A NEW CRYPTOSYSTEM FOR ENCRYPTION AND DECRYPTION USING ELLIPITIC CURVES IN CRYPTOGRAPHY OVER FINITE FIELDS

[1]MOHAMMED RAFIQ NAMIQ, [2]WRYA K. KADIR, [3]ARAM M. AHMED

[1]Department of Mathematics, College of Science, University of Sulaimani, Sulaymaniyah, Iraq.
[2]Department of Mathematics, College of Science, University of Sulaimani, Iraq.
[2]Information Technology Department, College of Science and Technology, University of Human Development, Iraq.
[3]Kurdistan Institution for Strategic Studies and Scientific Research, Department of Information Technology.
[3]Computer Science institute, Sulaimani Polytechnic University.
E-mail: [1]mohammed.namiq@univsul.edu.iq, [2]wrya.kadir@univsul.edu.iq[1], wrya.kadir@uhd.edu.iq[2], [3]aramahmed@kissr.edu.krd , [3]aram.ahmed@spu.edu.iq

ABSTRACT

This paper considers the use of cryptography with elliptic curves. It is presented and defined a new cryptosystem algorithm for encryption and decryption using elliptic curves with more than one secret and public keys. Furthermore, it is described the mathematical concepts related to elliptic curves, particularly the discrete logarithm problem on elliptic curves. A description of the Diffie-Hellman algorithm on elliptic curves and elliptic curve encryption algorithm with the recipients' public keys are represented.

Keywords: *Cryptography, Public-Key Cryptography, Computer Security, Algebraic Geometry, Elliptic Curves, And Finite Fields.*

1. INTRODUCTION

The birth of cryptography and the art of hiding messages date back to ancient times. The encryption, after having played several different roles according to historical events, is today indispensable, for example, in commercial and private sectors. With the spread of the network and electronic commerce, symmetric encryption was not satisfactory as there was a major issue with the key exchanges that had to remain secret in order to maintain the security of the encryption methods. To solve this issue, the first public- key cryptosystem was introduced by Diffie and Hellman in 1976 [1]. Then, in 1978, R.Rivest, A.Shamir and L.Adleman created the first public-key cryptosystem for encryption and digital signatures; known as RSA [2]. After that time, the introduction of encryption algorithms based on elliptic curves cryptography (ECC) were, independently, suggested and then invented in 1985 by Miller [3] and Koblitz in 1986 [4]. The ECC is relatively recent, however, in the last twenty years this technique has rapidly established itself as an alternative to public-key cryptographic systems, which were already widely used as RSA and digital signature standard (DSS) [5]. Furthermore, the main attraction of ECC is that elliptic curves over finite fields deliver an inexhaustible source of finite abelian groups [6], which (even if they are large) are convenient for computation and have a rich structure [7]. At this moment, there are no sufficiently fast algorithms that can solve the mathematical problems in which are based on elliptic curve discrete logarithm problems (ECDLP). Moreover, ECC offers the same degree of safety of traditional systems, such as RSA, DSA and Diffie-Hellman, by using a smaller key size [8,9]. The more general equation of an elliptic curve defined over a field K is an algebraic curve formed from the left is conic and on the right is cubic:

$$y^2+\alpha_1x^2+\alpha_2xy+\alpha_3y+\alpha_4x+\alpha_5=x^3+\beta_1x^2+\beta_2x+\beta_3$$

where α_i, β_i are constants, we can then combine the constant and linear terms to form what is known as the generalized Weierstrass equation [10]:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with a_1, a_2, a_3, a_4 and a_6 are constants, the field K can be the set of real, complex, but also any other field, for example, in encryption the finite fields are usually used. The curve must be smooth or *non-singular*, that is, the gradient (discriminant) must be different from zero for each pair of values $(x, y) \in K\times K$. In the definition of the elliptic curve, there is also a single element denoted by O_∞, where $O_\infty = (0,1,0)$, and called the point at infinity; the name is derived from projective geometry, which has fundamental importance. Moreover, an elliptic curve over a field K in the form of non-homogeneous coordinates is defined as follows:

$$E(K) := \{(x,y) \in K\times K: y^2 + a_1xy + a_3y\text{-}x^3\text{-}a_2x^2\text{-}a_4x\text{-}a_6 = 0\} \cup \{O_\infty\}.$$

In the present paper for the purpose of the encryption and decryption using elliptic curves, it is considered the equation:

$$E: y^2 = x^3 + bx + c$$

This curve is symmetric about the x-axis since for each value of x, there are a positive and negative values of y.

In addition, the ECC is asymmetric key cryptography, this is because two different keys are used: public and private, where the knowledge of the public key cannot determine the private key. From 1986 till now, a lot of research has been done to have efficient and secure implementations of these cryptographic schemes. In this paper, it is allowed each user to generate two private keys and three public keys to offer a stronger key to encryption and decryption.

2. THE STRUCTURE OF POINTS ON ELLIPITIC CURVES

Let E be a non-singular elliptic curve over field K, with char $K \neq 2,3$ [10], and be given by:

$$E(K): y^2 = x^3 + bx + c$$

with the discriminant:

$$\Delta = -16(4b^3 + 27c^2)$$

and j-invariant:

$$j(E) = 1728\frac{4b^3}{4b^3 + 27c^2}$$

The addition operation, +, can be defined over elliptic curves in order to obtain an abelian group $(E(K), +)$. This operation of addition is also called chord-and-tangent rule for its geometric interpretation. The addition operation that defined in an abelian group has the following properties:

1) Associativity. If $P, Q, R \in E(K)$, then $P + (Q + R) = (P + Q) + R$.
2) Identity. The point at infinity O_∞ is the identity element of the group, that is, $O_\infty = \text{-}O_\infty$ and for all $P \in E(K)$ we have that $P + O_\infty = O_\infty + P = P$.
3) Inverses. If $P \neq O_\infty$ then $\text{-}P$ is the only other point on the curve E with x-coordinate equal to P and $P + (\text{-}P) = (\text{-}P) + P = O_\infty$.
4) Commutativity. If $P, Q \in E(K)$, then $P + Q = Q + P$.

The group structure of points of elliptic curves over a field can be defined as follows:

2.1 Modular Arithmetic

For a positive integer n, two integers a and b are called congruent modulo n (or a is congruent to b modulo n), if a and b have the same remainder when divided by n (or equivalently if $a\text{-}b$ is divisible by n, $n|(a\text{-}b)$) [11]. It can be expressed as $a \equiv b \bmod n$, where n is called the modulus. That means

$$\equiv \bmod n := \{(a,b): n|(a\text{-}b)\}.$$

2.2 Addition and Inverse Formulas on Elliptic Curves

Consider the points $P, Q, R \in E(K)$ with coordinates $(x_1, y_1), (x_2, y_2)$ and (x_3, y_3), respectively [12] and where

$$f(x,y) = y^2\text{-}x^3\text{-}bx\text{-}c,$$

then

1) Inverse of a point. The negative of the point $P = (x_1, y_1)$ is defined to be $-P = (x_1, \text{-}y_1)$.
2) Addition of points. The operation of addition of points is defined on the curve E by $R = P + Q$. There are two cases:
   a) If $P \neq \pm Q$, then:

$$\text{Slpoe} = m := \frac{y_2\text{-}y_1}{x_2\text{-}x_1}$$

$$x_3 = m^2\text{-}x_1\text{-}x_2$$

$$y_3 = m(x_1\text{-}x_2)\text{-}y_1$$

b) If $P = Q$, point doubling, $P + P = 2P$:

$$m = \frac{dy}{dx}|_P = \text{-}\frac{\frac{\partial f}{\partial x}}{\frac{\partial f}{\partial y}}|_P = \frac{3x_1^2 + b}{2y_1}$$

$$x_3 = m^2\text{-}2x_1$$

$$y_3 = m(x_1\text{-}x_2)\text{-}y_1$$

2.3 Elliptic Curve Scalar Multiplication

Let k be an integer and P be a point on an elliptic curve E defined over a field $\mathbb{F}_q$. In an abelian group, the multiplication is defined by the scalar integer k, as it may be considered as the sum of the point P of the curve in all k times, defined as follows:

$$Q := \begin{cases} [k]P = \underbrace{P + P + \cdots + P}_{k\text{-times}}, & \text{if } k > 0 \\ [k]P = O_\infty, & \text{if } k = 0 \\ [\text{-}k]P = \underbrace{(\text{-}P) + (\text{-}P) + \cdots + (\text{-}P)}_{|k|\text{-times}}, & \text{if } k < 0 \end{cases}$$

2.4 Discrete Logarithm Problem Using ECC (DLPEC)

Given a curve E on a finite field $\mathbb{F}_q$, we can represent the main operation called scalar multiplication in ECC as follows:

$$Q = [k]P,$$

where P and Q are points on ECC. That means, the problem of finding the smallest positive integer $k, 1 \leq k \leq n - 1$, given the points P and Q.

3. ELLIPITIC CURVES DEFFIE-HELLMAN KEY EXCHANGE

The first encryption algorithms based on elliptic curves were, independently, purposed by Miller in 1985 and Koblitz in 1986 [3,4]. They did not in fact propose new algorithms, but applied the existing ones on the additive group formed by the points of an elliptic curve over a finite field. In this protocol, the two parties, Alice and Bob, want to share a secret key.

First of all, they openly select a prime number q, $q \approx 2^{180}$, and choose an elliptic curve E over a finite field $\mathbb{F}_q$. The key is based on a random point K on the elliptic curve E. If they have the random point K, then, for example, it gives the x-coordinate of the random element of $\mathbb{F}_q$, which can then be converted into an m-bit integer in the p-ary number system where $q = p^m$, and this number can be the key in their cryptosystem. They should choose the point K, so that all of their messages to each other are open and so no one but the two of them would know anything about K.

Secondly, Alice and Bob, openly choose a point $B \in E(\mathbb{F}_q)$ as the base, B plays the same role as a generator g in the Diffie-Hellman algorithm for finite fields. However, it is not required that B is a generator of the group of points of E, in this protocol. This group may not be cyclic. Even whether it is cyclic group or not, time should not be wasted checking that B is a generator element, or even finding the total number of points on E that will not be needed in the future.

To generate a key Alice and Bob perform the following scheme:

1) Alice chooses an integer s_A, $1 \leq s_A \leq n\text{-}1$. This number is Alice's private key and must be kept in secret. Then Alice calculates her public key $P_A = [s_A]B$. The public key is a point in the group of points on the elliptic curve.
2) Similarly, Bob selects a private key s_B, $1 \leq s_B \leq n\text{-}1$, and calculates his public key $P_B = [s_B]B$.
3) Alice and Bob share their public keys publicity over unsecured channel.
4) Alice calculates the secret key $K = [s_A]P_B$, and Bob calculates the secret key $K = [s_B]P_A$.

The last two expressions give the same result, because:

$$[s_A]P_B = [s_A]([s_B]B) = [s_B]([s_A]B) = [s_B]P_A.$$

In addition, to solving the discrete logarithm problem, an attacker, Eve, has to find s_A from B and $[s_A]B$ or s_B from B and $[s_B]B$. There seems to be no way to find $K = [s_A s_B]B$, knowing only $B, [s_A]B$ and $[s_B]B$. Moreover, the Diffie-Hellman key exchange is not protected from the enemy Eve, who has access to the communication channel and it can be forwarded to substitute points P_A and P_B to her point $P_E = [s_E]B$. Therefore, Eve can either act on behalf of one of the users by setting a secret relationship with another, or by controlling the channel, to be a translator of their correspondence, through free decoding and reading all the posts; such an active cryptanalyst called man in the middle. Protecting against eavesdropping and forgery is an extremely important task of authenticating users.

4. THE TWO SECRET KEYS CRYPTOSYSTEM ON ELLIPTIC CURVES

Now, we are going to describe the new cryptosystem, which adapts to use with elliptic curves. Suppose Alice wants to send a secret message to Bob. Alice and Bob choose an elliptic curve E, defined over a finite field $\mathbb{F}_q$, so that the discrete logarithm problem is difficult to solve when using $E(\mathbb{F}_q)$. First, Bob makes the public keys as follows:

1) He selects the points A as a secret point and B as a base point on E such that the order of B is a large prime number.
2) He chooses two secret integers s_B and s_{B_1} such that $1 \leq s_B, s_{B_1} \leq n$-1.
3) He computes
$$P_B = [s_B]B$$
$$P_{B_1} = [s_{B_1}]A$$
$$P_{B_2} = [s_{B_1}](P_{B_1} + P_B)$$
with P_B, P_{B_1} and P_{B_2} being Bob's public keys and s_B and s_{B_1} being Bob's secret (privates) keys.
4) He sends B, P_B, P_{B_1} and P_{B_2} to Alice.

To send the message, Alice proceed as follows:

1) She obtains Bob's public keys.
2) She encodes the message into a point $M \in E(\mathbb{F}_q)$.
3) She chooses two secret integers s_A and s_{A_1} such that $1 \leq s_A, s_{A_1} \leq n$-1, and computes
$$P_A = [s_A]B$$
$$P_{A_1} = [s_{A_1}]P_B$$
$$P_{A_2} = [s_{A_1}]P_{B_1}$$
$$K = [s_A]P_B$$
$$K_A = [s_{A_1}]P_{B_2} + K$$
4) She sends P_A, P_{A_1} and P_{A_2} to Bob.

After received the Alice's information, Bob calculates his keys

$$K = [s_B]P_A$$

$$K_B = [s_{B_1}](\text{-}P_{A_2} + (\text{-}P_{A_1})) + (\text{-}K)$$

Then to encrypt the message M, Alice computes:

$$E = M + K_A$$

To decrypt the message M, Bob calculates:

$$M = E + K_B$$

Note. It is important that each time Alice uses, she sends the encrypted message to Bob by using Bobs public key, a different private key s_A or s_{A_1}. In fact, if she uses the same private keys s_A and s_{A_1} keys for two different messages M and M', then an attacker who captured the two coded messages will notice and be able to calculate:

$$M\text{-}M' = M + K_A\text{-}M'\text{-}K_A = E\text{-}E'.$$

Suppose that for some reason the message M was made public as soon as the information was no longer valid, then the attacker could easily calculate M', which would be $M\text{-}E + E'$.

4.1 Example

Consider the elliptic curve E over a finite field $\mathbb{F}_{73}$ described by the equation

$$E(\mathbb{F}_{73}): y^2 = x^3 + 5x - 12$$

The number of points on E are the following:

Table 1: Points of the Elliptic Curve E.

(0,34)	(0,39)	(1,33)	(1,40)	(2,15)
(2,58)	(4,27)	(4,46)	(5,24)	(5,49)
(7,1)	(7,72)	(9,18)	(9,55)	(10,4)
(10,69)	(12,30)	(12,43)	(16,21)	(16,52)
(18,17)	(18,56)	(23,15)	(23,58)	(27,13)
(27,60)	(29,33)	(29,40)	(30,36)	(30,37)
(31,2)	(31,71)	(35,25)	(35,48)	(37,23)
(37,50)	(38,9)	(38,64)	(43,33)	(43,40)
(44,36)	(44,37)	(48,15)	(48,58)	(53,8)
(53,65)	(56,10)	(56,63)	(57,22)	(57,51)
(61,5)	(61,68)	(66,11)	(66,62)	(68,35)
(68,38)	(69,14)	(69,59)	(70,26)	(70,47)

(72,36)	(72,37)	O_∞

Thus, the number points on E over $\mathbb{F}_{73}$, $\#E_{73} = 63$. The order of group $(E,+)$, the number of points on E, is $\#E = 63$. Where

$$\Delta = -16(4b^3 + 27c^2) = -70208 \equiv 18 \bmod 73,$$

$$j(E) = 1728\frac{4b^3}{4b^3+27c^2} = \frac{864000}{4388} \equiv 33 \bmod 73.$$

Let us apply our new Cryptosystem.

1) Bob selects two points on E, say $A = (27,13)$ and $B = (2,15)$ as a base point such that the order of B is a large prime number.
2) He chooses two secret random integers $s_B = 37$ and $s_{B_1} = 19$, which are in the interval $[1,62]$, since $[63](2,15) = O_\infty$.
3) He computes
   $P_B = [37](2,15) = (7,1)$
   $P_{B_1} = [19](27,13) = (9,18)$
   $P_{B_2} = [19]((9,18) + (7,1)) = (16,52)$
4) He sends B, P_B, P_{B_1} and P_{B_2} to Alice.

To send the message, Alice proceed as follows:

1) She obtains Bob's public keys.
2) She chooses two secret integers, say $s_A = 23$ and $s_{A_1} = 53$, which are in the interval $[1,62]$ and computes
   $P_A = [23](2,15) = (27,13)$
   $P_{A_1} = [53](7,1) = (61,68)$
   $P_{A_2} = [53](9,18) = (27,60)$
   $K = [23](7,1) = (31,71)$
   $K_A = [53](16,52) + (31,71) = (2,58)$
3) She sends P_A, P_{A_1} and P_{A_2} to Bob.

After received the Alice's information, Bob calculates his keys

$$K = [37](27,13) = (31,71)$$

$$K_B = [19]((27,-60) + (31,71)) = (2,15)$$

If Alice wants to send the message **Go Back** to Bob, Alice must convert all the text characters of the message into the points on the elliptic curves using the agreed upon code table. Now, let names the points on E as follows:

Table 2: Code Table of the Points of the Elliptic Curve E.

(0,34)	(0,39)	(1,33)	(1,40)	(2,15)
A	B	C	D	E
(2,58)	(4,27)	(4,46)	(5,24)	(5,49)
F	G	H	I	G
(7,1)	(7,72)	(9,18)	(9,55)	(10,4)
K	L	M	N	O
(10,69)	(12,30)	(12,43)	(16,21)	(16,52)
P	Q	R	S	T
(18,17)	(18,56)	(23,15)	(23,58)	(27,13)
U	V	W	X	Y
(27,60)	(29,33)	(29,40)	(30,36)	(30,37)
Z	a	b	c	d
(31,2)	(31,71)	(35,25)	(35,48)	(37,23)
e	f	g	h	i
(37,50)	(38,9)	(38,64)	(43,33)	(43,40)
j	k	l	m	n
(44,36)	(44,37)	(48,15)	(48,58)	(53,8)
o	p	q	r	s
(53,65)	(56,10)	(56,63)	(57,22)	(57,51)
t	u	v	w	x
(61,5)	(61,68)	(66,11)	(66,62)	(68,35)
y	z	0	1	2
(68,38)	(69,14)	(69,59)	(70,26)	(70,47)
3	4	5	6	7
(72,36)	(72,37)	O_∞		
8	9	space		

To encrypt the massage Alice uses the new cryptosystem. Also, she uses code table (2) to converts the plain text into the points on E, which are $(4,27),(10,4),O_\infty,(0,39),(29,33),(30,36),$ and $(38,9)$, respectively. Then she processes as follows:

- The first letter G corresponds to the point (4,27) in the code table (2).

$$E = (4,27) + (2,58) = (70,47) = 7$$

- the letter O corresponds to the point (10, 4).

$$E = (10,4) + (2,58) = (29,33 \ = \mathrm{a}$$

- the space = O_∞.

$$E = O\_\infty + (2,58) = (2,58) = \mathrm{F}$$

- the letter B = (0, 39).

$$E = (0,39) + (2,58) = (70,26) = 6$$

- the character a = (29, 33).

$$E = (29,33) + (2,58) = (1,33) = \mathrm{C}$$

- the letter c = (30, 36).

$$E = (30,36) + (2,58) = (4,27) = \mathrm{G}$$

- the character k = (38, 9).

$$E = (38,9) + (2,58) = (1,40) = \mathrm{D}$$

Alice sends the encrypted massages **7aF6CGD** to Bob. After Bob received the cipher text 7aF6CGD, he converts the cipher characters into the points on E, (70,47), (29,33), (2,58), (70,26), (1,33), (4,27), and (1,40), respectively, using the code table (2), and decrypts the messages as follows:

- The letter $7 = (70,47)$, to decrypt

$$M = (70,47) + (2,15) = (4,27) = \mathrm{G}$$

- the character a = (29, 33).

$$M = (29,33) + (2,15) = (10,4) = \mathrm{o}$$

- the character F = (2, 58).

$$M = (2,58) + (2,15) = O_\infty = \text{space}$$

- the letter 6 = (70, 26).

$$M = (70,26) + (2,15) = (0,39) = \mathrm{B}$$

- the letter C = (1, 33).

$$M = (1,33) + (2,15) = (29,33) = \mathrm{a}$$

- the letter G = (4, 27).

$$M = (4,27) + (2,15) = (30,36) = \mathrm{c}$$

- the letter D = (1, 40).

$$M = (1,40) + (2,15) = (38,9) = \mathrm{k}$$

The original massage is **Go Back**.

5. CONCLUSION

In recent decades, elliptic curve cryptography has become increasingly important, becoming part of industry standards. Elliptic curve cryptography appears as an alternative to traditional public key cryptosystems like RSA and ElGamal. The main advantage of elliptic curve cryptography is the ability to create smaller keys, thereby reducing storage requirements and transmission. One based on elliptic curve cryptography key can give the same level of security with 256-bit key as an RSA algorithm with a 2048-bit key. This article briefly describes the application of elliptic curves for asymmetric key encryption system. That is, using two secret keys to produce the encryption and decryption keys offer a greater difficulty for the discrete logarithm problem compared to the commonly used techniques of factorization of large numbers, Diffie-Hellman system or elliptic curves Diffie-Hellman key exchange. In addition, for the attacker Eve who knows one of private key cannot recover the massage because she needs the second private key for this purpose. As a result, the reliability of such cryptosystems depends heavily on the progress made in solving the discrete logarithm problems.

REFRENCES:

[1] W. Diffie and M. E. Hellman, “New directions in cryptography”, IEEE transactions on Information Theory, Vol 22, No. 6, 1976, pp. 644–654.

[2] R. L. Rivest, A. Shamir and L. Adleman, “A Method for Obtaining Digital Signatures and Public-key Cryptosystems”, ACM, Vol. 21, No. 2, 1978, pp. 120–126.

[3] V. S. Miller, “Use of elliptic curves in cryptography” *Conference on the Theory and Application of Cryptographic Techniques*, Springer, 1985, pp. 417–426.

[4] N. Koblitz, “Elliptic curve cryptosystems” Mathematics of computation, Vol. 48, No. 177, 1987, pp. 203–209.

[5] FIPS 186, “Digital signature standard” Federal Information Processing Standards Publication 186, U.S. Dept. of Commerce/National Institute of Standards and Technology, 1994.

[6] R. Schoof, “Elliptic curves over finite fields and the computation of square roots mod p”, Mathematics of computation, Vol. 44, No. 170, 1985, pp. 483–494.

[7] R. Schoof, “Counting points on elliptic curves over finite fields”, Journal de theorie des nombres de Bordeaux, Vlo. 7, No. 1, 1995, pp. 219–254.

[8] G. Harper, A. Menezes and S. Vanstone, “Public-key cryptosystems with very small key lengths”, *Work- shop on the Theory and Application of of Cryptographic Techniques*, Springer, 1992, pp. 163–173.

[9] L. C. Washington, “Elliptic curves: number theory and cryptography”, *Discrete mathematics and its applications*, Taylor and Francis Group, LLC and CRC press, Vol. 20, 2008.

[10] J. H. Silverman, “The arithmetic of elliptic curves” *Graduate Texts in Mathematics 106*, Springer Science & Business Media, 2009, pp. 47–55.

[11] R. Lidl and H. Niederreiter, “Finite fields” *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Vol. 20, 1997.

[12] J. H. Silverman and J. T. Tate, “Rational points on elliptic curves”, *Undergraduate Texts in Mathematics*, Springer 2nd, 1992, pp. 117–202.

[13] W. K. Kadir, O. H. Ahmed and M. R. Namiq. “A New Text Encryption Technique on Elliptic Curve Cryptography”, *Journal of Engineering and Applied Sciences,* 2017, vol. 12:pp.3329-3333.