The KR –Elliptic Curve Public Key Cryptosystem

Karrar Taher R. Aljamaly and Ruma Kareem K. Ajeena

Mathematics Department, Education College for Pure Sciences, University of Babylon, Iraq

E-mail: ruma.usm@gmail.com

Abstract. The connection between some fundamental mathematical problems in number theory with cryptography has been done in this work. A new version of the elliptic curve public key cryptosystem (ECPKC) has been proposed by Karrar Taher and Ruma Ajeena. Their main idea is to design this cryptosystem focusses on generating the elliptic curve group, its order divides the Euler phi function that is computed securely based on two large primes. Faster and more secure computations to generate the keys, encryption and decryption processes, on the KR-ECPKC algorithm are discussed. In comparing with other algorithms like RSA and ElGamal public key cryptosystem (EEPKC), the KR-ECPKC considers as an efficient algorithm. So, the KR-ECPKC is more appropriate for elliptic curve cryptographic applications.

1. Introduction

The elliptic curve cryptography (ECC) is more interested for many researchers, because it has employed in different applications such mobile devices, wireless sensor, network, image encryption and others [1,2,3]. The ECC has keys with small size that allows to be much efficient in comparing to other public key cryptosystems like RSA [4].

The RSA cryptosystem is proposed Rivest, R.L., et al, in 1978 through presenting a public key cryptosystem which was depended on the integer factorization problem, that factors a composite number into two large primes [4]. In 1985 Miller introduced proposed the Diffie-Hellman key exchange protocol based on elliptic curves [5]. In 1987, Koblitz proposed elliptic curve ElGamal public key cryptosystem [6]. In 2000, Neal Koblitz introduced the state of elliptic curve cryptography, he presented a survey about the elliptic curve cryptosystems [7].

In this work, we are looking for a small size key, faster and secure computation. So, our work focusses on the proposed new version of elliptic curve public key cryptosystem. That has faster computations of the encryption and decryption processes in comparing with other elliptic curve cryptosystems.

The outline of this work includes Section 2, which discussed the RSA cryptosystem in its first part. And in the second part, another public key cryptosystem which depended on elliptic curves is explained, this cryptosystem is called ELCGamal elliptic public key cryptosystem (EPPKC). In section 3, a new version of the elliptic curve cryptosystem is proposed. Section 4, discusses a study case of the proposed EC-Cryptosystem. Some computational results of the proposed EC-cryptosystem are explained in Section 5. Section 6, presents the comparison on the proposed EC-cryptosystem, RSA and EPPKC. The security considerations of the proposed EC-cryptosystem are determined in Section 7. Finally, Section 8, displays the conclusions.
2. Mathematical Background

The RSA cryptosystem proposed in 1978 by R. L. Rivest, A. Shamir, and L. Adleman [4]. A public key on the RSA cryptosystem is a pair of integers \((n,e)\), where \(n\) is a product of two secret primes \(p\) and \(q\) and \(e\) is an integer satisfying \(\gcd(e, \phi) = 1\), with \(\phi = (p-1)(q-1)\) is Euler phi function. Whereas, a private key \(d\) is an integer satisfying \(ed \equiv 1 \pmod{\phi}\). The ciphertext \(c\) of a plaintext \(m\) is computed by \(c = m^e \pmod{n}\). The original message can be recovered through decryption process that is computed by \(m = c^d \pmod{n}\).

On the other hand, the ElGamal elliptic curve public key cryptosystem (EECPKC) is proposed by ElGamal in 1987 [6]. The users, sender and receiver agree to choose a prime \(p\), an elliptic curve equation \(E: y^2 = x^3 + ax + b \pmod{p}\) [8,9] and to determine a generator elliptic point \(P\) as the public parameters. The receiver chooses a random integer \(d\) as his/her secret key and computes his/her public key \(dP\). The sender selects a message \(M\) as an elliptic point in \(pE\) and encrypt it by a pair \((C_1, C_2)\), where \(C_1 = eP\) and \(C_2 = M + e(dP)\). The receiver decrypts the ciphertext \((C_1, C_2)\) through computing \(C_2 - dC_1 = M + e(dP) - d(ep) = M\).

3. The KR-Elliptic Curve Cryptosystem

The encryption process is done as follows. A plaintext \(m\) selected and represented as elliptic point in \(E(F_p)\) [10]. Then a message \(M\) is encrypted by \(C = e'M\), where \(e'\) is computed by \(e' = e \pmod{N}\), with \(N\) is an order of \(M\). The ciphertext \(C\) considers as a scalar multiplication, which can be computed by ISD method [11,12]. Algorithm (3.2.1) is employed to compute the ciphertext \(C\).

3.1. The KR-Elliptic Curve Cryptosystem: Keys Generation Process

First, a set of the points on an elliptic curve group \((E(F_p), +)\) is computed. The order \(#E(F_p)\) of a group \((E(F_p), +)\) should divide a positive integer \(n\), where \(n = (q - 1)(t - 1)\) with \(q\) and \(t\) are two large primes that are selected secretly by a first user to compute his/her private key \(n\). The public key \(e\) is selected as an integer from the range \([2, n - 1]\) such that \(\gcd(e, n) = 1\). So, the public and private keys are \(e\) and \(n\) respectively. Algorithm (3.1.1), is used to generate the keys of the KR-EC cryptosystem.

Algorithm 3.1.1. The KR-EC Cryptosystem: Keys Generation Process.

1. Select \(a, b \in [1, n - 1]\) are coefficients of \(E\).
2. Compute \(n = (q - 1)(t - 1)\).
3. Select randomly \(e \in [2, n - 1]\)
4. If \(\gcd(e, n) = 1\) then
5. Return \(e\)
6. Else
7. Stop and go to step (3).
8. End if
9. Compute the elliptic curve set \(E(F_p)\).
10. Compute the order \(#E(F_p) = h\) of \(E(F_p)\).
11. If \(h | n\) then
12. Return the set \(E(F_p)\)
13. Else
14. Stop and go to step (1).
15. End if
16. Return \((n,e,E(F_p))\).

3.2. The KR-Elliptic Curve Cryptosystem: Encryption Process
The encryption process is done as follows. A plaintext \(m\) selected and represented as elliptic point in \(E(F_p)\) [10]. Then a message \(M\) is encrypted by \(C = e' M\), where \(e'\) is computed by \(e' = e (mod N)\), with \(N\) is an order of \(M\). The ciphertext \(C\) considers as a scalar multiplication, which can be computed by ISD method [11,12]. Algorithm (3.2.1) is employed to compute the ciphertext \(C\).

Algorithm 3.2.1. The KR-EC Cryptosystem: Encryption Process
INPUT: A set \(E(F_p)\) of elliptic points, a public key \(e\) and plaintext \(m\).
OUTPUT: The ciphertext \(C\).
1. Convert a message \(m\) as an elliptic point \(M \in E(F_p)\) [10].
2. Compute the order \(N\) of a point \(M\).
3. Compute \(e' = e (mod N)\).
4. Compute \(C = e' M\).
5. Return \(C\).

3.3. The KR-Elliptic Curve Cryptosystem: Decryption Process
Upon receiving the ciphertext to the first user, he/she wants to decrypt the ciphertext and recover the original message. First, he/she computes the key \(d\) secretly, where \(d \in [2,n-1]\) and \(ed \equiv 1 (mod n)\). Then \(d'\) is computed by \(d' = d (mod N)\) with \(N\) is an order of the \(C\) that is computed as an elliptic curve point. The original message is recovered by \(d' C = M\). The decryption process is proved mathematically in following proposition.

Proposition 3.3.1. The decryption process of KR-EC cryptosystem takes the expression \(M = d' C\).
Proof.
\[
d' C = d'( e' M ), \text{ since } C = e' M.
\]
\[
= deM
\]
\[
= (m+1)M \text{ such that } r \text{ is a positive integer, since } ed \equiv 1 (mod n).
\]
\[
= rM + M
\]
\[
= r(sN)M + M \text{ such that } s \text{ is a positive integer and } N \text{ the order of } M \text{ that is } (NM = O_E),
\]

since every order of elliptic point divide \(n\).
\[
= rs(NM) + M
\]
\[
= rs(O_E) + M
\]
\[
= M. \blacksquare
\]

For the computational results to recover a message \(M\), one can use Algorithm (3.3.2).

Algorithm 3.3.2. The KR-EC Cryptosystem: Decryption Process.
INPUT: A set \(E(F_p)\) of elliptic points, a public key \(e\), a privet key \(n\) and the ciphertext \(C\).
OUTPUT: A key \(d\) and a plaintext \(m\).
1. Choose randomly \(d \in [2,n-1]\)
2. If \( ed \equiv 1 \pmod{n} \) then
3. Return \( d \)
4. Else
5. Stop and go to step (1).
6. End if
7. Compute the order \( N \) of a point \( C \) that is a ciphertext.
8. Compute \( d' \equiv d \pmod{N} \).
9. Compute \( d' \cdot C = M \).
10. Convert \( M \) into \( m \).
11. Return \( m \).

4. The Study Case on the KR-EC Cryptosystem.

The keys, namely public and private are generated first. A prime \( p = 8123 \) is chosen and the elliptic points set \( E(F_{8123}) \) is determined by supposing the elliptic curve \( E : y^2 = x^3 + 5x + 13 \) as the public parameters. The set
\[
E(F_{8123}) = \{ (1,1548),(1,6575),(3,3067),(3,5056),(4,6052),(4,2071),\ldots,(8122,5994),(8122,2129),O_E \}.
\]
The \( \#E(F_{8123}) = 8144 \) such that \( 8144 \mid n \), where \( n \) is a private key for the first user. The private key is computed by \( n = (q - 1)(t - 1) = 12123438 \cdot 31423268 = 3809574206353584 \), where \( q = 12123439 \) and \( t = 314232169 \) are two large primes that are selected secretly. The public key \( e \) is selected randomly from the range \([2,3809574206353583]\) and
\[
gcd(e,n) = gcd(12326106299,3809574206353584) = 1.
\]
So, the public and private keys are \( e = 12326106299 \) and \( n = 3809574206353584 \) respectively. Now for encryption process, suppose second user chooses a message \( M = (1000,5149) \) which is an elliptic curve point in \( E(F_{8123}) \). The order of a point \( M \) is 4072, namely
\[
4072M = 4072(1000,5149) = O_E.
\]
He/She computes \( e' = 3491 \) through computing \( e' = e \mod(4072) \). The ciphertext \( C \) is computed as a scalar multiplication \( C = e' \cdot M = 3491(1000,5149) = (5375,4448) \). The ciphertext \( C = (5375,4448) \) will be sent to the first user. After receiving the ciphertext \( C \) into the first user, he/she computes
\[
d = 618131 \text{ such that } ed \equiv 1 \pmod{n}.
\]
The order of a ciphertext \( C \) which is considered as an elliptic curve point is computed to be \( N = 4072 \), since
\[
4072C = 4072(5375,4448) = O_E.
\]
The parameter \( d' = 3259 \) is computed, where \( d' \equiv d \mod(4072) \). First user computes a scalar multiplication
\[
d' \cdot C = 3259(5375,4448) = (1000,5149) = M.
\]

5. The Computational Results on the KR-EC Cryptosystem.

Some simple computational results about the KR-EC cryptosystem have been done. The experimental samples with different values of a primes \( q \) and \( t \) are chosen. The computational results to generate the keys, encryption and decryption processes are shown in Tables (1), (2) and (3) respectively.

| Table 1. The experimental results of the KR-EC cryptosystem: key generation process. |
|---|
| \( q \) | \( t \) | \( n = (q - 1)(t - 1) \) | \( e \) | \( F_p \) | \( E(a,b) \) | \( \#E(F_p) \) |
Table 2. The experimental results of the KR-EC cryptosystem: encryption process.

| $M \in E(F_p)$ | $N$ is the order of $M$ | $e' = e \mod(N)$ | $C = e'M$ |
|-----------------|-------------------------|------------------|-----------|
| (395,229)       | 284                     | 147              | (131,403) |
| (151,67)        | 193                     | 188              | (41,172)  |
| (999,123)       | 1162                    | 377              | (200,260) |
| (650,313)       | 1639                    | 94               | (1146,1645) |
| (2021,1131)     | 271                     | 173              | (1787,2080) |
| (527,600)       | 1048                    | 105              | (1761,1402) |
| (993,111)       | 386                     | 259              | (2920,1652) |
| (1176,533)      | 640                     | 121              | (820,356) |
| (1611,101)      | 1640                    | 29               | (358,704) |
| (1715,1227)     | 922                     | 887              | (1595,55) |

Table 3. The experimental results of the KR-EC cryptosystem: decryption process.

| $d$ | $N$ is the order of $C$ | $d' = d \mod(N)$ | $M = d'C$ |
|-----|------------------------|------------------|-----------|
| 199 | 284                    | 199              | (395,229) |
| 77  | 193                    | 77               | (151,67)  |
| 937 | 1162                   | 937              | (999,123) |
| 959 | 1639                   | 959              | (650,313) |
| 47  | 271                    | 47               | (2021,1131) |
| 45593 | 1048          | 529              | (527,600) |
| 743591 | 386          | 155              | (993,111) |
| 4900681 | 640          | 201              | (1176,533) |
| 509 | 1640                   | 509              | (1611,101) |
| 79  | 922                    | 79               | (1715,1227) |
6. Comparison on the KR-EC, RSA and EEPK Cryptosystems

By using the proposed KR-EC cryptosystem, there is no problem to choose the small primes \( q \) and \( t \) for computing \( n = (q - 1)(t - 1) \), since \( n \) is a private key. In comparing with that, the RSA public key cryptosystem needs the choice of the large primes for increasing the security. The public key generation process in elliptic curve ElGamal public key cryptosystem (EC-EPKC) requires more computations to solve the discrete logarithm problem (DLP) comparing with the new version KR-EC cryptosystem that is proposed to choose a public key as a number in the range \([2, n - 1]\) with \( \gcd(e, n) = 1 \). Also, computing a public key on the EC-EPKC requires finding the generator point on elliptic curve group in comparing to the KR-EC cryptosystem which is not required that.

As well as, the proposed version KR-EC cryptosystem is considered faster public key algorithm in compare with EC-EPKC, since on the KR-EC cryptosystem, the encryption and decryption processes need computing only the scalar multiplication operation while on the EC-EPKC requires for these processes computing the scalar multiplication and addition operations, so the last cryptosystem needs extra computations.

7. The Security Considerations on Proposed Public Key Cryptosystems

The security of the proposed encryption scheme determines through some main points. The first one is about the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECLP) [13]. The ECLP, means computing the value of \( k \) that lies in the range \([1, z - 1]\) and satisfies the relation \( kP = Q \) for given \( P \) and \( Q \) which are elliptic curve points and \( z \) is a prime order of \( P \). The second one is the hardest to find the private key \( d \) others, where \( e \) is a public key such that \( ed \equiv 1 (\text{mod} n) \) because \( n \) is a secret key. The element \( d \) here represents the inverse element of \( e \) modulo \( n \), and since \( n \) is computed securitly, so it is more difficult to compute the value of \( d \) modulo \( n \).

8. Conclusion

This work presented a new version of the elliptic curve public key cryptosystem which is called the KR-EC public key cryptosystem. It depended on the hardness computation of the elliptic curve discrete logarithm problem (ECDLP) and some mathematical computation problems from the number theory. On the proposed KR-EC public key cryptosystem, faster computations to generate the keys, encryption and decryption processes are done. The security of the KR-EC public key cryptosystem is determined based on the difficulty of computing the ECDLP and selecting the primes to compute the Euler phi function secretly. So, the KR-EC public key cryptosystem considers as a brilliant insight for elliptic curve encryption schemes.

References

[1] Liu A and Ning P 2008 April TinyECC A configurable library for elliptic curve cryptography in wireless sensor networks International Conference on Information Processing in Sensor Networks, IEEE pp 245-256

[2] Szczechowiak P, Oliveira L B, Scott M., Collier M, & Dahab R. 2008 NanoECC: Testing the limits of elliptic curve cryptography in sensor networks. In European conference on Wireless Sensor Networks, Springer, Berlin, Heidelberg pp 305-320

[3] Abd El-Latif A A & Niu X 2013 A hybrid chaotic system and cyclic elliptic curve for image encryption AEU-International Journal of Electronics and Communications 67(2) 136-143

[4] Rivest R L, Shamir A & Adleman L 1978 A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2) 120-126

[5] Miller V S 1985 Use of elliptic curves in cryptography In Conference on the theory and application of cryptographic techniques Springer, Berlin, Heidelberg pp 417-426

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

[7] Koblitz N, Menezes A & Vanstone S 2000 The state of elliptic curve cryptography Designs codes and cryptography 19(2-3) 173-193
[8] Hoffstein J, Pipher J, Silverman J H & Silverman J H 2008 *An introduction to mathematical cryptography* (Vol. 1). New York: Springer

[9] Washington L C 2008 Elliptic curves *number theory and cryptography* CRC press

[10] Trappe Wade 2006 Introduction to cryptography with coding theory *Pearson Education India*

[11] Ajeena R K & Kamarulhaili H 2014 Point multiplication using integer sub-decomposition for elliptic curve cryptography *Applied Mathematics & Information Sciences* 8(2) 517

[12] Ajeena R K Integer 2015 Sub-decomposition (ISD) Method for Elliptic Curve Scalar Multiplication. *Diss. Universiti Sains Malaysia*

[13] Bos J W, Kaihara M E, Kleinjung T, Lenstra A K & Montgomery P L 2012 Solving a 112-bit prime elliptic curve discrete logarithm problem on game consoles using sloppy reduction *International Journal of Applied Cryptography* 2(3) 212-228