DOI: 10.24996/ijs.2024.65.1.31

ISSN: 0067-2904

ECC Based Encryption for the Secured Proactive Network Forensic Framework

A. Abirami[1,2*], S. Palanikumar[1]

[1]*Department of Information Technology, Noorul Islam Centre for Higher Education, Thuckalay, Kumaracoil-629180 Tamilnadu, India.*

[2] *Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Erode District, Tamil Nadu, India.*

Received: 29/3/2022 Accepted: 12/12/2022 Published: 30/1/2024

Abstract

Elliptic Curve Cryptography (ECC) is one of the public key cryptosystems that works based on the algebraic models in the form of elliptic curves. Usually, in ECC to implement the encryption, the encoding of data must be carried out on the elliptic curve, which seems to be a preprocessing step. Similarly, after the decryption a post processing step must be conducted for mapping or decoding the corresponding data to the exact point on the elliptic curves. The Memory Mapping (MM) and Koblitz Encoding (KE) are the commonly used encoding models. But both encoding models have drawbacks as the MM needs more memory for processing and the KE needs more computational resources. To overcome these issues the proposed enhanced Koblitz encoding technique is used with the ECC for enhancing the security. The proposed model was compared to the existing model and found to be more efficient in terms of security. The proposed model ensure confidentiality with the encryption technique, Integrity by using the Hashing method, and authenticity and non-repudiationwith the utilization of digital signature.

Keywords: Wireless sensor networks, Cyber Security, ECC, Koblitz encoding

1. Introduction

Security is one of the important strategies of information technology that prevents unauthorized access of organizational assets such as computers, networks, and data [1,2]. It is imposed for maintaining the integrity as well as confidentiality of all the sensitive information of the organization by blocking the access of hackers [3,4].

Cryptography is a method used to protect the communication as well as information with the use of codes. This allows only the expected people to access the information; that is to read or process it. Diffie and Hellman [5] described a protocol on public key cryptography in which two different persons may share the common secret information via insecure communication channel. This protocol provides security based on the problem's presumed intractability. Later during 1985, EIGamal [22] have overcome the above problem by proposing the method that exploits the intractability for constructing the signature as well as public-key encryption scheme. These protocols can be generalized to use it in an arbitrary finite cyclic group.

*Email: abi.lecturer@gmail.com

During 1985 Miller and Koblitz developed a public key cryptosystem called ECC[6].When compared with other cryptographic models, the ECC allows only the smaller keys for providing the equivalent security that is as provided by the other models. Usually, the elliptic curves are applied for pseudo random generators, key agreements, digital signatures, and other tasks for empowering security [7]. It can also be used for encryption by combining the symmetric encryption with the key agreements. Based on the elliptic curves they are also used in integer factorization algorithms that have their application in cryptography. As said above it is based on the certain mathematical problems using intractability property.

The security of ECC depends on the point multiplication that is computed and with the given product points it is incapable of computing multiplicand [8]. The elliptic curve size that is measured using the total number of integer pairs will determine the difficulty in the problem. The National Institute of Standards and Technology commonly known as NIST of United States have endorsed the ECC for their suite B set of recommended algorithms. The Elliptic Curve Diffi-Hellman is specifically endorsed for key exchange, and for digital signature Elliptic Curve Digital Signature Algorithm is endorsed.

Miller and Koblitz employed the ECC over different dataset to improve the efficiency by employing various encryption techniques. One of the important and attractive advantages over the cryptography is the use of ECC in a constrained environment where power consumption, storage bandwidth and processing power is a major concern. Hence the advantage of ECC includes small key size, lower memory usage and lower power consumption [9-11].

In ECC, the encoding for message data has to be carried out on the elliptic curve for implementing the encryption which seems to be a preprocessing step. Likewise, after the decryption, a post processing step must be carried out for mapping or decoding to the corresponding data to the exact point on the elliptic curve. The Memory Mapping (MM) and Koblitz Encoding (KE) are the commonly used encoding models. However, both encoding models have drawbacks. The MM needs more memory for processing and the KE needs more computational resources. To overcome these issues the proposed enhanced Koblitz encoding techniques is used with the ECC. It provides more security for transmitting the data over the Wireless Sensor Networks (WSN) with more integrity and confidentiality.

2. Related Works

Several related works are discussed below to highlight the need for the proposed work.
Menezes and Vanstone[12] developed an arithmetic processor for computing the elliptic curves in finite fields by implementing the model in hardware. They also analyzed the elliptic curve of the Elgamal cryptosy stem.

Chandravathi and Roja,[13] states that on comparing the ECC to the RSA model the security offerings are the same for smaller size and the processing overhead is reduced. They state that before encryption the plain text encoding must be done. Since the ECC encoding and decoding works with curve points, they used Koblitz method for representing the curve points.

Abirami [7] stated that the appropriate security schemes must be used for protecting the data communication in WSN. The major constrain for the wireless sensor network is energy consumption and memory usage. So, the model developed for enabling the security in the WSN should use minimal resource and lower energy. Thus, the ECC is one of the best models that use smaller size of keys when compared to the RSA algorithm. Also, the encoding of data in the ECC depends on the elliptic curve points; that is, the position or point where it lies in the curve.

ECC on resource-constrained microcontroller is focused on by Seo, etal.[14]. The proposed method combined Block-Comb method and Karatuba to speed up the multiplication performance. Optimized squaring method is utilized with 8-bit look up which yield a faster result as compared with the 4-bit look up table. The authors also found that there is a possibility of achieving high performance in terms of binary fields by the combination of methods with sub-quadratic complexity.

Omar [15] proposed an image encryption scheme based on the operations such as add, double and multiply that lies on the elliptic curve. He used both Koblitz encoding and the image encryption schemes for converting the plain image pixels into the elliptic curve coordinates.

Rehiman and Veni [16] state that the IoT (Internet of Things) enables the communication of sensors with the human in a virtual form using the Internet. They have suggested that the data must be compressed after encoding it into curve point without affecting the performance of the devices.

Seo [17] proposed two different versions of ECC model for enhancing the security by optimizing the performance of ECC. They used the polynomial multiplication based approach that works with multiplier encoding to reduce the number of registers used thereby allowing a larger size of data to be handled. By considering the 8-bit AVR ATmega microcontrollers model they have optimized the squaring and the reduction method. Thus, they provided two different highly fast and secure models for enhancing the security with the use of ECC.

Almajed, et al. [18] state that smart phones work with limited resources where the elliptic curve cryptography can be used which is most suitable. It reduces the consumption of energy and increases the efficiency of the devices by using the same length of small crypto keys. For this reason, it is used in different fields such as wireless sensor networks, Internet of Things and so on. They have provided the study on existing ECC techniques that are used in the mapping. They also suggested optimal mapping method with the padding size for securing the communications.

3. Proposed Algorithm

The main aim of the proposed algorithm is to provide high security of data transmission in WSN. The proposed algorithm provides confidentiality and integrity. The confidentiality is provided by ECC, and the integrity is provided by the hashing methods and the digital signature. As a part of confidentiality, it has been proved in [7] that ECC with Koblitz encoding enhance the security.

3.1 ECC with enhanced Koblitz's Encoding:

Let, EC be the Elliptical Curve over a finite point Fp , p be a prime number considered. a and $b$are the coefficients belongs to Fp. The ASCII value is considered as the x coordinate for the point,(x, y) on the EC. The corresponding y coordinate is obtained by substituting the value of $x$in the given equation

$$y^2 = x^3 + \ ax + b, \text{ where } x, y \ \in Fp \qquad (1)$$

For every$x$, $x \in \{0,1, \dots \dots (p-1)\}$, there need not necessarily exist a corresponding y value, which is the major problem of ECC. The Koblitz's encoding method brings the solution of the problem by extending the range of $x$values, which enables the encryption of entire message set in EC.

In Koblitz's method, for a message character, m, its x value is computed by:

$$x :(m * k) + 1 \tag{2}$$

where, k is an auxiliary base parameter. This computed x value is substituted in (1). For this x, if the corresponding y point exists, then the $(x, y)$is the encoding point of the message on the EC. Else, iteratively identify the value y by varying x from

$$x : [(m * k) + 2] \text{ to} x :[(m * k) + (k - 1)] \tag{3}$$

If there does not exist a y value, then value of k is incremented by 1. The highest value of $k$is concluded as the auxiliary parameter for the entire message set.

At the receiver side, the decryption of the received cipher point results a message point on the EC. By taking the x- coordinate of this message point, $(x - 1)/k$ is calculated. The quotient of this division operation corresponds to the ASCII value of the message, m. Decoding takes a smaller number of computations than encoding. From Table 1, it can be seen that the number of modulo operations required for the Koblitz's encoding is about 35 percent less than that of the ECC encryption [7].

3.2 Algorithm: ECC with enhanced Koblitz's encoding

Input: Data of various sizes

Output: Enhanced security of data transmission in WSN

Steps:

1. The ASCII values of all the messages are mapped with Elliptic Curve (EC).
2. The ASCII value is considered as the x coordinate for the point, (x, y) on the EC. The corresponding y coordinate is obtained by substituting the value of x in the given equation 1
3. The range of x values are extended, which enables the encryption of entire message set in EC.
4. Using Koblitz's method, for a message character m, its x value is computed by equation 2
5. The computed x value is substituted in the y coordinate. For this$x$, if the corresponding y point exists, then the $(x, y)$is the encoding point of the message on the EC.
6. Iteratively the value $y$is identified by varying x from as equation 3
7. Even after substituting $x = (3)$, if there does not exist a y value, then value of k is incremented by 1 and the highest value of k is concluded as the auxiliary parameter for the entire message set.
8. At the receiver side, the decryption of the received cipher point results a message point on the EC. By taking the x- coordinate of this message point, $(x - 1)/k$is calculated.
9. The quotient of this division operation corresponds to the ASCII value of the message$m$.

Table 1: Example

Message Digest (M)	Koblitz Encoded (P_M)	Cipher Point (P_C)	No of Modulo operations Koblitz's Encoding	No of Modulo Operations ECC Encryption
'T'	(840, 620)	(1185, 863)	625	1309
'@'	(642, 38)	(177, 764)	647	1331
'o'	(1110, 262)	(537, 978)	267	949
'm'	(1090, 450)	(226, 886)	455	1135

MD5 hashing function can be used in the proposed algorithm since it is one of the fastest hashing method. The lack of security in MD5 will be covered by the other modules of the proposed algorithm.[19,20]. The imput taken by the MD5 will be a variable length data thatis then converted in to a fixed sizeoutput of 128 Bits. Normal block size considered as an input is 512 bits, which are processed for 4 rounds with each round containinga porocessing of sub-blocks of 32-bits. The sub-blocks are generated from 512-bit block[21].

The encoded message from the Koblitz's encoder module is encrypted using ECC algorithm, then a hash is generated using MD5 and is digitally signed to make the message more secured. The reverse operation is done in the receiver side. The overall model is shown in Figure 1.

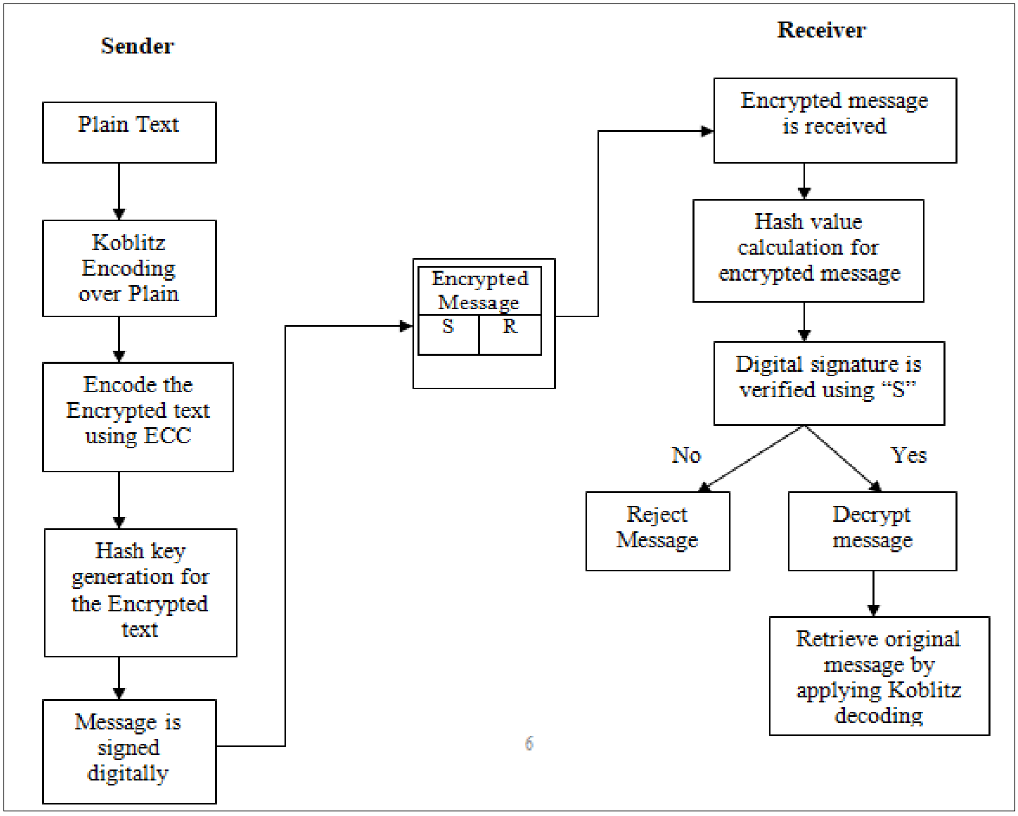
Sender
Receiver
Plain Text
Koblitz Encoding over Plain
Encode the Encrypted text using ECC
Hash key generation for the Encrypted text
Message is signed digitally
Encrypted Message
S
R
Encrypted message is received
Hash value calculation for encrypted message
Digital signature is verified using "S"
No
Yes
Reject Message
Decrypt message
Retrieve original message by applying Koblitz decoding

Figure 1: Model of the proposed work

4. Implementations and result discussion

The proposed ECC with Koblitz encoding method was implemented on the Ubuntu Linux operating system (64-bit) with an Intel Core i5-6200U CPU @ 2.40 GHz and 8.00 GB RAM. A Java Pairing-Based Cryptography library (JPBC) v.2.0.0 was used on this system to execute ECC algorithm and Koblitz encoding. Also, it helps the entities to communicate with each other.

Using Java libraries (java.security and java.security.spec),communication among the entities was measured. Further, the communication was secured via Secure Socket Layer. The parameters such as Koblitz encoding time, ECC key generation time, encryption time, Koblitz decoding time, file decryption time, and security overhead are measured to evaluate the performance of the proposed scheme in a proactive network forensic environment.

4.1 Computation time of Koblitz encoding and decoding

The time taken to perform Koblitz encoding on the input data blocks of various size was measured. The size of the data blocks were, 1024KB, 2048KB, 3072KB and 4096 KB(see Table 2).

As a general scenario, when the block size of the input message increases, the encryption and the decryption time will also increase. When compared to the encryption time, the time to decrypt the data block is very less.

Table 2: Computation time of Koblitz encoding and decoding

Size of the data block	Computation time to perform Koblitz encoding (Seconds)	Computation time to perform Koblitz decoding (Seconds)
1024	0.056	0.001
2048	0.089	0.002
3072	0.132	0.003
4096	0.156	0.004

4.2 Time taken to generate keys of proposed ECC method.

The time taken to generate the keys of the ECC algorithm was measured. The key generation time in this system was calculated for the set of 10 data block to 100 data block at the time interval of 10 units. Figure 2 represents the comparative analysis of the proposed model and the existing system in terms of time in millisecond.

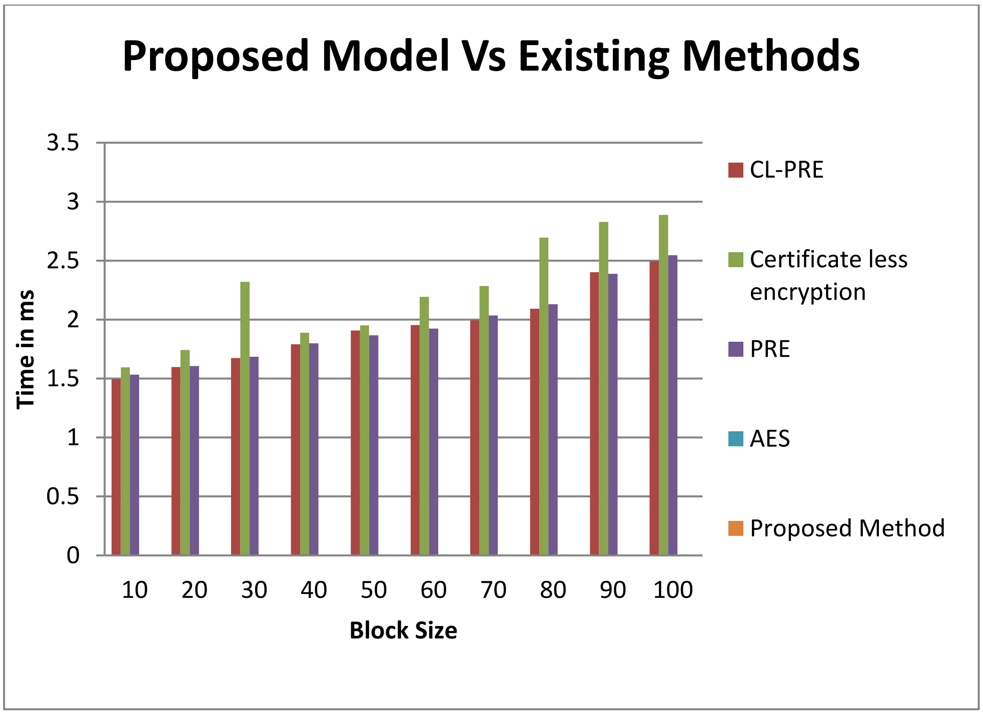

Figure 2: Comparison of proposed model with the existing models

Also, the time taken to generate keys for ECC algorithm was compared with existing scheme in the below Table 3.

Table 3: Comparison of proposed model with the existing models

Data Blocks	Methodologies (Time in Seconds)				
	CL-PRE (Xu et al. 2012)	Certificateless encryption (Seo et al. 2014)	PRE (Khan et al. 2014)	AES (Ali et al. 2017)	Proposed ECC
10	1.494	1.594	1.534	0.004	0.00212
20	1.598	1.741	1.606	0.00425	0.00235
30	1.673	2.321	1.684	0.00476	0.00286

40	1.791	1.888	1.799	0.005	0.00302
50	1.907	1.952	1.866	0.00512	0.00328
60	1.954	2.193	1.923	0.0055	0.0035
70	1.994	2.286	2.034	0.00598	0.00398
80	2.092	2.694	2.129	0.00632	0.00427
90	2.401	2.827	2.388	0.00664	0.00463
100	2.495	2.887	2.545	0.00697	0.00499

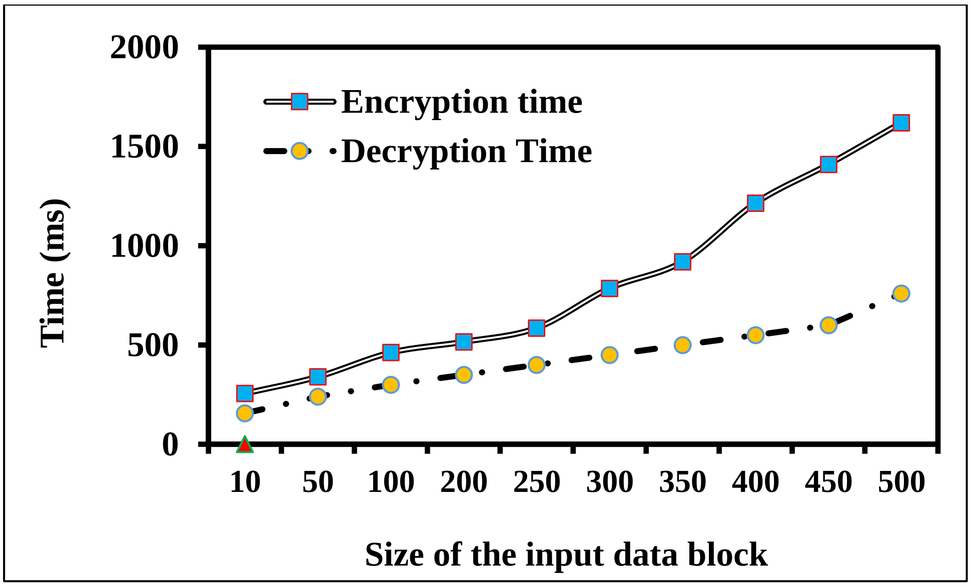

Figure 3: Time taken to encrypt and decrypt the data block using ECC algorithm

4.3 Time taken to encrypt and decrypt the data block using ECC algorithm

Figure 3 shows the time taken to encrypt and decrypt the data block using ECC. The time taken to encrypt the data block by the user was measured. The file encryption time, the file decryption time, and the key computation time were considered to estimate the computational overhead in the file upload and download process. Both encryption and decryption times were estimated with different file sizes from 0.1 MB to 500 MB.

5. Conclusion

In ECC, for implementing the encryption and decryption, the mapping is one of the important processes that must be done. Thus, the MM and KE are the commonly used encoding models. But both the encoding models have drawbacks as the MM needs more memory for processing and the KE needs more computational resources. To overcome these issues the proposed enhanced Koblitz encoding techniques is used with the ECC. It provides more security for transmitting the data over the WSN with more integrity and confidentiality.

The proposed model handles the memory and computation in an efficient way. In terms of security, the proposed system yields better security in terms of confidentiality, Integrity, authenticity, and non-repudiation. The confidentiality of the security goal is attained with the help of ECC encryption algorithm. The integrity of the data is provided with the help of hashing technique and the rest is taken care of by the digital signature.

References

[1] Z. Liu, H. Seo, J. Grosschadl, and H. Kim, "Efficient implementation of NIST-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 7, pp. 1385–1397, 2016.

[2] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in 2008 *International Conference on Information Processing in Sensor Networks* (ipsn 2008), 2008.

[3] L. Xu, X. Wu, and X. Zhang, "CL-PRE: A certificateless proxy re-encryption scheme for secure data sharing with public cloud," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, 2012.

[4] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, "An efficient certificateless encryption for secure data sharing in public clouds," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2107–2119, 2014.

[5] V. Roman'kov, "An improvement of the Diffie–Hellman noncommutative protocol," *Des. Codes Cryptogr.*, vol. 90, no. 1, pp. 139–153, 2022.

[6] K. T. R. Aljamaly and R. K. K. Ajeena, "The KR-elliptic curve public key cryptosystem," *J. Phys. Conf. Ser.*, vol. 1879, no. 3, p. 032046, 2021.

[7] S. Abirami, "A complete study on the security aspects of wireless sensor networks," in *International Conference on Innovative Computing and Communications, Singapore: Springer Singapore*, 2019, pp. 223–230.

[8] W. Easttom, "Elliptic Curve Cryptography," in *Modern Cryptography, Cham: Springer International Publishing*, 2021, pp. 245–256.

[9] Renita, EdnaElizabeth, and N. Asokan, "Implementation and performance analysis of elliptic curve cryptography using an efficient multiplier," *JSTS J. Semicond. Technol. Sci.*, vol. 22, no. 2, pp. 53–60, 2022.

[10] A. Aguglia, L. Giuzzi, and A. Sonnino, "Near-MDS codes from elliptic curves," *Des. Codes Cryptogr.*, 2021.

[11] 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.

[12] A. Menezes and S. Vanstone, "*The implementation of elliptic curve cryptosystems," in Advances in Cryptology — AUSCRYPT '90, Berlin/Heidelberg: Springer-Verlag*, 2006, pp. 1–13.

[13] K. E. Abdullah, & N. H. M. Ali, "A Secure Enhancement for Encoding/ Decoding data using Elliptic Curve Cryptography," *Iraqi J. Sci.*, vol. 59, no. 1A, 2018.

[14] H. Seo, Z. Liu, J. Choi, and H. Kim, "Karatsuba-Block-Comb technique for elliptic curve cryptography over binary fields: Karatsuba-Block-Comb technique for elliptic curve cryptography over binary fields," *Secur. Commun. Netw.*, vol. 8, no. 17, pp. 3121–3130, 2015.

[15] O. Reyad, "Text message encoding based on elliptic curve cryptography and a mapping methodology," *Inf. Sci. Lett.*, vol. 7, no. 1, pp. 7–11, 2018.

[16] C. Chauhan, M. K. Ramaiya, A. S. Rajawat, S. B. Goyal, C. Verma, and M. S. Raboaca, "Improving IoT security using elliptic curve integrated encryption scheme with primary structure-based block chain technology," *Procedia Comput. Sci.*, vol. 215, pp. 488–498, 2022.

[17] S. C. Seo and H. Seo, "Highly efficient implementation of NIST-compliant koblitz curve for 8-bit AVR-based sensor nodes," *IEEE Access*, vol. 6, pp. 67637–67652, 2018.

[18] H. Almajed, A. Almogren, and M. Alabdulkareem, "ITrust-A trustworthy and efficient mapping scheme in elliptic curve cryptography," *Sensors* (Basel), vol. 20, no. 23, p. 6841, 2020.

[19] M. C. Ah Kioon, Z. S. Wang, and S. Deb Das, "Security analysis of MD5 algorithm in password storage," *Appl. Mech. Mater.*, vol. 347–350, pp. 2706–2711, 2013.

[20] A. Sivaprasad, "Secured proactive network forensic framework," in 2017 *International Conference on Current Trends in Computer, Electrical, Electronics and Communication* (CTCEEC), 2017.

[21] K. Barik, K. Konar, A. Banerjee, S. Das, and A. Abirami, “An exploration of attack patterns and protection approaches using penetration testing,” in *Intelligent Data Communication Technologies and Internet of Things, Singapore: Springer Singapore*, 2022, pp. 491–503.

[22] Ç. K. Koç, F. Özdemir, and Z. Ödemiş Özger, “ElGamal Algorithm,” in *Partially Homomorphic Encryption, Cham: Springer International Publishing*, 2021, pp. 51–62.