Bulletin of Electrical Engineering and Informatics
Vol. 14, No. 3, June 2025, pp. 2300~2308
ISSN: 2302-9285, DOI: 10.11591/eei.v14i3.8587

Elliptic curve cryptography based light weight technique for information security

Marwan Alshar'e[1], Sharf Alzu'bi[2], Ahed Al-Haraizah[3], Hamzah Ali Alkhazaleh[4], Malik Jawarneh[5], Mohammad Rustom Al Nasar[6]
[1]Faculty of Computing and Information Technology, Sohar University, Sohar, Oman
[2]Department of Information Technology, College of Engineering and Technology, Royal University of Women, West Riffa, Bahrain
[3]Faculty of Finance and Business, The World Islamic Sciences and Education University, Amman, Jordan
[4]College of Engineering and Information Technology, University of Dubai, Academic City, Dubai, United Arab Emirates
[5]College of Information Technology, Amman Arab University, Amman, Jordan
[6]Department of Information Technology Management, American University in the Emirates, Academic City, Dubai, United Arab Emirates

Article Info

Article history:

Received Apr 13, 2024
Revised Jan 2, 2025
Accepted Mar 25, 2025

Keywords:

Digital signature
Elliptic curve Diffie-Hellman
Elliptic curve elgamal cryptosystem
Light weight cryptography
Small key size

ABSTRACT

Recent breakthroughs in cryptographic technology are being thoroughly scrutinized due to their emphasis on innovative approaches to design, implementation, and attacks. Lightweight cryptography (LWC) is a technological advancement that utilizes a cryptographic algorithm capable of being adjusted to function effectively in various constrained environments. This study provides an in-depth analysis of elliptic curve cryptography (ECC), which is a type of asymmetric cryptographic method known as LWC. This cryptographic approach operates over elliptic curves and has two applications: key exchange and digital signature authentication. Next, we will implement asymmetric cryptographic algorithms and evaluate their efficiency. Elliptic curve elgamal algorithms are implemented for encryption and decryption of data. Elliptic curve Diffie-Hellman key exchange is used for sharing keys. Experimental results have shown that ECC needs small size keys to provide similar security. ECC takes less time in key generation, encryption and decryption of plain text. Time taken by ECC to generate a 2,048 bit long key is 1,653 milliseconds in comparison to 4,258 millisecond taken by Rivest-Shamir-Adleman (RSA) technique.

Corresponding Author:

Marwan Alshar'e
Faculty of Computing and Information Technology, Sohar University
Sohar, Oman
Email: mshare@su.edu.om

1. INTRODUCTION

Technological and wireless communication has been firmly embedded in today's surroundings. In light of the fact that the majority of online transactions and financial transfers may now be conducted with or without the use of a credit card, it is crucial for organizations to possess a means of communication and information sharing, regardless of the sensitivity of the content. The lack of sufficient security controls in this context makes it simple to compromise the security of network transactions or their applications. This category encompasses efforts implemented to mitigate the consequences of such incidents [1].

The shared data transmission contains precise information to ensure easy comprehension by the receiver [2]. Information, furthermore, is simply data that is generated as a consequence of actions and their results [3]. The receiver can easily comprehend both the acts and their outcomes. Any physical or non-physical manifestation can be used for the safe conveyance of data [4]. The objective of information and communication security is to achieve a well-balanced level of protection by guaranteeing the confidentiality, integrity, and availability of data during online transactions and transmissions [5].

Data security refers to the implementation of appropriate measures to prevent unwanted access and misuse of data. The primary objective is to safeguard data communications from both interference and hostile individuals. The integrity of the information must be preserved during the implementation of security procedures. Data analysis conducted on internet-transmitted data adheres to particular protocols, hence enhancing the security of the transmitted data. Information theft occurs when data is duplicated or captured during its transmission or communication to its intended recipient. Administrators and researchers employ information security techniques to thwart data theft [6].

In public-key encryption, the sender encrypts their data using the recipient's public key when interacting with them. By following a properly defined algorithm for key generation, it is possible to acquire the private key that corresponds to this public key. By utilizing the generated private key, the sender is able to engage in confidential communication with their selected recipient. The recipient has the option to encrypt the data using the private key of the sender. Only individuals possessing the correct private key will be recognized as recipients, and unauthorized users will be unable to decipher the material. The confidentiality of the supplied data will be effectively safeguarded in this manner.

Elliptic curves serve as the fundamental framework for elliptic curve cryptography (ECC), a cryptographic method that operates within limited domains. ECC allows for the use of smaller keys for encryption and decryption compared to prior methods of public key cryptography [7]. ECC is based on Galois fields and provides an equivalent level of security. The basis of public-key cryptography is rooted in the inherent characteristics of mathematical functions. Previously, the process of decomposing the multiplier value of a big number into two prime numbers, each with many factors, was seen as challenging due to specific assumptions about the public-key system. According to a subsequent fundamental assumption, it will be challenging, if not unattainable, to compute the discrete logarithm of the random point on the elliptic curve. The term used to refer to this is "elliptic curve discrete logarithm problem" [8]. In 1976, Whitfield Diffie and Martin Hellman introduced their asymmetric key cryptosystem. Ralph Merkle's public key distribution technique also influenced this system around the same year. Diffie-Hellman published a method for public-key agreement. The mechanism used to rapidly exchange keys is known as the Diffie-Hellman key exchange algorithm. Initially, without employing previously revealed confidential information, the publicly shared secret key was activated through an allowed means of communication [9].

The ECC algorithm greatly enhances security in comparison to Rivest-Shamir-Adleman (RSA). In order to enhance the arithmetic operations in mathematics using finite fields, ECC enables all users to communicate using a finite field Fp [10]. Therefore, to improve mathematical functions, it will be essential to utilize hardware that is identical. To provide consumers with additional assurance, they can choose from a range of elliptical curves or switch between them as desired [11].

Typically, when data is transmitted over the Internet, most assaults only reveal one key at a time. This method is also employed for a range of elliptical curve attacks. In this scenario, the likelihood of compromising information security is higher due to all users employing the same elliptical curve and point for data encryption. The time needed to find the private key K of the same elliptic curve is also around K times longer. These data indicate that ECC cryptographic security provides better protection compared to other cryptographic systems like RSA and digital signature algorithm (DSA) [12].

2. LITERATURE SURVEY

Lara-Nino *et al.* [13] conducts a survey to determine the factors that contribute to the practicality, lightness, and suitability of an ECC-based solution in constrained applications. In this study, the authors present a method for creating elliptic curve lightweight cryptography (ECLC) systems. They assert that they have introduced the concept and specifications for ECLC for the first time in their research. We also discuss the unresolved inquiries that these systems must address. Moreover, this technology introduces multiple hazards that could jeopardize ECLC systems, as well as the potential it offers for the development of novel internet of things (IoT) systems. The authors argue that ECLC fulfills the requirement for effective and strong security components that impose minimal device burdens, a crucial aspect for developing upcoming networked systems [13].

Park *et al.* [14] analyzed the learning with error (LWE) based key encapsulation mechanism (KEM) algorithms from the National Institute of Standards and Technology (NIST) post-quantum cryptography (PQC) round 3 candidates. The focus of their study was on polynomial multiplication using RSA/ECC coprocessors. The Exynos2100 smart secure platform (SSP), a commercial mobile system-on-chip (SoC), incorporates RSA/ECC coprocessors that include all established techniques for polynomial multiplication, as developed by the developers. Furthermore, they have not only presented and analyzed the outcomes of simulations for various outdated hardware accelerators, but they have also furnished guidelines for achieving the most efficient implementation. The article provides instructions on implementing the PQC candidate process utilizing existing outdated hardware and discusses the limitations that must be taken into account. The authors establish the superiority of older RSA/ECC hardware accelerators by comparing the results of the polynomial multiplication method with those obtained using the number theoretic transform (NTT) [14].

Harkanson and Kim [15] provide a predicted outline of the applications of ECC. The authors explore the mathematical structure and operations of elliptic curves to understand their utility in cryptography. Subsequently, the authors analyze the level of security and efficiency exhibited by ECC in contrast to other widely recognized cryptographic techniques utilized for digital signatures and key exchange. We focus on the traditional and practical applications of ECC, including DNS security extensions (DNSSEC) and key exchange for web browsers. In addition, we have examined the diverse mobile applications of ECC, such as cellular phones and the IoT. We examine several contemporary applications of curves, such as E-health, smart grid, iris recognition, and radio frequency identification. The study finishes by briefly discussing the application of ECC in the context of post-quantum encryption [15].

Wu *et al.* [16] propose a key agreement system for an ECC-enabled smart grid that is both efficient and verifiably secure. The authors employ a technique for smart grid authentication and key establishment between service providers (SPs) and smart meters (SMs). A formal proof based on authenticated key agreement is conducted due to the extremely low likelihood of success for the attacker. The suggested solution surpasses other competing schemes in terms of performance and security characteristics. By employing NS-3 for the simulation analysis, we have determined that the proposed work is both highly effective in communication and highly practical in its usefulness [16].

Velliangiri *et al.* [17] propose a lightweight, efficient, and adaptable authentication technique as part of an access control strategy for secure data transfer in-vehicle networks. The proposed procedure includes the combination of concatenation, XOR, simple operations, hash functions, and other like characteristics. This study further demonstrates the resilience of IoT networks against diverse security threats and confirms the implementation of an authentication technique. The empirical results indicate that the compute process requires a duration of 7.96 seconds, the communication process involves the transmission of 834 bits, and the resource consumption is at a level of 11%. The mean duration for verification is 7 milliseconds. Based on their practical analysis, the authors deduce that their proposed approach surpasses the current cutting-edge methods in terms of efficiency, by reducing expenses related to processing, communication, verification, and resource utilization. Through conducting security research and performance evaluations, we successfully achieved our objective of implementing a streamlined and efficient cryptographic solution for Industry 4.0, utilizing ECC.

Authors propose utilizing fuzzy logic to generate random numbers as a novel approach for authenticating and encrypting ECC. The suggested key generation procedure is evaluated using discrete Fourier transform (DFT) tests, run tests, frequency testing with and without monoblocks, run tests, and advanced DFT tests. The current implementation of ECC utilizing shift registers is demonstrated to have lower efficiency in terms of performance. Attack algorithms such as Pollard's ρ and Baby-step Giant-step algorithms are employed for vulnerability assessment. The suggested solution relies heavily on generating code using fuzzy logic, which has significantly enhanced the error correction code (ECC) for authentication and encryption issues in the IoT. Studies indicate that conventional ECCs relying on pseudorandom integers are more vulnerable to breaches compared to their fuzzy logic counterparts [17].

Chaudhry *et al.* [18] offer a privacy-preserving and lightweight authentication technique, called LAS-SG, for smart grid environments. The strategy utilizes ECC. As to the authors, the suggested technique is deemed secure when evaluated using the standard model. It successfully carries out an authentication round in a time span of 20,331 milliseconds, utilizing only 2 messages and transmitting 192 bytes of data. The research suggests that the LASGS, which has been proposed, is more effective in SG environments. LAS-SG facilitates the establishment of a secure connection between smart meters and NAN gateways by exchanging a session key. The proposed schemes not only meet the security requirements but also resist known attacks, so the verification is finished [18].

Authors propose the use of fog-based vehicle networks (FVNs) as a means to enhance communication and service in vehicle networks. Ensuring the confidentiality and integrity of the entire network infrastructure are crucial for the development of large-scale FVNs. The recommended existing methods are experiencing a rise in the costs related to communication and computing. The proposed security protocol utilizes self-certified public key cryptography to enable the authentication of online vehicle-to-fog node communication. This obviates the need for a trusted authority. Furthermore, the protocol utilizes ECC, which does not utilize bilinear pairing operation. Consequently, the certified batch of fog nodes is tasked with processing the data transmitted by the automobiles. The outcome is a reduced waiting period. In time-critical applications, the performance analysis demonstrates that reduced communication and financial resources are required [19]. Researchers also proposed an elliptic curve cryptosystem with the symmetric key for vietnamese text encryption and decryption. It was time efficient solution [20].

3. METHOD
3.1. Elliptic curve key pairs
The elliptic curve key pair is associated with a certain set of domain parameters D, which include q, FR, S, a, b, G, n, and h. A point PU is selected at random from the group generated by G and is utilized as the public key. There exists a corresponding private key [21]. The logarithm of G PU is equal to PR. Entity A, the key pair generator, requires absolute certainty over the accuracy of the domain parameters. Any conceivable entity that may use A's public key in the future must be capable of verifying the correlation between domain parameters and the key. Actually, this connection can be created using cryptographic techniques (such as when a certification authority provides a certificate confirming this relationship) or contextual considerations (such as when all entities use the same domain parameters) [22].

The described Algorithm 1 is a key generation algorithm for elliptic curve cryptography (ECC), which is a widely used asymmetric cryptographic algorithm. This algorithm starts with generating a public-private key pair using elliptic curve mathematics. Private key is denoted by PR and it is a securely generated random number. Public key in denoted by PU and it is a point on the elliptic curve, derived using the private key.

Algorithm 1. KeyGeneration( )
```
Input: Domain parameters
Output: Public key PU, private key PR
{
Select private key PR from random numbers between 1 to n-1

Calculate public key PU = PR.G
Return (PR, PU)
}
```

The essence of the elliptic curve discrete logarithm problem (ECDLP) is the task of determining a private key PR using only the corresponding public key PU. Hence, it is crucial to select the domain parameters D in a manner that renders the ECDLP extremely difficult to solve. Furthermore, it is imperative that the PR numbers are generated randomly, ensuring that the probability of selecting any specific value is sufficiently low. This is necessary to prevent adversaries from utilizing this information to their advantage by optimizing their search method.

3.2. Elliptic curve encryption scheme
The finite field Fp serves as the mathematical framework for performing all computations in an ElGamal encryption scheme that relies on an elliptic curve [23], [24]. The methods "EncECE" and "DecECE" refer to the encryption and decryption procedures for the elliptic curve, which are based on the basic ElGamal encryption approach, respectively [25].

ECC is a type of asymmetric encryption that uses ECC to securely encrypt and decrypt messages. It is widely used in secure communication protocols like TLS, SSL, and in blockchain technologies. The encryption and decryption Algorithm 2 for ECC are as follows:

Algorithm 2. EncECE( )
```
Input: plaintext PM, public key PU, Domain parameters
Output: Cipher text
{
Select I as a random number between 1 to n-1
Calculate C1= IG
Calculate C2= PM + IK
Return (C1, C2)
```

Algorithm DecECE( )
```
Input: Domain Parameters, private key PR, cipher text
Output: Plain Text
{
Calculate PM= C2 PR C1
Extract m from PM
Return (plaintext m)
}
```

3.3. Elliptic curve Diffie-Hellman scheme

Parabolic spiral key agreement systems, such as elliptic curve digital signature (ECDH), enable two parties to generate a mutually agreed secret key that may be used with private key Algorithms 3. Both parties exchange some publicly accessible information. These entities establish the shared secret by merging the publicly accessible information with their own private data. In order for ECDH to produce a shared secret, A and B must agree on the elliptic curve domain parameters by reaching an agreement. The key pair consists of a public key (G) and a private key (a randomly selected integer lower than n), which are used by both entities. The private key is linked to the elliptic curve domain parameters, while the public key is linked to the generator point.

Algorithm 3. ECDH private key()
```
Input: domain parameters
Output: private key
{
Sender selects a random number between 1 to n-1 as the private key. It is denoted by SR
Sender calculate public key as SP= SR.G
Receiver selects a random number between 1 to n-1 as the private key. It is denoted by RR
Receiver calculate public key as RP= RR.G
Sender calculate ssk= SR.RP
Receiver calculate ssk= RR.SP

Return ssk
}
```

4. RESULT ANALYSIS AND DISCUSSION

Algorithms are implemented on Core i5 Processor with 8 GB RAM. The input data used in the experimental work is as follows.

The input plain text is: ABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIAB CDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFG HIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCD EFGHIABCDEFGHIABCDEFGHIABCDEFGHIABCDEFGHI

Results are presented in Figures 1-4. Figure 1 presents comparison of sender key generation time. Figure 2 depicts comparison of receiver key generation time. Figure 3 shows comparison of encryption time. Figure 4 presents comparison of decryption time. Time taken by ECC to generate a 2,048 bit long key is 1,653 milliseconds in comparison to 4,258 millisecond taken by RSA technique.

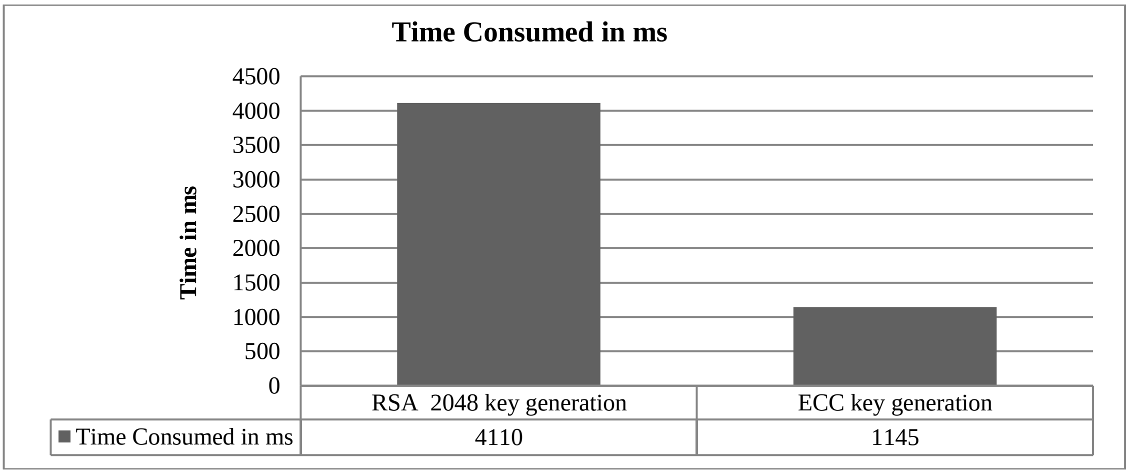

Figure 1. Comparison of sender key generation time

One must take into account the size-to-security ratio when comparing ECC and RSA encryption keys. The required key sizes for achieving equivalent security levels between RSA and ECC are shown in Table 1. Based on the information shown in the table, it is determined that RSA would need a key space of 1,024 bits, while ECC would require a key space of 160 bits, in order to satisfy the security criteria of the 80-bit advanced encryption standard (AES).

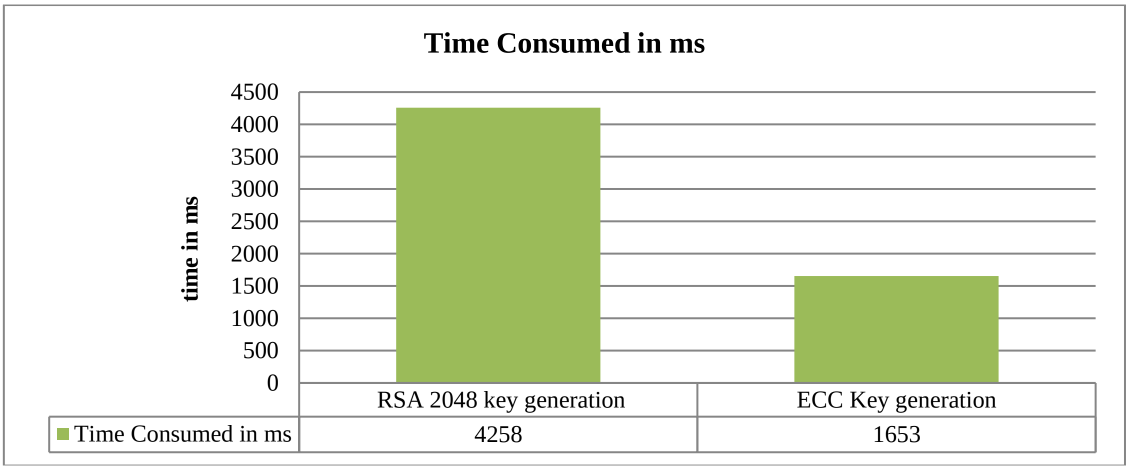

Figure 2. Comparison of receiver key generation time

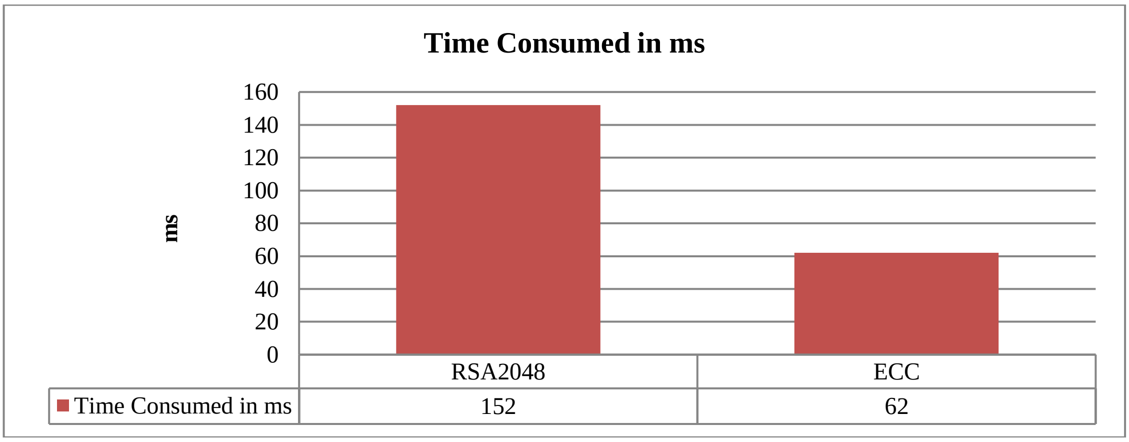

Figure 3. Comparison of encryption time

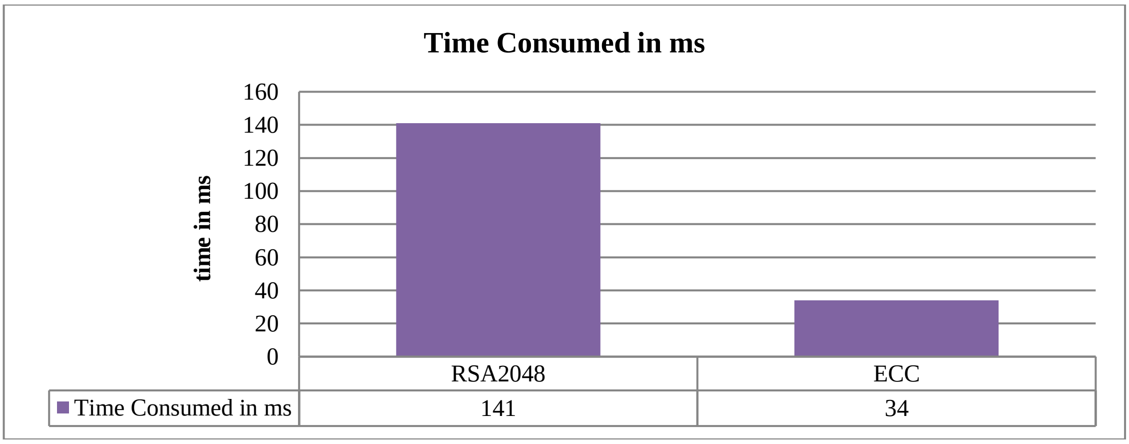

Figure 4. Comparison of decryption time

Table 1. Security level of RSA and ECC

RSA key size in bits	ECC key size in bits
1,024	160
2,048	224
3,072	256
7,680	384
15,360	521

ECC offers a level of security equivalent to AES but with a much lower key size compared to RSA, representing a substantial disparity. The relationship between ECC and RSA key sizes is not linear. Thus, it illustrates that increasing the size of an RSA key by a factor of two does not lead to a proportional rise in the size of an ECC key. The difference in efficiency between ECC's key generation and signature operations compared to RSA's is evident, since ECC requires less memory use. Unlike ECC, RSA's public and private keys may be represented as integers. In ECC, the private key is represented as an integer, while the public key is represented as a point on a curve. An ECC has many advantages over other encryption methods. It produces a smaller ciphertext, enables faster key generation, and allows for speedier signature production. The lightning-fast decryption and encryption times will go unnoticed by you. The ECC achieves reduced latency compared to the inverse by performing signature calculation in two stages.

5. CONCLUSION

Elliptic curves serve as the foundation for ECC, a cryptographic technology that operates inside specific domains. ECC enables the use of smaller keys for encryption and decoding than previous methods of public key cryptography. ECC is based on Galois fields and gives the same level of security. An extensive summary of the cryptographic algorithm's development, analysis, optimization, and security aspects is given in this work. An introduction to both lightweight and general cryptography is given by research work. We clarify the significance of ECC and offer a thorough explanation of the mathematical concepts underpinning the cryptographic technique. A comprehensive review of the literature covering a wide range of ECC topics was conducted in order to focus the investigation. We will then put asymmetric cryptographic methods into practice and assess their effectiveness. Elliptic curve elliptic curve methods are used for data encryption and decryption. Key sharing is done via elliptic curve Diffie-Hellman key exchange. According to experimental findings, ECC requires tiny size keys in order to offer comparable security. ECC is faster at generating keys, encrypting data, and decrypting plain text.

ACKNOWLEDGMENTS

We are deeply thankful to our institutions for providing the necessary resources and facilities that enabled the successful completion of this research.

FUNDING INFORMATION

No funding received for this research work.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Marwan Alshar’e	✓	✓	✓	✓	✓	✓		✓	✓				✓	
Sharf Alzu’bi		✓				✓		✓	✓	✓	✓	✓		
Ahed Al-Haraizah	✓		✓	✓	✓	✓		✓		✓			✓	
Hamzah Ali Alkhazaleh		✓	✓	✓		✓		✓	✓				✓	
Malik Jawarneh		✓				✓		✓	✓	✓	✓	✓		
Mohammad Rustom Al Nasar	✓	✓	✓	✓		✓	✓			✓	✓		✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review &**E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] G. Farid, N. F. Warraich, and S. Iftikhar, "Digital information security management policy in academic libraries: A systematic review (2010–2022)," *Journal of Information Science*, Apr. 2023, doi: 10.1177/01655515231160026.

[2] A. Raghuvanshi *et al.*, "Intrusion Detection Using Machine Learning for Risk Mitigation in IoT-Enabled Smart Irrigation in Smart Farming," *Journal of Food Quality*, pp. 1–8, Feb. 2022, doi: 10.1155/2022/3955514.

[3] M. Paricherla, M. Ritonga, S. R. Shinde, S. M. Chaudhari, R. Linur, and A. Raghuvanshi, "Machine learning techniques for accurate classification and detection of intrusions in computer network," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2340–2347, Aug. 2023, doi: 10.11591/eei.v12i4.4708.

[4] S. Chandel, W. Cao, Z. Sun, J. Yang, B. Zhang, and T. Y. Ni, "A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption," in *Lecture Notes in Networks and Systems*, vol. 70, 2020, pp. 988–1003, doi: 10.1007/978-3-030-12385-7_67.

[5] A. K. Shukla, A. Shukla, and R. Singh, "Neural networks based face recognition system for biometric security," *Indian Journal of Engineering*, vol. 20, no. 53, pp. 1–9, May 2023, doi: 10.54905/disssi/v20i53/e16ije1640.

[6] A. Kanade *et al.*, "Analysis of wireless network security in internet of things and its applications," *Indian Journal of Engineering*, vol. 21, no. 55, pp. 1–12, Apr. 2024, doi: 10.54905/disssi.v21i55.e1ije1675.

[7] K. E. Abdullah and N. H. M. Ali, "Security improvement in elliptic curve cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 5, pp. 122–131, 2018, doi: 10.14569/IJACSA.2018.090516.

[8] R. Balamurugan, V. Kamalakannan, G. D. Rahul, and S. Tamilselvan, "Enhancing security in text messages using matrix based mapping and ElGamal method in elliptic curve cryptography," in *Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014*, IEEE, Nov. 2014, pp. 103–106, doi: 10.1109/IC3I.2014.7019749.

[9] N. Dinarvand and H. Barati, "An efficient and secure RFID authentication protocol using elliptic curve cryptography," *Wireless Networks*, vol. 25, no. 1, pp. 415–428, Jan. 2019, doi: 10.1007/s11276-017-1565-3.

[10] T. J. Wong, L. F. Koo, F. H. Naning, A. F. N. Rasedee, M. M. Magiman, and M. H. A. Sathar, "A Cubic El-Gamal Encryption Scheme Based on Lucas Sequence and Elliptic Curve," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 11, pp. 3439–3447, Nov. 2021, doi: 10.37418/amsj.10.111.5.

[11] P. Perumal and S. Subha, "An analysis of a secure communication for healthcare system using wearable devices based on elliptic curve cryptography," *World Review of Science, Technology and Sustainable Development*, vol. 18, no. 1, pp. 51–58, 2022, doi: 10.1504/WRSTSD.2022.119327.

[12] M. Rashid, M. M. Hazzazi, S. Z. Khan, A. R. Alharbi, A. Sajid, and A. Aljaedi, "A novel low-area point multiplication architecture for elliptic-curve cryptography," *Electronics*, vol. 10, no. 21, pp. 1–16, Nov. 2021, doi: 10.3390/electronics10212698.

[13] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic Curve Lightweight Cryptography: A Survey," *IEEE Access*, vol. 6, pp. 72514–72550, 2018, doi: 10.1109/ACCESS.2018.2881444.

[14] J. Y. Park, Y. H. Moon, W. Il Lee, S. H. Kim, and K. Sakurai, "A Survey of Polynomial Multiplication with RSA-ECC Coprocessors and Implementations of NIST PQC Round3 KEM Algorithms in Exynos2100," *IEEE Access*, vol. 10, pp. 2546–2563, 2022, doi: 10.1109/ACCESS.2021.3138807.

[15] R. Harkanson and Y. Kim, "Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications," in *ACM International Conference Proceeding Series*, New York, NY, USA: ACM, Apr. 2017, pp. 1–7, doi: 10.1145/3064814.3064818.

[16] F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah, and M. S. Obaidat, "A Lightweight and Provably Secure Key Agreement System for a Smart Grid with Elliptic Curve Cryptography," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2830–2838, Sep. 2019, doi: 10.1109/JSYST.2018.2876226.

[17] S. Velliangiri *et al.*, "An Efficient Lightweight Privacy-Preserving Mechanism for Industry 4.0 Based on Elliptic Curve Cryptography," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6494–6502, Sep. 2022, doi: 10.1109/TII.2021.3139609.

[18] S. A. Chaudhry, K. Yahya, S. Garg, G. Kaddoum, M. M. Hassan, and Y. Bin Zikria, "LAS-SG: An Elliptic Curve-Based Lightweight Authentication Scheme for Smart Grid Environments," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1504–1511, Feb. 2023, doi: 10.1109/TII.2022.3158663.

[19] X. Zhang, H. Zhong, J. Cui, I. Bolodurina, and L. Liu, "LBVP: A Lightweight Batch Verification Protocol for Fog-Based Vehicular Networks Using Self-Certified Public Key Cryptography," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5519–5533, May 2022, doi: 10.1109/TVT.2022.3157960.

[20] M. M. Trung, "Proposing an Elliptic Curve Cryptosystem with The Symmetric Key for Vietnamese Text Encryption and Decryption," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 4158–4162, Jun. 2020, doi: 10.30534/ijatcse/2020/246932020.

[21] A. O. David and O. Sulaimon, "Text Encryption with Improved Elliptic Curve Cryptography," *Journal of Advances in Mathematics and Computer Science*, pp. 32–41, Feb. 2023, doi: 10.9734/jamcs/2023/v38i31749.

[22] M. R. Khan *et al.*, "Analysis of Elliptic Curve Cryptography & RSA," *Journal of ICT Standardization*, vol. 11, no. 4, pp. 355–378, Nov. 2023, doi: 10.13052/jicts2245-800X.1142.

[23] G. N. M. Chowdary, M. P. S. R. Lakshmi, Y. Nylu, B. Deepthi, K. V. Prasad, and S. K. Kannaiah, "Elliptic Curve Cryptography for Network Security," in *6th International Conference on Inventive Computation Technologies, ICICT 2023 - Proceedings*, IEEE, Apr. 2023, pp. 1500–1503, doi: 10.1109/ICICT57646.2023.10134492.

[24] D. M. Ghadi, "Modification of Elgamal Elliptic Curve Cryptosystem Algorithm," in *Full Text Book of Minar Congress 6*, Rimar Academy, Oct. 2022, pp. 117–127, doi: 10.47832/minarcongress6-8.

[25] S. R. Kim and R. Kyung, "Study on Modified Public Key Cryptosystem Based on ElGamal and Cramer-Shoup Cryptosystems," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023*, IEEE, Mar. 2023, pp. 280–284, doi: 10.1109/CCWC57344.2023.10099297.

BIOGRAPHIES OF AUTHORS

Marwan Alshar'e is working in Faculty of Computing and Information Technology, Sohar University, Oman. Experienced Lecturer with a demonstrated history of working in the Higher Education industry. Skilled in lecturing, educational technology, training, research, and teaching. Strong education professional with a Doctor of Philosophy (Ph.D.) focused in Computer Science from National University of Malaysia. His research interests include network security, and deep learning. He can be contacted at email: mshare@su.edu.om.

Sharf Alzu'bi is working as a Faculty in the Department of Information Technology, College of Engineering and Technology, Royal University of Women, West Riffa, Bahrain. He is having a vast experience in teaching, research, and administration. He can be contacted at email: salzubi@ruw.edu.bh.

Ahed Al-Haraizah is working at Faculty of Finance and Business in The World Islamic Sciences and Education University. His research interests include machine learning, big data analytics and network security in finance technology. He can be contacted at email: ahed.alharaizah@wise.edu.jo.

Hamzah Ali Alkhazaleh College of Engineering and Information Technology, University of Dubai, Academic City, 14143, Dubai, UAE. He is an esteemed Assistant Professor within the College of Engineering and Information Technology at the University of Dubai. With over a decade of dedicated experience in academia and research, his stands as a distinguished scholar in the field. He earned his Ph.D. in Computer Science, specializing in Artificial Intelligence, from the prestigious National University of Malaysia in 2016. Prior to this, he obtained his M.Sc. in Information Technology from the Northern University of Malaysia and his B.Sc. in Management Information Systems from Al Albyte University, Jordan. He can be contacted at email: halkhazaleh@ud.ac.ae.

Malik Jawarneh College of Computer Science and Informatics, Amman Arab University, Jordan. He holds a Ph.D. from the National University of Malaysia (2016), a Master's in Information Technology from the Northern University of Malaysia (2008), and a Bachelor's in Computer Science from Al-Albayt University, Jordan (2006). He has a rich background in teaching, curriculum development, and research, with notable positions in Oman and Malaysia. He can be contacted at email: M.jawarneh@aau.edu.jo.

Mohammad Rustom Al Nasar is an esteemed Assistant Professor in the College of Engineering and Technology at the American University in the Emirates (AUE), Dubai, UAE. He holds a Ph.D. in Information Science from the National University of Malaysia (2017), an M.Sc. in IT from Northern University of Malaysia (2010), and a B.Sc. in MIS from Yarmouk University, Jordan (2008). His research interests include information retrieval (IR), artificial intelligence (AI), and personal information management (PIM). He can be contacted at email: mohammad.alnasar@aue.ae.