Optimal Asymmetric Data Encryption Algorithm

Kuryazov D.M.[1]

[1] National University of Uzbekistan, Uzbekistan

Received: 12 June 2021 Accepted: 4 July 2021 Published: 15 July 2021

Abstract

Today, public-key cryptosystems are particularly vulnerable to fetching cipher text 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.

Index terms— asymmetric algorithms, elliptical curves, encoding and decoding

1 Introduction

o date, the durability of modern asymmetric algorithms (data encryption and digital signature) is characterized by their properties to withstand all kinds of attacks and the laboriousness of the best known hacking algorithm **??**1][2][3] **??**4] **??**5] **??**6] **??**7] **??**8] **??**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. **??**oblitz and V. Miller in 1985, in which the role of a onesided 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][19][20]. They were then adapted for cryptanalysis of public key cryptosystems.

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, -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 II.

3 Mainpart

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?F p , satisfying the identityy 2 ? x 3 + ax + b (mod ?) , (1)

where a, b? F p and 4a 3 + 27b 2 is not comparable to zero mod p.

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

.

An invariant of an elliptic curve is a magnitude J (E) that satisfies the identity) (mod 27 4 4 1728) (2 3 3 p b a a E J + = ,**(2)**

The coefficients a, b of the elliptic curve E, according to the known invariant J (E) are determined as follows? ? ? ? ?), (mod 2) (mod 3 p k b p k a (3) where, p), (-J(E) J(E) k mod 1728 = J(E) ? 0 or 1728.

Pairs (x, y) that satisfy identity (1) are called points of the elliptic curve E; x and yare the x-and ycoordinates 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 ? 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 t he following formula? ? ? ? ? ? ? ? ? ? ?), (mod) (

), (mod1 3 1 3 2 1 2 3 p y x x y p x x x ? ? (4)

where ,

). (mod1 2 1 2 p x x y y ? ? ? ? If the equalities holdx 1 =x 2 andy 1 = y 2 ? 0 ,then we define the coordinates of the point G 3 , as follows ? ? ? ? ? ? ? ? ? ? ?), (mod) ( ), (mod 2 1 3 1 3 1 2 3 p y x x y p x x ? ? (5) Where,). (mod 2 3 1 2 1 p y a x + ? ?

In the case when the conditionx 1 =x 2 andy 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 ycoordinates. 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, (**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) , (**7**) G 1 (x 1 , y 1) -G 2 (x 2 , y 2)=G 1 (x 1 , y 1) +G 2 (x 2 , -y 2),**(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 p w p p 2 1 2 1 + + ? ? ? + ,**(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 equalityN k N N T k] [" "..." " = + + = ? ?? ? ?? ? ,**(10)**

4 III. Asymmetric Encryption Algorithm Parameters

The parameters of the asymmetric data encryption algorithm are:

1. Prime number p is the modulus of an elliptic curve satisfying the inequality ?>2 255 . The upper bound of this number should be determined with a specific implementation of the asymmetric algorithm; 2. Elliptic curve E defined by its invariant J (E) or coefficientsa, b?F ? ; 3. Integer w is the order of group points of the elliptic curve E 4. 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: The above parameters of the asymmetric encryption algorithm are subject to the following requirements:? ? ? < < ? ? =

1. The condition ? i ? 1(mod n)must be fulfilled,for all integersi=1, 2?, B , where ? satisfies the inequality B ? 31; 2. The inequality must be satisfied w ? ?.

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

1. The private key of the asymmetric algorithm d is an integer satisfying the inequality 0<d<n; 2. 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 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: 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.

6 a) 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. and compare p? and S as µ -bit binary numbers (div-operation of taking quotient). If p? ? 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". b) 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. ? ? ? = k k ? µ divided into blocks { }, ,..., , 2 1 v m m m M = length µ = i m

bits, where k 0 ,k 1 -natural numbers, ? -a character that determines the length of a given prime number p, each m iblocks, separately encrypted according to the sequence below.

2. Randomly generate l -message of length k 1 bits.

7 Calculate

8 ( ) ( )

l Hesh m S k i 1 0 || 0 1 ? =

, where Hesh1hash function [10] of length0 k + µ bits. 4. Calculate ( ) 1 2 2 S Hesh l S ? =

, where Hesh2 -hash function [10] of length 1 k bits.

9 Perform the operation

C 2 (x,y)=M(x,y)+R(x,y), q x t C || 2 =

, and go to step 12 (where | q | = 2 bits). 11. Assign 1 to the variable q and calculateC 2 (x,y)=M(x,y)+R(x,y), q x t C || 2 =

, and go to step 13. 12. Assign 0 to the variable q and calculate C 2 (x,y)=M(x,y)+R(x,y), q x t C || 2 = . 13. E i ={C 1 (x,y),t} -declare as blocks of ciphertext.

10 d) 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. M x x M x x M x x M x x M G k d G d k G k d Q k C d R u C = ? ? = = ? ? = = ? ? = ? =]][[ ]][[ ]][[ ] [ ] [1 2

2 nd case, (q=1 orq=3):( ) ( ) ( ) ( ) ( ) ( )) , ( ]][[ ]][[,

Optimal Asymmetric Data Encryption Algorithm

3. Calculate w = (x C 3 2 + ax C 2

4. Calculate y 1 , 2 = ± w (mo

5. 8. Calculate M (x , y) = ( ) (C U y x , 2 ? U x

9. M (x, y) is expressed as message S.

10. Set the initial µ + k 0

11. Calculate l Sm = 2 = S ( ) 1 2 S ( ) l Hesh Hesh 1 1 ? ? S . .

12. Calculate

13.

45

1. Generate a random integer k satisfying the inequality0<k<n, calculate C 1 =[k]G and R=[k] Qelliptic curve points.

( ) H

1. Calculate (U x u

2. If q=0, then calculate S

10.

Figure 1:

[// Journal of Information Security Issues ()] , *// Journal of Information Security Issues* 2013. (3) p. .

[Moldovyan and Ryzhkov] *A commutative encryption method based on probabilistic coding*, N A Moldovyan , A V Ryzhkov .

[Sattarov ()] 'About the algorithm of data encryption BTS'. A B Sattarov . *International Journal of Advances in Computer Science and Technology* June 36-39, 2018. 7 (6) .

[Abdurakhimov and Sattarov ()] *Algebraic immunity of Boolean function // Computational technologies*, B F Abdurakhimov , A B Sattarov . 10.25743/ ICT.2019.24.5.002. 2019. p. .

[Kuryazov (2020)] 'Algorithm for ensuring message confidentiality using elliptic curves // International journal of Advanced Trends in'. D M Kuryazov . `30534/ijatcse/2020/44912020` *Computer Science and Engineering (IJATCSE)* January -February 2020. 9 (1) p. .

[Aripov and Kuryazov (2018)] 'Algorithm of without key hash-function based on Sponge-scheme'. M M Aripov , D M Kuryazov . *International Journal of Advances in Computer Science and Technology* June. 2018. 7 (6) p. .

[Bolotov et al.] *Algorithmic foundations of elliptic cryptography*, A A Bolotov , S B Gashkov , Others . Moscow: MEI. p. .

[Abdurakhimov and Sattarov ()] 'An algorithm for constructing S-boxes for block symmetric encryption'. B F Abdurakhimov , A B Sattarov . */ Universal Journal of Mathematics and Applications* May 29-32. 2018. 1.

[Gorbenko and Balagura][Gorbenko and Balagura]Analysis of the software results shows the following: 1. EA on EC increases the s *Directional encryption schemes in groups of points on an elliptic curve*, I D Gorbenko , D S Balagura .

[Koblitz ()] *Introduction to elliptic curves and modular forms // Translated from English*, N Koblitz . 1988. Moscow: Mir.

[Mao ()] Wenbo Mao . *Modern cryptography: theory and practice. -M.: Publishing house "Williams*, 2005. (768 p)

[Bellare and Rogaway ()] 'Optimal asymmetric encryption'. M Bellare , P Rogaway . *Advances in Cryptology-Proceedings of EUROCRYPT'94*, Lecture Notes in Computer Science A De Santis (ed.) 1995. Springer-Verlag. 950 p. .

[These results were obtained using a computer with the following configuration: 64-bit Intel (R) Core (TM) 2 Quad CPU Q8400 '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. 14-15'. *Tashkent. Part* 2013. 1 p. .

[Miller ()] 'Use of elliptic curves in cryptography // Advances in cryptology-CRYPTO'85'. V Miller . Lecture Notes in Comput. Sci 1985. 1986.