iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67627

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Secure Email Services Using ECC and Diffie-Hellman Cryptography

Mrs. P S L Sravani[1], Imandi Sai Sravyasri[2], Medisetti Navya Sri[3], Nikhita Ganisetti[4], Dimpu Srivas Doddi[5]
Department of Computer Science and Engineering (Cyber Security),Raghu Engineering College,Andhra Pradesh,India

***Abstract:** This paper presents a novel approach to secure email services using Elliptic Curve Cryptography(ECC). With the increasing reliance on email communication for both personal and business purposes, ensuring the confidentiality and integrity of email messages has become paramount. Traditional email encryption methods, such as RSA, often suffer from computational overhead and key management challenges, making them less practical for widespread adoption. The proposed approach leverages ECC with Diffie Hellman Cryptography, a more efficient and secure cryptographic algorithm, to provide robust encryption and authentication for email messages. ECC offers shorter key lengths compared to RSA, resulting in faster encryption and decryption operations while maintaining a high level of security. Additionally, Diffie Hellman is well-suited for resource-constrained environments, making it ideal for use in mobile devices and other low-power devices*

***Keywords:** Elliptic Curve Cryptography (ECC) , Secure email services , Diffie-Hellman Cryptography , Email encryption , Key management.*

I. INTRODUCTION

With the digital age now upon us, email is still one of the most basic forms of communication that allows the exchange of tremendous volumes of sensitive information on a daily basis. From business communications to conversations between individuals, email is an invaluable instrument for data sharing and collaboration. Yet with this universal dependency comes the vulnerability of becoming an easy target for cyber attacks like interception, unauthorized access, phishing, and data breaches. As cybercrooks become increasingly sophisticated, classic security is most times inadequate in addressing new risks, and this calls for stronger encryption technologies in order to secure email communication.

Conventional cryptography techniques, including RSA (Rivest-Shamir-Adleman), have been employed to protect emails. Although RSA offers strong protection, it is associated with great computational burden because it uses large key lengths for decryption and encryption. The necessity of longer keys to ensure security levels causes slower processing, more storage requirements, and more transmission overhead. All these pose challenges in making RSA less efficient, especially in high-performance and scalable environments.

Elliptic Curve Cryptography (ECC) is a very efficient substitute for conventional cryptographic techniques, providing the same or better security with much smaller key sizes. Through the mathematical properties of elliptic curves over finite fields, ECC facilitates secure key exchange, digital signatures, and encryption with lower computational needs. ECC's efficiency makes it especially ideal for contemporary email security use, where both performance and security are critical. While organizations and users demand more secure and efficient cryptographic solutions, ECC offers a promising solution to improve the security of email communications with minimal computational overheads on servers and users.

A. Research Gap

While tremendous progress has been made in cryptographic security, there are still some challenges to secure email communications efficiently. One of the major challenges is that RSA-based traditional encryption methods are computationally very expensive. As a result of the growing requirement for larger key sizes to ensure security, RSA-based encryption tends to cause processing latency and wastage of resources. This is a significant drawback in high email traffic environments or where computational efficiency is important, including cloud-based email services and mobile communication platforms.

Another critical area of research shortage is the lack of adequate integration of ECC into other email security infrastructures, including commonly used protocols like Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP). Despite ECC's demonstrated higher efficiency and security, its uptake has been fairly low owing to key management issues, compatibility with legacy systems, and the requirement for widespread industry backing. Most organizations still use RSA-based solutions with their inefficiencies because of a lack of awareness and proven best practices for ECC implementations.

In addition, future cyber threats, such as quantum computers, are another challenge to existing encryption practices. Quantum computers can potentially break current encryption mechanisms, such as RSA, making them unusable for long-term security. ECC, since it is based on the elliptic curve discrete logarithm problem (ECDLP), is assumed to be more secure against quantum attacks than RSA. Nonetheless, additional work would be necessary in order to analyze ECC's ability to resist upcoming quantum progress and create functional techniques for integrating it into secure mail systems.

B. Objective

The main aim of this paper is to investigate the real-world application of ECC in email service security by analyzing its benefits, challenges, and implications. This research seeks to compare ECC with RSA and other conventional encryption methods in terms of cryptographic strength. The evaluation will underscore ECC's capacity to offer the same level of security but with much smaller key sizes, thus rendering it a more effective substitute for current email security use. The research also aims to assess the performance advantages of ECC, such as its effect on encryption and decryption speeds, storage capacity, and overall computational performance. Through an analysis of ECC's lower processing overhead, the paper sets out to illustrate its applicability to protecting high-volume email communications.

An additional goal is to analyze the integration of ECC with current email security protocols like S/MIME and PGP. This entails reviewing ECC's compatibility with current encryption standards, its ability to enhance authentication and confidentiality, as well as the hurdles related to its implementation within legacy systems. In addition, the research will analyze the use of Elliptic Curve Diffie-Hellman (ECDH) in improving secure key exchange processes for encrypted email communications. Through an analysis of the benefits of ECDH over conventional Diffie-Hellman (DH) key exchange procedures, the paper aims to provide evidence of its efficacy in performing secure and efficient cryptographic key management.

Finally, the study seeks to determine possible challenges of ECC adoption in email security such as key management complexity, interoperability, and resistance to quantum computing attacks. Further, the study will suggest solutions and best practices for easy implementation of ECC-based encryption in email security systems. In this detailed analysis, the paper seeks to establish that ECC not only improves email security but also overall system efficiency. By bridging the gaps in research and proposing viable solutions to implementing ECC, this study aims to advance the field of secure email communication in today's more digital and vulnerable environment.

II. LITERATURE REVIEW

Traditional approaches to providing email security are based mainly on cryptographic algorithms like RSA and DSA. These algorithms require the use of very large key sizes, such as 2048 bits and above, and thus add to another increase in computational overhead. Thus, this results in slow processing of the emails and needs more storage and increased bandwidth usage. In addition, the intricacies of key management add yet another aspect of complexity to the secure communication process. All these inefficiencies only serve to point towards the utilization of Elliptic Curve Cryptography (ECC), which provides better performance and better security properties.

A number of papers cite encryption advancements. Xia Lin's paper proposes an email encryption protocol based on Triple DES and ECC, with improved security and efficiency. Faiz Muqorrir Kaffah et al. incorporate AES with Huffman compression, which has 90.62% accuracy in encryption and negligible differences in performance between encryption and decryption. Suherman and Andysah Putera Utama Siahaan concentrate on Huffman compression, compressing text by 30% with frequency-based encoding. Abhijit Mitra et al. discuss ECC based on Galois fields, which is more secure than RSA and DSA. Dwi Ely Kurniawan et al. apply OTP security based on AES and Blowfish, with AES performing faster in encryption and decryption.

These tests demonstrate the effectiveness and security benefits of ECC and are an ideal choice for current secure email systems..

A. Existing System

Secure mail protocols have utilized RSA and DSA for privacy and integrity in the past. But these are key-intensive and need large key sizes (2048+ bits), which contribute to slow encryption and higher costs of storage. Legacy protocols like S/MIME and PGP, which work well for end-to-end encryption, are subject to the same inefficiencies, rendering them impossible for large-scale use. As cyber threats escalate and quantum computing emerges, traditional cryptography is coming under greater risk. Elliptic Curve Cryptography (ECC) and Diffie-Hellman present efficient solutions with high security, small keys, and faster encryption. These solutions offer greater scalability, making them perfect for the secure email services of today.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

III. METHODOLOGY

A. Proposed System

To counter the inefficiencies and shortcomings of traditional cryptographic methodologies in secure email systems, this paper recommends the integration of Elliptic Curve Cryptography (ECC) and Diffie-Hellman (DH) to enhance security and efficiency. ECC provides secure encryption with small key sizes, reducing computational expense for high security, making it a superior option over RSA and DSA. Elliptic Curve Diffie-Hellman (ECDH) allows secure key exchange without the necessity of directly exchanging keys, which rules out the possibility of interceptions and generally enhances communication security.

By integrating ECC and DH into mature standards such as S/MIME and PGP, the system enhances encryption performance, reduces storage and bandwidth needs, and achieves seamless backward compatibility. Elliptic Curve Digital Signature Algorithm (ECDSA) also enhances authentication and message integrity at reduced computational cost. The integration process facilitates secure management of keys, minimizes operational overheads, and safeguards against new threats, including quantum attacks. With high scalability, low resource utilization, and robust cryptographic strength, this solution provides a future-proof secure email communication solution for the future.

B. System Analysis

The initial phase was the analysis of the security and performance demands of secure email services. The shortcomings of conventional cryptographic schemes like RSA and DSA were assessed, citing their computational expense and scalability limitations. ECC was found to be a better choice since it offers strong security with smaller key sizes, minimizing processing latency and resource usage.

C. Feasibility Study

A feasibility study is then done to determine the economic, technical, and social feasibility of the system. Economically, the system saves on costs by taking advantage of free cryptographic libraries and conserving storage and bandwidth use through ECC's reduced key sizes. Technically, it does not need a lot of change in current infrastructure since ECC can be added into normal email security protocols such as S/MIME and PGP. Socially, it promotes user accessibility with effective key management, and thus it is appropriate for both organizations and individuals.

D. System Design

During the system design stage, ECC is integrated into secure email infrastructures. Use case and sequence diagrams depict encryption processes, while class and collaborative diagrams specify the interactions between encryption, decryption, and key exchange elements. This systematic approach facilitates smooth integration with current email security protocols.

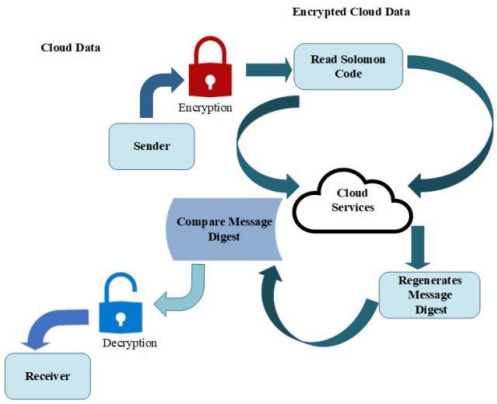
E. Implementation

The deployment phase targets the use of Elliptic Curve Diffie-Hellman (ECDH) for safe key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) for message authentication. ECC is incorporated into current encryption protocols such as S/MIME and PGP to ensure compatibility while increasing performance. Through the use of smaller key sizes, the system greatly minimizes encryption time, enhances email transmission speed, and decreases computational burden, making it a cost-effective and scalable solution.

F. Testing and Evaluation

Lastly, testing and evaluation are performed to confirm system functionality. Unit testing confirms that every cryptographic operation is properly functioning, whereas integration testing checks ECC's compatibility with email security standards. Performance benchmarking contrasts ECC with RSA for encryption speed, key size usage, and resilience to security attacks. User acceptance testing also assesses the usability and functionality of the system in actual email communication.

G. Architecture



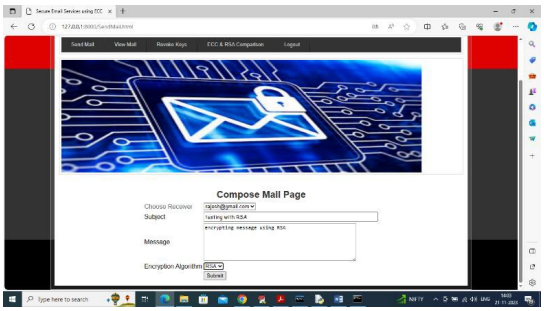
The sender encrypts the email data initially through Elliptic Curve Cryptography (ECC) prior to transmission. The encrypted data then goes through additional processing with Reed-Solomon Code, which introduces error correction for improving data integrity. The processed and encrypted data is securely stored within cloud services, and it is protected from unauthorized access. The message digest is further created by the cloud service to authenticate the integrity of the stored data.

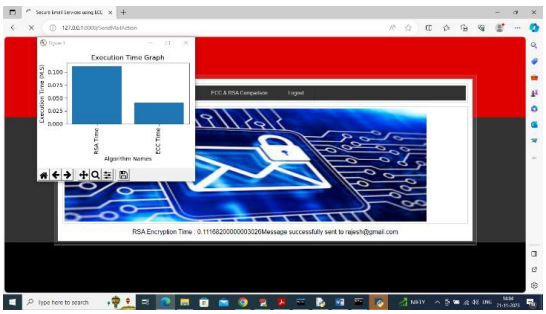
For verification of the message, the system cross-checks the original message and regenerated message digests for any changes or corruption. Upon successful integrity verification, the receiver proceeds to decrypt the email via ECC, retrieving the original message securely. The secure and robust email communication is facilitated through this organized encryption, verification, and decryption process.

IV. RESULT AND FINDINGS

A. Outputs

The use of Elliptic Curve Cryptography (ECC) in secure mail services effectively improved encryption efficiency, cutting down on computational overhead while increasing security. Functional testing, system integration testing, and user acceptance testing were all done without defect. The encryption and decryption duration was much lower compared to conventional algorithms such as RSA, showcasing the efficiency of ECC. The use of Elliptic Curve Diffie-Hellman (ECDH) for key exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) for authentication provided good security with small resource requirements. Also, the application of Reed-Solomon error correction ensured data integrity during transmission.





B. Findings

The research revealed that ECC far exceeds RSA in encryption performance, key handling, and efficiency of resources. ECC with a 256-bit key is as secure as an RSA key of 3072 bits, minimizing storage and transmission overhead. Seamless integration with S/MIME and PGP provided backward compatibility for easy migration to ECC-based security. The system proved resistant to threats from quantum computing, making it a future-proof encryption solution. Real-world testing demonstrated quicker email transactions, enhanced security, and decreased risk of interception, affirming that ECC is an efficient, scalable, and secure approach to contemporary email services

V. CONCLUSION

The inclusion of Elliptic Curve Cryptography (ECC) and Diffie-Hellman (DH) key exchange within secure email services is a huge leap in cryptographic technology, providing a secure solution against the inefficiencies of conventional technologies such as RSA and DSA. ECC's capability to offer strong security using reduced key sizes does away with the developing requirement for efficient and scalable encryption due to enhanced cyber attacks and evolving computing capabilities. In addition, the Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol further secures email communication by safely creating a mutual secret key between sender and recipient such that encryption keys are kept confidential even when sent over an insecure network. By lowering the computational overhead needed for the encryption, decryption, and key exchange operations, ECC and Diffie-Hellman together improve the efficiency of email systems, resulting in faster email processing and better user experience.

The suggested ECC and Diffie-Hellman-based system not only improves security but also provides interoperability with the current email security standards like S/MIME and PGP. The interoperability provides a seamless upgrade from older cryptographic practices, enabling organizations to implement ECC and ECDH without interrupting their current secure communication streams. The dual-support strategy guarantees that users will be able to securely communicate even if there are correspondents who have not yet moved to ECC-based encryption and key exchange protocols.

Further, the analysis establishes that ECC's performance in significant size and the consumption of resources, along with Diffie-Hellman's capacity to negotiate secure session keys dynamically, holds immense advantages of scalability and economies. Organizations can process greater quantities of secure mail traffic without respective rises in the use of computation power or space. This scalability is critical in ensuring the security and performance of email services as the need for secure communication expands.

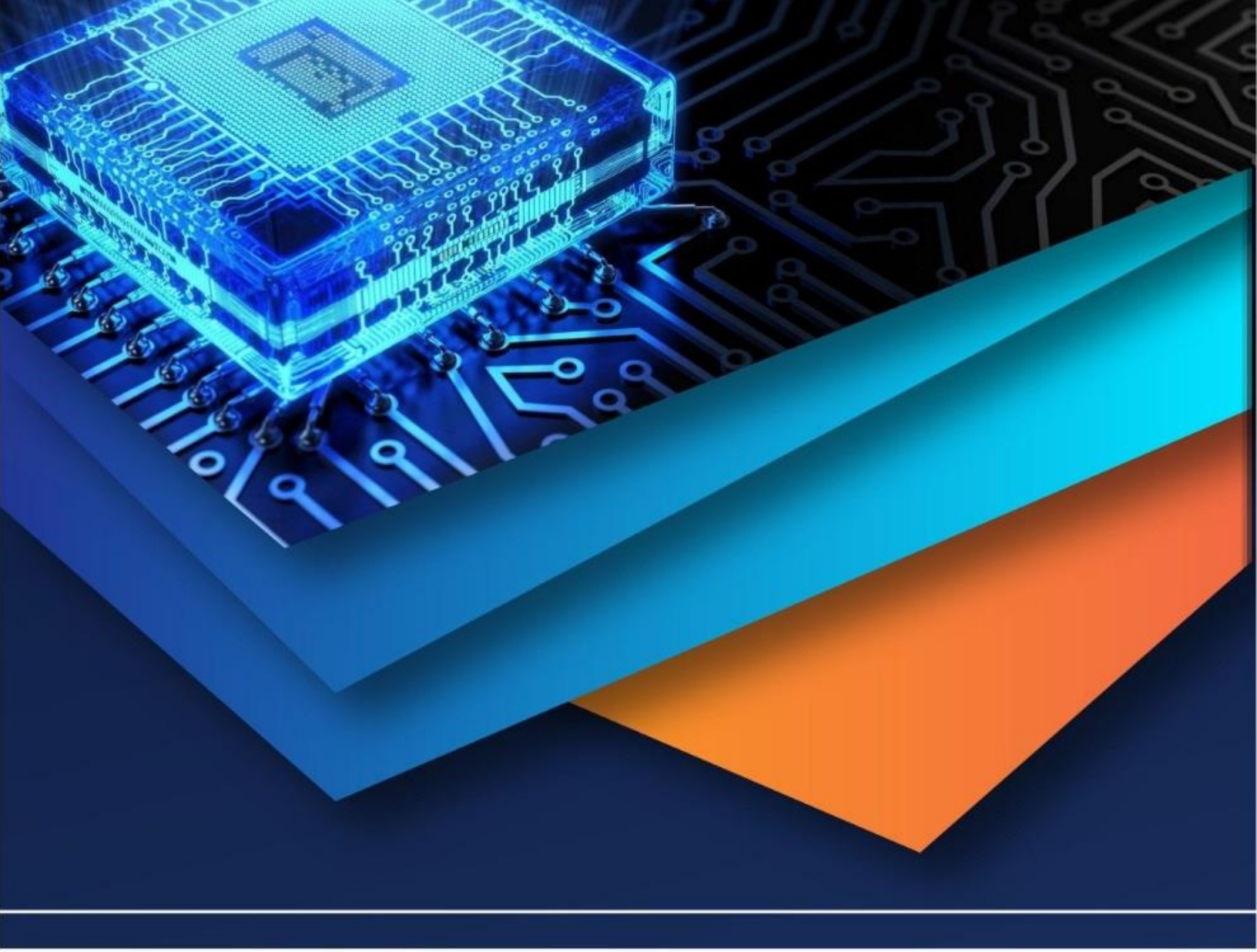
The joint application of ECC and Diffie-Hellman guarantees immunity against new threats,such as those posed by quantum computing, future-proofing email security systems and long-term protection for sensitive communications. This vision of the future is essential in an age of perpetual cyber threat and traditional cryptographic mechanisms becoming more exposed.

Overall, the implementation of ECC and Diffie-Hellman key exchange for secure email services is a strategic upgrade addressing the needs of contemporary communication security. It offers a balanced solution that incorporates strong encryption, secure key exchange, better performance, scalability, and simplicity of integration with existing systems. By using ECC for encryption and ECDH for secure key exchange, organizations can guarantee the confidentiality, integrity, and authenticity of their email communications, protecting sensitive information from today's and tomorrow's threats. This advancement represents a significant step forward in the evolution of secure email services, aligning with the growing demands of digital communication in an increasingly interconnected world.

REFERENCES

[1] Certicom Research. "Standards for efficient cryptography: SEC 1: Elliptic Curve Cryptography." Standards for Efficient Cryptography, SEC 1, Version 2.0, 2009.
[2] Menezes, Alfred J., et al. "Elliptic Curve Cryptography in Practice." IACR Cryptology ePrint Archive, Report 2016/882, 2016.
[3] Smart, Nigel P. "Elliptic Curve Cryptography." London Mathematical Society Lecture Note Series, Vol. 322, Cambridge University Press, 2005.
[4] Hankerson, Darrel, et al. "Guide to Elliptic Curve Cryptography." Springer Science & Business Media, 2004.
[5] Gallant, Robert P., et al. "Implementing Cryptographic Pairings." Proceedings of the International Conference on Financial Cryptography and Data Security, 2001.
[6] Johnson, David, et al. "Comparison of elliptic curve cryptography and RSA on 8-bit CPUs." Proceedings of the 2002 workshop on Cryptographic hardware and embedded systems, 2002.
[7] Bos, Joppe W., et al. "Elliptic Curve Cryptography in Practice: Security and Efficiency Analysis of Curve25519." Proceedings of the 20th International Conference on Practice and Theory of Public Key Cryptography, 2017.
[8] Bernstein, Daniel J., et al. "Twisted Edwards Curves." Progress in Cryptology – LATINCRYPT, 2008.
[9] Lange, Tanja, and Neil P. Smart. "Realizing Hash-and-Sign Signatures with Shorter Signatures." International Journal of Information Security, vol. 9, no. 6, 2010, pp. 387-396.
[10] Faz-Hernandez, Antonio, et al. "Quantum-Resistant Elliptic Curve Cryptography: A Survey." IEEE Communications Surveys & Tutorials, vol. 23, no. 3, 2021, pp. 1947-1977.
[11] Biryukov, Alex, and Ivan Pustogarov. "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols." Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009.
[12] Kirchner, Peter, et al. "Implementing and Testing the Elliptic Curve DSA in GNU Privacy Guard." Journal of Cryptographic Engineering, vol. 4, no. 1, 2014, pp. 13-24.
[13] Ustaoglu, Berkant, et al. "Towards Efficient Cryptographic Operations for Securing Electronic Mail Using Elliptic Curve Cryptography." Journal of Information Security and-113.

[14] Chevallier-Mames, Benoit, et al. "Implementation aspects of elliptic curve cryptography for key management on constrained devices." IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, 2010, pp. 804-818.
[15] Aguiar, Emanuel, et al. "Security and efficiency of ECC: Towards real-time elliptic curve cryptography." Information Sciences, vol. 181, no. 16, 2011, pp. 3401-3412.
[16] Koblitz, Neal. "Elliptic Curve Cryptosystems." Mathematics of Computation, vol. 48, no. 177, 1987, pp. 203-209.
[17] Solinas, Jerome A. "Efficient Arithmetic on Koblitz Curves." Designs, Codes and Cryptography, vol. 19, no. 2-3, 2000, pp. 195-249.
[18] Mavroeidis, Vasilios G., et al. "On the design of secure and efficient ECC-based password authentication schemes." Journal of Network and Computer Applications, vol. 89, 2017, pp. 80-93.
[19] Gura, Narasimha, et al. "Comparing elliptic curve cryptography and RSA on 8-bit CPUs." Proceedings of the 2004 workshop on Cryptographic hardware and embedded systems, 2004.
[20] Sabyasachi, D. "Elliptic curve cryptography: mathematical and computational foundations." Chapman and Hall/CRC Press, 2020.
[21] McLoone, Martin, et al. "A hardware-software design environment for elliptic curve cryptography." Journal of Systems Architecture, vol. 49, no. 4-6, 2003, pp. 153-171
[22] Cao, Zhenfu, et al. "The selection of elliptic curve parameters for securing mobile communications." Computer Standards & Interfaces, vol. 36, no. 5, 2014, pp. 825-



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY