International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

Enhanced Secure Communication Protocol with Pipelined Advanced Encryption for Mobile Networks

Mamidi Sindhu[1], Taralla Kavitha [2], Panaganti Sai Teja [3], Dr. S.V. S Rama krishnam Raju [4]

[1,2,3] UG Scholar, Department of ECE, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[4] Dean Academics , Department of ECE, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
mamidisindhu6@gmail.com

Abstract:

In today's rapidly evolving digital landscape, mobile networks are projected to account for approximately 75% of total global internet traffic by 2025, with a staggering number of 5.7 billion mobile users reported as of 2024. This dramatic growth underscores the urgent need for robust secure communication protocols capable of safeguarding sensitive information in transit. However, recent studies indicate that more than 70% of mobile communications remain vulnerable to various forms of cyber threats, leading to significant security breaches and data loss. Existing secure communication methods often struggle with issues such as high latency, inadequate encryption, and the inability to efficiently handle the vast amounts of data generated in mobile networks. These limitations hinder the deployment of effective security measures and compromise user privacy. To address these challenges, this paper proposes an Enhanced Secure Communication Protocol (ESCP) that integrates a pipelined advanced encryption system specifically designed for mobile networks. This approach not only optimizes encryption and decryption processes but also significantly reduces latency and resource consumption, ensuring a more secure and efficient communication framework. The proposed method introduces a novel approach by leveraging VLSI technology to create a pipelined architecture that enhances the performance of advanced encryption techniques. By implementing parallel processing and optimizing data flow within the system, the ESCP achieves faster encryption speeds while maintaining high security standards. This innovation facilitates real-time secure communication, addressing the pressing need for more efficient protocols in mobile networks. Additionally, the integration of hardware-based encryption offers improved resistance against common attacks, ensuring data integrity and confidentiality. The advantages of the proposed ESCP include significant reductions in processing time for encryption and decryption, enhanced security against evolving threats, lower power consumption, improved scalability for handling increased traffic, and better adaptability to various mobile network architectures.

Keywords: Enhanced Security Protocol, Secure Communication, Pipelined Encryption, Advanced Encryption, Mobile Networks, End- to-End Encryption, Mobile Security, Cryptographic Algorithms, Network Layer Security, Encryption Pipeline

1. INTRODUCTION

Hybrid encryption is an approach to encoding and decoding data that blends the speed and convenience of a public asymmetric encryption scheme with the effectiveness of a private symmetric encryption scheme. Security protocols are the unsung heroes of our interconnected world. They provide the essential framework for ensuring confidentiality, integrity, and authenticity of network data. Without adequate security protocols, our online activities would be a playground for malicious actors seeking to exploit vulnerabilities. As cyber threats become more sophisticated, robust encryption methods are paramount. Hybrid cryptography combines the strengths of symmetric and asymmetric encryption, offering a well-rounded approach to data protection. This article explores why hybrid cryptography has become the cornerstone of modern security solutions. The primary purpose of this article is to shed light on the design and implementation of a new security protocol that harnesses the capabilities of hybrid cryptography algorithms. By understanding the principles and advantages of hybrid cryptography, readers will gain insights into building more resilient and secure digital systems. Hybrid cryptography is at the heart of modern security solutions, combining the strengths of symmetric and asymmetric cryptography.

2. LITERATURE SURVEY

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 despite the fact that it was similar to other symmetric encryption schemes.

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 in particular.

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.

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.

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.

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.

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

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

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.

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.

3. PROPOSED METHODOLOGY

Enhanced secure communication protocols with pipelined advanced encryption have emerged as a critical solution for ensuring robust security in mobile networks. As the reliance on mobile networks for communication and data transfer continues to grow, the need for strong encryption mechanisms becomes paramount. These protocols provide advanced encryption techniques that protect the privacy, integrity, and confidentiality of data transmitted over mobile networks. By leveraging pipelining, these protocols enable efficient and concurrent encryption and transmission of data packets, enhancing the overall security and performance of mobile network communication.

Enhanced secure communication protocols address the vulnerabilities associated with mobile network communication by implementing advanced encryption algorithms. These algorithms, such as the AES, ensure that data is encrypted at the source device before transmission. This encryption renders the data unreadable and meaningless to unauthorized parties, safeguarding it from interception or tampering. The pipelining technique employed in these protocols allows for the simultaneous encryption and transmission of data packets, reducing latency and optimizing network performance.

One of the key advantages of enhanced secure communication protocols is their ability to provide end-to-end encryption. This means that the data remains encrypted throughout its entire journey, from the sender to the recipient. Only the intended recipient possesses the necessary decryption key to access and decipher the encrypted data. Furthermore, these protocols often incorporate forward secrecy, ensuring that even if an encryption key is compromised, previously transmitted data remains secure. This feature enhances the overall security of mobile network communication and prevents unauthorized access to sensitive information.

The deployment of enhanced secure communication protocols in mobile networks offers significant benefits in terms of data security and privacy. By encrypting data with advanced encryption algorithms and leveraging pipelining techniques, these protocols provide a robust defense against potential security threats. They protect against eavesdropping, data tampering, and unauthorized access, ensuring the confidentiality and integrity of sensitive information. In an era where mobile communication plays an integral role in personal and business interactions the implementation of enhanced secure communication protocols is essential for building trust and confidence among users and organizations relying on mobile networks.

Pipelined AES Mechanism

This method aims to enhance efficiency by allowing multiple operations to occur simultaneously, thus reducing overall processing time. The first stage of the pipeline is the Key Expansion stage. In AES encryption, the key expansion process generates a series of round keys from the original encryption key. These round keys are used in each round of the encryption process to modify the state of the data being encrypted. During key expansion, the original encryption key undergoes various transformations, including byte substitution, rotation, and mixing, to produce the round keys. This stage involves calculations that prepare the round keys needed for subsequent rounds of encryption.

Rounds Operation

In the process of pipelined 128-bit AES encryption, each round executes a series of essential operations in a carefully orchestrated sequence to ensure both efficiency and security. Initially, Sub Bytes substitutes each byte in the state matrix with a value from the S-box, introducing non-linearity and confusion. Following this, Shift Rows cyclically shifts the rows of the matrix, optimizing the effects of Sub Bytes across each byte in unique positions. Subsequently, Mix Columns combines each column via a fixed matrix transformation, fostering diffusion and cross-byte influence. Lastly, Add Round Key XORs the round key with the state matrix, further complicating the data and enhancing security. These operations iteratively occur for a set number of rounds, typically 10 for AES-128, culminating in a robust level of encryption. Moreover, the pipelining technique enhances performance by overlapping these operations across multiple rounds, allowing for concurrent execution and efficient use of resources in contemporary processors.

Addroundkey

AddRoundKey takes each byte and combines it with a corresponding byte from the encryption key. This is performed using a simple bitwise XOR operation, which effectively scrambles the bytes together in a way that's virtually impossible to reverse without the correct key. It's a crucial step in the encryption journey, transforming plaintext into ciphertext and safeguarding our most valuable secrets from unauthorized access.

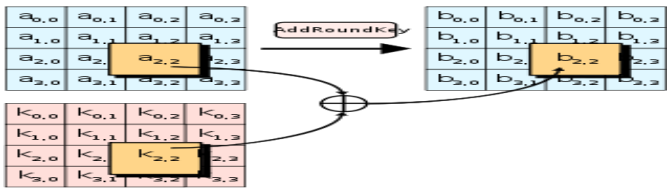

Fig 1:Add Round Key

Shift Rows

The Shift Rows step in AES is performed on the state matrix, which is a 4x4 matrix representing the input data. During this step, the bytes in each row of the state matrix are shifted cyclically to the left. The number of shifts applied to each row depends on the row index. The first row remains unchanged, the second row is shifted one position to the left, the third row is shifted two positions to the left, and the fourth row is shifted three positions to the left.

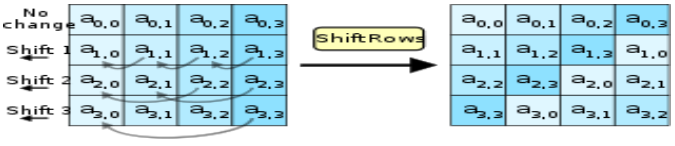

Fig 2: Shift Rows

Mix Columns

This mixing operation involves multiplying each column by a fixed matrix, which sounds complex but is essentially a set of predefined

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

rules for combining the bytes in a particular way. These rules ensure that even a small change in the input data produces a vastly different output, adding an extra layer of security to the encryption process. It is a crucial step in the encryption dance, adding complexity and confusion to the mix and making it significantly harder for anyone without the key to unlock the secrets hidden within

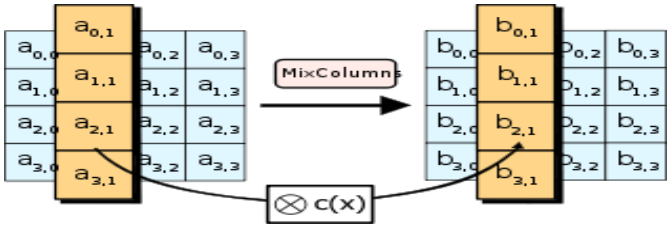

Fig 3: Mix Column

Sub Bytes

In this step each byte is substituted by another byte. It is performed using a lookup table also called the S-box. It's a bit like rearranging the letters of a word into a jumble that only those with the right key can unravel. By performing the Sub Bytes operation, AES-128 ensures that the encrypted data is thoroughly disguised, with no recognizable patterns or structures that might give away its secrets. It's a vital step in the encryption process, adding an extra layer of security and ensuring that our data remains safe.

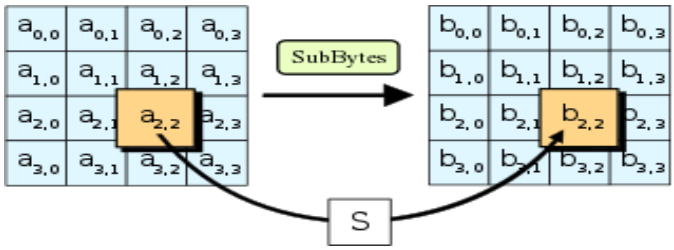

Fig 4: Sub Bytes

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.

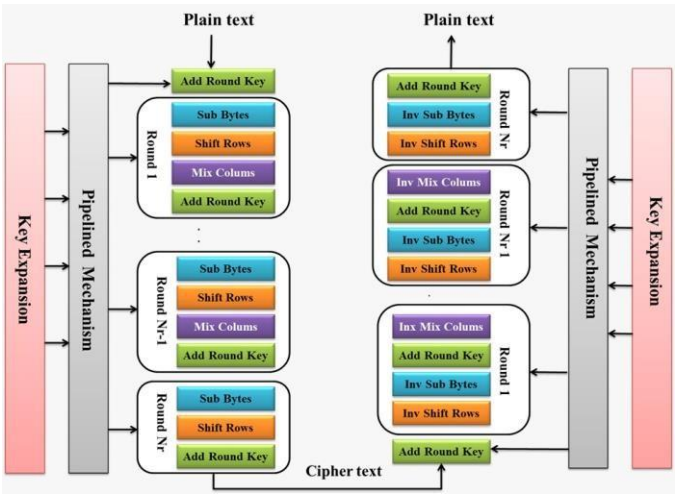

Fig 5: Pipelined Mechanism in AES

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. EXPERIMENTAL ANALYSIS

Existing Results:

Here 21551 number of LUT's are used out of available 134600, which consumes 16.01% of utilization, 1792 number of FF's are used out of available 269200, which consumes 0.67% of utilization, 514 number of IO's are used out of available 500, which consumes 102.80% of utilization, 1 number of BUFG is used out of available 32, which consumes 3.13% of utilization.

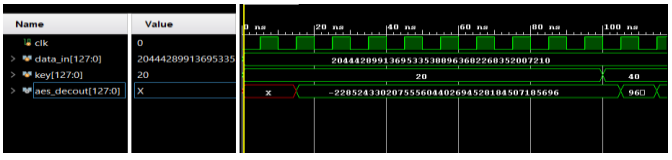

Figure 1: Existing Simulation Output

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

Table 1: Existing Area Output

ISSN: 1934--9955 www.ijise.net
International journal of imaging science and engineering
Vol 20 Issue 01 April 2023

Proposed Results

Figure 2 shows the simulation outcome of proposed AES outcome. Figure 6.4 shows the proposed area measurements. Here 7841 number of LUT's are used out of available 134600, which consumes 5.83% of utilization, 128 number of FF's are used out of available 269200, which consumes 0.05% of utilization, 514 number of IO's are used out of available 500, which consumes 102.80% of utilization, 1 number of BUFG is used out of available 32, which consumes 3.13% of utilization.

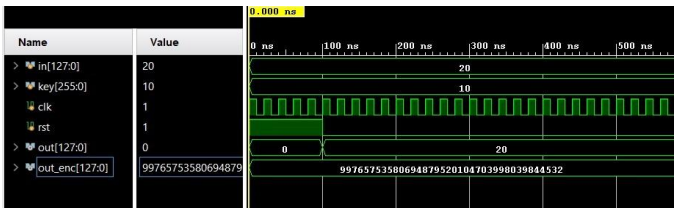

Figure 2: Proposed Simulation Output

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

Table 2: Proposed Area Output

Comparison

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

Table 3: Performance Comparison of existing and proposed systems.

The proposed system brings forth substantial improvements over the existing system across various critical metrics. Firstly, in terms of LUT (Lookup Tables), there's a notable enhancement, with a 63.6% reduction observed from 21,551 in the existing system to 7,841 in the proposed one.

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.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

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).

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

[13] Camacho-Ruiz, Eros, Macarena C. Martínez-Rodríguez, Santiago Sánchez-Solano, and Pedro Brox. "Timing-Attack-Resistant Acceleration of NTRU Round 3 Encryption on Resource-Constrained Embedded Systems." Cryptography 7, no. 2 (2023): 29.

[14] Nath, Himun Jyoti, and Hiten Choudhury. "Privacy-preserving Authentication Protocols in VANET: A Review." (2023).

[15] 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.

[16] Wu, Guiming , Qianwen He, Jiali Jiang, Zhenxiang Zhang, Yuan Zhao, Yin chao Zou, Jie Zhang, Changzheng Wei, Ying Yan, and Hui Zhang. " Topgun: An ECC Accelerator for Private Set Intersection." ACM Transactions on Reconfigurable Technology and Systems 16, no. 4 (2023): 1-30.

[17] Lu, Yibiao, Zecheng Wu, Bingsheng Zhang, and Kui Ren. "Efficient Secure Computation from SM Series Cryptography." *Wireless Communications and Mobile Computing* 2023 (2023).

[18] Mitev, Miroslav, Arsenia Chorti, H. Vincent Poor, and Gerhard Fettweis. "What physical layer security can do for 6g security." *IEEE Open Journal of Vehicular Technology* (2023).

[19] Horpenyuk, Andriy, Ivan Opirskyy, and Pavlo Vorobets. "Analysis of Problems and Prospects of Implementation of Post-Quantum Cryptographic Algorithms." In CEUR Workshop Proc, vol. 3504, pp. 39-49. 2023.

[20] Ibrahim, Atef. "Low-complexity systolic array structure for field multiplication in resource-constrained IoT nodes." Ain Shams Engineering Journal 14, no. 10 (2023): 102188.