IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Literature Review - Optimized Pipelined VLSI Implementation Of AES Algorithm For High Speed Data Encryption Applications

Charith P, Vijaya K

MTech Student, Assistant Professor

Department of Electronics & Communication Engineering,

BMSCE, Bengaluru, India

Abstract: The Advanced Encryption Standard (AES) is a cornerstone of modern cryptographic systems, widely utilized to ensure data security in a variety of applications. This thesis explores the optimization of AES for Very Large Scale Integration (VLSI) implementations, focusing on techniques to improve performance, efficiency, and security. Key optimization strategies such as parallelism, pipelining, SubBytes optimization, and key schedule enhancements are examined in detail. Various hardware architectures, including bit-slice, byte-slice, pipelined, and round-based designs, are analyzed to understand their impact on performance metrics like throughput, latency, area utilization, and power consumption. A comprehensive security analysis evaluates the VLSI implementations' resistance against classical cryptographic attacks and sophisticated side-channel attacks. Countermeasures such as power consumption randomization, constant-time execution, and electromagnetic shielding are discussed to bolster the hardware's resilience. The thesis concludes with a discussion on future work, emphasizing the potential of emerging technologies like post quantum cryptographic algorithms, advanced fabrication techniques, adaptive architectures, and the integration of machine learning for further enhancing the security and performance of AES hardware implementations. This research aims to contribute to the development of robust and efficient AES hardware, ensuring the continued protection of sensitive data in an increasingly digital and interconnected world.

Index Terms **-** Gain Enhancement, Positive feedback, Differential amplifier, Op-amp.

I. INTRODUCTION

Within the context of the contemporary world, information security has emerged as an essential component. The research that concerns the protection of knowledge for future generations is becoming an extremely important area of study In order to ensure the safety of information, it is necessary to provide a specialized approach not only to the process of transporting it but also to the process of storing it. The transfer of data was made more secure by the use of cryptography. The data must be protected against entry by unauthorized parties. Encryption conceals information from the general public and prevents it from being accessed. The original content of a data set can only be accessed by authorized individuals via the use of encryption, who are unable to read the data. In general, encryption techniques consist of a public key and a private key, which are sometimes referred to as symmetric keys. Because it requires two keys—one for encryption and another for decryption—the public key method is not only difficult to understand but also requires a significant amount of time to compute. Simple is the algorithm for the private key. There is only one key that can be used for both encryption and decryption. As a result, it is beneficial for implementations that are completed more quickly. The Data Encryption Standard (DES) was first implemented as the standard by the United States government in November of 1976. It has been regarded a standard for symmetric key encryption ever since it was first implemented in 1967. It was no longer secure since the DES has a key length of 56 bits, which is regarded to be a modest number at the moment and is readily cracked. In order to take the position of the more

traditional Data Encryption Standard, the NIST gave its approval to the algorithms that make up the AES on January 2, 1997. The draught is available for public consumption under the designation of FIPS-197, which stands for Federal Information Processing Standard number 197. The AES algorithm is a symmetric key block cypher that encrypts data with a block size of 128 bits. A broad range of platforms, including smart cards, digital video recorders, internet web servers, automated teller machines (ATMs), and mobile phones, are all devices that are compatible with the AES algorithm. The AES may be implemented in either software or hardware. Hardware implementation of the AES algorithm enhances both the speed and the level of physical security.To ensure the confidentiality and integrity of data has become of the utmost importance in our day and age, which is characterized by the prevalence of digital communication and the extensive flow of sensitive information.

When it comes to protecting sensitive information from being accessed or manipulated by unauthorized parties, cryptographic methods are an extremely important factor. Among these algorithms, the AES is widely recognized as a foundational component of contemporary cryptography. It is recognized for its resilience, efficiency, and broad usage. The need of implementing AES in Very Large Scale Integration (VLSI) designs in a way that is both efficient and effective is becoming more and more apparent as the demand for secure communication continues to rise. This thesis investigates the complex confluence of AES and VLSI, delving into the difficulties, techniques, and optimizations that are inherent in the process of developing and implementing AES within the limits of VLSI designs.

II. PREVIOUS RESEARCH ON HARDWARE IMPLEMENTATIONS OF AES IN VLSI

Only combinational logic is used in the design that Xinmiao and colleagues have presented. By eliminating the unbreakable delay that is caused by look-up tables in traditional techniques, the benefit of subpipelining may be further investigated. This is a direct result of the elimination of the delay. In addition to this, composite field arithmetic is used in order to lessen the minimum area requirements, and several solutions for the inversion in subfield (24) are compared. In addition, a critical expansion design that is both effective and appropriate for the subpipelined round units is provided here. A fully subpipelined encryptor with seven substages in each round unit can achieve a throughput of 21.56 Gbps on a Xilinx XCV1000 e-8 bg560 device in non-feedback modes by utilizing the proposed architecture. This is a faster and 79% more efficient implementation in terms of equivalent throughput/slice than the fastest previous FPGA implementation that has been known to date.

A hardware implementation approach for the SubBytes and InvSubBytes transformations of the Advanced Encryption Standard (AES) has been developed by Minling and Jinghong. This solution takes into consideration the fact that traditional look-up tables (LUT) have an unbreakable latency. Furthermore, if the affine transformation in Galois Field GF(28) is used, the changes would be very difficult to implement in hardware. It is going to result in a sluggish processing performance as well as a high cost of source. As a result, the deconstructing technique that is underpinned by combinational logic will be an efficient approach. In addition, the decomposition approach is helpful for the combined structure, which allows the SubBytes and the InvSubBytes to use the same transformation module. The first thing to note is that the GF(28) element may be broken down into GF(24) elements. Additionally, in the GF(24 Keywords- SubBytes; AES; combinational logic; Galois Field), we conduct an analysis of composite field arithmetic and counterpart isomorphic mapping. Arundhati et al. devised the S-Box method for the AES algorithm. A verilog implementation is used for the design structure that has been presented. In order to implement the S-Box of the AES algorithm, which resulted in a delay that was fixed and unbreakable, lookup tables were used. When compared to a lookup table that is based on ROM, the suggested design makes use of a combinational logic-based composite field arithmetic AES S-Box, which results in an optimized area in terms of FPGA slices. The suggested four-stage pipelined version of S-Box is carried out on the XC3S100E device of Xilinx FPGA using verilog code. This implementation needs 34 slices and 67 four-input LUTs, in addition to a maximum clock frequency of 187.071 MHz.

As a result of Ramya et al.'s proposal of an efficient cryptographic approach, Advanced Encryption Standard (AES) has overtaken Data Encryption Standard (DES) in comparison to other algorithms, such as SHA-1. It is conceivable to implement equipment stage conditions inferable from the reconfigurability, inexpensive cost, and publicizing space with the usage of field programmable entryway clusters (FPGAs). According to the RIJNDAEL algorithmic guideline, a square figure is used in order to scramble and decode complicated data. Additionally, it is capable of receiving cryptographic keys with lengths of 28,192 and 256 bits.

In the suggested pipelined design, the round keys, which are used throughout certain regions of encryption, are generated concurrently with the encryption technique. This is a wonderful standard for the pipelined design. The extension is dependent on the use of a dual-stage design. This approach allows for the possibility of operating at higher clock frequencies, which ultimately results in improved throughput and decreased power consumption.

The authors Pietro et al. proposed a cryptographic hardware (HW) accelerator that is capable of supporting multiple AES-based block cypher modes. These modes include the more advanced cipher-based MAC (CMAC), counter with CBC-MAC (CCM), Galois counter mode (GCM), and XOR-encrypt-XORbased tweaked-codebook mode with ciphertext stealing (XTS) modes. Access privilege methods, on-chip clock randomization, and enhanced encryption key security management are some of the cutting-edge and creative hardware features that are included into the architecture that has been suggested. On an Ultrascale + Xilinx field-programmable gate array (FPGA), the system has been tested in a RISC-V-based system-on-chip (SoC) that was created expressly for this purpose. A thorough analysis of the system's performance, as well as its resource and power consumption, has been performed. Following the synthesis of the cryptoprocessor using a 7-nanometer CMOS standard-cells technology, the information about its performances, complexity, and power consumption is analysed and compared with the current state of the art. It is now possible to include the suggested cryptoprocessor onto the cutting-edge microprocessor that is being developed by the European Processor Initiative (EPI). Standard for advanced encryption, often known as index terms.

Siddesh and Shruthi J are involved in the implementation of the hardware platform scenario because of the nature of its reconfiguration, the cheap fee, and the advertising space it provides. Through the use of pipelining, the primary purpose of this article is to cut down on the amount of time that is wasted in order to speed up the process. There is a possibility that the RIJNDAEL cryptography algorithmic rule is a block cypher that is used for the purpose of encrypting and decrypting digital information. It is able to utilize cryptographic keys that are 128, 192, and 256 bits in length. One of the distinctive features of the pipelined arrangement that has been presented is that the round keys that are used up throughout the many rounds of encryption are created in tandem with the encryption process. This results in a reduction in the total delay that is associated with each round key of coding delay of a plaintext block. The use of Xilinx programming with Verilog hardware may be simulated via the use of this technique through experimentation. The implementation of the language and hardware on the FPGA Spartan 3E is described.

A new full-custom compact 8-bit data-path architectural core was suggested by Nabihah and Hasan for use in a single-chip VLSI AES crypto-hardware accelerator. The use of unique circuit-level approaches, logic reduction, resource sharing, and low supply voltage has been implemented in order to optimize chip-area, power, and performance. Encryption and decryption in Electronic-Codebook-Mode (EBC) utilizing 128-bit keys are both supported by the proposed design, which is implemented in a CMOS process using a 130-nanometer technology. Through the use of a low-power Exclusive-OR (XOR) gate, novel S-box/InvS-box, MixColumn/InvMixColumn, and ShiftRow/InvShiftRow are utilized in order to reduce the amount of power that is put into operation. A total of 3120 gate-equivalents (GE) were used in this design. This design also included an on-the-fly key scheduling unit that had an active chip-area of 640μm × 325 μm (0.208 sq. mm), omitting bonding pads inside the design. It has a power consumption of 4.23 microwatts per megahertz (μW/MHz) and a throughput of 0.05 gigabits per second (Gbit/s) while operating at a clock frequency of 100 MHz. As a result, the suggested AES architecture was able to achieve low power dissipation, greater throughput, and a smaller chip size (silicon area) in comparison to other previous implementations.

A rapid and effective application of AES in memory (AESIM) was presented in the work by Anusha and Dhanalakshmi to encrypt either a portion of the memory or the complete memory only if it is required. This was done in order to combine the AES key and the ECC key in an alternative manner for the purpose of encryption and decryption. In order to implement the AESIM approach that was presented, the inherent logic working capacity of NVM was used. This was done in place of introducing extra processing components to the memory that was very sensitive to cost.

When it comes to overcoming the challenges that are associated with the bandwidth concentrated encryption technique, we make use of the aid that is offered by the design of the in-memory storage system, which includes a massive internal bandwidth and a significant decrease in the transit of data. S-box is used in conjunction with the AESIM technique in order to carry out the encryption process. Subsequently, the inverse S-box, which is utilized in conjunction with the AESIM, is brought into play in order to carry out the decryption process. AESIM surpasses existing approaches by embracing the huge parallelism of the memory, which results in improved performance while also reducing the amount of energy that is used. By measuring the minimum amount of time used, the minimum amount of time taken for the time before clock delivery, the

average amount of time required for operation after clock, the latency, and the amount of logic separately for the proposed AESIM encryption and decryption technique, the efficiency of the proposed AESIM technique is calculated for both the encryption and decryption processes.An method known as the Adaptive Counter-Clock (ACC) S-Box was proposed by Subramanian and colleagues. During the process of data encryption, this method corrects the mistake and protects the data from being accessed by hackers. Power consumption, power dissipation, and a reduction in the area size are all topics that have been covered in this work. Field Programmable Gate Arrays, often known as FPGAs, are used for the purpose of carrying out the encryption process in hardware. The decryption process has three stages: the Inverse Mix Column, the Inverse Sub Bytes (S-Box), and the Inverse Shift Row stages. These processes are necessary in order for the receiver to be able to read the message in plain text that was delivered by the sender. In order to do this, the receiver for the encryption process has to possess the same key that was used by the sender. RTL coding is carried out with the help of Verilog HDL, and Xilinx ISE 14.7 FPGA will be used for practical application.

III. Conclusion and Future Work

In conclusion, the VLSI implementation of the AES represents a critical advancement in the field of secure communications, offering significant improvements in speed, efficiency, and security over traditional software-based encryption methods. The rigorous exploration of hardware optimization techniques, including parallelism, pipelining, S-box optimization, and key schedule enhancement, demonstrates the potential of VLSI to achieve unparalleled performance metrics. These optimizations ensure that AES implementations can meet the high throughput and low latency requirements essential for modern cryptographic applications. Additionally, the detailed analysis of various hardware architectures, such as bit-slice, byte-slice, pipelined, round-based, key-based, mixed-precision, and reconfigurable architectures, provides valuable insights into the diverse design strategies available for tailored AES implementations. Dataflow architectures, with their ability to exploit parallelism and pipelining at a granular level, further highlight the flexibility and scalability of hardware-based AES solutions. However, the security of VLSI implementations remains paramount, necessitating comprehensive security analyses to evaluate resistance against cryptographic attacks and side-channel vulnerabilities. By incorporating advanced countermeasures such as power consumption randomization, constant-time execution, electromagnetic shielding, and robust packaging, designers can significantly enhance the resilience of AES hardware against sophisticated attacks. These measures are crucial in maintaining the integrity and confidentiality of sensitive data in environments where security is non-negotiable. Despite these advancements, the field continues to evolve, presenting numerous opportunities for future work. One area of ongoing research is the development of more efficient and secure hardware-friendly cryptographic primitives that can further enhance the performance and security of AES implementations. Additionally, exploring the integration of post-quantum cryptographic algorithms into VLSI designs is becoming increasingly important in anticipation of the advent of quantum computing. These algorithms, resistant to quantum attacks, will be essential in future-proofing cryptographic hardware against emerging threats. Moreover, advancements in fabrication technologies, such as the transition to smaller process nodes and the incorporation of 3D integration techniques, offer promising avenues for improving the density, performance, and power efficiency of AES hardware implementations. Leveraging these technologies can lead to the creation of even more compact and powerful encryption engines, suitable for a wide range of applications from IoT devices to high-performance computing systems. Another promising direction for future research is the development of adaptive and self-reconfiguring AES hardware architectures. These architectures could dynamically adjust their operational parameters and configurations in response to varying security requirements and environmental conditions, offering enhanced flexibility and robustness. This adaptability is particularly valuable in diverse application scenarios where security and performance needs may fluctuate. Furthermore, the integration of machine learning techniques into the design and optimization processes of AES hardware presents an exciting frontier. Machine learning algorithms can be employed to predict and mitigate potential vulnerabilities, optimize resource allocation, and enhance the overall performance of AES implementations. By leveraging the predictive and analytical capabilities of machine learning, designers can achieve more resilient and efficient cryptographic hardware. In summary, while significant strides have been made in the VLSI implementation of AES, the journey is far from over. The continuous pursuit of innovation in hardware optimization, security enhancement, and integration of emerging technologies will drive the future of cryptographic hardware.

These efforts will ensure that AES remains a cornerstone of secure communications, capable of withstanding the evolving landscape of cybersecurity threats. As we move forward, the collaboration between academia, industry, and governmental bodies will be crucial in advancing the state-of-the-art in VLSI-based cryptographic solutions, paving the way for a more secure and reliable digital world.

REFERENCES

[1] J. -S. Ng, J. Chen, K. -S. Chong, J. S. Chang and B. -H. Gwee, "A Highly Secure FPGA-Based Dual-Hiding Asynchronous-Logic AES Accelerator Against Side-Channel Attacks," *in IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 30, no. 9, pp. 1144-1157, Sept. 2022, doi: 10.1109/TVLSI.2022.3175180.

[2] Devika, K. N., and Ramesh Bhakthavatchalu. "VLSI implementation of crypto coprocessor using AES and LFSR." In *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 772-777. IEEE, 2022.

[3] Ramya, T., G. Ramya, Karthik Raju, J. Ravi, and Deepak Verma. "An Efficient AES Algorithm for Cryptography Using VLSI." *ECS Transactions* 107, no. 1 (2022): 5605.

[4] Padmavathi, R. Anusha, and K. S. Dhanalakshmi. "An advanced encryption standard in memory (aesim) efficient, high performance s-box based aes encryption and decryption architecture on vlsi." *Wireless Personal Communications* 123, no. 4 (2022): 3081-3101.

[5] Guo, Xinfei, Mohamed El-Hadedy, Sergiu Mosanu, Xiangdong Wei, Kevin Skadron, and Mircea R. Stan. "Agile-aes: Implementation of configurable aes primitive with agile design approach." *Integration* 85 (2022): 87-96.

[6] Priya, S. Sridevi Sathya, P. Karthigaikumar, and Narayana Ravi Teja. "FPGA implementation of AES algorithm for high speed applications." *Analog Integrated Circuits and Signal Processing* (2022): 1-11.

[7] Nannipieri, Pietro, Stefano Di Matteo, Luca Baldanzi, Luca Crocetti, Luca Zulberti, Sergio Saponara, and Luca Fanucci. "VLSI design of Advanced-Features AES CryptoProcessor in the framework of the European Processor Initiative." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 30, no. 2 (2021): 177-186.

[8] Ahmad, Nabihah, and SM Rezaul Hasan. "A new ASIC implementation of an AES crypto-hardware accelerator." *Microelectronics Journal* 117 (2021): 105255.

[9] Subramanian, K., M. Venkatachalam, and M. Saroja. "Adaptive counter clock gated S-Box transformation based AES algorithm of low power consumption and dissipation in VLSI system design." In *Journal of Physics: Conference Series*, vol. 1979, no. 1, p. 012066. IOP Publishing, 2021.

[10] Nandan, V., and R. Gowri Shankar Rao. "Minimization of digital logic gates and ultra-low power AES encryption core in 180CMOS technology." *Microprocessors and Microsystems* 74 (2020): 103000.

[11] Kumar, Raghavan, Vikram Suresh, Monodeep Kar, Sudhir Satpathy, Mark A. Anders, Himanshu Kaul, Amit Agarwal et al. "A 4900-$\mu $ m 2 839-Mb/s Side-Channel Attack-Resistant AES-128 in 14-nm CMOS With Heterogeneous Sboxes, Linear Masked MixColumns, and Dual-Rail Key Addition." *IEEE Journal of Solid-State Circuits* 55, no. 4 (2020): 945-955.

[12] Sunil, Joseph, H. S. Suhas, B. K. Sumanth, and S. Santhameena. "Implementation of AES Algorithm on FPGA and on software." In *2020 IEEE International Conference for Innovation in Technology (INOCON)*, pp. 1-4. IEEE, 2020.

[13] Devi, SistlaVasundhara, and Harika Devi Kotha. "AES encryption and decryption standards." In *Journal of Physics: Conference Series*, vol. 1228, no. 1, p. 012006. IOP Publishing, 2019.

[14] Ueno, Rei, Sumio Morioka, Noriyuki Miura, Kohei Matsuda, Makoto Nagata, Shivam Bhasin, Yves Mathieu, Tarik Graba, Jean-Luc Danger, and Naofumi Homma. "High throughput/gate AES hardware architectures based on datapath compression." *IEEE Transactions on Computers* 69, no. 4 (2019): 534-548.

[15] Kumar, Raghavan, Vikram Suresh, Monodeep Kar, Sudhir Satpathy, Mark Anders, Himanshu Kaul, Amit Agarwal et al. "A 4900× m 2 839Mbps Side-Channel Attack Resistant AES-128 in 14nm CMOS with Heterogeneous Sboxes, Linear Masked MixColumns and Dual-Rail Key Addition." In *2019 Symposium on VLSI Circuits*, pp. C234-C235. IEEE, 2019.

[16] Varkuti, Kumara Swamy, and Prabhu Benakop. "VLSI Design flow for Secure Integrated Circuits based on DES, TDES, AES and Blowfish Algorithms and their performance." *International Journal of Engineering & Technology* 7, no. 2.16 (2018): 94-97.

[17] Wong, Ming Ming, Dennis ML Wong, Cishen Zhang, and Ismat Hijazin. "Circuit and system design for optimal lightweight AES encryption on FPGA." (2018).

[18] Zhang, Xiwei, Meng Li, and Jing Hu. "Optimization and implementation of AES algorithm based on FPGA." In *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pp. 2704-2709. IEEE, 2018.

[19] Baby Chellam, Manjith, and Ramasubramanian Natarajan. "AES hardware accelerator on FPGA with improved throughput and resource efficiency." *Arabian Journal for Science and Engineering* 43 (2018): 6873-6890.

[20] Sandyarani, K., and P. Nirmal Kumar. "Vlsi architecture for nano wire based Advanced Encryption Standard (AES) with the efficient multiplicative inverse unit." *International Journal of VLSI design & Communication Systems* 8, no. 6 (2017).