TELKOMNIKA, Vol 16, No 1: February 2018, pp. 352~360
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i1.6953

Efficiency of 128-bit Encryption and Decryption Process in Elgamal Method Using Elliptic Curve Cryptography (ECC)

Dicky Nofriansyah*[1], Afzalur Syaref[2], Widiarti R Maya[3], Ganefri Ganefri[4], Ridwan[5]
[1,2,3]STMIK Triguna Dharma, Jl. A.H Nasution No.73 F Medan, Indonesia
[4,5]Universitas Negeri Padang, Jl. Air Tawar Padang, Sumatera Barat, Indonesia
*Corresponding author, email: dickynofriansyah@ymail.com, ganefri_ft@yahoo.com

Abstract

Cryptography is a growing science of data security. The integrity of a data is an important thing to keep the secrets contained in the data. In this research will be visualized the efficient quantities that use elliptic curves and do not use them. The Elgamal method is an asymmetric cryptographic algorithm whose complexity of processes. It is especially for digital signatures. This research will discuss about the use of ECC to optimize and streamline the Encryption and Decryption process in particular 128-bit Elgamal method. The hope is that by using elliptic curves the timing of the encryption and decryption process can run faster in the computation of Elgamal Method.

Keywords*: cryptography, elgamal, elliptic curve, encryption, decryption*

1. Introduction

Cryptography is a plaintext encryption process to ciphertext and ciphertext decryption to plaintext [1]. In cryptography, the encryption process can be used to secure messages and maintain confidentiality in the communication process between the sender and the recipient. Some functions of criteria such as maintaining data integrity, confidentiality, non-repudiation and authentication [2]. Cryptography can be used on technologies such as cloud computing, network, internet, digital device and online transaction [1],[3]. In the network world, cryptography can also be used for anti-phishing [4].

Cryptography of the elliptic curve includes a public key cryptography system that bases security on the mathematical problems of elliptic curves [5]. Unlike the discrete logarithm problem (DLP) and integer factorization problem (IFP), there is no known sub-optimal time algorithm for solving the mathematical problems of elliptic curve logarithm problem (ECDLP) [6]. A data security that form an application designed based on the science of cryptography would have to take into consideration the running processes with precise and meticulous corresponding algorithms, the accuracy of the data is decrypted without any parts missing, the time required in the process of encryption and decryption, as well as considering the use of processor time to do the whole computing in the process of encryption and decryption [7]-[9]. In response to these problems requires a study to analyze the process and stages of algorithm work in detail when the data or files that are secured to function properly, precise, fast and gated when implemented in a programming language by using algorithms cryptography to generate an application Which is in accordance with the analysis process and research objectives. [10]

Cryptography is also used to reduce cybercrime numbers. One effort made to reduce the level of phishing is a combination of cryptography with the field of bio-informatic such as patterns of fingerprint. The Internet as one of the important factors in human life also has a great chance of being targeted by irresponsible parties. In this case, concrete efforts are needed to improve the security of digital data among which is using cryptography. The elements in cryptography are plaintext, ciphertext, cryptogsystem, key, encryption and decryption [11], [2], [1], [3]-[4], [12]-[13].

The cryptographic algorithm in this study is the Elliptic Curve algorithm to form the key and ElGamal algorithm for encryption and decryption of plaintext to follow the rules on the

Received Aug 4 2017; Revised January 5, 2018; Accepted January 14, 2018

elliptic curve [11]. ElGamal encryption algorithms apply at points of the elliptic curve so that it uses the rules of operation on the elliptic curve. In the process of the formation of a private key and a public key generated automatically using elliptic curve cryptography which will then be used in the ElGamal cryptographic encryption and decryption algorithms[14], [10].

2. Related Works

2.1. Concept of Curve Eliptic Cryptography

ECC can optimize the encryption and decryption process of several methods in AES method cryptography [11] [15]. ECC can be used in some areas of network, hardware, and software. In this section of the discussion described in general how to implement the security of plaintext data using elliptic and elgamal curve algorithms[15]. There are several gradual processes as well as the development that streamlines operations to produce security that matches the theory of elliptic curves and the development of elgamal theory [7],[16], [17].

The plaintext encoding process begins with the formation of a private key pair and a public key using elliptic curve cryptography theory by generating prime numbers, having a set of value pairs (x, y) satisfying the equation y2=x3+ax+b and selecting a point as a public key. And choose integer d as private key.The point chosen as the public key will be used for the plaintext encryption process using modified elgamal cryptography (using operating rules on elliptic curve theory) to produce 2 ciphertext values, C1 and C2. The value will be returned to plaintext using private key as well.[17]

The ElGamal cryptographic generating algorithm with the elliptic curve returns the public key and private key consisting of an elliptic curve selected by Ep (a, b), so the first thing to do is to form an elliptical curve group. The ElGamal generator algorithm with general elliptic curve is as follows:

a. Select the elliptic curve number E (a, b) in GF (p).
b. Select α=(x1, y1) as the generating point on the elliptic curve group E (a, b).
c. Select integer d with terms d> 1 and d <p - 1.
d. Select β=d.α (point multiplication using elliptic curve operating theory).
e. Kpublic=(E (a, b), α, β) and Kprivate=d.

The following will explain in detail the process of forming an elliptical curve group to select the public key and its private key [18]. The first step in elgamal generator algorithm with elliptic curve is to select the elliptic curve number E (a, b) in GF (p). Select the prime number with the condition p> 3 for Fp, so the elliptic curve equation used is y2=x3+ax+b mod p with the condition of 4a3+27b2 ≠ 0. Suppose that is taken any prime number=19. Then the value of a and b is randomly generated for its coefficients so that the elliptic curve equation of GF (p) is formed by filling the values of a and b in the equation with values a and b between 1 and p - 1. Suppose a=1 and b=1 so that the elliptic curve equation becomes: Y2=x3+x+1 (mod 19), 4a3+27b2 ≠ 0 (mod p), 4 .13+27.12 (mod 19)=31 (mod 19)=12 ≠ 0. If the process of checking discriminant 4a3+27b2 (mod p) is 0, then the random formation process of values of a, b and p must be repeated until it qualifies [19-20].

2.2. ECC Procedure

Phase 1: Determining the main points of Elliptic Curve

Before proceeding with the second step in the ElGamal generator algorithm with the elliptic curve of choosing the point as the value of α, it will be explained first about how to determine the points on the elliptic curve [21], [18]. To determine the most important points of elliptic curve, it is necessary to identify elements of the elliptic group E19 over Fp, with Fp={0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18}. But before determining E19, first look for quadratic residue modulo 19 (quadratic residue modulo) which is symbolised by QR19. [7], [17]

Table 1. Quadratic Residue Modulo

F_p	y^2 (mod 19)	QR_{19}	F_p	y^2 (mod 19)	QR_{19}	F_p	y^2 (mod 19)	QR_{19}
0	0^2	0	7	7^2	11	14	14^2	6
1	1^2	1	8	8^2	7	15	15^2	16
2	2^2	4	9	9^2	5	16	16^2	9
3	3^2	9	10	10^2	5	17	17^2	4
4	4^2	16	11	11^2	7	18	18^2	1
5	5^2	6	12	12^2	11			
6	6^2	17	13	13^2	17			

According to Table 1, the set of quadratic residues of modulus 19 is QR19={0, 1, 4, 9, 16, 6, 17, 11, 7, 5}. Then determine the elliptic group element E19 (1,1) which is the settlement of the equation y2=x3+x+1 (mod 19), for x ∈ F19 and y2 ∈ QR19. Here are the steps to find elements of elliptic curve groups or dots on the elliptic curve based of elliptic curve equations that have been formed: [23]

a. Set x from 0 to p - 1, for this matter means x={0, 1,. . ., 18}.
b. Calculate the value of y2 based on the elliptic curve equation that has been formed, ie y2=x3+x+1 (mod 19).
c. check for quadratic residue y2 to find out whether y2 has square root or not. Checks are true if the result of value y2 is the quadratic residual set value, and is false if it is not a quadratic residue.
d. If y2 is a quadratic residue, then x above Fp is the point on the elliptic curve, with the point y being taken from the y2 value in Table 2.

Table 2. Elliptic Curve of QRM

x	$y^2=x^2+1$ (mod 19)	$y^2=QR_{19}$	$(x, y)=E_{19}$ (1,1)
0	1	*true*	(0,1) and (0,18)
1	3	*false*	-
2	11	*true*	(2,7) and (2,12)
3	12	*false*	-
4	12	*false*	-
5	17	*true*	(5,6) and (5,13)
6	14	*false*	-
7	9	*true*	(7,16) and (7,3)
8	8	*false*	-
9	17	*true*	(9,6) and (9,13)
10	4	*true*	(10,17) and (10,2)
11	13	*false*	-
12	12	*false*	-
13	7	*true*	(13,11) and (13,8)
14	4	*true*	(14,17) and (14,2)
15	9	*true*	(15,16) and (15,3)
16	9	*true*	(16,16) dan (16,3)
17	10	*false*	-
18	18	*false*	-

Based on Table 2, there are 20 points on the elliptic curve. For example for x=0 obtained:

- Y2=x3+x+1 (mod 19)
- Y2=03+0+1 (mod 19)=1 (mod 19)

Because based on table 2, 12 (mod 19)=1 and 182 (mod 19)=1, then values 1 and 18 are y points, so the points found are (0,1) and (0,18). Calculations for other x and y values are done in the same way. Thus, the elements of the elliptic modulus group 19 above F19 are ((0,1), (0,18), (2,7), (2,12), (5,6), (5,13), (7,16), (7,3), (9,6), (9,13), (10,17), (10,2), (13,11), (13,8), (14, 17), (14,2), (15,16), (15,3), (16,16), (16,3), ∞}. The number of main points on the curve=20 points and plus the infinity point (∞) so that the number of elliptic curve points with the equation y2=x3+x+1 (mod 19) is 21 dots. Finding the elliptical group element in the above

manner is less efficient because if the prime number chosen is large, it takes a repetition process as much as p times to determine the quadratic residual set of modulus p, for example the random prime number chosen is 317 (9-bit), it is required As many as 317 iterations to search for the set of QR17 and do 317 more iterations to find elements of the elliptic curve group.

Phase 2: Forming Public Key and Private Key

To find congruent quadratic residue modulo p will be easier if using Euler's criterion theory (equation 6), i.e., if the value of 1 mod p is a quadratic residue of modulus p, and if it is worth ≠1 mod p, it is a non-residue modulus p. While determining the y value at the point of the elliptic curve depends on the prime number p raised. Based on the theory that has been exposed about the quadratic congruent that to find the value of **y** at an elliptic curve point is very easy. It is using condition p ≡ 3 mod 4. the value of x referred to in the equation can be used to find the y on a Elliptic curve point.

To get the point that will be the private key and the public key does not need to find the entire point on the curve, but simply by taking just any point so that it will reduce the key generator process. Here's the algorithm:

a. Select the prime p at random terms p> 3 and p ≡ 3 mod 4
b. Select a and b randomly from 1 to p - 1 for the equation y2=x3+ax+b mod p with condition 4a3+27b2 ≠ 0 mod p.
c. Select x randomly from 0 to p - 1, then finds the value of y2 based on the elliptic curve equation that has been formed.
d. Check y2 is the quadratic residue of modulus p using euler criteria.
e. If the value is true, calculate the value of the root.

For example the values of a, b and p are randomly generated are the same as the previous examples that are a=1, b=1 and p=19 for easy comparing of processes and those values have met the required requirements. Then generate x values randomly, for example x=6

- Y2=x3+ax+b (mod p)
- Y2=63+1.6+1 (mod 19)=14 (mod 19)

The next step is a quadratic residue check modulo p with Euler Criteria:

A (p-1)/2 ≡ 1 mod p, where a=y2 ; 14 (19-1)/2 ≡ 18 (mod 19) ≠ 1 (mod 19). False value because y2 value ≠1 mod p, then it is not quadratic residue modulo p, it is necessary to repeat the step until y2 is worth 1 mod p. Suppose the value of x raised randomly is x=10, so that: Y2=103+1.10+1 (mod 19)=4 (mod 19), and 4 (19-1)/2 ≡ 1 (mod 19)

Is true because y2 is worth 1 mod p, then the next step is to find the value of y at the elliptic curve:

- Y1=a (p+1)/4 mod p and y2=-a (p+1)/4 mod p, where a=y2
- Y1=4 (19+1)/4 mod 19=45 mod 19=17 (mod 19)
- Y2=-4 (19+1)/4 mod 19=-45 mod 19=-17 (mod 19)=2 (mod 19)

The values found are x=10, y1=17 and y2=2, then the points on the arbitrarily formed elliptic curves are (10, 17) and (10,2). When compared with the previous sample data then the points found are the same/true. As a second step in the Elgamal generator algorithm with the elliptic curve can be taken one of the points from the example above that is α=(10.17). While the third step chooses integer d with d> 1 and d <p - 1, for example selected d=3. The next step is to calculate the value of β=d.α. Since α is the point on the elliptic curve and d is an integer, then this multiplication can be done by repeated addition as d using the elliptic curve point addition theory. Similar to the real number, that 5x3 equals five sums 3 times. Here is the calculation of the value of β, with d=3 and α=(10.17):

- B=d.α
- B=3 x (10.17)
- B=(10,17)+(10,17)+(10.17)

Finding the value of P+Q=R, with P=(10.17) and Q=(10.17). Since point P equals point Q, the sum of points can be performed using the elliptic curve point summing theory of P+P=R by finding the value of λ using Equation (1)

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

$$\lambda = \frac{3.10^2 + 1}{2.17} = \frac{3.100 + 1}{34} = \frac{301}{34} = 301.34^{-1} = 301.14 = 4214(mod19) = 15 \quad (1)$$

Looking for inverse multiplication value from 34-1 at ℤ19 can be done using extended Euclid theory by finding t value because of t=a-1. Here's an example with a=34 and m=19.

Table 3. Inverse Multiplication Using Extended Euclid Theory

k	A	B	Q	R	T_1	T_2	T	k
init	19(m)	34(a)			0	1		*init*
1	19	34	0	19	0	1	0	1
2	34	19	1	15	1	0	1	2
3	19	15	1	4	0	1	-1	3
4	15	4	3	3	1	-1	4	4
5	4	3	1	1	-1	4	-5	5
6	3	1	3	0	4	-5	19	6
7	1	0			-5	19		7

From the data in Table 3, it is found t=-5, so that 34-1=-5 in ℤ19. Because -5=19 - 5=15 at ℤ19, then 34-1=14 at ℤ19. Can be verified 34 x 14=47 ≡ 1 (mod 19) and gcd value (19,34) ≡ 1 (mod 19). Since the lambda value has been found, the next step is to find the values of x3 and y3 to derive new points using equation (2) and equation (3).

X_3=λ ^ 2-x_1-x_2
X_3= ⟦15] ^ 2-10-10=225-10-10=205 (mod19)=15 (2)

Y_3=λ (x_1-x_3) -y_1
Y_3=15 (10-15) -17=-92 (mod19)=3 (3)

The new point from the point doubling is P+P=2P=(15.3). Next do a sum of points between the new point and the point (10,17) to find 3P=2P+P=(15.3)+(10.17), since x1 ≠ x2 then use equation (4) to find the lambda value and continue. Using equation (5) and equation (6) to obtain a new point.

Λ=(y_2-y_1)/(x_2-x_1)
Λ=(17-3)/(10-15)=14/(- 5)=14/14=14.
[14] ^ (- 1)=14.15=210 (mod19)=1 (4)

X_3=λ ^ 2-x_1-x_2
X_3=1 ^ 2-15-10=-24 (mod19)=14 (5)

Y_3=λ (x_1-x_3) -y_1
Y_3=1 (15-14) -3=-2 (mod19)=17 (6)

Then the new point found is 3P=(14,17), so β= d.α=3x (10.17)=(10.17)+(10.17)+(10.17)=(14.17). After obtaining the lambda value, the final step of the ElGamal key forming algorithm with the Elliptic Curve is to determine the public and private keys. In this case, the public key is the elliptic curve parameter, α and β. While private key is integer d, so: UK public=(E (a, b), α, β) and UK private=d. Kpublic={(E (1,1) GF (19)), (10,17), (14,17)} and K private=3.

Multiplication of points or sum of points repeatedly as the above means will be less efficient if the number of repetition (integer d is selected) is large because the sum of the point needs to be done as much as integer d. It is necessary to apply square and multiply algorithm,

by substituting the power operation to multiply the point (R+R) and multiplication into the sum of the starting point P with the point R. For example, 11 x (10.17), represent 11 in binary, i.e., 1011 and set initial value R=∞ then do the following calculation:

Table 4. Calculation of Initial Value

i	r_i	*R+R*	*P+R*
3	1	∞+∞=∞	(10,17)+∞=(10,17)
2	0	(10,17)+(10,17)=(15,3)	-
1	1	(15,3)+(15,3)=(14,2)	(10,17)+(14,2)=(15,16)
0	1	(15,16)+(15,16)=(14,17)	(10,17)+(14,17)=(14,2)
i	r_i	*R+R*	*P+R*

Phase 3: Encoding

The original text as the input of the ElGamal cryptographic system encryption algorithm with the Elliptic Curve is a point on the elliptic curve. Before doing the encoding process, it is necessary to map plaintext at elliptic curve points. The process of mapping or encoding plaintext into elliptic curve points can be done using the koblitz method. But to find the value of x based on the plaintext encryption algorithm by the to blitz method must select the appropriate elliptic curve parameter. Suppose that the selected k is k=10, while the maximum value of ASCII value is 128 and the minimum value of x is m.k+1 for example 128 x 10+1=1281 as a character representation.[24] To obtain a point with coordinates x>=1281, it is necessary to select an elliptic curve with a prime not smaller than 1281. The selection of elliptic curve parameters corresponding to blitz method depends on the value of k selected. If simplified, the maximum value of k allowed is p/128.

Here's an example with plain text "Aceh":

a. The elliptic curve E (1,1) GF (1879).
b. The "Aceh" plaintext in the ASCII decimal code is {65, 99, 101, 104}.
c. the selected integer k is k=11.
d. Do looping x=m.k+1. Then check whether it has a y value on the elliptic curve or not, this can be done using euler criteria theory.

For m=65:
X=m.k+1=65 x 11+1=716
Then calculate the value of y2
Y2=x3+ax+b=7163+1.716+1=1642 (mod 1879)
Checking point on the curve is by quadratic check of residue using Euler criteria
A (p-1)/2 ≡ 1 mod p, with a=y2
1642 (1879-1)/2 ≡ 1642939 ≡ 1878 (mod 1879), is not a quadratic of modulo residue 1879 so it is necessary to continue x=m.k+2:
X=m.k+2=65 x 11+2=717
Y2=x3+ax+b=7173+1.717+1=980 (mod 1879)
980 (1879-1)/2 ≡ 980939 ≡ 1 (mod 1879), is a quadratic residue so that:
Y=a (p+1)/4 mod p=980 (1879+1)/4=980470=556 (mod 1879)
The encoding result m=65 is (717,556).
For m=99:
X=m.k+1=99 x 11+1=1090
Y2=x3+ax+b=10903+1.1090+1=743 (mod 1879)
743 (1879-1)/2 ≡ 743939 ≡ 1878 (mod 1879), is not a quadratic residue modulo 1879
it needs to continue x=m.k+2:
X=m.k+2=99 x 11+2=1091
Y2=x3+ax+b=10913+1.1091+1=94 (mod 1879)
94 (1879-1)/2 ≡ 94939 ≡ 1 (mod 1879), is a quadratic residue so that:
Y=a (p+1)/4 mod p=941879+1)/4=94470=1024 (mod 1879)
The encoding result m=99 is (1091,1024).
For m=101:
X=m.k+1=101 x 11+1=1112
Y2=x3+ax+b=11123+1.1112+1=873 (mod 1879)
873 (1879-1)/2 ≡ 873939 ≡ 1 (mod 1879), is a quadratic residue so that:

Y=a (p+1)/4 mod p=8731879+1)/4=873470=1510 (mod 1879)
The encoding result m=101 is (1112,1510).
For m=104:
X=m.k+1=104 x 11+1=1145
Y2=x3+ax+b=11453+1.1145+1=1066 (mod 1879)
1066 (1879-1)/2 ≡ 1066939 ≡ 1 (mod 1879), is a quadratic residue so that:
Y=a (p+1)/4 mod p=10661879+1)/4=1066470=351 (mod 1879)
The encoding result m=104 is (1145,351).

From the above data operation results, obtained point (717,556), (1091,1024), (1112,1510), (1145,351) which will be input as plain text which has been mapped to ElGamal encryption process with elliptic curve.

Phase 3: Encryption

The original text (P) as the input of the ElGamal cryptographic system encryption algorithm[25] with the Elliptic Curve are the points on the elliptic curve and the key UK public=(E (a, b), α, β). The encryption selects a random integer r and then calculates the cypher text as follows:

$$C1=r \times \alpha \quad (7)$$

$$C2=P+r \times \beta$$

The above formula is the development of the plaintext encryption formula using ElGamal, by substituting the power operation into multiplication and multiplication operations into sums. For example, with plaintext "Aceh", if the generator of the key algorithm selects the elliptic curve K public=(E (1,1), (275, 676), (1225, 1248)) and K private=22 with the elliptic curve in GF (1879). Given the elliptic curve y2=x3+x+1 GF (1879), α=(275, 676), and β=(1225, 1248). While the plaintext has been mapped to {(717, 556), (1091, 1024), (1112, 1510), (1145, 351)}, Then the encryption does the following:

Select randomly integer r, for example selected r=17. Calculating C1=r x α and C2=P+(r x β), with P being plaintext that has been mapped into elliptic curve points. While point multiplication can utilize square and multiply theory as in table 5.
C1=r x α=17 x (275, 676)=(964, 1091)
(R x β)=17 x (1225, 1248)=(807, 789)

Table 5. Map of Elliptic Curve Points

P	$C_2=P+r \times \beta$
(717,556)	(717,556)+(807, 789)=(271, 1392)
(1091,1024)	(1091, 1024)+(807, 789)=(842, 1372)
(1112,1510)	(1112, 1510)+(807, 789)=(1082, 1210)
(1145,351)	(1145, 351)+(807, 789)=(1099, 868)

Phase 4: ElGamal Decryption Process Using Elliptic Curves

Encrypt after obtaining C1 and C2 can recover the original text **P** by using private key **K** private=d and compute **P**=C2 - (d x C1). It can be proved that the P obtained is equal to P by encryptor:

$$P=C2 - (d \times C1)=P+r \times \beta - (d \times r \times \alpha)=P+r.d \times \alpha - r.d \times \alpha=P \quad (8)$$

By cipher (964, 1091), (271, 1392), (842, 1372), (1082, 1210), (1099, 868), it can be known from the sequence that C1=(964, 1091) and C2=(271, 1392), (842, 1372), (1082, 1210), (1099, 868). Here is the process of decryption:

P=C2 - (d x C1).
P1=(271, 1392) - (22 x (964, 1091))
=(271, 1392) - (807, 789)
=(271, 1392)+(807, 1090)
=(717, 556)
P2=(842, 1372) - (22 x (964, 1091))

=(842, 1372) - (807, 789)
=(842, 1372)+(807, 1090)
=(1091, 1024)
P3=(1082, 1210) - (22 x (964, 1091))
=(1082, 1210) - (807, 789)
=(1082, 1210)+(807, 1090)
=(1112, 1510)
P4=(1099, 868) - (22 x (964, 1091))
=(1099, 868) - (807, 789)
=(1099, 868)+(807, 1090)
=(1145, 351)
The plaintext sequence obtained is (717, 556), (1091, 1024), (1112, 1510), (1145, 351).

Phase 5: Decoding

Since the result of password recovery is still the points on the elliptic curve, it is necessary to return the mapping to ASCII decimal values again using the koblitz method by calculating m=| (x-1)/k |.

For P1=(x1, y1)=(717, 556):
M1=| (x-1)/k |=| (717 - 1)/11 |=| (717 - 1)/11 |=65
For P2=(x1, y1)=(1091, 1024):
M2=| (x-1)/k |=| (1091 - 1)/11 |=| (1091 - 1)/11 |=99
For P3=(x1, y1)=(1112, 1510):
M3=| (x-1)/k |=| (1112 - 1)/11 |=| (1112 - 1)/11 |=101
For P4=(x1, y1)=(1145, 351)
M4=| (x-1)/k |=| (1145 - 1)/11 |=| (1145 - 1)/11 |=104
The order of ASCII code value is (65, 99, 101, 104)=(A, c, e, h).

3. Performance Analysis

In testing the two forms of encryption above can be seen how the workings of elliptic curve cryptography to cryptography ElGamal with the existence of targets for a shorter time, the accuracy of data when encryption and decryption. Here are the results of testing the process of encryption and decryption using methods with efficiency and without efficiency.

Table 6. Speed Test of Encryption and Decryption Process

No	Process	Method	Time/second
1	Encryption	Not Using ECC	0.032000
		Using ECC	0.021000
2	Decryption	Not Using ECC	0.032000
		Using ECC	0.002000

The table above shows the time difference between the method without efficient and efficient method when performing the process of encryption or decryption. The average acceleration during computing is **> 6.25%** compared to when not using ECC. For time difference data during encryption or decryption using the efficient and efficient method with random data input on an attribute, public key and private key and the use of 128 and 256-bit numbers are in the attachment.

4. Conclusion

The process of encryption and decryotion on the ElGamal method more efficiently from a time perspective is when we use elliptic curve cryptography. Using the elliptic curve algorithm as the key constructor and ElGamal algorithm for encryption and decryption by following the rules on elliptic curve points, the security level can be designed as expected. The application of the formation of private keys and public keys that are generated automatically by elliptic curve algorithm is very influential on cryptographic computations when performing calculations correctly, quickly and concisely.

Acknowledgements

This research was supported by STMIK Triguna Dharma and Universitas Negeri Padang. We thank our colleges from department of Information System. We thank Prof. Ganefri and Dr. Ridwan for his guidance that greatly improved the research and manuscript.

References

[1] WJSBS Smanchat. Finding the Optimal Value for Threshold Cryptography on Cloud Computing, *International Journal of Electrical and Computer Engineering (IJECE).* 2016; 6(6): 2979-2988
[2] MRAHMM. Saikia, A Cloud Based Secure Voting System using Homomorphic Encryption for Android Platform, *International Journal of Electrical and Computer Engineering (IJECE).* 2016; 6(6): 2994-3000
[3] ARKASNCASCS Sastry, A Hybrid Cryptographic System for Secured Device to Device Communication. *International Journal of Electrical and Computer Engineering (IJECE)*. 2016; 6(6): 2962-2970
[4] ANH Gupta, Anti-Phishing Techniques in Cryptography, *International Journal of Electrical and Computer Engineering (IJECE).* 2015*;* 5(6): 1511-1515.
[5] H Dalziel, Chapter 9 - Cryptography, in Infosec Management Fundamentals, ed Boston: Syngress, 2015: 33-34.
[6] L Ogiela, Cryptographic techniques of strategic data splitting and secure information management, *Pervasive and Mobile Computing.* 2016; 29: 130-141, 2016/07/01/.
[7] MS Samta Gajbhiye, Samir Dashputre, A Survey Report on Elliptic Curve Cryptography, *International Journal of Electrical and Computer Engineering (IJECE). 2011;* 1(2): 195-201.
[8] HI Hsiao, J Lee, Fingerprint image cryptography based on multiple chaotic systems, *Signal Processing*. 2015; 113: 169-181, 2015/08/01/.
[9] S Yuan*, et al.*, Cryptanalysis and security enhancement of optical cryptography based on computational ghost imaging, *Optics Communications.* 2016; 365: 180-185, 2016/04/15/.
[10] J Wu*, et al.*, Color image encryption based on chaotic systems and elliptic curve ElGamal scheme, *Signal Processing.* 2017; 141: 109-124, 2017/12/01/.
[11] PGSUGSNBR Srikanth, Hybrid Cryptography for Random-key Generation based on ECC Algorithm, *International Journal of Electrical and Computer Engineering (IJECE).* 2017; 7(3): 1293-1298.
[12] YZLYJ Li, Mobile Internet Information Security Analysis and Countermeasures, *TELKOMNIKA (Telecommunication Computing Electronics and Control).* 2016; 14(3A): 333-337.
[13] AOMPB Mane, Watermarking and Cryptography Based Image Authentication on Reconfigurable Platform, *Bulletin of Electrical Engineering and Informatics (BEEI).* 2017; 6(2): 181-187.
[14] A Sridhar and VR Josna, CASH on Modified Elgamal: A Preventive Technique for False Channel Condition Reporting Attackin Ad-hoc Network, *Procedia Technology.* 2016; 24: 1276-1284, 2016/01/01/.
[15] SGMSS Dashputre, A Survey Report on Elliptic Curve Cryptography, *International Journal of Electrical and Computer Engineering (IJECE).* 2011; 1(2): 195-201.
[16] KMarisa W. Paryasto, Sarwan et al, Issues in Elliptic Curve Crypyography implementation, *Internetworking Indonesial Journal.* 2009; 1.
[17] LD Singh, KM Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, *Procedia Computer Science.* 2015l; 54: 73-82, 2015/01/01/.
[18] M Ahmad*, et al.*, Efficient cryptographic substitution box design using travelling salesman problem and chaos, *Perspectives in Science.* 2016; 8: 465-468, 2016/09/01/.
[19] S Chandra*, et al.*, Content Based Double Encryption Algorithm Using Symmetric Key Cryptography, *Procedia Computer Science.* 2015; 57: 1228-1234, 2015/01/01/.
[20] P Patil*, et al.*, A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish, *Procedia Computer Science.* 2016; 78: 617-624, 2016/01/01/.
[21] NBF Silva*, et al.*, Case studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer, *Journal of Network and Computer Applications.* 2016; 60:130-143, 2016/01/01/.
[22] B Poudel*, et al.*, Evolving side-channel resistant reconfigurable hardware for elliptic curve cryptography, in *2017 IEEE Congress on Evolutionary Computation (CEC)*. 2017; 2428-2436.
[23] S Nimbhorkar and L Malik, Comparative Analysis of Authenticated Key Agreement Protocols Based on Elliptic Curve Cryptography, *Procedia Computer Science.* 2016; 78: 824-830, 2016/01/01/.
[24] K Javeed*, et al.*, High performance hardware support for elliptic curve cryptography over general prime field, *Microprocessors and Microsystems.* 2017; 51: 331-342, 2017/06/01/.
[25] H Wang*, et al.*, Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography, *Future Generation Computer Systems*.