Academic Science Journal

An Enhancement of the Elliptic Curve Cryptography by Using the Pairing Function

Sarah. H. Namous*, Hamza B. Habib and Rifaat Z. Khalaf

Department of mathematics, College of Science, University of Diyala, Diyala, Iraq

*mathmathsara99@gmail.com

Received: 27 March 2024 **Accepted: 11 June 2024**

Published: July 2025

DOI: https://dx.doi.org/10.24237/ASJ.03.03.866C

Abstract

In this paper, we propose two new algorithms to increase the security of the Elliptic Curve Cryptography (ECC) by using a pairing function. Each algorithm is built on combining a pairing function, which is either the Cantor pairing function or the Elegant pairing function, with the ECC. Both algorithms merge two ciphertexts (two points on the elliptic curve EC) into one ciphertext (one point on the elliptic curve EC). This means that only one ciphertext is sent in any of the two proposed algorithms. Sending one ciphertext results in a shorter transmission time. The proposed algorithms are safe according to security analysis. Therefore, the use of the proposed algorithms provides a high level of security and shortens the transmission time compared to classical ECC.

The results present number and type of keys that generated, as shown in Table 1. These keys are strong for using in public key algorithms, in addition to the difficulty of guessing the keys by attacker, because these keys are generated from a normal video that does not raise any suspicions in the attacker when exchanging them.

Keywords: Number Theory, Elliptic Curve, Elliptic Curve Cryptography, Pairing Function, Cantor Pairing Function, Elegant pairing function.

Introduction

Number theory is a broad and intriguing area of mathematics that includes the study of prime factorization and prime number properties. An arrangement or plan known as a cryptosystem is used to securely encode and decode messages by converting plaintext to cipher text and then to the original plaintext back. A shortening of "cryptographic system" is "cryptosystem" which designates a computer system with number theory that makes use of cryptography. Information that is in plaintext can be encrypted so that only authorized people can read it. By using algorithms on the data, this is accomplished. Symmetric key encryption and asymmetric key encryption are the two basic categories of encryption techniques. In symmetric key encryption, the problem is to securely transfer the key that will be used in this operation. The sender encrypts the data using a key, and the recipient uses the same key to decrypt it. When using asymmetric key cryptography, both the sender and the recipient have two sets of keys: a private key that is kept secret and is used to decipher messages encrypted with the public key [1]. The cryptosystem algorithms were applied with some mathematical terms to improve the security of the sent data, for example, Legendre Symbol, Chebyshev polynomial, etc. [2-4]

The study of elliptic curves got the attention of several number theorists dating back to the middle of the nineteenth century. The Elliptic Curve Cryptography (ECC), which is classified as one of the asymmetric cryptography algorithms, was discovered in 1985 by Neil Koblitz and Victor Miller [5]. The discrete logarithm problem of the elliptic curve ECDLP and the algebraic geometry of elliptic curves with finite fields are the foundations of the elliptic curve cryptosystem ECC. Various fundamental elliptic curves can be employed. A varying key length, performance, and encryption strength are offered by different curves. Elliptic curves are collections of points where a and$b$, the constants, satisfy the elliptic curve equation. The ECC keys setting is straightforward. The private key is an integer, that is, every positive integer represents a valid ECC private key. A set of coordinates (x, y) on the curve represents the public key [6]. Signatures and key negotiation are made feasible by public-key cryptography, and both functions are essential for modern internet computer systems used by governments and businesses. Since ECC has less computational complexity than other modular arithmetic systems like the Rivest-Shamir-Adleman algorithm (RSA), it is the recommended way for implementing these services [15]. And ECC uses a small key size, which makes it superior to the common cryptosystem RSA.

A pairing function is a function used to encode two natural numbers into one natural number in a unique way. In set theory, it is possible to demonstrate that rational numbers and integers have any pairing function identical cardinality to that of natural numbers [7]. Pairing functions play an important role in computability theory, and have practical applications in computer science. A general technique for constructing a pairing function from any non-decreasing unbounded function is described. This technique is used to construct a binary proportional pairing function and its inverse [13]. The three most important methods of it Cantor pairing function, Rosenberg-Strong pairing function and Elegant pairing function.

In this paper, we propose two new algorithms of cryptography based on using paring functions. The first algorithm is based on applying the Cantor pairing function to ECC, and the second is based on applying the Elegant pairing function to ECC. In the first proposed algorithm, the sender encrypts the plaintext by the ECC and then uses the Cantor pairing function to convert each ciphertext to a single integer. That is, the two ciphertexts are converted into one ciphertext, which is then sent to the recipient. To recover the plaintext, the recipient first uses the inverse of the Cantor pairing function and then decrypts it using a decryption process of the ECC. In the second proposed algorithm, the sender encrypts the plaintext by the ECC and then uses the Elegant pairing function to convert each ciphertext to a single integer. That is, the two ciphertexts are converted into one ciphertext, and then sent to the recipient. To recover the plaintext, the recipient first uses the inverse of the Elegant pairing function and then decrypts it using the ECC decryption process. Implementing the two new algorithms reduces the data transmission time.

The rest of this paper is structured as follows: In Section 2, the Pairing functions (Cantor pairing function and Elegant pairing function) are described. In Section: 3, the ECC with some basic theorems and definitions are discussed. In Section 4, the proposed algorithm is presented. In Section 5, the security analysis of the proposed algorithm is provided. Finally, the conclusion is provided in Section 5.

1. The Elliptic Curve Cryptography

Definition 1.1: The EC $E_p(a,b)\colon y^2 = (x^3 + ax + b) \pmod p$, where $a\,, b\ \in F_p$ and $4a^3 + 27b^2 \neq 0 \pmod p$, gives the ECC over a finite prime F_p, [8].

Theorem 1.1: Let $R = (x_1, y_1)$ and $W = (x_2, y_2) \in$ EC, [9,10].

I. If $R \neq W$, then $R + W = (x_3, y_3)$ where

$$x_3 = \left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2\right) \pmod p \text{ and } y_3 = \left(\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 (x_1 - x_3) - y_1\right) \pmod p.$$

II. If $R = W$, then $R + W = (x_3, y_3)$ where

$$x_3 = \left(\left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1\right) \pmod p \text{ and } y_3 = \left(\left(\frac{3x_1^2+a}{2y_1}\right)^2 (x_1 - x_3) - y_1\right) \pmod p.$$

III. The point multiplication of a point R on EC is defined as doubling the point R on that curve. It is denoted by $\alpha R = R + R + \cdots + R$, α times.

IV. $-R + \infty = \infty + R = R$ for all EC. Where ∞ is the point at infinity.

Theorem 1.2: [9], The Elliptic curve $E_p(a,b)$ is defined as follows $y^2 = (x^3 + ax + b) \pmod p$. The number of points on $E_p(a,b)$ and the point at infinity ∞ is

$$\left|E_p(a,b)\right| = 1 + p \sum_{x\in F_p} \left(\frac{x^3 + ax + b}{p}\right) = 1 + p + \epsilon,$$

Where, $\left(\frac{x^3+ax+b}{p}\right)$ is the Legendre Symbol.

The EEC algorithm is described below [8-11].

The Key Generation process

i. The sender and the receiver (Alice and Bob respectively) agree on an elliptic curve $E_p(a,b)\colon y^2 = (x^3 + ax + b) \pmod p$, such that, p is a prime number. Also, they choose a point G on the EC.

ii. Alice chooses a random positive integer α (the private key), then calculates the public key $A = \alpha G$.

iii. Bob chooses a random positive integer β (the private key), then calculates the public key $= \beta G$.

The Encryption process

If Alice wants to send the message M to Bob, Alice then converts M to a point on the EC based on the agreed procedure. Alice selects a random number γ for the encryption process to be used in a different communication point, and she calculates,

$$E_1 = \gamma G \tag{1}$$

$$E_2 = M + \gamma B. \tag{2}$$

Alice send E_1 and E_2 to Bob.

The Decryption process

Bob receives E_1 and E_2 and decrypt the message as follows:

$$M = E_2 - \beta E_1 \tag{3}$$

2. Pairing Functions

2.1 Cantors Pairing Function

The cantor pairing function, [12,13], $\mathrm{C}: \mathbb{N}^2 \rightarrow \mathbb{N}$ and the inverse cantor pairing function $\mathrm{C}^{-1}: \mathbb{N} \rightarrow \mathbb{N}^2$ are two bijections one inverse to the other. They are given as:

$$C = \frac{1}{2}(x + y)(x + y + 1) + x, \tag{4}$$

and

$$\mathrm{C}^{-1} = \left(\mathrm{C} - \frac{r(r+1)}{2}, \frac{r(r+3)}{2} - \mathrm{C}\right) \tag{5}$$

where $r = \left\lfloor \frac{\sqrt{1+8\mathrm{C}} - 1}{2} \right\rfloor$. Figure 1 shows the Cantor pairing function.

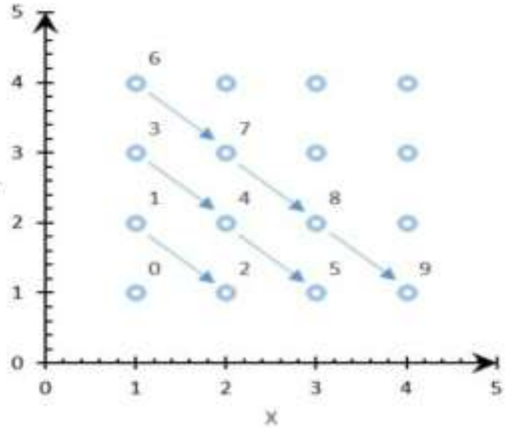

Figure 1: Cantor Pairing Function

Example 2.1.1: Consider the point $(x, y) = (14,7)$ by Eq. (4), we have

$$C = \frac{1}{2}(14 + 7)(14 + 7 + 1) + 14 = 245$$

To get the point (x, y) back, we have

$$r = \left\lfloor \frac{\sqrt{1 + 8(245)} - 1}{2} \right\rfloor = 21.$$

Using Eq. (5),

$$\mathrm{C}^{-1} = \left(245 - \frac{21(21 + 1)}{2}, \frac{21(21 + 3)}{2} - 245\right) = (14,7).$$

Then $(x, y) = (14,7)$.

2.2 Elegant Pairing Function

The Elegant pairing function, [13,14]**,** $\mathcal{E}$ produces a single natural number from a pair of natural numbers x and y as shown in Figure 2. It is given as

$$\mathcal{E} = \begin{cases} y^2 + x & x \neq \max(x, y)\,, \\ x^2 + x + y & x = \max(x, y)\,. \end{cases} \tag{6}$$

The inverse Elegant pairing function, which returns the pair corresponding to each natural number, is given as:

$$\mathcal{E}^{-1} = \begin{cases} \left(\mathcal{E} - \lfloor\sqrt{\mathcal{E}}\rfloor^2, \lfloor\sqrt{\mathcal{E}}\rfloor\right) & \mathcal{E} - \lfloor\sqrt{\mathcal{E}}\rfloor^2 < \lfloor\sqrt{\mathcal{E}}\rfloor, \\ \left(\left(\lfloor\sqrt{\mathcal{E}}\rfloor, \mathcal{E} - \lfloor\sqrt{\mathcal{E}}\rfloor^2 - \lfloor\sqrt{\mathcal{E}}\rfloor\right) & \mathcal{E} - \lfloor\sqrt{\mathcal{E}}\rfloor^2 \geq \lfloor\sqrt{\mathcal{E}}\rfloor. \end{cases} \tag{7}$$

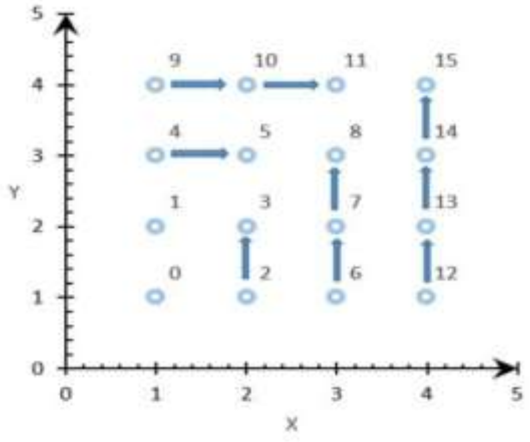

Figure 2: Elegant Pairing Function

Example 2.2.1: Consider the point $(x, y) = (14,7)$. Then, by Eq. (6) we have

$$\mathcal{E} = 14^2 + 14 + 7 = 217$$

By Eq. (7), the point is recovered as

$$\mathcal{E}^{-1} = \left(\lfloor\sqrt{217}\rfloor, 217 - \lfloor\sqrt{217}\rfloor^2 - \lfloor\sqrt{217}\rfloor\right) = (14,7)$$

Then $(x, y) = (14,7)$.

3. The Proposed Algorithm.

In this section, two proposed algorithms are introduced based on using the pairing functions with the ECC, such that, their construction is similar to the one that is covered in Section 2 regarding the determination of public and private key values, Bob publishes G and B, while β is the private key.

3.1 Cantor Pairing Function with the EEC

- **Encryption Process**

Alice transforms the plaintext into corresponding points on $E_p(a, b)$ based on an agreed procedure. After selecting a random positive integer γ, Alice calculates $E_1 = (x_1, y_1)$ and $E_2 = (x_2, y_2)$ by Eq. (1) and Eq. (2).

Now, by Eq. (4) Alice uses the Cantor pairing function for the points E_1 and E_2

$$\mathrm{C}_{E_1} = \frac{1}{2}(x_1 + y_1)(x_1 + y_1 + 1) + x_1, \qquad (8)$$

And

$$\mathrm{C}_{E_2} = \frac{1}{2}(x_2 + y_2)(x_2 + y_2 + 1) + x_2. \qquad (9)$$

Then, $(\mathrm{C}_{E_1}, \mathrm{C}_{E_2})$ are the ciphertext, and they are sent to Bob.

- **Decryption Process**

After receiving $(\mathrm{C}_{E_1}, \mathrm{C}_{E_2})$, Bob calculates the formula for the inverse of the Cantor pairing function C_{E_1} and C_{E_2} by Eq. (5)

$$\mathrm{C}_{E_1}^{-1} = \left(\mathrm{C}_{E_1} - \frac{r_1(r_1+1)}{2}, \frac{r_1(r_1+3)}{2} - \mathrm{C}_{E_1}\right) \qquad (10)$$

where $r_1 = \left\lfloor \frac{\sqrt{1+8\,\mathrm{C}_{E_1}} - 1}{2} \right\rfloor$, and

$$\mathrm{C}_{E_2}^{-1} = \left(\mathrm{C}_{E_2} - \frac{r_2(r_2+1)}{2}, \frac{r_2(r_2+3)}{2} - \mathrm{C}_{E_2} \right) \tag{11}$$

where $r_2 = \left\lfloor \frac{\sqrt{1+8\,\mathrm{C}_{E_2}}-1}{2} \right\rfloor$.

Now, Bob performs the decryption process as follows:

$$M = \mathrm{C}_{E_2}^{-1} - \beta \mathrm{C}_{E_1}^{-1} \tag{12}$$

Example 3.1 In this example, we discuss the Cantor pairing function with the ECC algorithm. Suppose that Alice and Bob consider the elliptic curve $E_{43}(18,3): y^2 \equiv (x^3 + 18x + 3) \pmod{43}$, and the initial point $(3,16)$ on $E_{43}(18,3)$. The agreed procedure between Alice and Bob is selected arbitrarily, and it is given in Table 1 as follows**:**

Table 1: The agreed procedure of $E_{43}(18,3)$.

	A	B	C	D	E	F	G	H	I	J
∞	(3,16)	(15,37)	(20,8)	(29,19)	(21,15)	(34,12)	(30,18)	(8,33)	(4,15)	(37,18)
K	L	M	N	O	P	Q	R	S	T	U
(28,23)	(16,1)	(35,11)	(18,28)	(2,2)	(19,18)	(19,25)	(2,41)	(18,15)	(35,32)	(16,42)
V	W	X	Y	Z	1	2	3	4	5	6
(28,20)	(37,25)	(14,22)	(8,10)	(30,25)	(34,31)	(21,28)	(29,24)	(20,35)	(15,6)	(3,27)

Also, suppose Bob selects the point $G = (2,2)$ and selects the private key $\beta = 6$. Then, Bob calculates the public key as $B = \beta G = 6(2,2) = (4,28)$.

Assume Alice wishes to send Bob the message M = "THEORY." Alice then converts M to the appropriate points using the agreed procedure. That is, “T” = $(35,32)$, and Alice chooses $\gamma = 9$. Then, by the Eq. (1) and Eq. (2)

$$E_1 = \gamma G = 9(2,2) = (20,8),$$

$$\begin{aligned} E_2 &= \mathrm{T} + \gamma B \\ &= (35,32) + 9(4,28) \\ &= (35,32) + (2,41) = (21,15). \end{aligned}$$

and by Eq. (8) and Eq. (9)

$$\mathrm{C}_{E_1} = \frac{1}{2}(20+8)(20+8+1) + 20 = 426.$$

$$\mathrm{C}_{E_2} = \frac{1}{2}(21+15)(21+15+1) + 21 = 687.$$

Alice sends only (426,687) to Bob.

Now, $r_1 = \left\lfloor \frac{\sqrt{1+8(426)}-1}{2} \right\rfloor = 28$ and $r_2 = \left\lfloor \frac{\sqrt{1+8(687)}-1}{2} \right\rfloor = 36$, then by Eq. (10) and Eq. (11)

$$\mathrm{C}_{E_1}^{-1} = \left(426 - \frac{28(28+1)}{2}, \frac{28(28+3)}{2} - 426\right) = (20,8)$$

$$\mathrm{C}_{E_2}^{-1} = \left(687 - \frac{36(36+1)}{2}, \frac{36(36+3)}{2} - 687\right) = (21,15).$$

Then, $\mathrm{C}_{E_1}^{-1} = (20,8)$ and $\mathrm{C}_{E_2}^{-1} = (21,15)$. Now by Eq. (12)

$$M = \mathrm{C}_{E_2}^{-1} - \beta \mathrm{C}_{E_1}^{-1}$$
$$= (21,15) - 6(20,8)$$
$$= (21,15) - (2,41)$$
$$= (21,15) + (2,2) = (35,32) = \mathrm{T}$$

Table 2: The encryption and decryption processes by the Cantor pairing function with the ECC.

The Letters	The Point	Encryption by Alice				Decryption by Bob				
		γ	E_1	E_2	$(\mathrm{C}_{E_1}, \mathrm{C}_{E_2})$	r_1	r_2	$\mathrm{C}_{E_1}^{-1}$	$\mathrm{C}_{E_2}^{-1}$	M
T	(35,32)	9	(20,8)	(21,15)	(426,687)	28	36	(20,8)	(21,15)	(35,32)
H	(8,33)	7	(34,12)	(28,23)	(1115,1354)	46	51	(34,12)	(28,23)	(8,33)
E	(21,15)	14	(16,1)	(28,23)	(169,1354)	17	51	(16,1)	(28,23)	(21,15)
O	(2,2)	5	(4,15)	(20,8)	(194,426)	19	28	(4,15)	(20,8)	(2,2)
R	(2,41)	19	(16,42)	(16,1)	(1727,169)	58	17	(16,42)	(16,1)	(2,41)
Y	(8,10)	17	(4,28)	(29,19)	(532,1205)	32	48	(4,28)	(29,19)	(8,10)

3.2 Elegant pairing function to the EEC

- **Encryption Process**

Alice transforms the plaintext into corresponding points on $E_p(a,b)$ based on the agreed procedure. After selecting a random positive integer γ, Alice does the calculation $E_1 = (x_1, y_1)$, and $E_2 = (x_2, y_2)$ by Eq. (1) and Eq. (2).

Now, Alice uses the Elegant pairing function for the points E_1 and E_2 by Eq. (6)

$$\mathcal{E}_{E_1} = \begin{cases} {y_1}^2 + x_1 & x_1 \neq \max(x_1, y_1) \\ {x_1}^2 + x_1 + y_1 & x_1 = \max(x_1, y_1) \end{cases} \quad (13)$$

and

$$\mathcal{E}_{E_2} = \begin{cases} {y_2}^2 + x_2 & x_2 \neq \max(x_2, y_2) \\ {x_2}^2 + x_2 + y_2 & x_1 = \max(x_2, y_2) \end{cases} \quad (14)$$

Then, $\left(\mathcal{E}_{E_1},\ \mathcal{E}_{E_2}\right)$, which are the ciphertexts, and they are sent to Bob.

- **Decryption Process**

After receiving$\left(\mathcal{E}_{E_1}, \mathcal{E}_{E_2}\right)$, Bob calculates the formula for the inverse of the Elegant pairing function $\mathcal{E}_{E_1}$ and $\mathcal{E}_{E_2}$ by Eq. (7)

$$\mathcal{E}_{E_1}^{-1} = \begin{cases} \left(\mathcal{E}_{E_1} - \left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor^2, \left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor\right) & \mathcal{E}_{E_1} - \left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor^2 < \left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor \\ \left(\left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor, \mathcal{E}_{E_1} - \left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor^2 - \left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor\right) & \mathcal{E}_{E_1} - \left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor^2 \geq \left\lfloor\sqrt{\mathcal{E}_{E_1}}\right\rfloor \end{cases} \quad (15)$$

and

$$\mathcal{E}_{E_2}^{-1} = \begin{cases} \left(\mathcal{E}_{E_2} - \left\lfloor\sqrt{\mathcal{E}_{E_2}}\right\rfloor^2, \left\lfloor\sqrt{\mathcal{E}_{2}}\right\rfloor\right) & \mathcal{E}_{E_2} - \left\lfloor\sqrt{\mathcal{E}_{E_2}}\right\rfloor^2 < \left\lfloor\sqrt{\mathcal{E}_{E_2}}\right\rfloor \\ \left(\left\lfloor\sqrt{\mathcal{E}_{E_2}}\right\rfloor, \mathcal{E}_{E_2} - \left\lfloor\sqrt{\mathcal{E}_{E_2}}\right\rfloor^2 - \left\lfloor\sqrt{\mathcal{E}_{E_2}}\right\rfloor\right) & \mathcal{E}_{E_2} - \left\lfloor\sqrt{\mathcal{E}_{E_2}}\right\rfloor^2 \geq \left\lfloor\sqrt{\mathcal{E}_{E_2}}\right\rfloor \end{cases} \quad (16)$$

Now, Bob performs the decryption process as follows:

$$M = \mathcal{E}_{E_2}^{-1} - \beta\mathcal{E}_{E_1}^{-1} \quad (17)$$

Example 3.2.1: Consider the elliptic curve $E_{43}(18,3)$: $y^2 = x^3 + 18x + 3 \pmod{43}$, and the point (3,16) on $E_{43}(18,3)$. Also, suppose Bob selects the point $G = (2,2)$ and selects the private key $\beta = 6$. Then, Bob calculates the public key as $B = (4,28)$. Assume Alice wishes to send Bob the message M = "THEORY." Alice then converts M to the appropriate points using the agreed procedure. That is, $T = (35,32)$, and Alice chooses $\gamma = 9$.

Then, by the Eq. (1) and Eq. (2) $E_1 = (20,8)$ and $E_2 = (21,15)$. Also, by Eq. (13) and Eq. (14) $\mathcal{E}_{E_1} = 428$ and $\mathcal{E}_{E_2} = 477$. Then, Alice sends only (428,477) to Bob.

Now, by Eq. (15) and Eq. (16)

$$\mathcal{E}_{E_1}^{-1} = (20,428 - 400 - 20) = (20,8)$$

And

$$\mathcal{E}_{E_2}^{-1} = (21,477 - 21^2 - 21) = (21,15).$$

By Eq. (17)

$$M = (21,15) - 8(20,8)$$

$$= (21,15) - (2,41)$$

$$M = (21,15) + (2,2) = (35,32) = \text{T}$$

In the same way, the rest of the message M is encrypted and decrypted as shown in Table 3.

Table 3: The encryption and decryption processes by the Elegant pairing function with the ECC.

The Letters	The Point	Encryption by Alice				Decryption by Bob		
		γ	E_1	E_2	$(\mathcal{E}_{E_1}, \mathcal{E}_{E_2})$	$\mathcal{E}_{E_1}^{-1}$	$\mathcal{E}_{E_2}^{-1}$	M
T	(35,32)	9	(20,8)	(21,15)	(428,477)	(20,8)	(21,15)	(35,32)
H	(8,33)	7	(34,12)	(28,23)	(1202,835)	(34,12)	(28,23)	(8,33)
E	(21,15)	14	(16,1)	(28,23)	(273,835)	(16,1)	(28,23)	(21,15)
O	(2,2)	5	(4,15)	(20,8)	(229,428)	(4,15)	(20,8)	(2,2)
R	(2,41)	19	(16,42)	(16,1)	(1780,273)	(16,42)	(16,1)	(2,41)
Y	(8,10)	17	(4,28)	(29,19)	(788,889)	(4,28)	(29,19)	(8,10)

4. The Security Analysis

Encryption algorithms always look for the security of the transmitted data and the speed of the transmission process. From the sent ciphertext, E_1 and E_2, the attacker can guess the value of p used in the equation $E_p(a,b)$ from the results of (x,y). In the two proposed algorithms, points are converted into a new unique single point. The Cantor pairing function is used in the first proposed algorithm, so that the range of points becomes $C= \frac{1}{2}(x+y)(x+y+1)+x$. The Elegant pairing function is used in the other proposed algorithm, such that, $\mathcal{E} = \begin{cases} y^2 + x & x \neq \max(x,y) \\ x^2 + x + y & x = \max(x,y) \end{cases}$. Therefore, it is difficult for the attacker to guess the value of p used in the equation $E_P(a,b)$ in both algorithms, which makes such an attack a useless attack. The complexity level of the proposed algorithm is very large because it consists of the complexity of DLP for the EC and the complexity of the pairing function.

The ECC is considered secure when the key length is greater than or equal to 160-bit, and the proposed algorithm uses a key length of 160-bit. Moreover, every pair of positive integers is converted into only one number. Even if the attacker could convert the number back to the original pair by calculating the order using the pollar-roh method or by Baby-step Gaint-step, he faces another complexity: calculating DLP for the EC.

In other words, the complexity of the proposed algorithm consists of two parts, which are the paring and the other is DLP for the EC. Also, the proposed algorithm sends one number instead of a pair of numbers leading to a faster transmitting time of the message.

Conclusion

We present two new cryptosystem algorithms which are combined with the ECC. The first algorithm uses the Cantor pairing function with the ECC, and the second algorithm uses the Elegant pairing function with the ECC. In both algorithms, every pair of ciphertexts (every pair of points on the EC) is converted into only one ciphertext (one point of the EC). Moreover, the data sent is only one point and this leads to reducing the transmission time between the two parties. The security analysis shows that the proposed algorithm is safe compared to the classic ECC. Thus, the proposed algorithm provides a high level of safety for sending data.

Source of funding: None

Conflict of interest: None

Ethical clearance: None

References

[1] J. B. Daniel, Search security cryptosystem, SEARCH SECURITY, June (2019)

[2] H. B. Habib, Modifying Playfair Cipher Algorithm by using Legendre Symbol, Diyala Journal for Pure Science, 15(04), (2019), DOI(http://dx.doi.org/10.24237/djps.15.04.502A)

[3] H. B. Habib, the Application of Chebyshev Polynomial on the Three-Pass Protocol, Diyala Journal for Pure Science, 18(03), (2022), DOI(https://dx.doi.org/10.24237/djps.1803.587A)

[4] R. Z. Khalaf, H. B. Habib, S. K. Aljaff, Attacking the Application of Three-Pass Protocol in Hill-Cipher, In Next Generation of Internet of Things: Proceedings of ICNGIoT 2021, 121-127(2021) Springer Singapore, DOI(http://dx.doi.org/10.1007/978-981-16-0666-3_12)

[5] V. S. Miller, Use of elliptic curves in cryptography, In H.C. Williams, editor, Advances in Cryptology CRYPTO'85, 218 of Lecture Notes in Computer Science, 417-426(1986)

[6] D. R. Stinson, Cryptography Theory and Practice, 3rd edition, (Chapman & Hall/CRC, New York, 2006).

[7] MERI, LII, SOME REMARKS ON THE CANTOR PAIRING FUNCTION, LXII -FASC. I, 5565(2007)

[8] D. Natanael, and D. Suryani, Text encryption in android chat applications using elliptical curve cryptography (ECC), Procedia Computer Science, 135, 283-291(2018), DOI(http://dx.doi.org/10.1016/j.procs.2018.08.176)

[9] S.Y. Yan, Computational number theory and modern cryptography, (John Wiley & Sons, , 2013)

[10] K. NEAL, and M. ALFRED, The State of Elliptic Curve Cryptography, Dept. of C&O, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1, (2000), DOI(http://dx.doi.org/10.1023/A:1008354106356)

[11] N. Koblitz, Elliptic curve cryptosystems, Mathematics of computation, 48(177), 203-209(1987)

[12] G. Cantor, Contributions to the Founding of the Theory of Transfinite Numbers, (Dover, New York, 1955)

[13] M. P. Szudzik, Binary Proportional Pairing Functions, ArXiv, abs/1809.06876, DOI(https://doi.org/10.48550/arXiv.1809.06876)

[14] A. Solís-Rosas, S. L. Canchola-Magdaleno, M. T. García-Ramírez, An Enhanced Run Length Encoding using an Elegant Pairing Function for Medical Image Compression. International Journal of Computer Science and Software Engineering, 8(5), 104-111(2019)

[15] O. W Eide, Elliptic Curve Cryptography Implementation and Performance Testing of Curve Representations, Master’s Thesis Spring (2017)