Enhanced Secure Communication Protocol with Pipelined Advanced Encryption for Mobile Networks

A. HariKrishna[1], Devasani Bindu[1], Cherukuru Sowmya[1], Gumparlapati Varshitha[1], Challagundla Tharunasree[1]

[1]Department of Electronics and Communication Engineering, Geethanjali Institute of Science and Technology, Nellore.

Abstract: In today's increasingly connected world, the demand for secure mobile communications is paramount. The security protocols are specifically tailored for mobile communication systems, ensuring the confidentiality and integrity of sensitive data transmitted over wireless networks. It can be seamlessly integrated into various mobile applications such as messaging platforms, VoIP services, and mobile banking apps, providing end-to-end encryption for user privacy. Current encryption protocols used in mobile communications often face challenges related to performance and security. Traditional encryption methods may not adequately address the evolving threats posed by sophisticated attackers. Moreover, the computational overhead associated with encryption and decryption processes can impact the overall efficiency of mobile communication systems. This work presents a novel approach to enhancing the security of mobile communications through the design of a Pipelined Advanced Encryption Based Cryptography Protocol (PAEBCP). The proposed protocol aims to address the vulnerabilities present in existing encryption methods by leveraging a pipelined architecture for efficient encryption and decryption processes. The proposed PAEBCP protocol introduces a pipelined architecture that optimizes the encryption and decryption processes for mobile communication systems. By dividing the encryption process into multiple stages and parallelizing key operations, the protocol enhances both security and performance.

Keywords: Pipelined Advanced Encryption Based Cryptography Protocol, Add round key. sub bytes, shift Rows, Mix Columns

1. Introduction

Through the years, the flow of data and its transmission has increased tremendously and so has the security issues to it. cryptography in recent years with the advancement of VLSI has led to its implementation of encryption and decryption techniques, where the process of translating and converting plaintext into cypher text and vice versa was made possible. In this literature, the review of various aspects of VLSI's implementation of encryption and decryption are covered. To systemize the material, the information about methods such as Private Key Encryption, Index Technique, Blowfish Algorithm, and many more are reviewed. Ultimately, with this review, the basic understanding of different VLSI techniques of encryption and decryption can be studied and implemented. Rajput, Gurudayal Singh, et.al [1] considered the use of cryptography in algorithms has seen to be safe and effective. The secret key distribution was still regarded as a crucial problem even though it was like other symmetric encryption schemes. One single block of data (128 bits) must be encrypted or decrypted, and this requires more computer work that uses more power.

Rajski, Janusz, Maciej Trawka, et.al [2] designed a Provided Protection on the integrated circuits (ICs) against hardware security threats has been tackled by many schemes proposed to mitigate risks associated with an unauthorized access and usage of ICs in general, and intellectual property (IP) cores. Typically, this was accomplished by virtue of hardware roots of trust whose crucial security primitives entail cryptographic hash functions. Alatawi, Mohammed Naif, et.al [3] developed the proliferation of sensor networks and other Internet of Thing's devices has prompted growing privacy and safety concerns. These devices have very little memory, computing power, and storage space. Security for low-powered IoT devices, such as RFID tags, nodes in wireless sensor networks (WSNs), etc., has become increasingly difficult. Peng Zhou, Yazheng Tu, et.al [4] implemented Along with National Institute of Standards and Technology (NIST) post-quantum cryptography (PQC) standardization process, lightweight PQC-related research, and development had also gained substantial attention from the research community. Althobaiti et.al [5] developed Ad-hoc networks have gained significant attention in the realm of communication due to the proliferation of mobile and IoT devices and wireless networks. Ad- hoc Networks offer a decentralized approach, where each node can function as a router and a terminal. Ensuring data safety and integrity in ad hoc networks remains a challenge, necessitating the use of robust security mechanisms.

2. Literature Survey

Vidaković, et.al [6] proposed the continuous development of quantum computing necessitates the development of quantum-resistant cryptographic algorithms. In response to this demand, the National Institute of Standards and Technology selected standardized algorithms including Crystals-Di lithium, Falcon, and Sphincs+ for digital signatures. This literature provides a comparative evaluation of these algorithms across key metrics. Feng, et.al [7] developed with the rapid development of the Internet of Things (IoT), device and data security has attracted huge academic attention in recent years since conventional security methods are barely feasible in IoT circumstances. Traditional encryption methods require extensive computation complexity, which requires several hardware resources and power consumption. Trujillo-Toledo, et.al [8] proposed a new medical cryptosystem based on four chaotic maps was presented as a case study. The message queuing telemetry transport (MQTT) protocol was used in

this research to propose an end-to-end chaotic encryption technique that would enhance security and secrecy to the transmission of medical images from any Healthcare Internet of Things (H-IoT) device connected to the Internet.

Dam, et.al [9] suggested information security was a fundamental and urgent issue in the digital transformation era. Cryptographic techniques and digital signatures have been applied to protect and authenticate relevant information. However, with the advent of quantum computers and quantum algorithms, classical cryptographic techniques had been in danger of collapsing because quantum computers can solve complex problems in polynomial time. Oladipupo, Esau Taiwo, et.al [10] Implemented the need to ensure the longevity of Wireless Sensor Networks (WSNs) and secure their communication had spurred various researchers to come up with various WSN models. Prime among the methods for extending the life span of WSNs is the clustering of Wireless Sensors (WS), which reduces the workload of WS and thereby reduces its power consumption. Li, Bin, et.al [11] proposed a postquantum cryptography (PQC), polynomial multiplication was complex and time-consuming, which affects the overall computational efficiency. In addition, the parameters of different lattice-based algorithms require different number theoretic transform (NTT) structures, which limits the versatility of hardware design. To this end, this article proposes scalable and parallel optimization of the NTT based on a field-programmable gate array (FPGA).

Della Sala, Riccardo, et.al [12] Proposed the Physical Unclonable Functions (PUFs) and True Random Number Generators (TRNGs) were both needed in the Privacy Preserving Mutual Authentication (PPMA) protocol, often used in IoT Applications to generate, and secure cryptographic keys. Since to guarantee security of IoT nodes in an untrusted setting, the PPMA key and encrypted data must be located on the same chip, the concept of integrating both a PUF and a TRNG on the same device has emerged as a new security paradigm. Camacho-Ruiz, et.al [13] Suggested the advent of quantum computing with high processing capabilities will enable brute force attacks in short periods of time, threatening current secure communication channels. To mitigate this situation, post-quantum cryptography (PQC) algorithms have emerged. Among the algorithms evaluated by NIST in the third round of its PQC contest was the NTRU cryptosystem. Nath, Himun, et.al [14] Introduced the Vehicular Ad hoc Network (VANET) was a versatile and ad hoc network, where the vehicles must be authenticated before sharing any critical information. During authentication, privacy of the users must be preserved. There were several surveys on privacy-preserving authentication schemes in VANET. Thi, Sang Duong, et.al [15] Proposed the Advanced Encryption Standard (AES)and Ascon algorithms were highly secure and compact, suitable for computing in Internet of Things (IoT)systems. However, existing research lacks a flexible and power -efficient hardware architecture for these algorithms on IoT devices.

3. Proposed Methodology

A pipelined mechanism in the context of AES refers to a method of organizing the encryption or decryption process to improve efficiency and throughput as shown in Figure 1. AES is a symmetric encryption algorithm widely used for securing data. In a pipelined mechanism, the processing stages of AES are overlapped or parallelized to maximize utilization of computational resources and reduce latency. The AES algorithm consists of several key stages, including SubBytes, ShiftRows, MixColumns, and AddRoundKey, which are repeated for multiple rounds depending on the key size. Each stage involves various operations such as substitution, permutation, and bitwise operations on the data. In a pipelined mechanism, these stages are divided into smaller tasks, and multiple tasks are executed concurrently. For example, while one block of data is undergoing the SubBytes stage, another block can simultaneously undergo the ShiftRows stage, and so on. This allows for parallel processing of multiple blocks of data, which can significantly improve throughput compared to a serial processing approach.

The pipelined mechanism requires careful synchronization and management of data dependencies between stages to ensure correct operation. Data must be passed between stages efficiently, and the results of each stage must be available when needed by subsequent stages. This typically involves buffering and inter-stage communication mechanisms. One of the main benefits of a pipelined mechanism in AES is improved throughput, as multiple blocks of data can be processed simultaneously. This is particularly useful in scenarios where high-speed encryption or decryption is required, such as in network communication or data storage systems. By overlapping the processing of different blocks, the overall time taken to encrypt or decrypt a large volume of data can be reduced. However, implementing a pipelined mechanism can also introduce complexity and overhead, particularly in terms of managing data dependencies and ensuring correct synchronization between stages. Additionally, the efficiency of the pipelined mechanism may be affected by factors such as the size of the data blocks, the number of processing stages, and the characteristics of the underlying hardware architecture. A pipelined mechanism in the context of AES (Advanced Encryption Standard) refers to a method of organizing the encryption or decryption process to improve efficiency and throughput. AES is a symmetric encryption algorithm widely used for securing data. In a pipelined mechanism, the processing stages of AES are overlapped or parallelized to maximize utilization of computational resources and reduce latency.

The AES algorithm consists of several key stages, including SubBytes, ShiftRows, MixColumns, and AddRoundKey, which are repeated for multiple rounds depending on the key size. Each stage involves various operations such as substitution, permutation, and bitwise operations on the data. In a pipelined mechanism, these stages are divided into smaller tasks, and multiple tasks are executed concurrently. For example, while one block of data is undergoing the SubBytes stage, another block can simultaneously undergo the ShiftRows stage, and so on. This allows for parallel processing of multiple blocks of data, which can significantly improve throughput compared to a serial processing approach. The pipelined mechanism requires careful synchronization and management of data dependencies between stages to ensure correct operation. Data must be passed between stages efficiently, and the results of each stage must be available when needed by subsequent stages. This typically involves buffering and inter-stage communication mechanisms.

One of the main benefits of a pipelined mechanism in AES is improved throughput, as multiple blocks of data can be processed simultaneously. This is particularly useful in scenarios where high-speed encryption or decryption is required, such as in network communication or data storage systems. By overlapping the processing of different blocks, the overall time taken to encrypt or decrypt a large volume of data can be reduced. However, implementing a pipelined mechanism can also introduce complexity and overhead, particularly in terms of managing data dependencies and ensuring correct synchronization between stages. Additionally, the efficiency of the pipelined mechanism may be affected by factors such as the size of the data blocks, the number of processing stages, and the characteristics of the underlying hardware architecture.

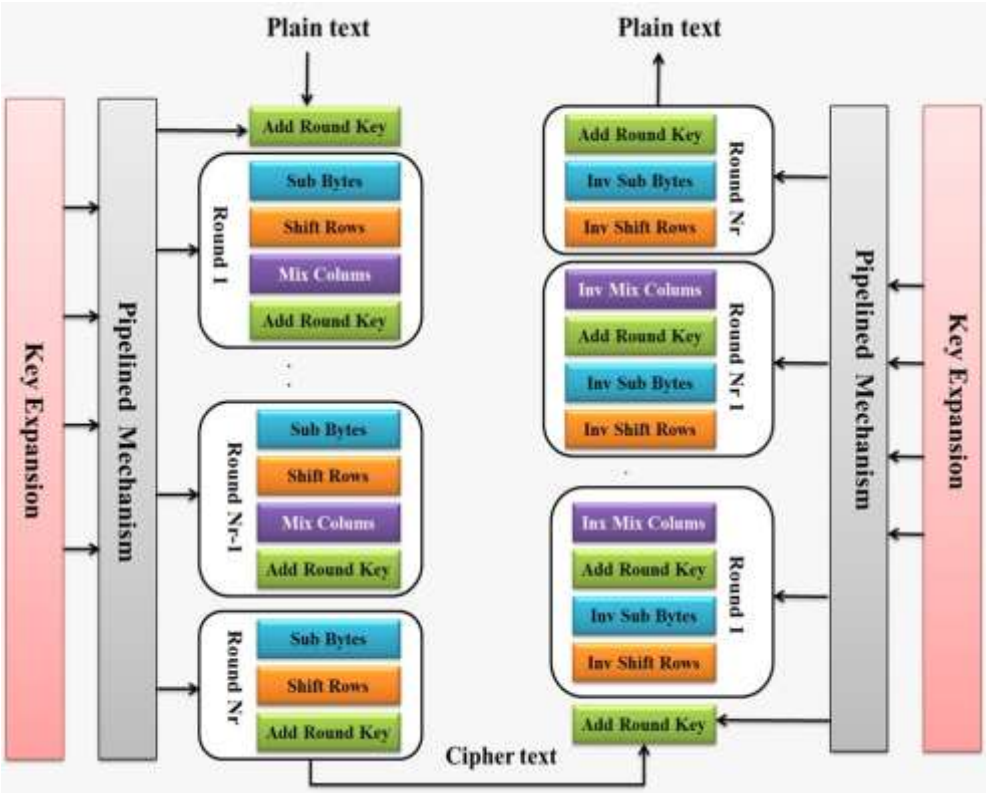

Figure 1. Pipelined Mechanism in AES

Key Expansion Mechanism: The key expansion mechanism is a fundamental component of the AES encryption process, responsible for generating a set of round keys from the original encryption key. These round keys are used in each round of the encryption algorithm. The key expansion process varies depending on the chosen key length, which can be 128 bits. At the outset, the initial round key is derived directly from the original encryption key. This key serves as the starting point for the key expansion process. The key schedule generation, the core of the key expansion mechanism, follows. It involves creating a set of round keys from the initial round key, ensuring uniqueness and complexity for each round. The Rcon (round constant) plays a crucial role in introducing variation during key expansion. Derived from the Rijndael finite field, it is utilized to XOR with certain words during the key expansion process, thus enhancing security. The key expansion process consists of several rounds, each of which generates a new round key based on the previous round key. Within each round, specific operations are applied to transform the previous round key into the next round key.

AddRoundKey: The AddRoundKey stage is the first stage of each round in the AES encryption process. Here, the data block undergoes an XOR operation with the round key generated from the key expansion mechanism. This operation ensures that each round uses a unique key, enhancing the security of the encryption process. By incorporating randomness introduced by the round key, the AddRoundKey stage mitigates the risk of cryptographic attacks such as linear and differential cryptanalysis.

Sub Bytes: Following the Add Round Key stage, the Sub Bytes stage substitutes each byte of the data block with a corresponding byte from the AES S-box. The S-box is a fixed substitution table that maps each input byte to a unique output byte based on mathematical properties. This non-linear substitution adds confusion to the encrypted data, making it more resistant to cryptanalysis techniques. The Sub Bytes operation contributes to the overall confusion and diffusion properties of the AES algorithm, enhancing its resistance to various cryptographic attacks.

Shift Rows: In the Shift Rows stage, the bytes within each row of the data block are cyclically shifted. This operation ensures that the relationship between input and output bytes is complex, thereby enhancing the diffusion property of the encryption process. By rearranging the byte positions within each row, Shift Rows ensures that changes in one byte affect multiple bytes in subsequent rounds. This adds another layer of security by making it more difficult for attackers to discern patterns or relationships within the encrypted data.

Mix Columns: The Mix Columns stage involves matrix multiplication on the columns of the data block. This operation provides additional diffusion and ensures that each byte in the output depends on multiple bytes in the input. By performing matrix multiplication, Mix Columns increases the complexity of the encryption process, making it more resistant to cryptanalysis techniques. This stage contributes to the overall security of AES by further obscuring the relationship between input and output bytes, thus thwarting attempts to reverse-engineer the encryption algorithm. The pipelined design of AES offers several advantages in the context of mobile networks. By breaking down the encryption process into multiple stages, AES can leverage parallel processing, thereby improving efficiency and speed. Additionally, the distinct stages of AES, coupled with the key expansion mechanism, enhance security by incorporating randomness, confusion, and diffusion into the encryption process. This robust combination of efficiency and security makes AES well-suited for securing data transmission in mobile network environments, where performance and protection are paramount.

4. Results and Discussion

Figure 2 likely shows the output or results of simulating the existing AES system. Figure 3 probably displays the area output of the existing AES system. Figure 4 likely represents the simulation output of the proposed AES system. Figure 5 presumably presents the area output of the proposed AES system, similar to Figure 3. Table 1 provides a performance comparison between the existing AES system and the proposed system across various metrics. These metrics include the number of LUTs, FFs, IO ports, and potentially other relevant parameters. The comparison highlights the differences in resource utilization between the two systems, with the proposed system showing significant reductions in LUTs, FFs, and potentially other resources compared to the existing system.

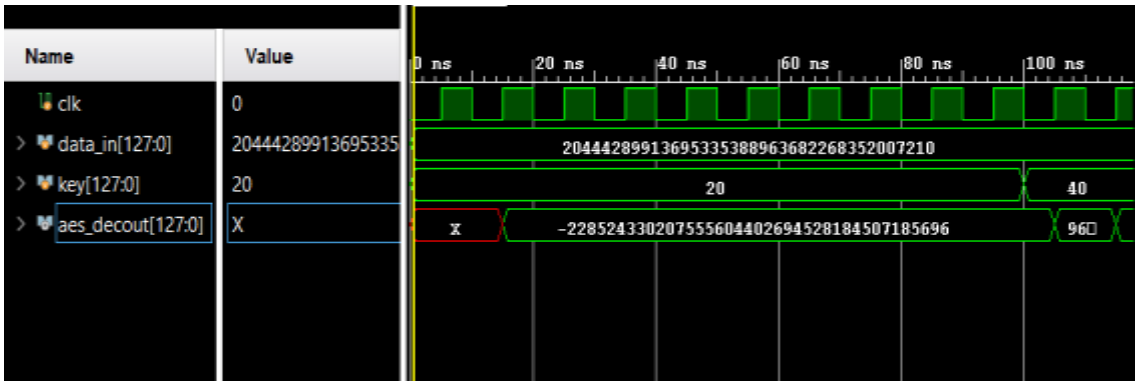

Figure 2. Existing Simulation Output.

Resource	Estimation	Available	Utilization...
LUT	21551	134600	16.01
FF	1792	269200	0.67
IO	514	500	102.80
BUFG	1	32	3.13

Figure 3. Existing Area Output

Figure 4. Proposed Simulation Output

Resource	Estimation	Available	Utilization...
LUT	7841	134600	5.83
FF	128	269200	0.05
IO	514	500	102.80
BUFG	1	32	3.13

Figure 5. Proposed Area Output.

Table1: Performance Comparison of existing and proposed systems.

Metric	Existing System	Proposed System
LUT	21551	7841
FF	1792	128
IO	514	514
BUFG	1	1

5. Conclusion

In the dynamic landscape of mobile networks, where the exchange of information occurs at unprecedented speeds, the imperative for robust and efficient secure communication protocols is paramount. The integration of pipelined advanced encryption mechanisms into mobile networks represents a significant leap forward in fortifying the

integrity and confidentiality of data transmission. Through the fusion of cutting-edge encryption techniques with streamlined communication protocols, this enhanced framework promises to redefine the paradigms of mobile security, ushering in a new era of trust and reliability. At its core, the enhanced secure communication protocol embodies a symbiosis of innovation and pragmatism, seamlessly integrating advanced encryption algorithms with the intricacies of mobile network architecture. By leveraging pipelined encryption, wherein multiple encryption stages operate concurrently, the protocol achieves a delicate balance between security and efficiency. This parallelization of cryptographic operations not only enhances the robustness of data protection but also minimizes latency and overhead, thereby ensuring optimal performance in resource-constrained mobile environments.

References

[1] Rajput, Gurudayal Singh, Rajeev Thakur, and Rovin Tiwari. "VLSI implementation of lightweight cryptography technique for FPGA-IOT application." Materials Today: Proceedings (2023).
[2] Rajski, Janusz, Maciej Trawka, Jerzy Tyszer, and Bartosz Włodarczak. "H2B: Crypto Hash Functions Based on Hybrid Ring Generators." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2023).
[3] Alatawi, Mohammed Naif. "A Hybrid Cryptographic Cipher Solution for Secure Communication in Smart Cities."
[4] He, Pengzhou, Yazheng Tu, Jiafeng Xie, and H. S. Jacinto. "Kina: Karatsuba initiated novel accelerator for ring-binary-lwe (rblwe)-based post-quantum cryptography." *IEEE Transactions on Very Large-Scale Integration (VLSI) Systems* (2023).
[5] Althobaiti, Hamad, and Ahmed Adas. "Simulation of Elliptical Curve Cryptography in IPSec on Ad-Hoc Networks." European Journal of Engineering and Formal Sciences 6, no. 1 (2023): 1-26.
[6] Vidaković, Marin, and Kruno Miličević. "Performance and Applicability of Quantum Digital Signature Algorithms in Resource-Constrained Environments." Algorithms 16, no. 11 (2023): 518.
[7] Feng, Jundong, Junchao Wang, Yubin Zhu, and Kaining Han. "A Hybrid Chaotic Encryption ASIC with Dynamic Precision for Internet of Things." IEEE Internet of Things Journal (2023).
[8] Trujillo-Toledo, D. A., O. R. López-Bonilla, E. E. García-Guerrero, J. J. Esqueda-Elizondo, J. R. Cárdenas-Valdez, U. J. Tamayo-Pérez, O. A. Aguirre-Castro, and E.Inzunza-González. "Real-time medical image encryption for H-IoT applications using improved sequences from chaotic maps." Integration 90 (2023): 131-145.
[9] Dam, Duc-Thuan, Thai-Ha Tran, Van-Phuc Hoang, Cong-Kha Pham, and Trong-Thuc Hoang. "A survey of post-quantum cryptography: Start of a new race." Cryptography 7, no. 3 (2023): 40.
[10] Oladipupo, Esau Taiwo, Oluwakemi Christiana Abikoye, Agbotiname Lucky Imoize, Joseph Bamidele Awotunde, Ting-Yi Chang, Cheng-Chi Lee, and Dinh-Thuan Do. "An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks." IEEE Access 11 (2023): 1306-1323.
[11] Li, Bin, Yunfei Yan, Yuanxin Wei, and Heru Han. "Scalable and Parallel Optimization of the Number Theoretic Transform Based on FPGA." IEEE Transactions on Very Large-Scale Integration (VLSI) Systems (2023).
[12] Della Sala, Riccardo, and Giuseppe Scotti. "Exploiting the DD-Cell as an ultra-compact entropy source for an FPGA-based re-configurable PUF-TRNG architecture." IEEE Access (2023).
[13] U. Penchalaiah and V. S. Kumar, "Design and Implementation of Low Power and Area Efficient Architecture for High Performance ALU", Parallel Processing Letters., vol. 32, no. 01n02, pp. 2150017, 2022.
[14] Camacho-Ruiz, Eros, Macarena C. Martínez-Rodríguez, Santiago Sánchez-Solano, and Piedad Brox. "Timing-Attack-Resistant Acceleration of NTRU Round 3 Encryption on Resource-Constrained Embedded Systems." Cryptography 7, no. 2 (2023): 29.
[15] Nath, Himun Jyoti, and Hiten Choudhury. "Privacy-preserving Authentication Protocols in VANET: A Review." (2023).
[16] Thi, Sang Duong, Hoai Luan Pham, Vu Trung Duong Le, Ren Imamura, Thi Hong Tran, and Yasuhiko Nakashima. "Small-footprint Reconfigurable Heterogeneous Cryptographic Accelerator for Fog Computing." environment 3: 4.