Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 3, pp. 981–990
DOI : 10.47974/JDMSC-2257

A novel approach for Menezes-Vanstone elliptic curve cryptosystem

Pankaj Kakati *
Nayan Jyoti Bordoloi †
Department of Mathematics
Jagannath Barooah College
Jorhat 785001
Assam
India

Abstract

Cryptographic algorithms are widely used to safeguard data and information over the internet. One of the most efficient technique used for this purpose is the Elliptic Curve Cryptosystem (ECC) which recently gained a lot of interest due to its high performance. It is based upon the hardness of Elliptic Curve Discrete Logarithmic Problem (ECDLP) and till date there is no efficient algorithm that can solve the problem in polynomial time. In this paper an innovative algorithm for ``Menezes-Vanstone Elliptic curve cryptosystem (MVECC)'' have been proposed to make it more efficient. In comparison to the original algorithm, the proposed algorithm has no inverse operation making it faster and less computationally complex.

Subject Classification (2020): *11G07, 11T71.*

Keywords: *EC, ECC, ECDLP, MVECC.*

1. Introduction

Cryptography is the science of making communications incomprehensible to everyone except to the authorized parties. It is the only practical method available for safeguarding data sent across open communication networks like the internet, landlines, fax machines etc. The purpose of it is to protect communication between sender and receiver across an unsecured communication channel, such the internet. Encryption is the technique of changing data/information from a form that can be understood to an unintelligible form.

* *ORCID-ID:* **0000-0003-1786-4457**
† *ORCID-ID:* **0009-0000-7774-1155**

* *E-mail:* **pankaj07kakati@gmail.com (Corresponding Author)**
† *E-mail:* **nayanjyotibordoloi.jrt@gmail.com**

The process of changing the unintelligible data to the appropriate form is called decryption [1].

The idea of using elliptic curve into cryptography was introduced by Miller [2] and Koblitz [3] in mid 1980s. The classical cryptosystem like RSA is based on the Integer Factoring Problem (IFP) [4], while ECC is founded on ECDLP [5]. The key advantage advantage of ECC arises from its efficiency in tackling elliptic curve discrete logarithm problem that involves exponential time complexity. Hence elliptic curve cryptosystem can offer equal degree of security as the classical cryptosystem while using smaller key. For instance, to attain 256 bit of encryption an RSA-based encryption scheme requires a key size of 15360 bit, whereas an ECC-based encryption scheme only needs a 512 bit [6]. While implementing ECC, choosing the right kind of curve is essential. Dhanda, S. S. et al. [7] extensively examine the choice of curve models and specific curves, as well as the various attacks targeting ECC. Their paper also provides a detailed demonstration of implementing ECC using ElGamal encryption on the NIST P- 256 curve. Luhaib, Qasim Mohsin, and Ajeena, Ruma Kareem K. [8] introduced an enhanced version of the Elliptic Curve Discrete Logarithm (ECDL) protocol by incorporating the Elliptic Curve Matrix (ECM). From a security perspective, this proposed protocol appears to offer greater reliability and robustness compared to the original versions.

One of the famous technique that uses ECC to secure data is Menzes-Vanstone Elliptic Curve Cryptosystem (MVECC) [9]. Numerous researchers have presented a number of studies on ECC. For instance in his book *"Cryptography and Network Security: Principles and Practices"* William Stalling introduced the study about ECC [10]. Ali Mukki Sagheer [11] and Al-Saffer and Said [12] proposed a variant of MVECC [9]. Kurt and Yerlenkaya [13] proposed a modified version of MVECC [9] by using hexadecimal to encrypt data. Tariq and Kadhim [14] designed a new approach for MVECC by using inverse operator only once.

By reducing the computational complexity, we have presented a novel method in this study that is more economical than MVECC. To do this, we use addition and multiplication in place of the inverse operation.

1.1 *Motivation*

Security is becoming increasingly important in an age of fast scientific and technological advancement. MVECC being one of the most widely used cryptographic techniques, also requires some tweaking. Because the original technique employs an inverse operation and the process of determining the inverse is inefficient, it is complicated and so requires more memory. We simplify the method to make the scheme more effective, which can be especially useful for resource-constrained devices like smart cards or applications that demand frequent encryption and decryption.

1.2 *Purpose of the study*

We suggested a novel approach for data encryption and decryption using MVECC in this work. Only addition and multiplication operations are employed

in this strategy. As no inverse operation is performed, this proposed method is more efficient.

The paper is structured as follows. In Section 2 we discuss some fundamental definitions and notions related to ECC and MVECC. Section 3, proposes the novel approach on MVECC followed by an implementation example. In section 4, we compare our proposed method with the original method as proposed by Menezes and Vanstone. In section 5, advantages of the proposed algorithm is mentioned. Finally, section 6 concludes our study with some discussion on the future scope.

2. Prerequisite

In this section, we assemble the pertinent concepts necessary for the preparation of the current article.

Definition 2.1: [15] For $\mathfrak{q} \neq 2,3$ an "elliptic curve" $\mathcal{H}$ "over a prime field" $\mathcal{K}_{\mathfrak{q}}$ is the set of points defined by the equation

$$\mathcal{H}: v^2 \equiv u^3 + cu + d \ (mod\ \mathfrak{q}) \tag{1}$$

where $c, d \in \mathcal{K}_{\mathfrak{q}}$ and the discriminant $\Delta = 4c^3 + 27d^2$ is non zero. The equation mentioned above is called Weierstrass normal form.

For cryptanalysis purposes, we consider the set $\mathcal{H}(\mathcal{K})$ of the points on an elliptic curve over a field $\mathcal{K}$ together with the point at infinity denoted by $\mathcal{O}$. So,

$$\mathcal{H}(\mathcal{K}) = \{(u, v): v^2 = u^3 + cu + d\} \cup \{\mathcal{O}\}$$

$\mathcal{H}$ denotes an "abelian group", with $\mathcal{O}$ acting as the "identity element".

2.1 *Elliptic curve operations*

Definition 2.2: (Point Addition). [15-20] Let $\mathcal{R} = (u_r, v_r)$ and $\mathcal{S} = (u_s, v_s)$ be a pair of points on an elliptic curve $\mathcal{H}$ defined by the equation 2.1. Also let $\mathcal{R} \neq \mathcal{S}$ and none of them are identity element. Then the sum of $\mathcal{R}$ and $\mathcal{S}$ is a third point $\mathcal{T} = (u_t, v_t)$ on the elliptic curve $\mathcal{H}$ whose coordinates are given by

$$u_t = \left(\frac{v_s - v_r}{u_s - u_r}\right)^2 - u_r - u_s \text{and } v_t = \left(\frac{v_s - v_r}{u_s - u_r}\right)(u_r - u_r) - v_r$$

Definition 2.3: (Point Doubling). [15-20] On an elliptic curve $\mathcal{H}$ defined by the eq. (2.1), let us consider a point $\mathcal{R}$ whose coordinates are given by (u_r, v_r). Point doubling means addition of a points to itself to get a new point $\mathcal{S} = (u_s, v_s)$ on $\mathcal{H}$ where the coordinates are given by

$$u_s = \left(\frac{3u_r^2 + c}{2v_r}\right)^2 - 2u_r \text{ and } v_s = \left(\frac{3u_r^2 + c}{2v_r}\right)(u_r - u_s) - v_r$$

Definition 2.4: (Point Multiplication). [15-20] Let $\mathcal{R}$ be any point on the elliptic curve $\mathcal{H}$. Multiplication operation over $\mathcal{R}$ is defined by the repeated addition with the point itself. Thus $n\mathcal{R} = \mathcal{R} + \mathcal{R} + \cdots + \mathcal{R}$ upto n times.

2.2 *Menezes Vanstone Cryptosystem*

In this section we are going to study about Menezes Vanstone Cryptosystem [9] which is a cryptosystem based on elliptic curve. In ECC, for ElGamal encryption, the sender initiate mapping each character of the plaintext message to a point on the EC. Finding the elliptic curve coordinates that correspond to the characters in the plaintext is the first stage in mapping. The encryption algorithm then creates the ciphertext using this mapped representation.

On the other hand, plaintext characters are not necessary to be mapped to points on the EC in MVECC. Instead, an ordered pair that may or may not match a legitimate point on the EC for substituting each character. Instead of mapping to points on the elliptic curve, this replacement phase includes encoding the plaintext characters into an ordered pair and then masked the ordered pair in such a way that it can be unmasked only by the intended receiver, not by an eavesdropper. As a result of skipping the mapping stage, MVECC is more efficient than ElGamal encryption in terms of calculation and processing overhead. [14].

2.3 *Procedure of Encryption and Decryption*

To demonstrate the procedure of encryption and decryption as suggested by Menezes et al. [9], let A and B are the two communicating parties. Prior to the communication, A and B came to an agreement to use elliptic curve $\mathcal{H}(\mathcal{K}_{\mathfrak{q}})$ along with a source point $\mathcal{G}$ within the curve. B chooses his "private key" $\mathfrak{d}$ and computes his "public key" $\mathcal{Q} = \mathfrak{d}\mathcal{G}$. Likewise B, A also select her private key $\mathfrak{e}$ and generate her public key $\mathfrak{e}\mathcal{G}$. From B's public key $\mathcal{Q}$, Alice calculate $\mathfrak{e}\mathcal{Q} = (\mathfrak{f}_1, \mathfrak{f}_2)$. Now to encrypt a message $\mathcal{M} = (\mathfrak{m}_1, \mathfrak{m}_2)$ to $\mathcal{C} = (\mathfrak{c}_1, \mathfrak{c}_2)$. A computes the following:

$$\text{“}\mathfrak{c}_1 = \mathfrak{m}_1 * \mathfrak{f}_1 \bmod \mathfrak{q}\text{”} \text{ [9]}$$

$$\text{“}\mathfrak{c}_2 = \mathfrak{m}_2 * \mathfrak{f}_2 \bmod \mathfrak{q}\text{”}. \text{ [9]}$$

Now A will send the ciphertext $\mathcal{C}_{\mathfrak{m}} = \{\mathcal{C}, \mathfrak{e}\mathcal{G}\}$ to B.

To decrypt the ciphertext B first compute $\mathfrak{d}(\mathfrak{e}\mathcal{G}) = (\mathfrak{f}_1, \mathfrak{f}_2)$. To get the original message $\mathcal{M} = (\mathfrak{m}_1, \mathfrak{m}_2)$, B computes $\mathfrak{m}_1$ and $\mathfrak{m}_2$ using

$$\text{“}\mathfrak{m}_1 = \mathfrak{c}_1 * {\mathfrak{f}_1}^{-1} \bmod \mathfrak{q}\text{” [9]}$$

$$\text{“}\mathfrak{m}_2 = \mathfrak{c}_2 * {\mathfrak{f}_2}^{-1} \bmod \mathfrak{q}\text{” [9].}$$

2.4 *Implementation Example*

To give an example on how the system as suggested by Menezes et al.[9] works, assume A wishes to convey a message $\mathcal{M} = (253,612)$ to B. First, they agree on an elliptic curve $\mathcal{H}(\mathcal{K}_{709})$: $v^2 = u^3 + 269u + 119$. On the curve, they additionally established a base point $B = (38,116)$. To begin, B selects an integer $d = 329$ as his private key and computes $\mathcal{Q} = \mathfrak{d}B = 329(38,116) = (148,434)$, which he uses as his public key.

Following that, A chooses a random integer $\mathfrak{e} = 501$ as her private key and computes $\mathcal{R} = \mathfrak{e}B = 501(38,116) = (526,435)$ which she uses as her public key.

To encrypt the message M, A calculates $\mathfrak{e}\mathcal{Q} = 501(148,434) = (152,4)$. Then A computes $(\mathfrak{c}_1, \mathfrak{c}_2)$ as follows:-

$$\mathfrak{c}_1 = 253 * 152 \bmod 709 = 170$$
$$\mathfrak{c}_2 = 612 * 4 \bmod 709 = 321$$

After that A send the message as $(170,321)$ to B.

After receiving the encrypted message as $(170,321)$ B will do the following. He will first compute $\mathfrak{d}\mathcal{R} = 329(526,435) = (152,4)$. Then he compute

$$\mathfrak{m}_1 = 170 * 152^{-1} \bmod 709 = 170 * 14 \bmod 709 = 253$$
$$\mathfrak{m}_2 = 321 * 4^{-1} \bmod 709 = 321 * 532 \bmod 709 = 612$$

and finally decrypt the message as $(253,612)$.

3. A novel approach for MVEC cryptosystem

This section introduces a novel approach for the Menezes-Vanstone Elliptic Curve Cryptosystem. This improved version contains less computational complications and so it uses less resources. At the end of the section, we'll look at some instances of how to use the updated version of MVECC. Suppose A needs to transmit a message $\mathcal{M} = (\mathfrak{m}_1, \mathfrak{m}_2)$ to B. Likewise the original version of MVECC, here they also agrees upon an elliptic curve $\mathcal{H}(\mathcal{K}_\mathfrak{q})$ and a base point $\mathcal{G}$ which lies on the curve. B selects his private key $\mathfrak{d}$ and generate his public key $\mathcal{Q} = \mathfrak{d}\mathcal{G}$. Likewise B, A also selects a random integer $\mathfrak{e}$ as her private key and generate her public key $\mathcal{R} = \mathfrak{e}\mathcal{G}$. Using B's public key $\mathcal{Q}$, A calculates $\mathfrak{e}\mathcal{Q} = (\mathfrak{k}_1, \mathfrak{k}_2)$. Now to encrypt the message $\mathcal{M} = (\mathfrak{m}_1, \mathfrak{m}_2)$ to $\mathcal{C} = (c_1, c_2)$, A computes the following:

$$\mathfrak{c}_1 = (\mathfrak{m}_1 - \mathfrak{k}_1 * \mathfrak{k}_2) \bmod \mathfrak{q},$$
$$\mathfrak{c}_2 = (\mathfrak{m}_2 - \mathfrak{c}_1 * \mathfrak{k}_1) \bmod \mathfrak{q}.$$

After receiving the encrypted message B first calculate $\mathfrak{d}\mathcal{R} = \mathfrak{d}\mathfrak{e}\mathcal{G} = \mathfrak{e}\mathfrak{d}\mathcal{G} = \mathfrak{e}\mathcal{Q} = (\mathfrak{k}_1, \mathfrak{k}_2)$. Then he can decrypt the message to $(\mathfrak{m}_1, \mathfrak{m}_2)$ using

$$\mathfrak{m}_1 = (\mathfrak{c}_1 + \mathfrak{k}_1 * \mathfrak{k}_2) \bmod \mathfrak{q}$$
$$\mathfrak{m}_2 = (\mathfrak{c}_2 + \mathfrak{c}_1 * \mathfrak{k}_1) \bmod \mathfrak{q}.$$

3.1 *Implementation Example*

To demonstrate how the modified version of Menezes-Vanstone Elliptic Curve Cryptosystem works let us suppose that A desires to transmit a message $\mathcal{M} = (253,612)$ to B through an unsecure channel. First of all they agreed upon an elliptic curve $\mathcal{H}(\mathcal{K}_{709})$: $v^2 = u^3 + 269u + 119$. They also fixed a base point $\mathcal{G} = (38,116)$ on the curve. First B chooses an integer $\mathfrak{d} = 329$ as his private key and computes $\mathcal{Q} = \mathfrak{d}\mathcal{G} = 329(38,116) = (148,434)$ and set it as his public key.

Next A chooses a random integer $\mathfrak{e} = 501$ as her private key and computes $\mathcal{R} = \mathfrak{e}\mathcal{G} = 501(38,116) = (526,435)$ and set it as her public key.

Next A calculate $e\mathcal{Q} = 501(148,434) = (152,4)$. Then she encrypts the message by computing

$$\mathfrak{c}_1 = (253 - 152 * 4) \bmod 709 = 354$$

$$\mathfrak{c}_2 = (612 - 354 * 152) \bmod 709 = 688$$

and send the message as $(354, 688)$ to B.

Now to decrypt the message B first compute $\mathfrak{d}\mathcal{R} = 329(526,435) = (152,4)$. Then he computes

$$\mathfrak{m}_1 = (354 + 152 * 4) \bmod 709 = 253$$

$$\mathfrak{m}_2 = 688 + 354 * 152) \bmod 709 = 612$$

and finally decrypt the message as $(253,612)$.

4. Outcomes and Exploration

In this section we are going to compare the original Menezes-Vanstone Elliptic Curve Cryptosystem (MVECC) with our proposed varient of MVECC. The table 1 outlines a number of operations required for each approach.

Table 1
Operation cost of the original and proposed method

Method	Encryption	Decryption
Original MVECC [9]	2 Mult	2 Inv +2 Mult
Proposed MVECC	2 Mult +2 Add	2 Mult +2 Add

In the table 1 multiplication operation is denoted by Mult, inverse operation is denoted by Inv and addition & subtraction operation is denoted by Add. As addition and subtraction are not costly operation compared to multiplication and inverse operation so the operation cost for the addition and subtraction can be neglected. So we can see that the operation cost for encryption in both the methods are almost same but for decryption we see that in the case of original method there are two multiplication and two inverse operation whereas in our method there are two multiplication and two addition operation. So our proposed method is cost efficient.

Next, we will compare the computational complexity of Memezes-Vanstone and our suggested method's encryption and decryption functions. We assume the input message size as n and calculate using bit operation needed for encryption and decryption. Lower the bit operation higher is the performance.

For Menezes-Vanstone Elliptic Curve cryptosystem [11]

1. The encryption scheme is defined as:

$$\text{“}\mathfrak{c}_1 = \mathfrak{m}_1 * \mathfrak{k}_1 \bmod \mathfrak{q}\text{”}$$

$$\text{“}\mathfrak{c}_2 = \mathfrak{m}_2 * \mathfrak{k}_2 \bmod \mathfrak{q}\text{”}$$

Then

“$\mathcal{T}(\mathfrak{c}_1) = \mathcal{O}(\log n)^2$” bit operations

"$\mathcal{T}(\mathfrak{c}_2) = \mathcal{O}(\log n)^2$" bit operations.

2. The decryption scheme is defined as:

$$\mathfrak{m}_1 = \mathfrak{c}_1 * \mathfrak{k}_1^{-1} \bmod \mathfrak{q}$$
$$\mathfrak{m}_2 = \mathfrak{c}_2 * \mathfrak{k}_2^{-1} \bmod \mathfrak{q}$$

Then "$\mathcal{T}(\mathfrak{m}_1) = \mathcal{O}(\log n)^2 + \mathcal{T}(\mathfrak{k}_1^{-1})$"
By extend Euclid's method "$\mathcal{T}(\mathfrak{k}_1^{-1}) = \mathcal{O}(\log n)^3$"
Therefore,
"$\mathcal{T}(\mathfrak{m}_1) = \mathcal{O}(\log n)^2 + \mathcal{O}(\log n)^3$" bit operations
"$\mathcal{T}(\mathfrak{m}_2) = \mathcal{O}(\log n)^2 + \mathcal{O}(\log n)^3$" bit operations.

For the proposed MVECC varient

1. The encryption scheme is:

$$\mathfrak{c}_1 = \mathfrak{m}_1 - \mathfrak{k}_1 * \mathfrak{k}_2 \bmod \mathfrak{q}$$
$$\mathfrak{c}_2 = \mathfrak{m}_2 - \mathfrak{c}_1 * \mathfrak{k}_1 \bmod \mathfrak{q}$$

Then

$$\text{“}\mathcal{T}(\mathfrak{c}_1) = O(\log n) + O(\log n)^2\text{”}$$
$$\text{“}\mathcal{T}(\mathfrak{c}_2) = O(\log n) + O(\log n)^2\text{”}$$

2. The decryption scheme is:

$$\text{“}\mathfrak{m}_1 = \mathfrak{c}_1 + \mathfrak{k}_1 * \mathfrak{k}_2 \bmod \mathfrak{q}\text{”}$$
$$\text{“}\mathfrak{m}_2 = \mathfrak{c}_2 + \mathfrak{c}_1 * \mathfrak{k}_1 \bmod \mathfrak{q}\text{”}$$

Then,

$$\text{“}\mathcal{T}(\mathfrak{m}_1) = \mathcal{O}(\log n) + \mathcal{O}(\log n)^2\text{”}$$
$$\text{“}\mathcal{T}(\mathfrak{m}_2) = \mathcal{O}(\log n) + \mathcal{O}(\log n)^2\text{”}$$

Thus, we see that in our proposed variant of MVECC there are less computational complexities. Thus our proposed method would be much faster than the original method proposed by Menezes and Vanstone [9].

5. Advantages of the Proposed Method

As we have seen above the proposed method has a number of advantages over the original method as proposed by A. J. Menezes et al. This includes

- Less computational complexities so useful for devices with less memory power.
- More efficient as it take less CPU time in the operations.

6. Conclusion and scope for future work

In this paper, we have proposed a modification to the Menezes-Vanstone Elliptic Curve Cryptography and see an example of its implementation. We also compare our result with original method and observe that our method is more effective as it has less computational complexities.

This cryptosystem is vulnerable to several forms of attack. In the future, the effectiveness of those attacks on the cryptosystem when we use NIST (National Inistitute of Standerds and Technology) recommanded elliptic curve parameter[21] can be investigated. Hardware implementation and further optimization of the technique can also be attempted. The system's efficacy in employing ASCII values for letters verses hexadecimal values for letters may also be investigated. Image encryption can also be attempted using this approach.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Disclosure of Potential Conflicts of Interest

The authors assert that there are no conflicts of interest.

References

[1] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. A. D. Abed, and A. T. Hammid, "Implementation of el-gamal algorithm for speech signals encryption and decryption," *Procedia Computer Science,* vol. 167, pp. 1028–1037 (2020).

[2] V. S. Miller, "Use of elliptic curves in cryptography," in Conference on the theory and application of cryptographic techniques, pp. 417–426, Springer (1985).

[3] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209 (1987).

[4] D. Dachman-Soled, J. Loss, and A. O'Neill, "Breaking rsa generically is equivalent to factoring, with preprocessing," Cryptology ePrint Archive (2022).

[5] D. S. Sakkari and M. M. ulla, "Review on insight into elliptic curve cryptography," in *Modern Approaches in Machine Learning & Cognitive Science: A Walkthrough*, pp. 81–93, Springer (2022).

[6] E. B. Barker, W. C. Barker, W. E. Burr, W. T. Polk, and M. E. Smid, "Recommendation for key management, part 1: General (revision 3)," (2006).

[7] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 463–470 (2020).

[8] Q. M. Luhaib and R. K. K. Ajeena, "Elliptic curve matrices over group ring to improve elliptic curve–discrete logarithm cryptosystems," *Journal of Discrete Mathematical Sciences & Cryptography,* vol. 26, no. 6, pp. 1699–1704 (2022).

[9] A. J. Menezes and S. A. Vanstone, "Elliptic curve cryptosystems and their implementation," *Journal of cryptology,* vol. 6, pp. 209–224 (1993).

[10] W. Stallings, Cryptography and network security, 4/E. Pearson Education India, 2006.

[11] A. M. Sagheer, "Elliptic curves cryptographic techniques," in 2012 6th International Conference on Signal Processing and Communication Systems, pp. 1–7, *IEEE* (2012).

[12] N. H. Al-Saffar, M. R. M. Said, and M. Rushdan, "On the mathematical complexity and the time implementation of proposed variants of elliptic curves cryptosystems," *International Journal of Cryptology Research,* vol. 4, no. 1, pp. 42–54 (2013).

[13] K. Meltem and Y. Tarik, "A new modified cryptosystem based on menezes vanstone elliptic curve cryptography algorithm that uses characters hexadecimal values," in 2013 The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering, pp. 449–453, IEEE (2013).

[14] A. T. Sadiq and N. J. Kadhim, "Enhanced menezes-vanestone elliptic curves cryptosystem," *Al Nahrain Journal of Science*, vol. 12, no. 1, pp. 162–165 (2009).

[15] D. Hankerson, A. J. Menezes, and S. Vanstone, Guide to elliptic curve cryptography. Springer Science & Business Media (2004).

[16] G. Barwood, "Elliptic curve cryptography faq v1. 12 22nd," (1997).

[17] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, Handbook of elliptic and hyperelliptic curve cryptography. CRC press (2005).

[18] J. H. Silverman, The arithmetic of elliptic curves, vol. 106. Springer (2009).

[19] L. C. Washington, Elliptic curves: number theory and cryptography. Chapman and Hall/CRC (2008).

[20] A. K. Bhandari, D. Nagaraj, B. Ramakrishnan, and T. Venkataramana, Elliptic curves, modular forms and cryptography: proceedings of the Advanced Instructional Workshop on Algebraic Number Theory. Springer (2003).

[21] L. Chen, D. Moody, A. Regenscheid, and K. Randall, "Recommendations for discrete logarithmbased cryptography: Elliptic curve domain parameters," tech. rep., National Institute of Standards and Technology (2019).

Received February, 2024