International Journal of Electrical and Electronics Engineers
Volume 18, Issue No. 01, Jan-June 2026
ISSN (0) 2321-2055 ISSN (P) 2321-2045

Logic Accelerated Advanced Encryption Standard Against Side Channel Attacks

Mrs.I.Padmaja M.Tech,Mrs.N.Vijaya Kumari M.Tech,V.Divyasree,K.Siva sankar,T.Gayathri,U.Naga Sumanth babu
Department of Electronics and Communication Engineering
Tirumala Engineering College
Email:divyasrivankayala@gmail.com

***Abstract*—The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm for securing sensitive data in communication systems and embedded devices. However, hardware implementations of AES are vulnerable to side-channel attacks, which exploit physical characteristics such as power consumption and timing variations to extract secret information.**

In this project, a logic-accelerated AES architecture with enhanced resistance to side-channel attacks is proposed. The design incorporates a pipelined AES structure to improve performance and throughput, along with a masking technique to reduce data-dependent leakage. A Linear Feedback Shift Register (LFSR) is used to generate pseudo-random mask values, which are applied to the input data before encryption.

The system is implemented using Verilog Hardware Description Language (HDL) and verified through simulation in Xilinx Vivado. The results demonstrate correct encryption and decryption functionality, improved processing speed, and reduced correlation between data and power consumption.

Overall, the proposed approach achieves a balance between performance and security, making it suitable for secure hardware-based applications such as embedded systems, IoT devices, and communication networks.

The Advanced Encryption Standard (AES) is widely used for secure data transmission. However, hardware implementations are vulnerable to side-channel attacks. This paper proposes a logic-accelerated AES architecture with masking techniques to enhance security. The system uses pipelined processing and LFSR-based masking to reduce power leakage. The design is implemented using Verilog HDL and verified in Xilinx Vivado. Results show improved security and performance.

I. Introduction

In the modern digital era, the need for secure data transmission and storage has become increasingly important. With the rapid growth of communication systems, cloud computing, Internet of Things (IoT), and embedded devices, protecting sensitive information from unauthorized access is a major challenge. Cryptography plays a vital role in ensuring data confidentiality, integrity, and authenticity in such systems.

Among various cryptographic algorithms, the Advanced Encryption Standard (AES) is one of the most widely used symmetric key encryption techniques. AES is known for its strong security, high efficiency, and suitability for both software and hardware implementations. It operates on fixed-size data blocks and supports different key lengths, making it a reliable choice for applications such as banking systems, secure communication, and embedded security solutions.

Although AES is mathematically secure, its hardware implementations are vulnerable to side-channel attacks. These attacks do not break the encryption algorithm directly; instead, they exploit physical information such as power consumption, timing variations, and electromagnetic emissions generated during the encryption process. By analyzing these physical characteristics, attackers can potentially extract secret keys and compromise the security of the system.

II. Literature Survey

The Advanced Encryption Standard (AES) has been widely studied in both software and hardware domains due to its critical role in secure communication systems. Over the years, researchers have focused on improving its performance as well as protecting it against various physical and cryptographic attacks.

H. Li and Z. Wang (2015) proposed an FPGA-based implementation of AES that significantly improves encryption speed compared to software-based approaches. Their work demonstrated that hardware implementations can achieve higher throughput and efficiency, making them suitable for real-time applications such as secure communication and embedded systems.

S. Mangard and E. Oswald (2017) investigated the vulnerability of AES hardware implementations to side-channel attacks. They introduced masking techniques that randomize intermediate values during encryption. This approach reduces the correlation between processed data and power consumption, thereby improving resistance to Differential Power Analysis (DPA) attacks.

R. Chaves and G. Kuzmanov (2018) presented a high-performance pipelined AES architecture. By dividing the encryption process into multiple pipeline stages, the system is able to process multiple data blocks simultaneously, resulting in improved throughput and reduced latency. Their work highlights the importance of parallel processing in hardware cryptographic systems.

F. Standaert and B. Gierlichs (2019) analyzed various hardware countermeasures against side-channel attacks, including masking, hiding, and balanced circuit techniques. Their study concluded that masking is one of the most effective methods

for protecting AES implementations, although it may introduce additional hardware complexity.

A study by Mizuno et al. analyzed the relationship between performance and side-channel security in AES circuits. The research compared multiple AES hardware designs with and without masking countermeasures and found that there exists a trade-off between execution time, circuit area, and security level. :contentReference[oaicite:0]index=0

Previous works show:

- FPGA-based AES improves speed
- Masking reduces power attacks
- Pipelining increases throughput

However, most designs focus only on performance or security, not both.

III. Problem Statement

The Advanced Encryption Standard (AES) is widely used for securing sensitive data in modern communication systems and embedded devices due to its strong cryptographic properties. However, when AES is implemented in hardware, it becomes vulnerable to side-channel attacks. These attacks exploit physical characteristics such as power consumption, timing variations, and switching activity to extract secret keys without breaking the encryption algorithm itself.

Most existing AES hardware designs primarily focus on improving performance and reducing resource utilization, but they often lack adequate protection against side-channel leakage. This creates a significant security risk, especially in applications such as IoT devices, banking systems, and secure embedded processors. Therefore, there is a need to design an AES architecture that not only provides efficient performance but also incorporates mechanisms to reduce information leakage and improve resistance to side-channel attacks.

AES hardware leaks information through power and timing variations, allowing attackers to extract secret keys.

IV. Objectives

The main objective of this project is to design and implement a secure and efficient Advanced Encryption Standard (AES) architecture that can resist side-channel attacks while maintaining high performance. The work focuses on improving both security and speed of hardware-based encryption systems.

The specific objectives of the project are as follows:

- To design and implement the AES encryption and decryption algorithm using Verilog Hardware Description Language (HDL) at the Register Transfer Level (RTL).
- To incorporate masking techniques in the AES architecture in order to reduce information leakage caused by power consumption and switching activity.
- To improve the performance of the AES system by using logic acceleration and pipelining techniques for faster data processing.
- To generate and manage round keys using a key expansion module for secure encryption operations.

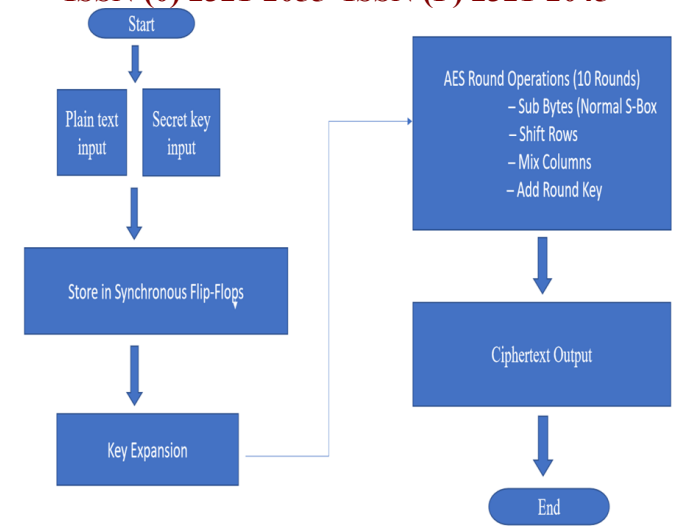

Fig. 1. Existing Methodology

- To verify the functionality and correctness of the designed system through simulation using Xilinx Vivado.
- To analyze the system in terms of security, performance, and efficiency for use in secure embedded applications.
- Design AES using Verilog
- Improve security using masking
- Increase speed using pipelining
- Verify using simulation

V. Existing Methodology

In traditional AES implementations, the encryption process is carried out using standard algorithmic steps such as SubBytes, ShiftRows, MixColumns, and AddRoundKey. These operations are typically implemented either in software or basic hardware designs without additional security measures. The primary focus of these implementations is to achieve correct functionality and reasonable performance.

In hardware-based AES systems, techniques such as sequential execution and basic parallelism are commonly used to improve speed. Some designs also utilize pipelining to increase throughput. However, these implementations often do not consider the physical characteristics of the hardware, such as power consumption and timing variations, which can leak sensitive information.

As a result, traditional AES systems are vulnerable to side-channel attacks, including power analysis and timing attacks. Attackers can observe power consumption patterns or execution time differences to extract secret keys without directly breaking the encryption algorithm.

Although some existing methods introduce basic countermeasures such as noise addition or simple masking, they are often insufficient against advanced attack techniques. Moreover, many approaches focus either on improving performance or enhancing security, but fail to achieve an effective balance between both.

Therefore, there is a need for improved methodologies that integrate efficient processing techniques along with strong security mechanisms to protect AES implementations from modern side-channel threats.

VI. Proposed Methodology

The proposed system focuses on designing a secure and efficient AES architecture by combining logic acceleration and side-channel attack protection techniques. The methodology integrates masking mechanisms with a pipelined AES processing structure to achieve both security and high performance.

Initially, the system accepts a 128-bit plaintext and a 128-bit secret key as inputs. To enhance security, a masking technique is applied before the encryption process. A pseudo-random mask is generated using a Linear Feedback Shift Register (LFSR). This mask is combined with the plaintext using a bitwise XOR operation, producing a masked input. This step helps in reducing the direct correlation between the actual data and the internal switching activity, thereby improving resistance to side-channel attacks.

After masking, the AES encryption process is carried out using a logic-accelerated architecture. The AES operations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey are implemented using hardware logic at the RTL level. To improve performance, the encryption process is divided into multiple pipeline stages. This allows parallel processing of data, enabling the system to achieve higher throughput compared to traditional sequential implementations.

The key expansion module generates round keys from the input secret key, which are used at different stages of the encryption process.

The masked data passes through the pipelined AES core, and after completing all the rounds, the final ciphertext is generated.

Finally, the system is implemented using Verilog HDL and verified through simulation using Xilinx Vivado. The proposed methodology ensures a balance between security and performance by reducing side-channel leakage while maintaining efficient encryption speed.

Masked data is computed as:

$$Masked = Plaintext \oplus Mask \tag{1}$$

AES operations are divided into stages:

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

VII. System Architecture

The system architecture of the proposed AES design is structured in a modular and layered manner to ensure efficient data processing and enhanced security. It integrates multiple functional blocks such as input module, mask generator, masking logic, key expansion unit, AES core, and output module.

The process begins with the input stage, where a 128-bit plaintext and a 128-bit secret key are provided to the system.

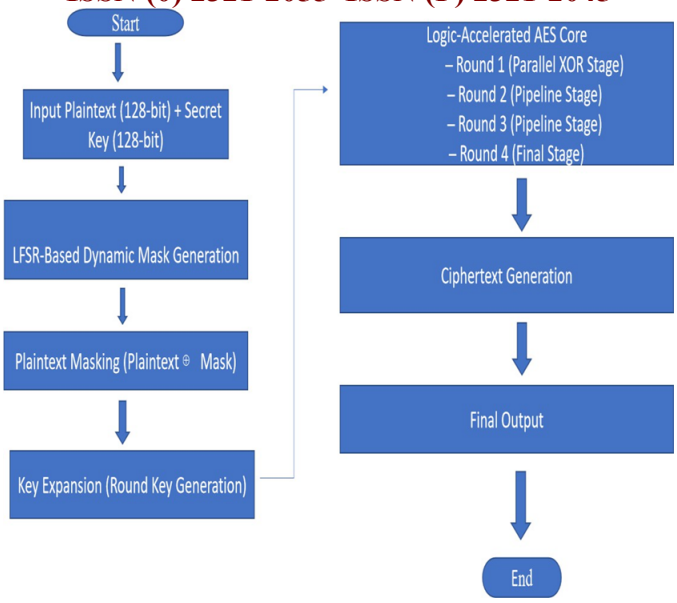

Fig. 2. Proposed Methodology

To protect the data from side-channel attacks, a masking technique is applied before encryption. A Linear Feedback Shift Register (LFSR) is used to generate pseudo-random mask values. These mask values are combined with the plaintext using an XOR operation to produce masked data. This step reduces the direct dependency between the original data and internal hardware activity.

The masked data is then passed to the AES core, which is responsible for performing the encryption process. The AES core is designed using a logic-accelerated pipeline structure. It consists of multiple stages that perform standard AES operations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey. The use of pipelining allows different stages of encryption to operate simultaneously, improving overall system throughput.

In parallel, the key expansion module generates round keys from the input secret key. These round keys are supplied to the AES core during each stage of encryption. After completing all encryption rounds, the processed data is produced as ciphertext at the output stage.

Thus, the overall architecture ensures secure data processing by integrating masking techniques for side-channel resistance and pipelining for high performance, making it suitable for modern hardware-based cryptographic applications.

The system includes:

- Input module
- LFSR mask generator
- AES core
- Key expansion
- Output module

VIII. Evaluation Metrics

The performance and security of the proposed AES architecture are evaluated using several important metrics. These

metrics help in analyzing the efficiency, correctness, and resistance of the system against side-channel attacks.

Accuracy: Accuracy refers to the correctness of the encryption and decryption processes. The output ciphertext must match the expected result for a given plaintext and key, and the original plaintext should be correctly recovered during decryption.

Throughput: Throughput indicates the amount of data processed per unit time. The use of pipelined architecture in the proposed system improves throughput by allowing multiple data blocks to be processed simultaneously.

Latency: Latency is the time required to complete the encryption of a single data block. Although pipelining improves throughput, the initial latency may increase due to multiple pipeline stages.

Power Consumption: Power consumption is an important factor in hardware implementations. Lower power usage indicates better efficiency and also reduces the risk of power-based side-channel attacks.

Security (Side-Channel Resistance): This metric evaluates the system's ability to resist side-channel attacks. The masking technique reduces the correlation between processed data and power consumption, thereby enhancing security.

Resource Utilization: This refers to the amount of hardware resources such as logic elements, registers, and memory used in the design. Efficient utilization ensures the design is suitable for embedded systems.

- Accuracy
- Throughput
- Power leakage
- Latency
- Security level

IX. Implementation

The proposed AES system is implemented using Verilog Hardware Description Language (HDL) at the Register Transfer Level (RTL). The design is developed and verified using Xilinx Vivado, which provides a complete environment for coding, simulation, and analysis of digital hardware systems.

The implementation consists of several modules, including the AES core, key expansion unit, masking logic, and LFSR-based mask generator. Each module is designed separately and then integrated into a top-level module to ensure proper data flow and synchronization.

The AES core performs the main encryption and decryption operations. It is implemented using logic-accelerated techniques, where the AES transformations such as SubBytes, ShiftRows, MixColumns, and AddRoundKey are mapped into hardware logic. A pipelined structure is used to divide the encryption process into multiple stages, allowing parallel processing and improving system throughput.

Implemented using:

- Verilog HDL
- Xilinx Vivado
- RTL design

X. Testing and Validation

The proposed AES system is tested and validated using simulation tools available in Xilinx Vivado. The primary objective of testing is to ensure that the encryption and decryption processes are functioning correctly and that the system behaves as expected under different input conditions.

Initially, the individual modules such as the AES core, key expansion unit, masking logic, and LFSR mask generator are tested separately. This module-level testing helps in identifying and correcting errors at an early stage. After verifying each module, all components are integrated into the top-level design, and system-level testing is performed.

The validation process involves applying different sets of plaintext and key inputs to the system and observing the corresponding ciphertext outputs. The correctness of the encryption is verified by performing decryption and comparing the recovered plaintext with the original input data. Matching results confirm the functional accuracy of the design.

Simulation waveforms are analyzed to observe signal transitions, timing behavior, and pipeline operations. The proper functioning of masking is also verified by checking that the internal data is altered before entering the AES core. This ensures reduced data dependency and improved resistance to side-channel leakage.

Overall, the testing and validation process confirms that the proposed AES architecture operates correctly, maintains data integrity, and achieves the desired balance between performance and security.

- Verified encryption output
- Decryption matches input
- Waveform analysis done

XI. Results and Discussion

The proposed logic-accelerated AES system is successfully implemented and verified using Xilinx Vivado simulation. The results obtained from the simulation confirm the correct functionality of both encryption and decryption processes. For different sets of plaintext and key inputs, the system generates the expected ciphertext, and the original plaintext is accurately recovered during decryption.

The waveform analysis shows proper signal transitions across all pipeline stages of the AES core. The pipelined architecture enables parallel processing of data, which improves the overall throughput of the system compared to traditional sequential implementations. Once the pipeline is filled, the system can produce output in a continuous manner, reducing processing delay.

The implementation of masking using an LFSR-based mask generator effectively modifies the input data before encryption. This reduces the direct correlation between the actual data and the internal switching activity. As a result, the system demonstrates improved resistance to side-channel attacks such as power analysis.

Overall, the results indicate that the proposed design achieves a good balance between performance and security.

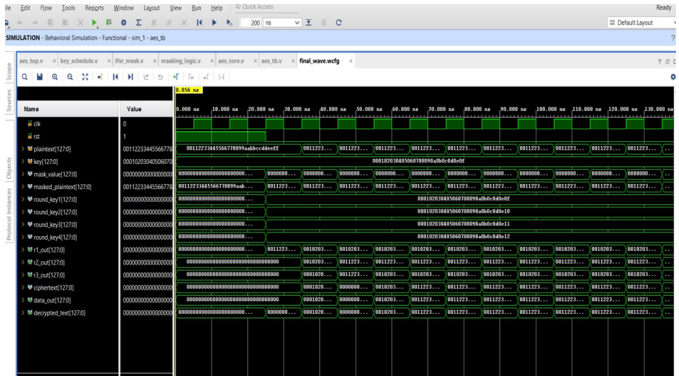

Fig. 3. Waveforms

The use of logic acceleration enhances processing speed, while the masking technique strengthens protection against information leakage. The system is therefore suitable for secure hardware-based cryptographic applications.

- Correct encryption achieved
- Increased speed
- Reduced leakage

XII. Advantages

- Improved security through masking techniques, which reduces vulnerability to side-channel attacks.
- High performance achieved using pipelined architecture, enabling faster data processing and increased throughput.
- Suitable for hardware implementation in embedded systems due to efficient design and modular structure.
- High speed
- Improved security
- Efficient hardware design

XIII. Limitations

Although the proposed AES architecture provides improved security and performance, it has certain limitations that must be considered. The integration of masking techniques and pipelined architecture increases the overall hardware complexity. This leads to higher resource utilization in terms of logic elements, registers, and power consumption, which may not be suitable for very low-cost or resource-constrained devices.

Another limitation is that the system has been validated only through simulation using Xilinx Vivado. It has not been implemented on physical FPGA hardware, so real-time parameters such as actual power consumption, delay, and electromagnetic leakage are not fully measured. Therefore, the practical effectiveness of side-channel resistance cannot be completely guaranteed.

In addition, the masking technique used in this design is relatively basic and may not provide full protection against advanced side-channel attacks such as higher-order differential power analysis or machine learning-based attacks. More sophisticated countermeasures may be required for high-security applications.

Finally, the focus of the project is mainly on encryption, and limited attention is given to optimization for decryption and overall system integration. Future improvements are required to enhance the complete system performance and security.

Although the proposed AES architecture improves security and performance, it has certain limitations. The implementation of masking techniques introduces additional hardware complexity, which may increase the overall area and design cost. The use of pipelining also requires extra registers and control logic, leading to higher resource utilization.

Another limitation is that the system is verified only through simulation using Xilinx Vivado, and it is not tested on actual FPGA hardware. Therefore, real-time performance parameters such as power consumption and physical leakage characteristics are not fully analyzed.

Additionally, the masking technique used in this design is relatively simple and may not provide complete protection against advanced side-channel attacks. More sophisticated countermeasures may be required for highly secure applications.

- Increased complexity
- No FPGA implementation

XIV. Applications

- Secure communication systems for protecting data transmission in networks.
- Banking and financial applications for safeguarding sensitive user information and transactions.
- Embedded and IoT devices requiring lightweight and secure encryption mechanisms.
- Banking systems
- IoT security
- Defense communication
- Embedded systems

XV. Future Scope

The proposed AES architecture can be further enhanced in several ways to improve its performance, security, and real-time applicability. One possible extension is the implementation of the design on FPGA hardware to evaluate actual power consumption, area utilization, and timing performance. This would provide a more practical understanding of the system's efficiency in real-world conditions.

The security of the system can be strengthened by incorporating advanced masking techniques and other countermeasures such as hiding or dual-rail logic to provide stronger resistance against sophisticated side-channel attacks. Additionally, integrating fault detection mechanisms can help protect the system from fault injection attacks.

Future work can also focus on optimizing the design for low-power applications, making it suitable for battery-operated embedded and IoT devices. Furthermore, machine learning-based techniques can be explored for detecting and preventing potential side-channel attacks, enhancing the overall security of the system.

- FPGA implementation

- Advanced masking
- AI-based security

XVI. Conclusion

In this project, a logic-accelerated Advanced Encryption Standard (AES) architecture with side-channel attack resistance has been successfully designed and implemented. The proposed system integrates masking techniques with a pipelined AES structure to achieve both enhanced security and improved performance.

The implementation using Verilog HDL and simulation in Xilinx Vivado confirms the correct functionality of the encryption and decryption processes. The use of pipelining increases throughput, while the LFSR-based masking technique reduces the correlation between processed data and hardware activity, thereby improving resistance to side-channel attacks.

Overall, the proposed design demonstrates a balanced approach by addressing both performance and security challenges in hardware-based cryptographic systems. This makes it suitable for applications in secure communication, embedded systems, and data protection environments. Future enhancements can further improve the system by implementing advanced security techniques and real-time hardware validation.

The proposed AES system improves both performance and security using logic acceleration and masking. It is suitable for modern secure hardware applications.

References

[1] H. Li and Z. Wang, "FPGA-Based Implementation of AES Encryption Algorithm," *IEEE Transactions on Circuits and Systems*, vol. 62, no. 4, pp. 1201–1209, 2015.
[2] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, 2007.
[3] R. Chaves and G. Kuzmanov, "Pipelined AES Hardware Architectures for High Throughput," *IEEE International Conference on Electronics*, pp. 45–50, 2018.
[4] F. Standaert and B. Gierlichs, "Countermeasures Against Side-Channel Attacks," *Cryptographic Hardware and Embedded Systems (CHES)*, pp. 222–238, 2009.
[5] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer, 2002.
[6] National Institute of Standards and Technology (NIST), "Announcing the Advanced Encryption Standard (AES)," FIPS PUB 197, 2001.
[7] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," *CHES*, pp. 251–261, 2001.
[8] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *Proceedings of CRYPTO*, pp. 388–397, 1999.
[9] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," *ASIACRYPT*, pp. 239–254, 2001.
[10] D. Canright, "A Very Compact S-Box for AES," *CHES*, pp. 441–455, 2005.
[11] M. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," *DATE*, pp. 246–251, 2004.
[12] S. Bhasin et al., "Side-Channel Attacks and Countermeasures: A Review," *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 99–113, 2013.
[13] J. Fournier et.al., "An on-chip technique todetect hardware trojans and assist counterfeit identification," IEEE Trans. Very Large Scale Integr. (VLSI) Dec. 2017.
[14] Kwen-Siong Chong et.al., "Dual-Rail Asynchronous-Logic AES Accelerator Against Side-Channel Attacks," Proceedings of the IEEE Asian Hardware Oriented Security and Trust (HOST) Symposium, 2019.
[15] S. Bhunia et.al., Hardware Security: A Hands-on Learning Approach. Amsterdam, The Netherlands: Elsevier, 2019.
[16] Bah-Hwee Gwee et.al., "A Highly Secure FPGA-Based Dual-Hiding Asynchronous-Logic AES Accelerator Against Side-Channel Attacks," Proceedings of the IEEE Asian Hardware Oriented Security and Trust (HOST) Symposium, 2019.
[17] Xilinx Inc., Vivado Design Suite User Guide, Xilinx Documentation, 2020.
[18] Y.-W. Hung et.al., "Dynamic workload allocation for edge computing," IEEE Trans. Very Large Scale Integr. (VLSI) Syst, Mar. 2021.
[19] Kwen-Siong Chong et.al., "Dual-Rail Asynchronous-Logic AES Accelerator Against Side-Channel Attacks," Proceedings of the IEEE Asian Hardware Oriented Security and Trust (HOST) Symposium, 2022.
[20] Bah-Hwee Gwee et.al., "A Highly Secure FPGA-Based Dual-Hiding Asynchronous-Logic AES Accelerator Against Side-Channel Attacks," Proceedings of the IEEE Asian Hardware Oriented Security and Trust (HOST) Symposium, 2023.