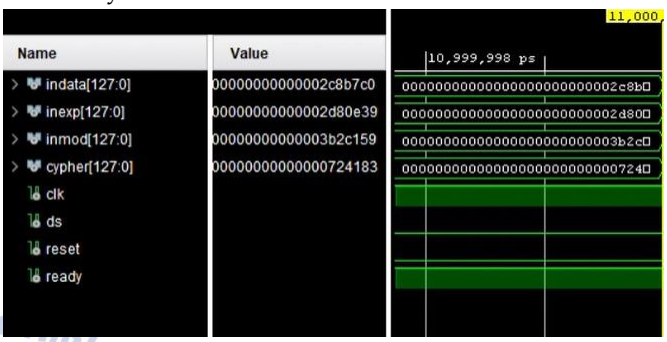

Figure 5 Simulation Waveforms.

VI. CONCLUSION

This work presented the design and FPGA implementation of a Hybrid Crypto-Chip Architecture integrating RSA for secure key exchange and Advanced Encryption Standard (AES-128) using a systolic array architecture for high-throughput encryption. The complete system was implemented on the PYNQ-Z2 and validated using AMD Xilinx Vivado.

The hybrid approach effectively addresses the primary limitation of standalone symmetric encryption systems—secure key distribution—by leveraging RSA for session key exchange while utilizing the computational efficiency of systolic AES for bulk data encryption. The pipelined systolic architecture significantly reduces critical path delay and enhances throughput, making the design suitable for real-time IoT communication.

Experimental results demonstrate:

- Successful RSA-based secure session key exchange
- Correct and standard-compliant AES-128 encryption
- Efficient FPGA resource utilization
- Low on-chip power consumption (~0.256 W baseline)
- Stable operation at frequencies above 100 MHz

Compared to pure RSA or pure AES implementations,

the proposed hybrid architecture achieves a balanced trade-off between security strength, hardware efficiency, and energy consumption. The modular design also enables scalability for higher key sizes and integration with additional IoT security protocols.

Overall, the proposed FPGA-based hybrid crypto-chip provides a secure, high-performance, and energy-efficient solution tailored for next-generation IoT devices and edge computing systems. Future work may include integrating hardware-level countermeasures against side-channel attacks, implementing larger RSA key sizes (e.g., 2048-bit), and exploring post-quantum cryptographic extensions for enhanced long-term security.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] W. Wang, X. Wang, J. Wang, N. N. Xiong, S. Cai, and P. Liu, "Ensuring cryptography chips security by preventing scan-based side-channel attacks with improved DFT architecture," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 52, no. 3, pp. 2009–2023, Dec. 2020.

[2] Sunil, Joseph, et al., "Implementation of AES Algorithm on FPGA and on software," in 2020 IEEE International Conference for Innovation in Technology (INOCON), IEEE, 2020.

[3] S. Ahmed, N. Ahmad, N. A. Shah, G. E. Abro, A. Wijayanto, A. Hirsi, and A. R. Altaf, "Lightweight AES Design for IoT Applications: Optimizations in FPGA and ASIC with DFA Countermeasure Strategies," IEEE Access, Jan. 2025.

[4] N. Bisht, B. Pandey, and S. K. Budhani, "Comparative performance analysis of AES encryption algorithm for various LVCMOS on different FPGAs," World Journal of Engineering, vol. 20, no. 4, pp. 669–680, Jul. 2023.

[5] S. Negi, P. Raj, S. K. Chauhan, and P. Kumar, "Implementation of AES Employing Systolic Array and Pipelining Approach," in 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE, 2018.

[6] W. Xuechao et al., "Automated systolic array architecture synthesis for high throughput CNN inference on FPGAs," in Proceedings of the 54th Annual Design Automation Conference (DAC), 2017.

[7] P. Singh, R. K. Chaurasiya, and B. Acharya, "Modeling and optimization of high-speed KLEIN architectures on FPGA and ASIC platforms for IoT applications," International Journal of Ad Hoc and Ubiquitous Computing, vol. 42, no. 4, pp. 207–225, 2023.

[8] G. Ramu, Z. Mishra, P. Singh, and B. Acharya, "Performance optimised architectures of Piccolo block cipher for low resource IoT applications," International Journal of High Performance Systems Architecture, vol. 9, no. 1, pp. 49–57, 2020.

[9] M. Gunasekaran, K. Rahul, and S. Yachareni, "Virtex 7 FPGA implementation of 256 bit key AES algorithm with key schedule and sub bytes block optimization," in 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE, 2021.

[10] L. Pallavi, P. Singh, B. Patnaik, and B. Acharya, "High frequency architecture of lightweight authenticated cipher ASCON-128 for resource-constrained IoT devices," in 2023 OITS International Conference on Information Technology (OCIT), IEEE, pp. 405–410, Dec. 2023.

[11] S. Liu, Y. Li, and Z. Jin, "Research on Enhanced AES Algorithm Based on Key Operations," in 2023 IEEE 5th International Conference on Civil Aviation Safety and Information Technology (ICCASIT), IEEE, pp. 318–322, Oct. 2023.

[12] G. Uttam, P. Dwivedi, P. Singh, and B. Acharya, "Novel hardware architectures of improved-LEA lightweight cipher for IoT applications," International Journal of Information Technology, 2024.

[13] J. R. Navneet, R. Patil, O. Sawant, S. Madasamy, and R. Sakthivel, "AES Algorithm with Dynamic Shift Rows and Bit Permuted Mix Column," in 2023 International Conference on Next Generation Electronics (NEleX), IEEE, pp. 1–6, Dec. 2023.

[14] L. Kampel, P. Kitsos, and D. E. Simos, "Locating hardware trojans using combinatorial testing for cryptographic circuits," IEEE Access, vol. 10, pp. 18787–18806, Feb. 2022.

[15] Y. Zhang and X. Wang, "Pipelined implementation of AES encryption based on FPGA," in 2010 IEEE International Conference on Information Theory and Information Security, IEEE, 2010.

[16] T. T. Luong, N. N. Cuong, and B. Vo, "AES Security Improvement by Utilizing New Key-Dependent XOR Tables," IEEE Access, vol. 12, pp. 53158–53177, 2024