Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/160112

New Algorithms for Electronic Digital Elliptic Curves

*Mirsaid Aripov and Davlatyor Kuryazov**

National University of Uzbekistan named after Mirzo Ulugbek, Republic of Uzbekistan

Received: 24 Jul. 2021, Revised: 25 Dec. 2021, Accepted: 28 Dec. 2021
Published online: 1 Jan. 2022

Abstract: The signature is the legal guarantor of the authorship of the document. With the wide distribution in the modern world of electronic forms of workflow, including confidential ones, the problem of establishing the authenticity and authorship of paperless electronic documentation has become especially urgent in the telecommunications network. The basic mechanism for solving such problems is an electronic digital signature. Based on the analysis of the development of digital signature standards, the article proposes and proves the correctness of new digital signature algorithms based on the complexity of the discrete logarithm on elliptic curves.

Keywords: Algorithm, digital signature, elliptic curve, discrete logarithm on an elliptic curve, factorization, discrete logarithm in a finite field.

1 Introduction

Cryptosystems on elliptic curves (EC) were proposed in 1985 by W. Miller and N. Koblitz [1,2,3,4].

The advantages of cryptographic algorithms on elliptic curves from a practical point of view are the large possibilities of choosing the group in which calculations are performed, the absence of a subexponential discrete logarithm algorithm in a group of points on an elliptic curve (with the exception of some special cases), that is, the lack of an algorithm $O\left(e^{\sqrt{n}}\right)$ is a complexity, since the exponential function that determines the basis of the cryptographic algorithm is not used here.

Nevertheless, most cryptographic algorithms, the durability of which is based on the complexity of discrete logarithm in a finite field, are quite easily transferred to the case of applications of elliptic curves.

The advantage of using EC to digitally sign messages, along with higher cryptographic strength, is that the signature length can be shortened (when using EC of a certain type over the GF(q) field).

This statement is based on the fact that, that the y coordinate of a point is uniquely determined by its sign and the value of the x coordinate . The sign of the y coordinate is found from the condition: if y>(p-1)/2, that's a plus, otherwise a minus. Therefore, instead of transmitting both coordinates of the point R EC, only the x coordinate and the sign of the y coordinate can be transmitted.

At the receiving end, to restore the value of the coordinate y, it is necessary to extract the square root from the right side of the equation EC f(x) modulo p and take the corresponding root value in the ring of integers Z_p.

If we compare the complexity of the problem of factorization of integers, discrete logarithm in multiplicative groups and discrete logarithm in the additive Abelian group of points EC, the latter look preferable.

This is shown in table 1, where is a comparison of approximate estimates of the complexity of cryptanalysis presented, based on the decomposition of integers (DI), discrete logarithm in a finite field (DLFF) and discrete logarithm in a group of points (DLGP) EC for different characteristics of fields and depending on the length of the key.

Taking into account that the complexity of performing the transformation in the Abelian group EC is estimated by the value $O(\log^2 q)$, and in the multiplicative group of the field- $O(\log^3 q)$, the advantages of using the former to build cryptosystems become obvious.

It should also be noted that cryptographic constructions whose complexity of analysis exceeds the value of 10^{50}, it is impractical to apply in practice [4,8], since these values exceed the capabilities of modern information processing technologies. Therefore, it is necessary to limit the key length to 400 bits in the EC.

* Corresponding author e-mail: kuryazovdm@mail.ru

Table 1: Comparison of the complexity of cryptanalysis

Key length (bit)	$DI\forall p$	$DLFF$ $for p=2$	$DLFF$ $for p\neq 2$	$DLGP\ \forall p$
100	$1,3*10^{7}$	$1,3*10^{7}$	$1,6*10^{11}$	$1,3*10^{15}$
200	$7,2*10^{9}$	$7,2*10^{9}$	$9,6*10^{16}$	$1,3*10^{30}$
300	$7,1*10^{11}$	$7,1*10^{11}$	$3,8*10^{21}$	$1,4*10^{45}$
400	$3*10^{13}$	$3*10^{13}$	$3,4*10^{25}$	$1,6*10^{60}$
500	$7,5*10^{14}$	$7,5*10^{14}$	$1,2*10^{29}$	$1,8*10^{75}$
600	$1,3*10^{16}$	$1,3*10^{16}$	$2,1*10^{32}$	$2*10^{90}$
700	$1,7*10^{17}$	$1,7*10^{17}$	$2,1*10^{35}$	$2,3*10^{105}$
800	$1,8*10^{18}$	$1,8*10^{18}$	$1,4*10^{38}$	$2,6*10^{120}$
900	$1,7*10^{19}$	$1,7*10^{19}$	$6,5*10^{40}$	$2,9*10^{135}$
1000	$1,3*10^{20}$	$1,3*10^{20}$	$2,3*10^{43}$	$3,3*10^{150}$

Thus, the durability of cryptographic transformation methods based on the use of the group law of addition of elements of an additive abelian group on the EC significantly exceeds the durability of similar methods based on the use of multiplicative fields.

The gain in durability is especially noticeable with large key sizes. This circumstance makes it possible to use cryptographic constructions of this type to build cryptographic protocols for various purposes.

Data encryption and digital signature algorithms based on elliptic curves and other mathematical complexities are proposed in [5,6,7,8,**?**,11,12,13,14,15,16].

In the article on the analysis of standards for electronic digital signatures of developed countries, new EDS algorithms on elliptic curves are proposed.

2 Main part

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

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

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

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

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

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

where, $k = \frac{J(E)}{1728-J(E)}(\mathrm{mod}\, p)$, $J(E) \neq 0$ 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

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

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

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

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

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

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.

$$G\text{“+”}0=0\text{“+”}G=G, (6)$$

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:

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

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:

$G_1(x_1, y_1) - G_2(x_2, y_2)$=$G_1(x_1, y_1) + G_2(x_2, -y_2)$, (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 [4] holds.

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

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

$$T = \underbrace{N'' +'' \ldots'' +'' N}_{k} = [k]N, (10)$$

The cryptographic stability of the proposed EDS scheme is based on the complexity of solving the discrete logarithm problem in a group of EC points [8, 13-16], and also on the durability of the hash function used [9].

Digital Signature Parameters:

–prime number p>2 -module EC;
–EQ E, given by coefficients a, b $GF(p)$ or invariant J(E);
–integer m = $E(GF(p))$ the order of the group of points EC;
–a prime number q is the order of a cyclic subgroup of a group of points EC whose value satisfies the conditions:

$$m = nq, n \in Z, n \geqslant 1, 2^{254} < q < 2^{256};$$

–point $P \in E(GF(p))$ with coordinates $(x_p, y_p) : P \neq O, [q]P = O$;
–the signature key is an integer $d : 0 < d < q$;
–signature verification key point $Q \in E(GF(p))$ with coordinates $(x_q, y_q) : [d]P = Q$.

Restrictions are imposed on the parameters of the EDS scheme:

–fulfilling the condition $p^t \neq 1 (\mathrm{mod} q)$, for everyone $t = 1, 2, ..., B$, where B satisfies the inequality $B \geqslant 31$;
–fulfilling the inequality $m \neq p$;
–fulfillment of the condition $J(E) \neq 0$ or $J(E) \neq 1728$, where is the invariant $J(E) = 1728(4a)^3/\Delta$, and $\Delta = -16(4a^3 + 27b^2)$.

3 1st Signature generation algorithm

Input data: message M, initial parameters (related to the elliptic curve) and the secret signature key. Output data: signature (r, s).

Steps of the signature generation algorithm:

1.Select a random number k in the interval $1 \leqslant k \leqslant q-1$, where q is the order of the base point G on a certain EC of the finite field.
2.Calculate $(x_1, y_1) = [k]G$, that is, we add the point G, k times on a certain EC one.
3.Calculate $r = x_1 \bmod q$. If r=0, then another k is generated and the calculation is performed anew.
4.Calculate the value of the "hash function" by the message M, that is, h=$H(M)$. If the value $H(M) \bmod q = 0$, then it is installed $H(M) \bmod q = 1$.
5.Calculate $s = (\mathrm{H(M)}d + kr)$, where the parameter d is the secret key is known only to the signatory.
6.If s = 0, then go back to step 1.
7.Output a pair (r, s) - signature to M.

Signature verification algorithm. Input data: message M, initial parameters (associated with an elliptic curve), public signature verification key and signature to M – pair (r, s). Output: a statement that the signature is valid or invalid.

Signature Verification Algorithm Steps:

1.If the conditions $1 \leqslant r, s \leqslant q-1$, if they are violated, then output "the signature is fake" and terminate the algorithm.
2.Calculate h= $H(M)$.
3.Calculate $w = r^{-1} \bmod q$.
4.Calculate $u_1 = sw \bmod q$.
5.Calculate $u_2 = (q - H(M))\, w \bmod q$.
6.Calculate $X = [u_1]G + [u_2]Q = (x_2, y_2)$.
7.If $x_2 \bmod q = r = x_1 \bmod q$, then output "the signature is valid", otherwise - "the signature is not valid", and terminate the algorithm.

Correctness of the 1-signature algorithm. The difference between this scheme and GOST R 34.10-2001 is that in the proposed modification, the expression $s = (\mathrm{H(M)}d + kr) \bmod q$, which will involve their different corresponding validation equations. Let's prove that any signature generated by the described algorithm will be "valid".

First of all, note that the parameters r and s do not exceed q-1, as residuals when dividing by q integers. At steps 3 and 6 of the signature generation algorithm, a check is performed that, that r, s $\neq$ 0. Therefore, the conditions of step 1 will be met whenever r and s are obtained by the signature generation algorithm.

Next, according to step 5 of the signature generation algorithm, we have $s = (H(M)d + kr) \bmod q$.

From here, we get $(H(M)d + kr - s)/q = t$ or $k = (qt + s - H(M)d)r^{-1}$.

These last three equalities are equivalent for an arbitrary non-negative integer t, including for t=d. Then for t=d from the last equality we get

$$k = sr^{-1} + (q - H(M))\, dr^{-1}.$$

The point G has the order q, that is $[q]G = 0$ and for everyone $k < q$ takes place $[k]\mathrm{G} \neq \mathrm{O}$.

The following equality holds:

$$[k]G = \left[sr^{-1} + (q - H(M))\, dr^{-1}\right] G =$$

$$= \left[sr^{-1}\right] G + \left[(q - H(M))\, r^{-1}\right] [d]G =$$

$$= [sw]G + [(q - H(M))\, w]Q = [u_1]G + [u_2]Q = X.$$

Where $[d]\mathrm{G} = \mathrm{Q}$, that is, the public key of the signatory subscriber.

This means that the point X obtained at step 6 of the signature verification algorithm coincides with the point [k]G, generated upon receipt of the signature by the generation algorithm. The first X coordinate will be equal to x_1, and its remainder mod q will be equal to r, that is $x_1 \bmod q = r$, according to step 3 of the signature generation algorithm. Thus, the correctness of the algorithm is proved.

4 2nd Signature generation algorithm

Input data: message M, initial parameters (related to the elliptic curve) and the secret signature key. Output data: signature (r, s).

Steps of the signature generation algorithm:

1. Select a random number k in the interval $1 \leqslant k \leqslant q-1$, where q is the order of the base point G on a certain EC of the finite field.
2. Calculate $(x_1, y_1) = [k]G$, that is, we add the point G, k times on a certain EC one.
3. Calculate $r = x_1 \bmod q$. If $r=0$ or $k = 2dr \pmod q$, then another k is generated and the calculation is performed anew.
4. Calculate the value of the "hash function" by the message M, that is, $h = H(M)$. If the value $H(M) \bmod q = 0$, then it is installed $H(M) \bmod q = 1$.
5. Calculate $e := h(M||r)$.
6. Calculate $z := e^{-1} \pmod q$.
7. Calculate $s := (k - dr)z \bmod q$, where the parameter d is the secret key is known only to the signatory.
8. If $s = 0$, then go back to step 1.
9. Output a pair (r, s) - signature to M.

Signature verification algorithm. Input data: message M, initial parameters (associated with an elliptic curve), public signature verification key and signature to M – pair (r, s). Output: a statement that the signature is valid or invalid.

Signature Verification Algorithm Steps:

1. If the conditions $1 \leqslant r,s \leqslant q-1$, if they are violated, then output "the signature is fake" and terminate the algorithm.
2. Calculate $e := h(M||r)$.
3. Calculate $u = e \cdot s \pmod q$.
4. Calculate $X = [u]G + [r]Q = (x_2, y_2)$.
5. If $x_2 \bmod q = r = x_1 \bmod q$, then output "the signature is valid", otherwise - "the signature is not valid", and terminate the algorithm.

Correctness of the 2-signature algorithm. It needs to be proven that an arbitrary signature created using a generation algorithm must be verified the same in the verification algorithm.

r and s parameters from signature generation algorithm are taken as remainder of q, thus both are less than q-1. Furthermore, according to the third and seventh steps these parameters have values different than zero. In this case, for r and s parameters the first condition of signature verification algorithm is always true.

Using 6th and 7th steps of signature generation algorithm we derive $es = k - dr \pmod q$ equation. This yields $k = (es+dr) \bmod q$. As per algorithm, point G has nth order:

$$[k]G = [se + dr]G = [se]G + [r][d]G = [u]G + [r]Q = X.$$

The point X from the 4th step of the signature verification algorithm is equal to [k]G. The first X coordinate will be equal to x_1, and its remainder mod q will be equal to r, that is $x_1 \bmod q = r$, according to step 3 of the signature generation algorithm. Thus, the correctness of the algorithm is proved.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] Schneier B. *Applied Cryptography. Protocols, algorithms, and source codes in C*. - M.: Publishing house TRIUMF, 816 pages, (2003).

[2] Aripov M.M., Pudovchenko Yu.E. *The basics of cryptology*, Tashkent, 136 pages, (2004).

[3] Aripov M.M., Kuryazov D.M. Digital signature algorithm with composite module, *Journal of the Academy of Sciences of the Republic of Uzbekistan*, **4**, 22-24,(2012).

[4] Kharin Yu.S., Bernik V.I., Matveev G.V., Agievich S.V. *Mathematical and computer foundations of cryptology: a textbook*, - Minsk: New Knowledge, 382 pages, (2003).

[5] Moldovyan N.A., Guryanov D.Yu. Enhancing blind signature protocol security, *Journal Information Security Questions*, **4**, 3-6, (2012).

[6] Dernova E.C., Moldovyan N.A. Synthesis of digital signature algorithms based on several computationally difficult problems, *Journal Information Security Questions*, **1**, 22-26, (2008).

[7] Dernova E.C., Moldovyan N.A. Collective digital signature protocols based on the complexity of solving two difficult tasks, *Journal Information Security Questions*, **2**, 79-85, (2008).

[8] Kuryazov D.M. Algorithm for ensuring message confidentiality using elliptic curves, *International journal of Advanced Trends in Computer Science and Engineering (IJATCSE)* **9 (1)**, 295-298, (2020). doi.org /10.30534 / ijatcse / 2020 / 44912020.

[9] 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*, **7(6)**, 40-42, (2018). doi.org /10.34534 / ijacst / 2018 / 04762018.

[10] 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. **2**, 59-63, (2014).
[11] 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, 35-39, (2015).
[12] Kuryazov D.M. Development of electronic digital signature algorithms with compound modules and their cryptanalysis, *International Journal Mathematical Sciences & Cryptography*, **24**, Number 4, 1085-1099 (15), (2021).
[13] Kuryazov D.M. Optimal asymmetric data encryption algorithm, *Global Journal of Computer Science and Technology*, **21** Issue 2, 29-33, (2021).
[14] Priyanka Jaiswal & Sachin Tripathi, Cryptanalysis of Olimid's group key transfer protocol based on secret sharing, *Journal of Information and Optimization Sciences*, **39:5**, 1129-1137, (2018). DOI: 10.1080/02522667.2017.1292655.
[15] Manoj Kumar Chande, Cheng-Chi Lee & Chun-Ta Li, Cryptanalysis and improvement of a ECDLP based proxy blind signature scheme, *Journal of Discrete Mathematical Sciences and Cryptography*, **21:1**, 23-34, (2018). DOI: 10.1080/09720529.2017.1390845.
[16] Nissa Mehibel & M'hamed Hamadouche, A new enhancement of elliptic curve digital signature algorithm, *Journal of Discrete Mathematical Sciences and Cryptography*, **23:3**, 743-757, (2020). DOI: 10.1080/09720529.2019.1615673.

Mirsaid Aripov Doctor of Physical and Mathematical Sciences, Professor of the Department of Applied Mathematics and Computer Analysis of the National University of Uzbekistan. Research interests: information security, Nonlinear differential equation, Mathematical modeling, IT and Cryptology. Publications: over 100 scientific publications.

Davlatyor Matyakubovich PhD of Physical and Mathematical Sciences, independent applicant for the Department of Applied Mathematics and Computer Analysis of the National University of Uzbekistan. Research interests: information security, cryptography, cryptanalysis and mathematical foundations of information security. Publications: more than 30 scientific publications.