International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Optimal Asymmetric Data Encryption Algorithm

Kuryazov D.M.

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

Abstract: ***Today, public-key cryptosystems are particularly vulnerable to fetching ciphertext and adaptively matched plaintext attacks. To prevent such attacks, in practice, optimal asymmetric algorithms are used, for example, RSA-OAEP and etc. In this article, using the method of encoding messages by points of an elliptic curve, an optimal asymmetric algorithm is proposed for data encryption which is based on elliptic curves.***

Keywords: asymmetric algorithms, elliptical curves, encoding and decoding

1. Introduction

To date, the durability of modern asymmetric algorithms (data encryption and digital signature) is characterized by their propertiesto withstand all kinds of attacks and the laboriousness of the best known hacking algorithm [1-9].

The standards of asymmetric data encryption algorithms used in practice are based on the problems of factorizing a composite number and discrete logarithm in a finite group of 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 compared to the size of the original message, and also the decreasing strength due to the development of mathematical methods and cryptanalysis tools.

In recent years, elliptic cryptography has been intensively developed, discovered independently by N. Koblitz and V. Miller in 1985, in which the role of a one-sided function is played by scalar multiplication of a point by a constant, implemented on the basis of operations of addition and doubling of points of elliptic curves (EC) in finite fields of various characteristics [14-15].

In [11], a status of the directional encryption was considered, possibilities of implementing directional encryption in groups of points on the EC were substantiated, in [12], a method of commutative encryption was proposed using computations on the EC, which ensures the exponential strength of the commutative encryption algorithm and its performance increase compared to other algorithms [13].

For cryptosystems (symmetric and asymmetric), there exist Chosen-plaintext attack (CPA), Chosen-cipher text attack (CCA), and adaptive chosen plaintext attack (CCA-2). The CPA and CCA attacks were originally intended for active cryptanalysis of secret key cryptosystems.

The purpose of this cryptanalysis is to break the cryptosystem using open and encrypted messages received during the attack [18-21]. They were then adapted for cryptanalysis of public key cryptosystems.

Analysis shows that public key cryptosystems are especially vulnerable to CCA and CCA-2 [17]. Therefore, to prevent such attacks, in practice, optimal asymmetric algorithms are used, for example RSA-OAEP [16] and etc.

The purpose of this work is to propose an optimal asymmetric data encryption algorithm for EC using the method of encoding messages with EC points.

In the EC encryption algorithm considered below, μ - bit data block of the message m is encoded by the EC point M, which is then transformed with a secret key. As a result, the cryptogram represents some point C.

The decryption procedure involves performing inverse transformations over point C, after which point M is restored and decryption is performed, leading to the receipt of message m.

2. Main part

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

$$y^2 \equiv x^3 + ax + b \pmod{p}, \quad (1)$$

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

An invariant of an elliptic curve is a magnitude J (E) that satisfies the identity

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \pmod{p}, \quad (2)$$

The coefficients a, b of the elliptic curve E, according to the known invariant $J(E)$ are determined as follows

$$\begin{cases} a \equiv 3k \pmod{p} \\ b \equiv 2k \pmod{p}, \end{cases} \quad (3)$$

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

Pairs (x, y) that satisfy identity (1) are called points of the elliptic curve E; x and $y$are the x- and y-coordinates of the point, respectively.

The points of the elliptic curve will be denoted by $G(x, y)$ or G. Two points of an elliptic curve are equal if their corresponding x- and y-coordinates are equal.

On the set of all points of the elliptic curve E we introduce the addition operation, which we will denote by the "+" sign. For two arbitrary points $G_1(x_1, y_1)$ and $G_2(x_2, y_2)$of the elliptic curve E, we consider several options.

Let the coordinates of the points $G_1(x_1, y_1)$and $G_2(x_2, y_2)$ satisfy the condition $x_1 \neq x_2$. In this case, their sum will be called the point $G_3(x_3, y_3)$, the coordinates of which are determined by the following formula

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

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

If the equalities hold $x_1 = x_2$and$y_1 = y_2 \neq 0$, then we define the coordinates of the point G_3, as follows

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 (\text{mod } p), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\text{mod } p), \end{cases} \quad (5)$$

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

In the case when the condition $x_1=x_2$and$y_1=-y_2$ (mod p) is satisfied sum of the points G_1 and G_2 will be called the zero point 0, without determining its x- and y-coordinates. In this case, the point G_2 is called the negation of the point G_1. For the zero point 0, the equalities holds.

$$G"+"0=0"+"G=G, \quad (6)$$

where$G$ is an arbitrary point of the elliptic curve E.

On the set of all points of the elliptic curve E, we introduce the subtraction operation which we denote by the sign "-". By the properties of points on elliptic curves, for an arbitrary point G (x, y) of an elliptic curve, the following equality holds:

$$-G(x, y)=G(x, -y), \quad (7)$$

In accordance with equality (7), 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:

$$G_1(x_1, y_1) - G_2(x_2, y_2)=G_1(x_1, y_1) +G_2(x_2, -y_2), \quad (8)$$

i.e. a subtraction operation can be converted to an addition operation.

With respect to the introduced operation of addition, the set of all points of the elliptic curve E, together with the zero point form a finite abelian (commutative) group of order w, for which the inequality [2] holds.

$$p+1-2\sqrt{p} \leq w \leq p+1+2\sqrt{p}\ , \quad (9)$$

A point T is called a point of multiplicity k, or simply a multiple point of an elliptic curve E, if for some point N the equality

$$T = \underbrace{N"+"..."+"N}_{k} = [k]N\ , \quad (10)$$

2.1 Asymmetric encryption algorithm parameters.

The parameters of the asymmetric data encryption algorithm are:

a) a) prime number p is the modulus of an elliptic curve satisfying the inequality $p>2^{255}$. The upper bound of this number should be determined with a specific implementation of the asymmetric algorithm;
b) elliptic curve E defined by its invariant J (E) or coefficients
$a, b \in F_p$;
c) integer w is the order of group points of the elliptic curve E
d) prime number n is the order of the cyclic subgroup of group points of the elliptic curve E, for which the following conditions are satisfied:

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

e) point $G \neq 0$of the elliptic curve E, with coordinates (x_0,y_0), satisfying the equality $[n]G=0$.

The above parameters of the asymmetric encryption algorithm are subject to the following requirements:
a) the condition $p^i \neq 1 (\text{mod } n)$ must be fulfilled,for all integers
$i=1, 2..., B$, where B satisfies the inequality $B \geq 31$;
b) the inequality must be satisfied $w \neq p$.

Each user of the asymmetric encryption algorithm must have private keys:

a) The private key of the asymmetric algorithm d is an integer satisfying the inequality $0<d<n$;
b) the public key of the asymmetric algorithm Q is a point of an elliptic curve with coordinates (x, y) satisfying the equality $[d]G=Q$.

An asymmetric encryption algorithm based on elliptic curves includes the following processes: expressing a message with elliptic curve points, encrypting a message, decrypting a message, expressing elliptic curve points as a message.

To implement these processes, each user must know the parameters of the asymmetric encryption algorithm. Also, each user must have d private and $Q(x, y)$ public keys of the encryption algorithm.

Below processes of expressing a message with elliptic curve points, encrypting, decrypting and expressing elliptic curve points as a message are given.

2.2 Algorithm for expressing a message by points of an elliptic curve [12].

Specified S - the message for the next sequence is represented by an elliptic curve point.

1) Assign value of the counter i = 0, calculate the value $p' = p\,div\,2^{16}$ and compare p' and S as μ - bit binary numbers (div- operation of taking quotient). If $p' \leq S$, then go to step 6.
2) If $i< 2^{16}$, then form a 16-bit string r, the binary value of which is i. Otherwise, display the message "The point of the elliptic curve does not exist".

3) Assign $S \| r$ to the variable x, where the sign "||" denotes a concatenation operation and calculate the value $w = \left(x^3 + ax + b\right) \bmod p$
4) Calculate the Legendre symbol $\lambda = \left(\frac{w}{p}\right)$. If $\lambda = -1$, then increase the counter ($i = i+1$)) and go to step 2.
5) Calculate two root values $y_{1,2} = \pm\sqrt{w} (\bmod p)$ where $y_{1,2} \in \{1,2,..., p-1\}$, assign the larger value of $y_{1,2}$ to y and go to step 10.
6) If $i<2^{15}$, then form a 15-bit string r, the binary value of which is equal to i. Otherwise, display the message "No elliptic curve point exists".
7) Assign the value $S \| r$ to the variable x and calculate the value $w = \left(x^3 + ax + b\right) \bmod p$
8) Calculate the Legendre symbol $\lambda = \left(\frac{w}{p}\right)$. If $\lambda = -1$, then increase the counter ($i = i+1$)) and go to step 6.
9) Calculate two root values $y_{1,2} = \pm\sqrt{w} (\bmod p)$ where $y_{1,2} \in \{1,2,..., p-1\}$, assign the larger value of $y_{1,2}$ to y.
10) Output a pair of values (x, y) as coordinates of the point M (x, y) of the elliptic curve for the given message S.

2.3. An algorithm for expressing the points of an elliptic curve in the form of a message [12].

Let, M (x, y) be a point of an elliptic curve. Then the sequence of transition of a given point to S - the message goes as follows.

1) Calculate the value $w = \left(x^3 + ax + b\right) \bmod p$.
2) Calculate two root values $y_{1,2} = \pm\sqrt{w} (\bmod p)$, where $y_{1,2} \in \{1,2,..., p-1\}$
3) If $y=y_1$ then, $S = x div 2^{15}$. Otherwise, calculate $S = x div 2^{16}$ and S - announced by the corresponding message of the point M (x, y).

2.4 Encryption process.

Given M message by conditions $\mu = \pi - k_0 - k_1 - 16$ divided into blocks $M = \{m_1, m_2, ..., m_v\}$, length $|m_i| = \mu$ bits, where k_0, k_1 – natural numbers, π - a character that determines the length of a given prime number p, each m_i - blocks, separately encrypted according to the sequence below.

1) Generate a random integer k satisfying the inequality $0<k<n$, calculate $C_1=[k]G$ and $R=[k]Q$ elliptic curve points.
2) Randomly generate l - message of length k_1 bits.
3) Calculate $S_1 = \left(m_i \| 0^{k_0}\right) \oplus Hesh1(l)$, where $Hesh1$ - hash function [10] of length $\mu + k_0$ bits.
4) Calculate $S_2 = l \oplus Hesh2(S_1)$, where $Hesh2$ - hash function [10] of length k_1 bits.
5) Perform the operation $S = S_1 \| S_2$
6) It is checked whether the message S is an elliptic curve point.
   If the message is not an elliptic curve point, then go to step 12.
7) Using the x - coordinate of the point M (x, y), calculate the value $w = \left(x^3 + ax + b\right) \bmod p$
8) Calculate $y_{1,2} = \pm\sqrt{w} (\bmod p)$
9) If $y = \min(y_1, y_2)$ then, go to step 12.
10) Assign 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 step 12 (where $|q| = 2$ bits).
11) Assign 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 step 13.
12) Assign 0 to the variable q and calculate $C_2(x,y)=M(x,y)+R(x,y)$, $t = x_{C_2} \| q$.
13) $E_i=\{C_1(x,y),t\}$ –declare as blocks of ciphertext.

2.5. Decryption of cipher texts blocks.

The sequence of decrypting the ciphertext E_i ($E_i=\{C_1(x,y),t\}$) into the plaintext is as follows.

1) Calculate $U(x_u, y_u) = [d]C_1$
2) If q=0, then calculate $S = x_{C_2} \oplus x_U$ and go to step 10.
3) Calculate $w = \left(x_{C_2}^3 + ax_{C_2} + b\right) \bmod p$
4) Calculate $y_{1,2} = \pm\sqrt{w} (\bmod p)$
5) If q=3, then go to step 7.
6) Calculate y=min (y_1,y_2) and go to step 7.
7) Calculate y=max(y_1,y_2).
8) Calculate $M(x,y) = \left(x_{C_2}, y\right) - U\left(x_U, y_U\right)$.
9) $M(x, y)$ is expressed as message S.
10) Set the initial $\mu + k_0$ bit of message S to S_1, the last k_1 bit to S_2. i.e. $S_1||S_2=S$.
11) Calculate $l = S_2 \oplus Hesh2(S_1)$.
12) Calculate $Sm = S_1 \oplus Hesh1(l)$.
13) If the last k_0 bit of the Sm message ends with zero values, then the message is genuine and the start μ bit is declared as a plaintext block m_i.Otherwise, the message is not genuine.

2.6. Correctness of the proposed algorithm.

$$m_i \| 0^{k_0} = Sm = S_1 \oplus Hesh1(l) =$$
$$\left(m_i \| 0^{k_0}\right) \oplus Hesh1(l) \oplus Hesh1(l) = m_i \| 0^{k_0}$$

1st case.(q=0):

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

2nd case.(q=1 or q=3):

$$M(x,y) = \left(x_{C_2}, y\right) - U\left(x_U, y_U\right) =$$
$$= M\left(x,y\right) + R(x_r, y_r) - U\left(x_U, y_U\right) =$$
$$= M\left(x,y\right) + [k]Q - [d]C_1 =$$
$$= M\left(x,y\right) + [k][d]G - [d][k]G = M(x,y)$$

Below a comparison of the software results of the proposed optimal encryption algorithm (EA), elliptic curve (EC) encryption algorithm (EA) is given, RSAand RSA-OAEP (Table 1 and 2)

Table 1: Comparison of the time spent on the encryption, decryption process and the volume of cipher texts for non-optimal algorithms based on EC and RSA

Encryption algorithm (EA)	*Encryption algorithm (EA) based on elliptic curve (EC)**		*AlgorithmRSA*	
Open message length (bytes)	151928	1 671 208	151928	1 671 208
Change in ciphertext volume (%)	21,65 %	21,65 %	3,21 %	3,21 %
Time spent on encryption process (seconds)	16,91	184,876	29,936	332,297
Time spent on decryption process (seconds)	16,926	182,49	56,41	621,086

* this algorithm differs from the proposed one by the absence of a complement scheme[22]

Table 2: Comparison of the time spent on the encryption, decryption process and the volume of cipher texts for optimal algorithms based on EC and RSA-OAEP

Encryption algorithm (EA)	*Optimal EA based on EC*		*RSA-OAEPalgorithm*	
Open message length (bytes)	151928	1 671 208	151928	1 671 208
Change in ciphertext volume (%)	199 %	199 %	154 %	154 %
Time spent on encryption process (seconds)	41,06	451,433	76,814	848,243
Time spent on decryption process (seconds)	41,356	451,83	140,135	1558,147

3. Conclusions

Analysis of the software results shows the following:

1) EA on EC increases the size of the cryptogram by 18.44% more than the RSA algorithm, and 2.2 times faster in speed.
2) The optimal EA on the EC increases the volume of the cryptogram by 45% more than the RSA-OAEP algorithm, and 2.4 times faster in speed.
3) These results were obtained using a computer with the following configuration: 64-bit Intel (R) Core (TM) 2 Quad CPU Q8400 2.67 GHz, 4 GB RAM

References

[1] O'zDSt 2826: 2014. State standard of the Republic of Uzbekistan. Information technology. Cryptographic information protection. Processes of formation and verification of electronic digital signature. "Uzstandart". Toshkent. 2014.
[2] O'zDSt 1092: 2009. State standard of the Republic of Uzbekistan. Information technology. Cryptographic information protection. Processes of formation and verification of electronic digital signature. "Uzstandart". Toshkent. 2009.
[3] Aripov M.M., Kuryazov D.M. On one EDS algorithm with a composite module // Reports of the Academy of Sciences of the Republic of Uzbekistan. No. 4, 2012, pp. 22-24.
[4] Kuryazov D.M. EDS algorithm on elliptic curves // Bulletin of the National University of Uzbekistan. No. 2, 2013, pp. 87-90.
[5] Kuryazov D.M. Modifications of the DSA EDS algorithm and their cryptanalysis // Bulletin of the Tashkent University of Information Technologies. No. 2, 2012, pp. 19-23.
[6] Kuryazov D.M. Modifications of the EDS algorithm GOST R34.10-94 and their cryptanalysis // Journal of Informatics and Energy Problems. No. 4-5, 2012, pp. 75-80.
[7] Kuryazov D.M. EDS on elliptic curves with increased durability// Collection of reports of the Republican scientific and technical conference of young scientists, researchers"Information technologies and problems of telecommunications", TUIT March 14-15, 2013, Tashkent. Part 1, pp. 254-255.
[8] Kuryazov D.M. EDS based on the complexity of solving two difficult problems // Collection in the materials of international scientific conferences, Actual problems of applied mathematics and information technology. Al-Khwarizmi 2014. SamarkandSeptember 15-17, 2014, Volume 2, pp. 59-63.
[9] Aripov M.M., Kuryazov D.M. About one EDS algorithm with increased durability // Proceedings of the III-International Scientific and Practical Conference, Astana October 15-16, 2015, pp. 35-39.
[10] Aripov M.M. and Kuryazov D.M. Algorithm of without key hash–function based on Sponge-scheme // International Journal of Advances in Computer Science and Technology, 7(6), June 40-42, 2018.
[11] Gorbenko I.D., Balagura D.S. Directional encryption schemes in groups of points on an elliptic curve. // Bulletin of the Kharkov National University of Radio Electronics. 2002, No. 2.
[12] Moldovyan N.A., Ryzhkov A.V. A commutative encryption method based on probabilistic coding. // JournalofInformationSecurityIssues. 2013, No. 3, p. 3-10.
[13] Bolotov A.A., Gashkov S.B. and others. Algorithmic foundations of elliptic cryptography. - Moscow: MEI, 200.-100p.
[14] Miller V. Use of elliptic curves in cryptography // Advances in cryptology–CRYPTO'85 (Santa Barbara, Calif., 1985). 1986. (LectureNotesinComput.Sci.; V.218).
[15] Koblitz N. Introduction to elliptic curves and modular forms // Translated from English. - Moscow: Mir, 1988.

[16] M.Bellare and P.Rogaway. Optimal asymmetric encryption. In A. de Santis, editor, Advances in Cryptology-Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science 950, pages 92-111. Springer-Verlag 1995.
[17] Mao, Wenbo. Modern cryptography: theory and practice.-M.: Publishing house "Williams", 2005.-768 p.
[18] Abdurakhimov B.F. and Sattarov A.B. An algorithm for constructing S-boxes for block symmetric encryption // Universal Journal of Mathematics and Applications, №1, May 29-32, 2018.
[19] Sattarov A.B. About the algorithm of data encryption BTS // International Journal of Advances in Computer Science and Technology, 7(6), June 36-39, 2018.
[20] Abdurakhimov B.F., Sattarov A.B. Algebraic immunity of Boolean function // Computational technologies. 2019. V.24. №5. pp. 4-12. doi.org 10.25743/ ICT.2019.24.5.002.
[21] Akhmedov B.B., Aloev R.D. Application of quadratic cryptanalysis for a five round XOR modification of the encryption algorithm GOST 28147-89 // International Journal of Science and Research (IJSR), Volume 9 Issue 8, August 2020, 1101 – 1109, ISSN: 2319-7064, India.
[22] Kuryazov D.M. Algorithm for ensuring message confidentiality using elliptic curves // International journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Vol. 9 (1), January - February 2020, pages 295- 298. doi.org /10.30534 / ijatcse / 2020 / 44912020.