Baghdad Science Journal

Volume 23 | Issue 1 Article 23

1-14-2026

A Proposed Cryptographic Algorithm Based on Three-Pass Protocol and the Elliptic Curve Cryptography

Rifaat Z. Khalaf
Department of Mathematics, College of Science, University of Diyala, Diyala, Iraq, drrifaat55@gmail.com

Hamza B. Habib
Department of Mathematics, College of Science, University of Diyala, Diyala, Iraq, halsaadi18@yahoo.com

How to Cite this Article

Z. Khalaf, Rifaat and B. Habib, Hamza (2026) "A Proposed Cryptographic Algorithm Based on Three-Pass Protocol and the Elliptic Curve Cryptography," *Baghdad Science Journal*: Vol. 23: Iss. 1, Article 23.
DOI: https://doi.org/10.21123/2411-7986.5185

RESEARCH ARTICLE

A Proposed Cryptographic Algorithm Based on Three-Pass Protocol and the Elliptic Curve Cryptography

Rifaat Z. Khalaf, Hamza B. Habib *

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

ABSTRACT

The internet lately has become an integral part of people's lifestyles. It impacts various aspects of their daily lives, including education, communication, etc. Hence, the need for efficient and fast cryptography algorithms has increased. In this paper, a new cryptographic algorithm is proposed using the authenticated Three-Pass Protocol (TPP) and the Elliptic Curve Cryptography (ECC). In the proposed algorithm, the ECC is used to encrypt and decrypt data (a text of size 128 bits), and the TPP is used for transmitting this data without sharing the keys. In the standard ECC, the receiver publishes the elliptic curve (EC) equation, the initial point, and the public key, while the only published information in the proposed algorithm is the EC equation. Moreover, in the standard ECC two ciphertexts are sent, while only one ciphertext is sent in the proposed algorithm in each pass, which reduces the transmitting time in the proposed algorithm. Also, the proposed algorithm is proved mathematically by presenting a new proposition with the proof. The NIST tests, such as approximate entropy, block frequency, etc., along with the entropy and histogram tests, are implemented on the cryptographic algorithm (encryption algorithm) to show the effectiveness of the proposed algorithm. The used key in the proposed algorithm is greater than or equal to 128 bit for the algorithm to be efficient against the attacks. The security analysis shows that the proposed algorithm is secure against several common attack algorithms. Thus, the proposed algorithm is secure, fast, and efficient in transmitting data.

Keywords: Cryptography, elliptic curve, elliptic curve cryptography, number theory, three-pass protocol

Introduction

Number Theory, which is a mathematics branch, studies integer numbers and their properties. It focuses on the topics of divisibility, prime numbers, modular arithmetic, and various algebraic properties. Number Theory has a huge role in cryptography to secure the communication and information that is transmitted amongst the parties.[1,2]

One of the cryptosystem algorithms is the Three-Pass Protocol (TPP) which provides data exchange in three passes without exchanging the keys. Therefore, it is considered an effective way to exchange the keys for a high level of security.[3] Several studies have been done to combine cryptosystem algorithms or mathematical concepts with the TPP to enhance the security of the transmitting data, for example, Caesar Cipher,[4] RSA and ElGamal algorithms,[5] Permutations,[6] Hill Cipher,[7] and Paillier cryptosystem.[8]

Moreover, Elliptic Curve Cryptography (ECC), which was presented independently by Miller[9] and Koblitz[10] respectively, is a cryptographic algorithm based on the mathematical properties of elliptic curves (EC). The ECC is better than the commonly used cryptosystem RSA because it uses a small key size.[11] Therefore, the ECC is particularly suitable for resource-constrained devices, such as devices of the Internet of Things,[12] mobile phones to secure applications,[13,14] and so on.

Received 18 January 2024; revised 21 December 2024; accepted 23 December 2024.
Available online 14 January 2026

* Corresponding author.
E-mail addresses: drrifaat55@gmail.com (R. Z. Khalaf), halsaadi18@yahoo.com (H. B. Habib).

https://doi.org/10.21123/2411-7986.5185

Several studies have been done to show the applications of the ECC, for example, the ECC is used with the Diffie-Hellman for key exchange in the image encryption.[15,16] Moreover, to enhance the encryption and authentication in IoT systems, the ECC is used. Fuzzy logic is applied to generate random numbers which is used in the ECC to get better performance.[17] Furthermore, the Rosenberg-Strong Pairing Function is applied to the ECC to enhance the security of the transmitted data over insecure channels.[18]

In this paper, a new cryptography algorithm is presented using the combination of the TPP and ECC. A mathematical proof of the proposed algorithm work is provided by presenting a new proposition and its proof. The proposed algorithm uses the ECC to encrypt and decrypt data (text, image, etc.), while the TPP is used to transmit the data without exchanging keys between the parties. In this algorithm, the only public information between the two parties is the EC equation, while the rest of the information is kept secret. Furthermore, the sender only needs to send one ciphertext (one point) to the receiver, compared to two in the classic ECC. This means data transmitting time is less in the proposed algorithm compared to the transmitting time in the standard ECC. The NIST tests (approximate entropy, block frequency, etc) are calculated for different numbers of characters and the results show that the proposed algorithm passes all of these tests. In the security analysis, it was found that the proposed algorithm is secure against most of the common ECC attacks. Therefore, the proposed algorithm is secure and highly efficient in transmitting data.

The rest of the paper is organized as follows. The three-pass protocol and the elliptic curve cryptography are discussed in the materials and methods. Also in this section, the proposed algorithm and its mathematical proof are presented. In the section Results and Discussion, the proposed algorithm is discussed by giving a working example. Moreover, the NIST tests the randomness of the proposed method is provided for different numbers of characters. The Security Analysis is discussed in this section to show the security of the proposed algorithm. Finally, a conclusion of the paper is given in the section conclusion.

Materials and methods

Three-pass protocol (TPP)

Alice and Bob can communicate securely without exchanging the encryption keys over an insecure channel by using the TPP.[3] The TPP provides a sequence of three passes between the parties, for instance, Alice encrypts the data on the first pass by using her encrypting key and then sending the result to Bob. Bob uses his public key during the second pass to encrypt the received data and then sends back the resulting data to Alice. Alice then uses her private key on the third pass to decrypt the received data and then sends it back to Bob. Bob finally decrypts the received data by using his private key to get the original data. Therefore, this protocol provides secure communication between the parties.[3–5]

The elliptic curve cryptography

Some basic definitions and theorems need to be provided before discussing the processes of the EEC algorithm.

Definition 1: An EC is a curve presented by the equation

$$y^2 = x^3 + ax + b,$$

where $a,\ b \in \mathbb{R}$ and $4a^3 + 27b^2 \neq 0$.[14,18]

Definition 2: An EC over a prime field, F_p, is given by the equation

$$E_p\left(a,\ b\right) : y^2 \equiv \left(x^3 + ax + b\right)\ (\mathrm{mod}\, p).$$

where $a,\ b \in \mathbb{R}$ and $4a^3 + 27b^2 \not\equiv 0\,(\mathrm{mod}\, p)$.[14]

Theorem 1: *Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on the elliptic curve $E_p(a, b) : y^2 \equiv (x^3 + ax + b)(\mathrm{mod}\, p)$, then the addition of them,[14] is given by*

$$P + Q = \begin{cases} O_\infty, & \text{if } x_1 = x_2, y_1 = -y_2; \\ (x_3, y_3) & \text{otherwise.} \end{cases}$$

where, $\mathcal{O}_\infty$ is the point at infinity,

$$x_3 \equiv \left(\lambda^2 - x_1 - x_2\right)\ (\mathrm{mod}\, p)$$

$$y_3 \equiv \left(\lambda\left(x_1 - x_3\right) - y_1\right)\ (\mathrm{mod}\, p)$$

and

$$\lambda \equiv \begin{cases} \left(\frac{3x_1^2 + a}{2y_1}\right)(\mathrm{mod}\, p) & \text{if } P = Q; \\ \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(\mathrm{mod}\, p) & \text{if } P \neq Q. \end{cases}$$

Fig. 1 illustrates the adding and doubling geometrically of the points on an EC.

Theorem 2:[19] *Let $E_p(a,\ b)$ be an elliptic curve over a prime field F_p given by $y^2 \equiv (x^3 + ax + b)\ (\mathrm{mod}\, p)$.*

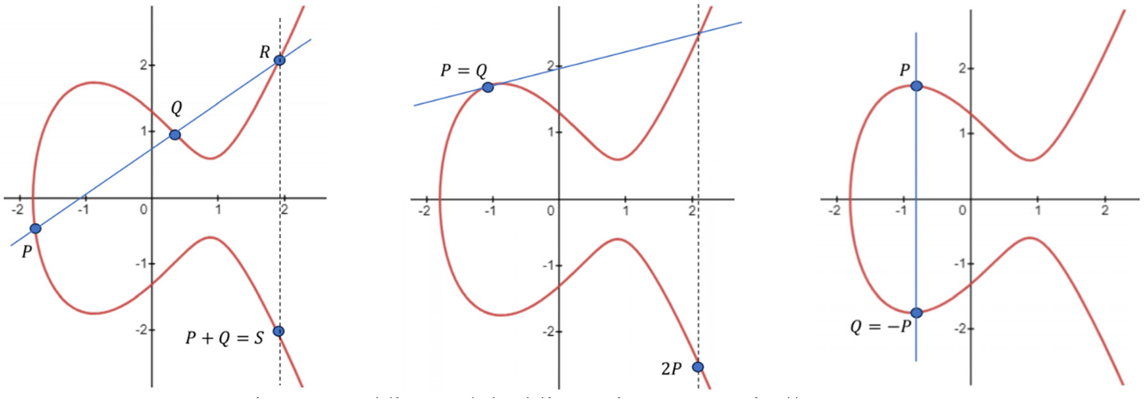


Fig. 1. Adding and doubling points geometrically on an EC.

Then, the number of points (including the point at infinity $\mathcal{O}_\infty$) on $E_p(a,\ b)$ is given by

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

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

Theorem 3 (Hasse Theorem[19]): $|\epsilon| \le 2\sqrt{p}$.

Therefore, from Theorem 2 and Theorem 3,

$$1 + p - 2\sqrt{p} \le \left|E_p\left(a,\ b\right)\right| \le 1 + p + 2\sqrt{p}.$$

Now, the EEC algorithm[9,10] over F_p is given below, such that, the sender (Alice) with the receiver (Bob) agree on choosing an EC equation

$$E_p\left(a,\ b\right): y^2 \equiv \left(x^3 + ax + b\right)\ (\mathrm{mod}\,p).$$

The key generation process

1. Bob chooses a point G of order n on $E_p(a,\ b)$.
2. Bob selects a random positive integer β, such that, $\beta < n$, then calculates the public key $B = \beta G$.
3. Bob publishes G and B, while β is the private key.

The encryption process

Suppose Alice wants to send the message M to Bob, then Alice converts M to points based on the agreed algorithm. Moreover, Alice chooses a random positive integer γ, and she calculates,

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

and

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

Then, E_1 and E_2, which are the ciphertexts, are sent to Bob.

The decryption process

After receiving E_1 and E_2, Bob performs the decryption process as follows

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

The proposed algorithm

Proposed algorithm methodology

In the proposed algorithm Alice and Bob agree on choosing an elliptic curve $E_p(a, b): y^2 \equiv (x^3 + ax + b)\ (\mathrm{mod}\,p)$.

Remark 1: The proposed algorithm can only be applied to the prime fields.

The construction of the agreed algorithm

Converting the plaintext to a numerical form is as follows:

1. Substituting $x_1 = 0$ in $E_p(a,\ b)$ to get y_1. That is, the first point on the $E_p(a,\ b)$ is $P_1 = P = (x_1, y_1)$.
2. By Theorem 1, P_1 is doubled as $P_2 = 2P = (x_1, y_1) + (x_1, y_1)$, which represents the second point on $E_p(a,\ b)$. In the same way, the rest of the points can be found.
3. The first point P_1 refers to the first letter "A" in the alphabet, the second point P_2 refers to the second letter, and so on.

Thus, the agreed algorithm consists of the doubled points on $E_p(a,\ b)$ and $\mathcal{O}_\infty$.

Key generation process

1. Alice and Bob respectively choose the points G_1 of order n_1 and G_2 of order n_2 on $E_p(a, b)$.
2. Alice selects a random positive integer α, such that, $\alpha < n_1$. Then, she calculates her public key $A = \alpha G_1$.
3. Bob selects a random positive integer β, such that, $\beta < n_2$. Then, he calculates his public key $B = \beta G_2$.

Note 1. Alice and Bob keep their public and private keys (A, α, B, and β) secret.

Encryption process

Based on the agreed algorithm, Alice converts the plaintext to corresponding points on $E_p(a, b)$. Alice chooses a random positive integer γ_1, then Alice calculates

$$E_1 = \gamma_1 G_1 \tag{4}$$

and

$$E_2 = M + \gamma_1 A \tag{5}$$

Alice performs the first pass by sending only E_2 to Bob.

After receiving the ciphertext E_2, Bob chooses a random positive integer γ_2. Then, Bob calculates

$$E_3 = \gamma_2 G_2 \tag{6}$$

and

$$E_4 = E_2 + \gamma_2 B \tag{7}$$

Then, Bob performs the second pass by sending only E_4 to Alice.

The decryption process

When E_4 is received, Alice decrypts E_4 by calculating M' as shown below.

$$M' = E_4 - \alpha E_1 \tag{8}$$

Then, the third pass is performed by Alice by sending M' to Bob.

Finally, Bob decrypts the received M' by the formula below to get the required plaintext.

$$M = M' - \beta E_3 \tag{9}$$

For more information see Fig. 2 and Fig. 3.

The mathematical proof of the proposed algorithm

Proposition 1: Let a and b be constants and $4a^3 + 27b^2 \not\equiv 0\,(\mathrm{mod}\,p)$. If $E_p(a,\ b) : y^2 \equiv (x^3 + ax + b)\ (\mathrm{mod}\,p)$ is an elliptic curve over a prime field F_p**,** then

$$M = M' - \beta E_3,$$

where M is the plaintext, M' is the Alice's decrypted transmitted ciphertext in the third pass, β is the Bob's private key, and E_3 is Bob's encrypted ciphertext.

Proof: From Eq. (8), then

$$M' - \beta E_3 = E_4 - \alpha E_1 - \beta E_3,$$

where E_1 is Alic's encrypted ciphertext, E_4 is Bob's encrypted transmitted ciphertext in the second pass, α is Alice's private keys. Then, from Eq. (7) and Eq. (6),

$$M' - \beta E_3 = E_2 + \gamma_2 B - \alpha E_1 - \beta\gamma_2 G_2,$$

where E_2 is Alice's encrypted transmitted ciphertext in the first pass, γ_2 is a random positive integer chosen by Bob, B is Bob's public key, and G_2 is a point on the $E_p(a,\ b)$ selected by Bob. Then, from Eq. (5) and Eq. (4),

$$M' - \beta E_3 = M + \gamma_1 A + \gamma_2 B - \alpha\gamma_1 G_1 - \beta\gamma_2 G_2$$

Since $A = \alpha G_1$, where G_1 is a point on the $E_p(a,\ b)$ selected by Alice, and $B = \beta G_2$ are the public keys of Alice and Bob respectively, then

$$\begin{aligned} M' - \beta E_3 &= M + \gamma_1 \alpha G_1 + \gamma_2 \beta G_2 - \gamma_1 \alpha G_1 \\ &\quad - \gamma_2 \beta G_2 = M. \end{aligned}$$

where, γ_1 is a random positive integer chosen by Alice.

Results and discussion

Practical example

In this section, the proposed algorithm is discussed in the example below.

Example 1: *Consider the elliptic curve* $E_{29}(8,\ 6) : y^2 \equiv x^3 + 8x + 6\ (\mathrm{mod}\,29)$*, then, the agreed algorithm is given as shown in Table 1.*

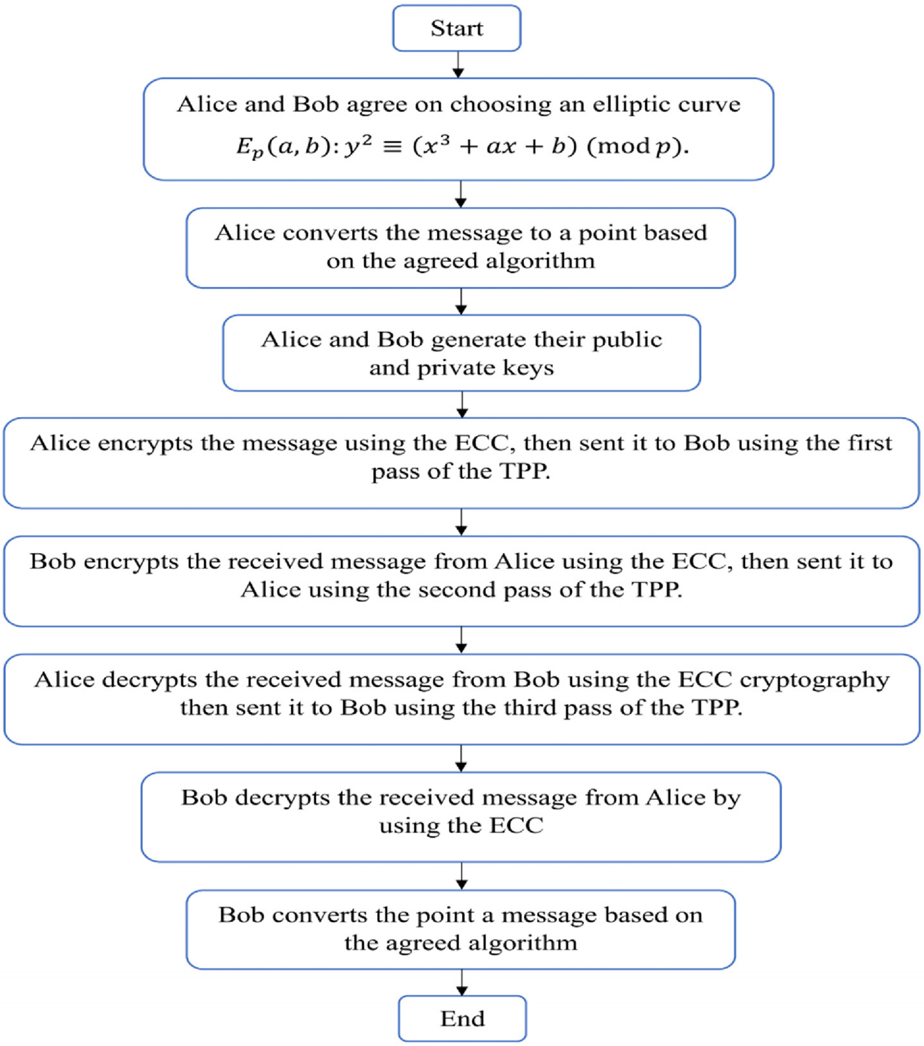

Start
Alice and Bob agree on choosing an elliptic curve $E_p(a,b): y^2 \equiv (x^3 + ax + b) \pmod p$.
Alice converts the message to a point based on the agreed algorithm
Alice and Bob generate their public and private keys
Alice encrypts the message using the ECC, then sent it to Bob using the first pass of the TPP.
Bob encrypts the received message from Alice using the ECC, then sent it to Alice using the second pass of the TPP.
Alice decrypts the received message from Bob using the ECC cryptography then sent it to Bob using the third pass of the TPP.
Bob decrypts the received message from Alice by using the ECC
Bob converts the point a message based on the agreed algorithm
End

Fig. 2. The main steps of the proposed algorithm in short.

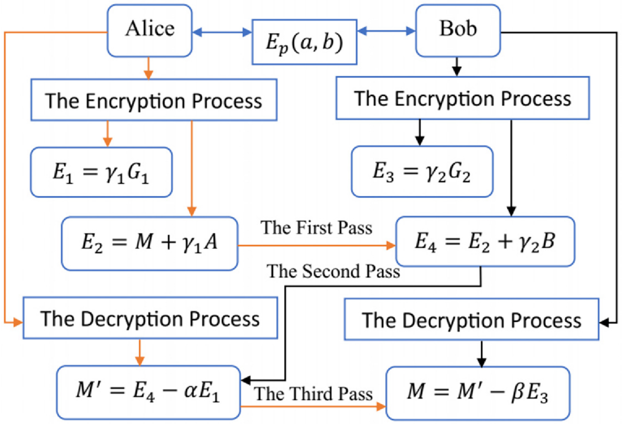


Fig. 3. The figure shows the proposed ECC algorithm.

Suppose that Alice chooses the point $G_1 = (11, 2)$ on $E_{29}(8,\ 6)$, and $\alpha = 5$, then

$$A = \alpha G_1 = 5\,(11, 2) = (3,\ 12)\,.$$

Bob chooses the point $G_2 = (9, 13)$ on $E_{29}(8,\ 6)$, and $\beta = 4$, then

$$B = \beta G_2 = 4\,(9, 13) = (17,\ 3)\,.$$

Suppose that Alice's message $M =$ "CRYPTOGRAPHY", then she selects $\gamma_1 = 3$. From the agreed algorithm "C" $= (13, 4)$, then by Eq. (4) Alice calculates

$$E_1 = \gamma_1 G_1 = 3\,(11, 2) = (0,\ 21)\,,$$

and by Eq. (5)

$$E_2 = M + \gamma_1 A = (13, 4) + 3\,(3,\ 12) = (13, 4) + (17,\ 26) = (22, 19)$$

Alice sends only $E_2 = (22, 19)$ to Bob.

Table 1. The agreed algorithm for the $E_{29}(8,6)$.

	A	B	C	D	E	F	G	H	I	J
$\mathcal{O}_\infty$	$(0,8)$	$(22,10)$	$(13,4)$	$(7,12)$	$(17,3)$	$(16,24)$	$(14,7)$	$(19,12)$	$(9,13)$	$(11,2)$
K	L	M	N	O	P	Q	R	S	T	U
$(2,1)$	$(3,17)$	$(6,3)$	$(10,10)$	$(26,10)$	$(26,19)$	$(10,19)$	$(6,26)$	$(3,12)$	$(2,28)$	$(11,27)$
V	W	X	Y	Z	1	2	3	4		
$(9,16)$	$(19,17)$	$(14,22)$	$(16,5)$	$(17,26)$	$(7,17)$	$(13,25)$	$(22,19)$	$(0,21)$		

Table 2. Encrypting and decrypting M by the proposed algorithm.

		Encryption by Alice (First Pass)			Encryption by Bob (Second Pass)			Decryption Alice (Third Pass)	Decryption Bob
The Letters	The Point	γ_1	E_1	E_2	γ_2	E_3	E_4	M'	M
C	$(13,4)$	3	$(0,21)$	$(22,19)$	7	$(0,8)$	$(22,10)$	$(14,7)$	$(13,4)$
R	$(6,26)$	10	$(14,7)$	$(9,16)$	5	$(10,10)$	$(26,19)$	$(3,17)$	$(6,26)$
Y	$(16,5)$	16	$(17,3)$	$(3,12)$	22	$(3,17)$	$(17,3)$	$(2,1)$	$(16,5)$
P	$(26,19)$	12	$(7,17)$	$(7,17)$	11	$(16,24)$	$(2,28)$	$(9,13)$	$(26,19)$
T	$(2,28)$	4	$(9,13)$	$(13,4)$	20	$(16,5)$	$(11,2)$	$(7,17)$	$(2,28)$
O	$(26,10)$	20	$(10,10)$	$(19,17)$	13	$(14,22)$	$(17,26)$	$(6,26)$	$(26,10)$
G	$(14,7)$	17	$(26,10)$	$(2,28)$	13	$(14,22)$	$(19,17)$	$(11,2)$	$(14,7)$
R	$(6,26)$	21	$(14,22)$	$(10,10)$	12	$(26,10)$	$(3,17)$	$(26,19)$	$(6,26)$
A	$(0,8)$	8	$(6,26)$	$(22,19)$	18	$(14,7)$	$(17,26)$	$(22,19)$	$(0,8)$
P	$(26,19)$	14	$(26,19)$	$(13,4)$	6	$(19,17)$	$(22,10)$	$(26,10)$	$(26,19)$
H	$(19,12)$	9	$(13,25)$	$(14,22)$	19	$(26,19)$	$(17,26)$	$(11,2)$	$(19,12)$
Y	$(16,5)$	13	$(16,24)$	$(14,22)$	17	$(22,19)$	$(26,19)$	$(10,19)$	$(16,5)$

Table 3. The NIST tests of the proposed algorithm.

		Test NIST										
#	Size File [KB]	APPROXIMATE ENTROPY	BLOCK FREQUENCY	CUMULATIVE SUMS	FFT	FREQUENCY	LEMPEL-ZIV COMPRESSION	LONGEST RUNS OF ONES	NONPERIODIC TEMPLATES	OVERLAPPING TEMPLATE OF ALL ONES T	RUNS TEST	SERIAL TEST
1	128	0.02385	0.502357	0.031457	0.64985	0.01685	0.78776	1	0.51155	1	0.66088	0.69306
2	225	0.3018	0.64985	0.34985	0.42435	0.48185	0.78821	1	0.02675	0.20645	0.85325	0.68272
3	512	0.0244	0.34985	0.77685	0.50645	0.05325	0.38124	1	0.30185	0.64985	0.34985	0.68124

When $E_2 = (22,19)$ is received, Bob selects $\gamma_2 = 7$, then by Eq. (6) he calculates

$$E_3 = \gamma_2 G_2 = 7\,(9,13) = (0,8)$$

and by Eq. (7)

$$E_4 = E_2 + \gamma_2 B = (22,19) + 7\,(17,3) = (22,19) + (7,12) = (22,10)\,.$$

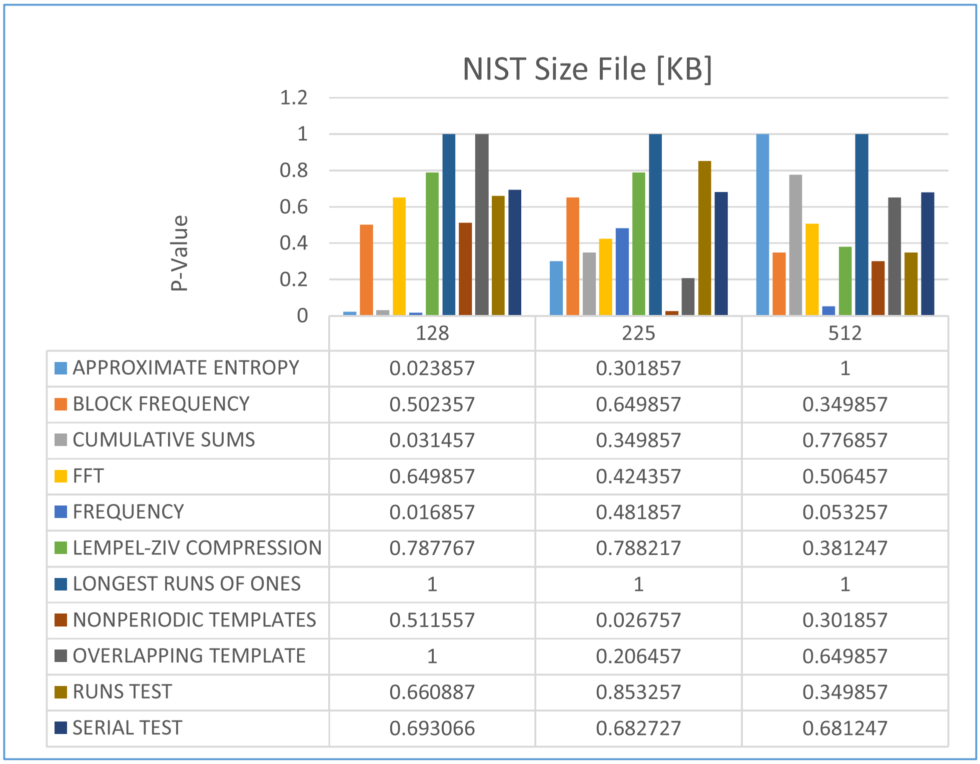
Then, Bob sends only $E_4 = (22,10)$ back to Alice. Alice now by Eq. (8) decrypts $E_4 = (22,10)$ as

$$\begin{aligned} M' &= E_4 - \alpha E_1 \\ &= (22,10) - 5\,(0,21) \\ &= (22,10) - (17,26) \\ &= (22,10) + (17,3) \\ \Rightarrow M' &= (14,7)\,. \end{aligned}$$

$$E_3 = \gamma_2 G_2 = 7\,(9,13) = (0,8)\,.$$

Alice sends $M' = (14,7)$ to Bob. Then, Bob uses by using Eq. (9) to decrypt $M' = (14,7)$ as below.

$$\begin{aligned} M' - \beta E_3 &= (14,7) - 4\,(0,8) \\ &= (14,7) - (7,12) \\ &= (14,7) + (7,17) \\ \Rightarrow M' - \beta E_3 &= (13,4)\,. \end{aligned}$$



	128	225	512
APPROXIMATE ENTROPY	0.023857	0.301857	1
BLOCK FREQUENCY	0.502357	0.649857	0.349857
CUMULATIVE SUMS	0.031457	0.349857	0.776857
FFT	0.649857	0.424357	0.506457
FREQUENCY	0.016857	0.481857	0.053257
LEMPEL-ZIV COMPRESSION	0.787767	0.788217	0.381247
LONGEST RUNS OF ONES	1	1	1
NONPERIODIC TEMPLATES	0.511557	0.026757	0.301857
OVERLAPPING TEMPLATE	1	0.206457	0.649857
RUNS TEST	0.660887	0.853257	0.349857
SERIAL TEST	0.693066	0.682727	0.681247

Fig. 4. The NIST tests of the proposed algorithm.

From Table 1, (13, 4) is the corresponding value of the letter "C". In the same way, the rest of M can be encoded and decoded, see Table 2.

Statistical tests analysis

Statistical tests [20] (NIST) are used to test the randomness of the quality of the outcome sequence of bits by noting that the value of the threshold of these tests is 0.01. That is, any value greater than 0.01 is accepted, while it is rejected if it is less than 0.01. In the NIST statistical tests, thirteen tests are applied to test the randomness of arbitrary length bits that are produced by pseudo-random number generators to assess the randomness of the proposed algorithm, see Table 3 and Figs. 4 to 6. All of the tests are applied and calculated by using a Python program.

The table and the figures above show that the proposed algorithm is better than the classic ECC to get highly secure data.

The security analysis

In this section, some attacking algorithms, [21] which might attack the proposed algorithm, are discussed.

1. Key Space Attack

The security of the encryption algorithms depends on the key size and the complexity of the encryption algorithm itself. Generally, when the encryption algorithm is known to the attackers, in this case, then a big encryption key size is used to make attacking the key impossible. That is, the EEC becomes harder to implement with a large encryption key.

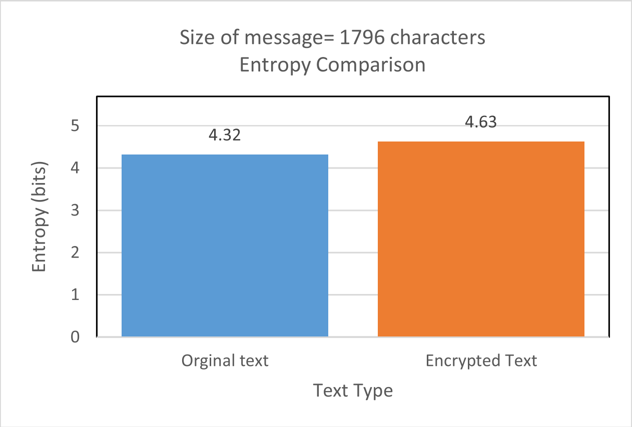


Fig. 5. The entropy test of the classic and proposed algorithms.

The security of the proposed algorithm depends on the complexity of the algorithm itself rather than using a big encryption key. Therefore, a suitable encryption key size can be used, and that leads to a fast encryption process. Moreover, the proposed algorithm depends on applying the TPP, that is, no key would be exchanged between Alice and Bob. As the

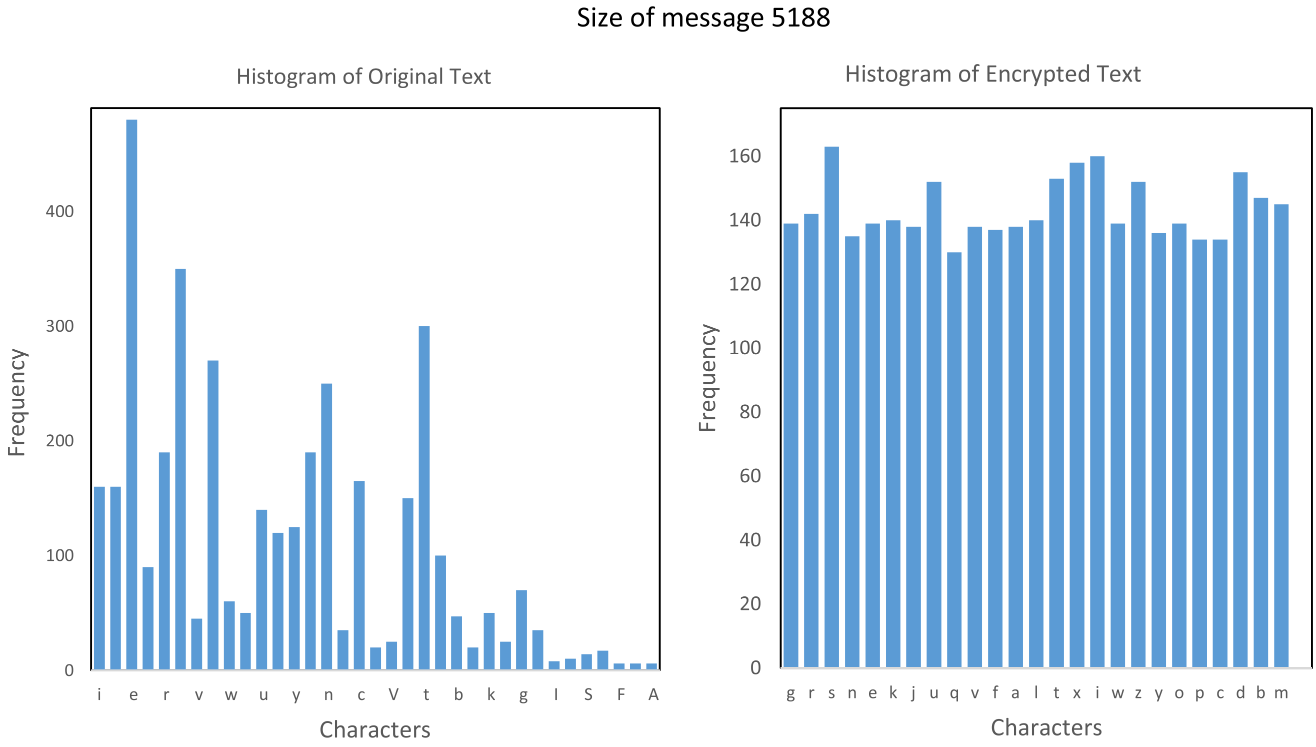


Fig. 6. The histogram of the class and the proposed algorithms.

Table 4. The complexity of the proposed algorithm for short texts.

n	Number of characters	The ECC	The proposed algorithm
1	10	26^{10}	26^{30}
2	20	26^{20}	26^{60}
3	30	26^{30}	26^{90}

proposed algorithm has three passes, then the general complexity of the proposed algorithm is calculated. As the number of alphabetical letters is 26 letters, then the general complexity of the standard ECC algorithm for a transmitted text consisting of 10 letters is 26^{10}, while it is 26^{30} of the proposed algorithm. That is, the complexity of the proposed algorithm for a text is 26^{3k}, where k is the length of the transmitted text, see Table 4 for different numbers of characters.

Thus, the common ECC attacking algorithms, for instance, the Baby Step Giant Step algorithm, Pollard's Rho Method, and the Pohlig-Hellman method cannot be applied to attack the proposed algorithm since there is no exchanging keys.

For the initial setting of the proposed algorithm for different values of p, see Table 5.

Ciphertext only attack

The attacker cannot recover the plaintext M even after knowing the encryption algorithm and the ciphertext because the only transmitted cipher from Alice to Bob is E_2, where $E_2 = M + \gamma_1 A$. That means, knowing M requires knowing all of α, γ_1 and G_1, which are all kept with Alice secretly.

Furthermore, the attacker cannot get M even after knowing the transmitted cipher E_4, which is the only transmitted cipher from Bob to Alice, where $E_4 = E_2 + \gamma_2 B$ because knowing M needs knowing α, γ_1, G_1 and β, γ_2, G_2 which are kept secretly with Alice and Bob respectively.

Also, even knowing the transmitted cipher M' from Alice to Bob, the attacker cannot get M because it needs to know all of $\alpha, \beta, G_1, G_2, \gamma_1$, and γ_2 which are impossible to be revealed.

2. Knowing plaintext attack

This attack is useless because assuming that even the attacker knows one or more of the pairs of the plaintext and the ciphertext still the values of α and β are independently different for the same message.

3. Brute force attack

The used key size in the proposed algorithm is greater than or equal to 128 bits. Using such a size of key provides a high level of security. In terms of security, a key of size 128 bits in the ECC is equivalent to a key of size 3072 bits in the RSA cryptosystem. A possible key of size 2^{128} makes the brute force impractical even with the advanced computers. Thus the proposed algorithm is secure against brute-force attackers.

Table 5. The initial setting of the proposed algorithm for different values of p.

p	Alice			Bob			Alice		Bob	
	α	G_1	A	β	G_2	B	E_1	E_2	E_3	E_4
29	28	(16,24)	(6,3)	6	(16,5)	(17,26)	(19,17)	(11,27)	(7,17)	(13,25)
97	37	(19,24)	(67,9)	29	(91,73)	(90,76)	(3,42)	(92,53)	(91,24)	(74,41)
997	845	(227,634)	(197,482)	579	(551,161)	(89,647)	(481,820)	(788,338)	(551,161)	(201,361)
1321	1279	(1145,1103)	(867,1294)	60	(833,975)	(989,126)	(1106,56)	(171,1142)	(1124,504)	(461,416)
1759	996	(1047,642)	(324,171)	421	(543,564)	(276,1720)	(1688,96)	(994,1314)	(1426,1554)	(932,957)

4. Shor's Algorithm

Shor's algorithm can break the ECC by calculating the Discrete Logarithm Problem (DLP) using a quantum computer. However, Shor's algorithm cannot be applied to the proposed algorithm because the proposed algorithm uses the TPP which means there is no exchanging of the keys in advance between the parties.

Conclusion

In the proposed algorithm, the only common information between the two parties is the EC equation, $E_p(a, b)$, that is, less public information is shared on the communication channels. The Diffe-Hellman and the TPP protocols are unauthenticated channels to send data because of the man-in-the-middle attack. Therefore, the data in the proposed algorithm is sent by an authenticated channel to prevent the data from being attacked. The transmitted data in the proposed algorithm is only one single point in each pass compared to two points in the standard ECC. This leads to a reduction in the transmitting time at each pass. Statistical tests (NIST) are used to test the randomness of the quality of the outcome sequence of bits. Table 3 shows that the proposed method is highly secure compared to the standard ECC algorithm. Moreover, Fig. 3 shows a high randomness of the proposed algorithm as the outcome sequence of different numbers of characters passes all of the randomness tests. The entropy test is provided, such that, for the text length of 1796 letters, the entropy of the original text is 4.32, and the entropy of the encrypted text is 4.63 as shown in Fig. 5. The histogram test is provided, such that, the uniform histogram shows the distribution of letters of the original text and the encrypted text as shown in Fig. 6. Because the proposed algorithm has three passes to encrypt and decrypt the text, then the general complexity of the proposed algorithm is 26^{3k}, where k is the length of the transmitted text, while it is only 26^k for the standard ECC algorithm. The security analysis of the proposed algorithm shows that it is secure against the common attacks on the standard ECC. Thus, the proposed algorithm provides high levels of security to the transmitted data, less size of transmitting data, and less transmitting time.

Acknowledgment

The authors would like to express their deep appreciation to the Department of Mathematics, College of Science, University of Diyala.

Authors' declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images that are not ours have been included with the necessary permission for republication, which is attached to the manuscript.
- No animal studies are present in the manuscript.
- No human studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at the University of Diyala.

Authors' contribution statement

R. Z. K. and H. B. H. contributed to the design, implementation, analysis, and writing of the study.

References

1. Easttom C. Modern Cryptography: Applied Mathematics for Encryption and Information Security. 2nd ed. Switzerland AG: Springer Cham; 2022 Oct 30. Chap 5, Essential Number Theory and Discrete Math. p. 75–107. https://doi.org/10.1007/978-3-031-12304-7_4
2. Peranginangin AP. Application of Number Theory in Cryptography. IJERE. 2024 Jan 15;3(1):67–76.
3. Rahim R, Zahri NA, Warip MN. Additional security using three-pass protocol and Pohlig-Hellman. IOP Conf Ser Mater Sci Eng. 2021 Feb 1;1088(1):1–5. https://doi.org/10.1088/1757-899X/1088/1/012046
4. Oktaviana B, Siahaan AU. Three-pass protocol implementation in caesar cipher classic cryptography. IOSR J Comput Eng. 2016;18(04):26–29. https://doi.org/10.9790/0661-1804032629

5. Sidik AP, Efendi S, Suherman S. Improving One-Time Pad Algorithm on Shamir's Three-Pass Protocol Scheme by Using RSA and ElGamal Algorithms. J Phys Conf Ser. 2019 Jun 1;1235(1):1–7. https://doi.org/10.1088/1742-6596/1235/1/012007
6. Faure E, Shcherba A, Lavdanskyi A, Makhynko M, Khizirova M. Three-Pass Protocol on Permutations: Implementation Example and Security. IEEE 2nd International Conference on Advanced Trends in Information Theory. 2024:110–125.
7. Mezher LS, Abbass AM. Mixed Hill Cipher methods with triple pass protocol methods. Int J Electr Comput Eng. 2021 Oct 1;11(5):4449–4457. http://doi.org/10.11591/ijece.v11i5.pp4449-4457
8. Qasim RA, Habib HB, Khalaf RZ. An implementation of three-pass protocol on a Paillier cryptosystem. AIP Conf Proc. 2024 Sep 19;3207(1):1–8. https://doi.org/10.1063/5.0234214
9. Miller VS. Advances in Cryptology: Proceedings of CRYPTO '85. 1st ed. Berlin, Heidelberg: Springer. 1985 Aug 18. 31, Use of elliptic curves in cryptography; 417–426. https://doi.org/10.1007/3-540-39799-X_31
10. Koblitz N. Elliptic curve cryptosystems. Math Comp. 1987;48(177):203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5
11. Ullah S, Zheng J, Din N, Hussain MT, Ullah F, Yousaf M. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. Comput Sci Rev. 2023 Feb 1;47:100530. https://doi.org/10.1016/j.cosrev.2022.100530
12. Lara-Nino CA, Diaz-Perez A, Morales-Sandoval M. Lightweight elliptic curve cryptography accelerator for internet of things applications. Ad Hoc Networks. 2020 Jun 1;103:102159. https://doi.org/10.1016/j.adhoc.2020.102159
13. Vincent OR, Okediran TM, Abayomi-Alli AA, Adeniran OJ. An identity-based elliptic curve cryptography for mobile payment security. SN Comput Sci. 2020 Mar;1(112):1–12. https://doi.org/10.1007/s42979-020-00122-1
14. Ramasamy P, Ranganathan V, Palanisamy V, Kadry S. Securing one-time password generation using elliptic-curve cryptography with self-portrait photograph for mobile commerce application. Multimed Tools Appl. 2020 Jun;79(23):17081–17099. https://doi.org/10.1007/s11042-019-7615-3
15. Obaid ZK, Al Saffar NF. Image encryption based on elliptic curve cryptosystem. Int J Electr Comput Eng (IJECE). 2021 Apr 1;11(2):1293–1302. http://doi.org/10.11591/ijece.v11i2.pp1293-1302
16. Parida P, Pradhan C, Gao XZ, Roy DS, Barik RK. Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. IEEE Access. 2021 Apr 9;9:76191–76204. https://doi.org/10.1109/ACCESS.2021.3072075
17. Abdaoui A, Erbad A, Al-Ali AK, Mohamed A, Guizani M. Fuzzy elliptic curve cryptography for authentication in Internet of Things. IEEE Internet Things J. 2021 Oct 19;9(12):9987–9998. https://doi.org/10.1109/JIOT.2021.3121350
18. Namous SH, Habib HB, Khalaf RZ. Constructing a Cryptosystem Algorithm by Applying the Rosenberg-Strong Pairing Function on the Elliptic Curve Cryptography. BIO Web Conf. 2024;97:1–10. https://doi.org/10.1051/bioconf/20249700168
19. Yan SY. Computational number theory and modern cryptography. USA: John Wiley & Sons; 2013 Jan 29.
20. Sulak F, Doğanaksoy A, Uğuz M, Koçak O. Periodic template tests: A family of statistical randomness tests for a collection of binary sequences. Discrete Appl Math. 2019 Dec 1;271:191–204. https://doi.org/10.1016/j.dam.2019.07.022
21. Vasundhara S. The advantages of elliptic curve cryptography for security. Global Journal of Pure and Applied Mathematics (GJPAM). 2017;13(9):4995–5011.

خوارزمية تشفير مقترحة تعتمد على استخدام بروتوكول التمريرات الثلاثة وتشفير المنحني الإهليلجي

رفعت زيدان خلف، حمزة بركات حبيب

قسم علوم الرياضيات، كلية العلوم، جامعة ديالى، ديالى، العراق.

الملخص

أصبح الإنترنت مؤخرا جزءا لا يتجزأ من أنماط حياة الناس حيث أن له تأثير واضح على جوانب مختلفة من حياتهم اليومية، بما في ذلك التعليم ,التواصل, والى اخره. ونتيجة الى ذلك فقد ازادت الحاجة إلى خوارزميات تشفير فعالة وسريعة. في هذا البحث، قمنا بتقديم خوارزمية تشفير جديدة تعتمد على استخدام بروتوكول التمريرات الثلاثة (TPP) الموثوق وخوارزمية تشفير المنحنى الإهليلجي (ECC). حيث أنه في الخوارزمية المقترحة، يتم استخدام خوارزمية ECC لتشفير وفك تشفير البيانات (نص ذو حجم 128 بت) في حين يتم استخدام بروتوكول TPP لنقل هذه البيانات عبر قنوات الأتصال من دون الحاجة الى مشاركة المفاتيح بين الطرفين. في ECC الأعتيادية، يحتاج المستلم إلى نشر معادلة المنحني الهليجي (EC)، والنقطة الأولية، والمفتاح العام، في حين أن المعلومات المنشورة الوحيدة في الخوارزمية المقترحة هي معادلة EC فقط. كذلك فأنه في خوارزمية ECC الأعتيادية يتم إرسال نصين مشفرين بينما يتم إرسال نص مشفر واحد فقط في الخوارزمية المقترحة في كل تمريرة مما يؤدي إلى تقليل وقت نقل البيانات في الخوارزمية المقترحة. كما تم اثبات عمل الخوارزمية المقترحة رياضيا من خلال تقديم قضية جديدة وبرهانها. كذلك تم حساب اختبارات NIST، مثلا الإنتروبيا التقريبية، وتردد الكتلة، وهكذا, الى جانب اختبارات النتروبيا و histogram لإظهار فعالية الطريقة المقترحة. المفتاح المستخدم في الخوارزمية المقترحة هو أكبر من أو يساوي 128 بت حتى تكون الخوارزمية فعالة ضد الهجمات. يوضح التحليل الأمني للخوارزمية المقترحة أن الخوارزمية آمنة ضد العديد من خوارزميات المهاجمة الشائعة. لذلك فإن الخوارزمية المقترحة آمنة, سريعة وفعالة في نقل البيانات.

الكلمات المفتاحية: التشفير، المنحني الإهليلجي، تشفير المنحنى الإهليلجي، نظرية الأعداد، بروتوكول التمريرات الثلاثة.