ISSN 2278-3091

Volume 9, No.1, January – February 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse44912020.pdf

https://doi.org/10.30534/ijatcse/2020/44912020

Algorithm for ensuring message confidentiality using elliptic curves

Kuryazov D.M.[1]

[1] Ph.D., competitor of the National University of Uzbekistan, Uzbekistan, kuryazovdm@mail.ru

ABSTRACT

In this paper, using the method of encoding messages with points of an elliptic curve a new asymmetric encryption algorithm is proposed based on elliptic curves.

Key words: Asymmetric algorithms, Elliptic curves, Encoding and decoding.

1. INTRODUCTION

Today, the resistance of modern asymmetric algorithms (data encryption and digital signature) is characterized by their ability to withstand all sorts of attacks and complexity of the best known cracking algorithm [1-12]. In the case of a digital signature algorithm, the use of strong hash functions is additionally required [16].

Practically used standards of asymmetric algorithms for data encryption are based on two basic tasks:

- The problem of factoring a composite number;
- The problem of discrete logarithm in a finite group of a large prime order.

The main problems in this class of cryptographic transformations are the low speed of such transformations, a significant increase in the size of the cryptogram in comparison with the size of the original message, and also the decreasing resistance due to the development of mathematical methods and means of cryptanalysis.

In recent years elliptic cryptography, which independently was opened by N.Koblitz and V.Miller in 1985 year, is intensive developing, in which role of one-sided function executes scalar multiplication of points to constant, which is realized on the basis of the operations of addition and doubling of points on elliptic curves (EC) over finite fields of different characteristics [14-15].

Permanently grown computerization of society and rising the valuable of information brings to necessity of improvement cryptographic methods and means of information protection. In terms of mutual distrust of information system subjects the protection is provided on the basis of methods of public key cryptography, which on one side is provides extensive functional possibilities, and on the other, is described by a significantly lower efficiency and larger size of information blocks compared with symmetric methods. The cryptosystems on EC are the most perspective among cryptosystems with public keys. So, using transformation in the group of elliptical curves points in comparison with transformations in the rings (e.g., asymmetric RSA algorithm is realized in the ring) and fields (e.g., Diffi-Helman and El-Gamal algorithm are realized in the Galua field) allows to reduce length of public keys and general system parameters for 4-6 times and more, or to significantly raise the resistance with the same parameters [4,7-9, 14].

At information interaction often is arisen the problem encoding information such away, that only recipient could decipher it. This task is successfully solved by scheme of directed encryption, the essence of which is that the information is encrypted with a public key of the recipient or a key, which is derived from the public key and decrypted by the private key of the recipient, or a key, which is obtained via a secret key.

The main problems in this class of cryptographic transformations are low speed of such transformations, also decreasing the resistance due to the progress of mathematical methods and cryptanalysis means.

In the work [13] was studied state of problem in the area of directed encryption, substantiated the possibility of it realization in the points group in the elliptical curves (EC). In the work [11] was invited the way of commutative encryption, which using calculation in the EC, which ensures the exponential resistance of the algorithm and rising efficiency compared with other algorithms [12]. The size of the cryptogram increased slightly compared to the size of the original message.

The purpose of this article is to propose an asymmetric algorithm for encrypting data on an elliptic curve using the method of encoding messages with points of an elliptic curve.

2. THE MAIN PART

Suppose the prime number $p > 3$. Then the elliptic curve E, defined over a finite field F_p, is the set of pairs of numbers (x, y), $x, y \in F_p$, satisfying the identity:

$$y^2 \equiv x^3 + ax + b \ (\text{mod}\ p), \qquad (1)$$

where: $a, b \in F_p$ and $4a^3 + 27b^2$ is not congruent to zero modulo p.

Invariant of an elliptic curve is the quantity J (E), satisfying the identity:

$$J(E) = 1728 \frac{4a^3}{4a^3 + 27b^2} (\text{mod}\ p) \qquad (2)$$

The coefficients a, b of the elliptic curve E, for the known invariants are defined as follows:

$$\begin{cases} a \equiv 3k(\text{mod}\ p) \\ b \equiv 2k(\text{mod}\ p), \end{cases} \qquad (3)$$

where: $k = \frac{\text{J(E)}}{1728\text{ - J(E)}} (\text{mod}\ p)$, $J(E) \neq 0$ *or 1728.*

Pair (x , y) which satisfies (1), is called points of an elliptic curve E , x and y - are, respectively, the x and y coordinates of the point .

Elliptic curve points will be denoted by $G(x, y)$ or simply G. Two elliptic curve points are equal if their respective x and y coordinates are equal.

On the set of all points of the elliptic curve E, we introduce the addition operation, which will be denoted by "+". For any two points G_1 (x_1, y_1) and G_2 (x_2, y_2) of the elliptic curve E, consider a few options.

Let the coordinates of points G_1 and G_2 satisfy $x_1 \neq x_2$. In this case, their sum will be called the point G_3 (x_3, y_3), coordinates of which are determined by comparing:

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 (\text{mod}\ p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\text{mod}\ p), \end{cases} \qquad (4)$$

where: $\lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} (\text{mod}\ p)$.

If $\boldsymbol{x_1 = x_2}$ and $\boldsymbol{y_1 = y_2 \neq 0}$, then the coordinates of the point $\boldsymbol{G_3}$ are determined as follows:

$$\begin{cases} x^3 = \lambda^2 - 2x_1 (\text{mod}\ p), \\ y^3 = \lambda(x_1 - x_3) - y_1 (\text{mod}\ p), \end{cases} \qquad (5)$$

where: $\lambda \equiv \frac{3x_1^2 + a}{2y_1} (\text{mod}\ p)$.

In the case when $\boldsymbol{x_1 = x_2}$ and $\boldsymbol{y_1 = -y_2}$ (mod $\boldsymbol{p}$) the amount of points G_1 and G_2 will be called the zero point 0 without specifying its x and y coordinates. In this case, the point G_2 *is* called as denial of point G_1. For the zero point 0 the equality $G + 0 = 0 + G = G$ have been performed, where: G – an arbitrary point of the elliptic curve E.

On the set of all points of an elliptic curve E, we introduce the operation subtraction, which we will denote by "–". According to the properties of points of elliptic curves, for an arbitrary point $G(x, y)$ of an elliptic curve the following equality holds:

$$-G(x, y) = G(x, -y) \qquad (6)$$

In accordance with equality (6), for two arbitrary points $G_1(x_1, y_1)$ and $G_2(x_2, y_2)$ of the elliptic curve E, the subtraction operation is defined as follows:

$$G_1(x_1, y_1) - G_2(x_2, y_2) = G_1(x_1, y_1) + G_2(x_2, -y_2) \qquad (7)$$

i.e., the subtraction operation can lead to the addition operation.

Regarding the presented addition operation the set of all points of an elliptic curve E, together with the zero point, form a finite Abelian (commutative) group of order w, for which the inequality[2]:

$$p + 1 - 2\sqrt{p} \leq w \leq p + 1 + 2\sqrt{p} \qquad (8)$$

have been performed.

Point G is called a point of multiplicity k, or simply fold point of the elliptic curve E, if for some point N the equality

$$G = \underbrace{N\text{"+"}\ldots\text{"+"}N}_{k} = [k]N \qquad (9)$$

have been performed.

The proposed algorithm uses the following parameters of EC:

a) prime p - module of an elliptic curve satisfying the inequality $p > \boldsymbol{2^{255}}$. Upper boundary of this number must be determined at the specific implementation of algorithm;

b) an elliptic curve E, defined by its invariant $J(E)$ or coefficients a, $b \in F_p$**;**

d) integer w - the order of the group of elliptic curve E;

e) prime n - the order of the cyclic subgroup of the elliptic curve E, for which the following conditions are performed:

$$\begin{cases} w = l * n, l \in Z, l \geq 1 \\ 2^{254} < n < 2^{256} \end{cases} \qquad (10)$$

f) point $G \neq 0$ of elliptic curve E, with coordinates $\boldsymbol{(x_p, y_p)}$, satisfying the equality $[n]G = 0$;

On the above parameters of the asymmetric algorithm impose the following requirements:

- must be satisfied $\boldsymbol{p^i} \neq 1$ (mod n) for all integers $i = 1, 2, \ldots, B$, where B satisfies $B \geq 31$;
- Should be performed the inequality $w \neq p$;

- Invariant of curve must satisfy the condition $J(E) \neq 0$ or 1728.

Each user of an asymmetric algorithm must have personal keys:

1**.** The public key of the encryption algorithm - the point of the elliptic curve *Q*, satisfying the equality $Q = [d]G$, where $G(x_0, y_0) \in E$ base point.

2. The private key of the encryption algorithm - an integer *d*, satisfying the inequality $0 < d < n$, where the order of the points of the elliptic curve, i.e. [*n*] G = 0.

Given *m* message on conditions $\rho = \pi - \mu = 16$ is divided into blocks $m = \{m_1, m_2, ..., m_i\}$, with a length $|m_i| = \mu$ bit, where π - symbol which defines capacity of a given prime number *p* and each m_i - blocks are separately encrypted in the following sequence.

2.1 The process of encryption.

1. Generate a random integer *k* that satisfies the inequality 0<*k*<*n*, calculate C_1=[*k*]*G* and *R*=[*k*]*Q* points of the elliptic curve.

2. The blocks of the message *m* are checked on the condition that the point is executed by an elliptic curve [11]. If the message is not a point of the elliptic curve, then go to the 6th step.

3. Using the *x*-coordinates of the point *M*(*x*, *y*) calculate the following value $w = (x^3 + ax + b) \bmod p$ and $y_{1,2} = \pm\sqrt{w} (\mathrm{mod}\ p)$.

4. If *y* = min(y_1,y_2) then, go to the 5th step.

5. Set value 3 to the variable *q* and calculate $C_2(x,y)=M(x,y)+R(x,y)$, $t = x_{C_2} \,||\, q$, and go to the 7th step (where |*q*| = 2 bits).

6. Set value 1 to the variable *q* and calculate $C_2(x,y)=M(x,y)+R(x,y)$, $t = x_{C_2} \,||\, q$, and go to the 7th step .

7. Set value 0 to the variable *q* and calculate $x_{C_2} = M \oplus x_R$, $t = x_{C_2} \,||\, q$.

8. $E_i=\{C_1(x, y), t\}$ – declare as blocks of encrypted text.

2.2 The process of decryption.

The sequence of decrypting an encrypted text E_i ($E_i=\{C_1(x, y), t\}$) to the open text is as follows.

1. Calculate $U(x_u, y_u) = [d]C_1$

2. If the condition *q*=0 is fulfilled go to the 8th step, otherwise perform the following calculation.

3. If *q*=3 go to the 4th step, in the case of *q*=1 go to the 6th step.

4. Calculate $w = x_{C_2}^3 + ax_{C_2} + b(\mathrm{mod}\ p)$.

5**.** Calculate $y_{1,2} = \pm\sqrt{w}(\mathrm{mod}\ p)$ and choose $y = \max(y_1, y_2)$, next go to the 9th step.

6. Calculate $w = x_{C_2}^3 + ax_{C_2} + b(\mathrm{mod}\ p)$.

7. Calculate $y_{1,2} = \pm\sqrt{w}(\mathrm{mod}\ p)$ and choose $y = \min(y_1, y_2)$, next go to the 9th step.

8. Compute plain text $M = x_{C_2} \oplus x_u$.

9. Compute text $M = (x_{C_2}, y) - U(x_u, y_u)$.

10. Using the algorithm [11] we transform the expression of points of the elliptic curve in the form of a message and obtain the open text *m*.

2.3 Correctness of the algorithm.

If the condition *q*=3 or *q*=1 is fulfilled, i.e. the message blocks are represented by the point of the elliptic curve:

$$
\begin{aligned}
&M(x, y) = (x_{C_2}, y) - U(x_u, y_u) = M(x, y) + R(x_r, y_r) - \\
&- U(x_u, y_u) = M(x, y) + [k]Q - [d]C_1 = \\
&= M(x, y) + [k][d]G - [d][k]G = M(x, y).
\end{aligned}
$$

When the condition *q*=0 is fulfilled, i.e. the message blocks are not represented by the point of the elliptic curve:

$$
\begin{aligned}
&M = x_{C_2} \oplus x_u = M \oplus x_R \oplus [d]C_1 = \\
&= M \oplus [k]Q \oplus [d][k]G = M \oplus [k][d]G \oplus [d][k]G = M
\end{aligned}
$$

An analysis of the increase in the size of the cryptogram for the proposed encryption algorithm compared to the size of the original message in different message length is given in table 1.

Table 1: Results of the size of the cryptogram.

Length of message (byte)	5242880	10485760	104857600
Expression by point EC (byte)	6429202	12841346	128510799
Encryption process (byte)	6378273	12757262	127572670
Decryption process (byte)	6429202	12841346	128510799
Recover message (byte)	5242880	10485760	104857600
Change of the size of cryptogram (%)	21,66%	21,66%	21,66%

3. CONCLUSION

Based on the result of the analysis, the proposed algorithm for encryption on elliptic curves in regard to the RSA algorithm increases the cryptogram size by 16% more than the size of the original message, and 2 times faster in speed.
In regard to the El-Gamal encryption algorithm has a 78% less cryptogram size and 4 times faster in speed.

The proposed algorithm in practice can be used not only to encrypt the transmission of the session key of a symmetric algorithm but also the message itself.

REFERENCES

1. O‘zDSt 2826:2014. ***State standard of the Republic of Uzbekistan. Information technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signature***. "Uzstandart". Tashkent. 2014.
2. GOST R 34.10-2012. ***The state standard of the Russian Federation. Information technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signature***. Gosstandart of Russia M.: 2012.
3. Aripov M.M., Kuryazov D.M. **Digital signature algorithm with composite module**, *Journal of the Academy of Sciences of the Republic of Uzbekistan*. Vol. 4, pp. 22-24, 2012.
4. Kuryazov D.M. **Digital signature algorithm on elliptic curves,** *VESTNIK National University of Uzbekistan*. Vol. 2, pp. 87-90, 2013.
5. Kuryazov D.M. **Modifications of DSA electron digital signature and their crypto analysis**, *VESTNIK Tashkent university of information technologies*. Vol. 2, pp. 19-23, 2012.
6. Kuryazov D.M. **Modifications of GOST R34.10-94 electron digital signature and their crypto analysis**, *Uzbek Journal of the problems of informatics and energetics*. Vol. 4-5, pp.75-80, 2012.
7. Kuryazov D.M. **Electronically digital signature on elliptical curves with increased durability**, *Collection of reports of the Republican Scientific and Technical Conference of young scientists, researchers, undergraduates "Information Technologies and Telecommunications Problems"*, Tashkent 14-15 march, 2013. Tashkent university of information technologies. Part 1. pp. 254-255.
8. Aripov M.M., Kuryazov D.M. **Signature algorithm the basis of the two independent difficult problems**, *Collection in the materials of the international scientific conferences, Actual problems of applied mathematics and information technologies. Al-Khorazmiy-2014.* Samarkand 15-17 September, 2014. Vol. 2, pp. 59-63.
9. Aripov M.M., Kuryazov D.M. **About one algorithm of digital signature with increased stability**, *Collection of materials of the III-International Scientific and Practical Conference*, Astana 15-16 October, 2015, pp. 35-39.
10. Dernova E.C., Moldovyan N.A. **Synthesis of digital signature algorithms based on several computationally difficult problems**, *Journal Voprosi zashiti informasi*, Vol. 1, pp. 22-26, 2008.
11. Moldovyan N.A., Ryzhkov A.V. **A method for commutative encryption based on probabilistic encryption**, *Journal Voprosi zashiti informasi*. Vol. 3, pp. 3-10, 2013.
12. Bolotov A.A, Gashkov S.B. and etc. ***Algorithmic foundations of elliptical cryptography***, Moscow: MPEI, 2000, -100 p.
13. Gorbenko I.D., Balagura D.S. **Directional encryption schemes in groups of points on an elliptic curve**, *Bulletin of Kharkiv National University of Radio Electronics.* Vol. 2, 2002.
14. Miller V. **Use of elliptic curves in cryptography**, *Advances in cryptology* – CRYPTO’85, Santa Barbara, Calif., 1985, Lecture Notes in Comput.Sci., Vol.218, 1986.
15. Koblitz N. ***Introduction to elliptic curves and modular forms.*** Translation from English, Moscow: World, 1988.
16. Aripov M.M., Kuryazov D.M. **Algorithm of without key hash–function based on Sponge-scheme**, *International Journal of Advances in Computer Science and Technology*, Vol. 7(6), June, pp. 40-42, 2018. https://doi.org/10.30534/ijacst/2018/04762018