UDC 681.3.06

Parameters of the Fastest Cryptographically Strong Twisted Edwards Curves

A. Bessalov[1, a], V. Dykyi[1, b], A. Malyshko[1, c], O. Tsygankova[1, d], D. Yadukha[1, e]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Institute of Physics and Technology*

Abstract

An overview of twisted Edwards curves is given. The complexity of group operations for twisted Edwards curves is estimated. A computation minimization method using curve parameters minimum values selection is proposed. The tables of system-wide parameters for the 25 fastest crypto-strong twisted Edwards curves with field modulus lengths of 192, 224, 256, 384 and 521 bits are given.

Keywords: twisted Edwards curves, complete Edwards curves, order of a curve, order of a point, quadratic residue, quadratic nonresidue, computational complexity

Introduction

The term «twisted Edwards curves» was defined by Bernstein Daniel J. and others [1]. In this paper, adding the second parameter into the curve equation was in fact only a generalization of the original modified form of the Edwards-Bernstein curve [2], named in [1] as complete Edwards curve. Since in our papers [3, 4, 5, 6, 7, 8] we justify and narrow the notion of «twisted Edwards curves» down to a separate class of curves in the generalized Edwards form with properties unique for this class, in Section 1 we give a brief overview of the properties of this class. It will help to avoid misunderstandings in terminology, ambiguous in world literature.

Section 2 dwells upon the possible techniques for searching crypto-strong twisted Edwards curves with minimal complexity of group operations. In this paper, we fix $a = 2$, which is its minimum possible value, and then gradually increase the second parameter d until we find curves of almost prime order. The results of the calculation of system-wide parameters of 25 curves with standard values of the field modulus are given. A comparative analysis of the results of this and previous paper [5] is given.

1. Definition and properties of twisted Edwards curves

In [1], *twisted Edwards curves* were defined as a generalization of curves [2] with one parameter d by adding a new parameter a into the equation

$$ax^2 + y^2 = 1 + dx^2y^2, \text{ where } a, d \in F_p^*,$$
$$d(a-d) \neq 0,\ d \neq 1,\ p \neq 2.$$

Such curve with $a = 1$ in [1] is called *Edwards curve*, but if d is quadratic nonresidue ($\mathcal{X}(d) = -1$), it is called *complete Edwards curve*. This term is associated with the completeness of curve point addition law [2]. Thus, class of complete curves is a subclass of Edwards curves, and the latter is a subclass of twisted curves. This leads to confusion while calculating the number of isomorphisms or isogenies of different intersecting classes of curves and to the necessity of their separation to non-overlapping classes with specific properties. This problem was solved in [3, 7]. Let's define *the curve in the generalized Edwards form* by the equation

$$E_{a,d}:\ x^2 + ay^2 = 1 + dx^2y^2, \text{ where } a, d \in F_p^*,$$
$$d(a-d) \neq 0,\ d \neq 1,\ p \neq 2. \quad (1)$$

Now modified point addition law has the form

$$(x_1, y_1) + (x_2, y_2) = \\ = \Big(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2},\ \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\Big). \quad (2)$$

Doubling of a point according to (2) takes the form

$$2(x_1, y_1) = \Big(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2},\ \frac{2x_1y_1}{1 + dx_1^2y_1^2}\Big). \quad (3)$$

The usage of modified laws (2) and (3) allows us to keep horizontal symmetry (relative to the x axis) of the inverse points, conventional in theory of elliptic curves, instead of vertical symmetry [1, 2]. Now, if we define inverse point as $-P = (x_1, -y_1)$, according to (1) we get coordinates of the group's neutral element:

$$O = (x_1, y_1) + (x_1, -y_1) = (1, 0).$$

Except for neutral element O, there always exists a second-order point $D_0 = (-1, 0)$ on the axis x, for which according to (3), $2D_0 = (1, 0) = O$. Depending on the properties of parameters a and d it is possible to acquire two exceptional second-order points and two or four fourth-order points. As we can see from

[a] bessalov@ukr.net
[b] vladislav.dykyi@gmail.com
[c] an.malyshko@gmail.com
[d] oksana.valent@gmail.com
[e] dariya.yadukha@gmail.com

(1), the fourth-order points $\pm F_0 = \left(0, \pm\frac{1}{\sqrt{a}}\right)$ can be found on the axis y, for which $\pm 2F_0 = D_0 = (-1, 0)$. These points exist over the field F_p if the parameter a is a square (quadratic residue). We emphasize right away that, in accordance with the new classification [3], we determine the twisted Edwards curve (1) with $\mathcal{X}(a) = \mathcal{X}(d) = -1$. The 4th-order points $\pm F_0$, which belong to the curve, do not exist over a prime field (they appear in the extension F_{p^2}).

From equation (1) we determine the squares:

$$x^2 = \frac{1 - ay^2}{1 - dy^2},\ y^2 = \frac{1 - x^2}{a - dx^2},$$

that in some cases generate exceptional points at infinity (we put the sign ∞ when divided by 0):

$$D_{1,2} = \Big(\pm\sqrt{\frac{a}{d}}, \infty \Big);\ \ \pm F_1 = \Big(\infty, \pm\frac{1}{\sqrt{d}}\Big). \quad (4)$$

They occur in cases $\mathcal{X}(ad) = 1$ and $\mathcal{X}(d) = 1$ respectively. According to the rules of passage to the limit and the doubling law (3), we can verify that $2D_{1,2} = O$ and $\pm 2F_1 = D_0 = (-1, 0)$. In other words, under the conditions of their existence the exceptional points $D_{1,2}$ have the 2nd order, and the exceptional points $\pm F_1$ are 4th-order points.

In addition, points of the 4th order may exist as non-exceptional with non-zero x and y coordinates.

The substantiation of the new classification of curves in the generalized Edwards form is given in [3, 7]. The definitions of the 3 classes of these curves and the list of their fundamental properties are given below.

Depending on the properties of the parameters a and d, the curves in the generalized Edwards form (1) are divided into 3 non-intersecting classes:

- *Complete Edwards curves* with condition C_1:
$$\mathcal{X}(ad) = -1;$$
- *Twisted Edwards curves* with conditions $C_{2.1}$:
$$\mathcal{X}(a) = \mathcal{X}(d) = -1;$$
- *Quadratic Edwards* with conditions $C_{2.2}$:
$$\mathcal{X}(a) = \mathcal{X}(d) = 1.$$

The main properties of these classes of curves [6, 7, 8]:

1) Regarding 2nd-order points, the first class of complete Edwards curves over a prime field is a class of *cyclic* curves (with an exceptional 2nd-order point), while the twisted and quadratic Edwards curves form classes of *non-cyclic* curves (3 points of the 2nd order). The maximum order of points of the curves of the last classes do not exceed $\frac{N_E}{2}$.
2) The class of complete Edwards curves does not contain exceptional points.
3) Twisted Edwards curves only contain two exceptional 2nd-order points $D_{1,2} = \Big(\pm\sqrt{\frac{a}{d}}, \infty \Big)$, and the quadratic Edwards curves, besides them, contain two more exceptional 4th-order points $\pm F_1 = \Big(\infty, \pm\frac{1}{\sqrt{d}}\Big)$.
4) Edwards' twisted and quadratic curves form quadratic twist pairs based on the transformation of the parameters: $a' = ca,\ d' = cd,\ \mathcal{X}(c) = -1$.
5) In Edwards' classes of twisted and quadratic curves, the replacement $a \leftrightarrow d$ leads to isomorphism $E_{a,d} \sim E_{d,a}$.
6) The complete and quadratic Edwards curves are isomorphic to the curves with parameter $a = 1$: $E_{a,d} \sim E_{1,\frac{d}{a}}$. The introduction of a new parameter a into the equation of the curve (1) is justified only for the class of twisted Edwards curves.
7) Twisted Edwards curves with $p \equiv 1 \bmod 4$ do not contain 4th-order points.
8) For the odd-order points, the points addition law (2) is always complete (that is, the sum of any pair of points does not give an exceptional point).

Let us analyze some new properties of the 4th-order points.

Theorem 1. Non-exceptional 4th-order points

$$\pm F_2 = \Big(\sqrt[4]{\frac{1}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}} \Big)$$

of a curve in the form (1) with nonzero x exist if and only if one of the following conditions is satisfied:

i) $p \equiv 3 \bmod 4$: $\mathcal{X}(a) = \mathcal{X}(d) = -1$;
ii) $p \equiv 1 \bmod 4$: $\mathcal{X}(a) = \mathcal{X}(d) = 1, \quad ad = c^4$.

Proof.

1) *Necessity.* Exceptional points $\pm F_1 = \Big(\infty, \pm\frac{1}{\sqrt{d}}\Big)$ according to formulas (4) arise when $\mathcal{X}(d) = 1$ are excluded from consideration in accordance with the theorem. The points $\pm F_0 = \Big(0, \pm\frac{1}{\sqrt{a}}\Big)$ at $x = 0$ are also not considered. Let $F_2 = (x_1, y_1)$ be a 4th-order point of the curve (1), then $2F_2 = 2(x_1, y_1) = D_1$. According to (3) and (4), we have two equations:

$$\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2} = \sqrt{\frac{a}{d}},\ \frac{2x_1y_1}{1 + dx_1^2y_1^2} = \infty.$$

Hence $1 + dx_1^2y_1^2 = 0$, i.e. $x_1^2 + ay_1^2 = 0$, then $x_1^2 = -ay_1^2$. Since $x_1 \neq 0$, it follows that $y_1 \neq 0$. Here the second equality is based on equation (1) of the curve. According to the first equation and equality $x_1^2 = -ay_1^2$ we have

$$\frac{2x_1^2}{1 + \frac{d}{a}x_1^4} = \sqrt{\frac{a}{d}};$$
$$dx_1^4 - 2\sqrt{ad}x_1^2 + a = 0;$$
$$x_1^2 = \frac{a}{d},\ y_1^2 = \frac{-1}{\sqrt{ad}}.$$

Thus, we get 4 points with coordinates:

$$\pm F_{2,3} = \Big(\pm\sqrt[4]{\frac{1}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}} \Big), \quad (5)$$

which are defined in the formulation of the theorem. When $p \equiv 3 \bmod 4$ the element (-1) is a quadratic nonresidue [3], then $(-a)$ is a quadratic residue under conditions (i) and the equality $x_1^2 = -ay_1^2$ correctly links the squares of the coordinates of the point F_2. Let β be a primitive element of a multiplicative group F_p^*, and β^2 be the square of this group, then under condition (i) we have

$$\beta^2 = \beta^2\beta^{p-1} = \beta^{2+4k+2} = \beta^{4(k+1)}.$$

Then any square has square roots and 4th-order roots at $p \equiv 3 \bmod 4$. The necessity of the existence of the first coordinates in (5) while considering conditions (i) is proved. Taking into account conditions (i) and taking the value $\mathcal{X}(-\sqrt{ad}) = 1$ (i.e. as a quadratic residue, $\sqrt{ad}$ is a quadratic nonresidue), we get two solutions for the second coordinates for each point from (5). Since the squares ad and $\frac{a}{d}$ have 4th-order roots, such points exist under the conditions of the theorem. The necessity of conditions (i) of the theorem is proved.

If $p \equiv 1 \bmod 4$ (condition (ii) of the theorem), (-1) is a quadratic nonresidue. Then equality $x_1^2 = -ay_1^2$ holds if $\mathcal{X}(a) = 1$. For a square of the element of multiplicative group,

$$\beta^2 = \beta^2\beta^{p-1} = \beta^{2+4k} = \beta^{2(2k+1)}.$$

In this case, if $\beta = c^2$, number of elements c^4 is $\frac{p-1}{4}$ for all nonzero c. Both coordinates of $\pm F_{2,3}$ exist if $\mathcal{X}(a) = \mathcal{X}(d) = 1$ and $ad = c^4$ (or $\frac{a}{d} = c^4$ if $c \in F_p$). Then also for second coordinate $\frac{1}{ad} = \frac{c^4}{a^2} = e^4$. So, the necessity of condition (ii) is proved.

2) *Sufficiency.* Let condition (i) or (ii) be fulfilled. Then there exist 4 points

$$\pm F_{2,3} = \Big(\pm \sqrt[4]{\frac{1}{d}}, \pm\sqrt{\frac{-1}{\sqrt{ad}}} \Big),$$

for which according to (3) we get $\pm 2F_{2,3} = D_{1,2}$. We know that doubling 4th-order points gives 2nd-order points, so defined $\pm F_{2,3}$ are the points of 4th order. This proves the sufficiency of this theorem.

We can interpret points $\pm F_{2,3}$ as results of the division of 2nd-order points by two: $\frac{D_{1,2}}{2}$ [3, 6].

Example 1. Consider the curve

$$x^2 + 2y^2 = (1 - 2x^2y^2) \bmod 13$$

in condition (i) of the theorem 1. According to the theorem, this curve does not contain 4th-order points. This curve order is $N_E = 20$. In addition to the neutral element $O = (1, 0)$ it has 2nd-order points $D_0 = (-1, 0), D_{1,2} = (\pm 5, \infty)$, four 5th-order points and twelve 10th-order points.

Proposition 1. All Edwards curves (1) with constraints $\mathcal{X}(a) = \mathcal{X}(d) = -1$ have order $N_E = 4n$ (n is odd) if $p \equiv 1 \bmod 4$.

Proof. In conditions $\mathcal{X}(a) = \mathcal{X}(d) = -1$ of the theorem 1, provided that $p \equiv 1 \bmod 4$, the curve does not contain 4th-order points, but it contains non-cyclic 4th-order subgroup $G = \{O, D_0, D_1, D_2\}$ of 2nd-order points. Thus, the orders of all other points can be n and $2n$ (along with possible odd factors on n). So, the subgroup G_4 of the curve has the least possible even order of 4, and the order of the curve is $N_E = 4n$. The proposition is proved.

Complexities of twisted Edwards curves group operations are given in the paper [5]. Let M be the multiplication complexity in a field, S – squaring complexity, U – the complexity of multiplying by a curve's parameter. Then complexity of points addition in projective coordinates is $V_E = 10M + 1S + 2U$, and points doubling complexity is $T_E = 3M + 4S + 1U$. One can minimize computations and get the fastest curves by looking for strong curves with minimal values of the parameters a and d. Thus, one can disregard the complexity U in group operations' complexity estimation. Paper [8] demonstrates that in such way one reaches the highest possible 1.6 times exponentiation acceleration compared to a curve in the canonical Weierstrass form.

2. Results of system-wide parameters calculation with minimal effort for secure twisted Edwards curves

In this section, we consider the prime fields with modulus length 192, 224, 256, 384 and 512 bit, which are recommended by FIPS-186-4-2013 standard, and we give a list of parameters of Edwards twisted curves with almost prime order $N_E = 4n$ (n – prime) over each of the fields. The results of system-wide parameters calculations in the hexadecimal numeric system are presented in tables 1, 2. Here modulus of length L are defined as p_L. Fields modulus $p \equiv 5 \bmod 8$ were chosen as prime numbers, where element 2 is a quadratic nonresidue and also with small Hamming's weight (3, 4 or 5). For these fields, value $a = 2$ is fixed as minimal nonresidue. After that by successive incrementation we determine the minimum value of parameter d, for which co-factor n of curves order is a prime number. This algorithm is more time-consuming, than in previous work [5], but provides a real minimization of computational complexity and, accordingly, a maximum speed of a point exponentiation. Particularly, value $a = 2$ corresponds to one addition in the field, and this operation usually considered as free and ignored when evaluating computational complexity. The values of p, a and d, orders $n = \frac{N_E}{4}$ of the generators of the cryptosystem and it's coordinates $G = (x_G, y_G)$ are given for every curve.

Note that the parameter $a = 2$ is a quadratic residue only if $p \equiv 3 \bmod 8$. It means that binary notation of p ends with three least significant bits of $101 = 5_{10}$ or $011 = 3_{10}$. Other more significant bits are 0 mod 8. In paper [5], only one $p = 2^{255} + 2^{38} + 2^2 + 1$ from the table 5 meets these requirements (in this case $a = 2$), so almost all curves in [5] have minimal parameter $a = 3, 4$ or 5. Also, in [5] curves' characteristics p varied, so parameters d have lower values for some modules.

For primality testing of p and n we used Miller–Rabin and Lucas–Lehmer algorithms. To get elliptic curves orders we used SEA algorithm implemented in PARI/GP. Points G as cryptosystem's generators were found by doubling a random point that satisfies equality (1) (points on the non-cyclic twisted curve of order $4n$ have maximum order of $2n$).

Each of the tables below contains the parameters of five Edwards twisted curves with the minimum value of the parameter $a = 2$. Next, the parameter d was chosen as the smallest of values for which the order of the curve $4n$ is almost a prime number (n is a prime). The order of the curves by length is comparable to the length of the field.

Table 1. Twisted Edwards curves of almost simple order over a field with a p_{192} module

$p = 2^{191} + 2^7 + 2^2 + 1$
$a = 2$ $d = 75$ $n = 3FFFFFFFFFFFFFFFFFFFFFFFA5E98D264A3247C2080279DB$ $G = (9DAD8642BB8512CD04D60027BE9493DE1640463A58DE59AB,$ $418EF23E77465969D162144845CBF44F56D83BBF115FA360)$
$a = 2$ $d = 403$ $n = 3FFFFFFFFFFFFFFFFFFFFFFFA4921E1363EC97477CE976A5$ $G = (98BE568BA5729A219E776803DB9F69C290AB59F4EF6F7EF4,$ $2E85304CEA7AB5B8842D90445D1DAD93895E2DB882BAE03C)$
$a = 2$ $d = 444$ $n = 3FFFFFFFFFFFFFFFFFFFFFFFBCF8C3F3A9427E41498D1FD7$ $G = (4510134781D78C52243D05163EC96E1305AB7BB5259D8B78,$ $D0F4A5F9ADEFFCB4D2C6593922D7C8A1ABFC2AF172094EF)$
$a = 2$ $d = 701$ $n = 3FFFFFFFFFFFFFFFFFFFFFFFCC301E7BC46B1B6268218C5B$ $G = (5DACE51991F3072E8DD1C43135BDA689253A3414AC6EBD0,$ $C72DC9542D77078112A9E5A3B8AD479E6756EA390D0C9C00)$
$a = 2$ $d = 843$ $n = 400000000000000000000001BB72D3747512C1541EF15FD$ $G = (BDE8DCDD5D89E41598AD4398B889FCC45139EA67CD0736E3,$ $182B341DB3801311853E37A512AB80663AF2AABA26DEF6)$

Table 2. Twisted Edwards curves of almost simple order over a field with a p_{224} module

$p = 2^{224} + 2^9 + 2^8 + 2^5 + 2^3 + 2^2 + 1$
$a = 2$ $d = 655$ $n = 3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFCAB454858600D4A86945E8C39067$ $G = (95C9314D92D4D2A405CED7232A11B6E71EC6ED88CF47C7A71DF73D7A,$ $BA5AA0B63361BA004E89926FA72D4C54E838F6BEC0123D1F15A89266)$
$a = 2$ $d = 670$ $n = 400000000000000000000000034C80D4A988D5CD6E64C903566F9$ $G = (27000A0EFF81CD5309C702A0EE7F2744A2CAE17C33033292CD1791AE,$ $60175E973D3B107318D9C310FCFC603241A719EB015AD4B5F3FD33A7)$
$a = 2$ $d = 685$ $n = 400000000000000000000000036EFD5552A12746E859EA27957E5$ $G = (9E8D7BD75F8748B2FB93F506D679CF8869B498CE7A5488D3F9D3093A,$ $AD7542271AAE175E2D11A045E52FC5C6C40571917643D01481B8C067)$
$a = 2$ $d = 762$ $n = 3FFFFFFFFFFFFFFFFFFFFFFFFFFFFF903D2500B1E3CFB910E06E7DCD87$ $G = (FCA3FE7FA003F14B757960258532DDEFA132140A4CA0384355007761,$ $3B859287B870DCFE2CD164B11544F0081B764091F8F5FFD8C4E37175)$
$a = 2$ $d = 821$ $n = 3FFFFFFFFFFFFFFFFFFFFFFFFFFFFE7D952E7062C084F854E76880B1F$ $G = (2FB5347EB9639FB5BD6929642245F8ACA647D4ED6D3059D41E1C200A,$ $E6C8F06ADFB6C86D0FD3217ECBD2D344B10C26844584B9D3E52BC6D)$

Let us compare these results with the calculated parameters of curves in [5]. For 192-bit and 521-bit modules, the best parameters ($d = 75$ and $d = 77$ respectively) were calculated in this paper. But for the other three modules, the least parameters d are less than ones from tables 1, 2: $d = 38$ if $L = 224$, $d = 108$ if $L = 256$, and $d = 236$ if $L = 384$. It is understandable because varying p create additional curve variants. Thus, while selecting an appropriate curve, one should also consider the results of the paper [5].

Conclusions

In this paper, we describe twisted Edwards curves and propose the method for minimization of computations by selecting the minimum values of the curve's parameters. We present tables of system-wide parameters for the fastest crypto-strong twisted Edwards curves.

We note that suggested for standardization and implementation of twisted Edwards curves have the fastest point exponentiation speed. All calculated curves along with minimal $a = 2$ most often consist of only two or three decimal digits, so on practice calculation complexity of $1U$ and $2U$ are negligible for twisted curves. Estimations of point addition complexity $V_E = 10M + 1S + 2U$ and point doubling $T_E = 3M + 4S + 1U$ reach their lower bounds $V_E = 10M + 1S = \frac{32}{3}M$ and $T_E = 3M + 4S = \frac{17}{3}M$ if $S = \frac{2}{3}M$ [2]. Analogous results for the complete Edwards curve [3] are inferior to the results of this paper, because they have parameters d comparable to the sizes of modules, and $1U \cong 1M$. Also, in this paper, unlike in [3], the curves for the highest standard module p_{521} were calculated.

References

[1] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters, "Twisted Edwards Curves", *IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498,* 2008, pp. 1-17.

[2] D.J. Bernstein, T. Lange, "Faster Addition and Doubling on Elliptic Curves", *Advancesin Cryptology - ASIACRYPT'2007* (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security, Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833, Berlin: Springer, 2007, pp. 29–50.

[3] A.V. Bessalov, *Ellipticheskie krivyie v forme Edvardsa i kriptografiya. Monografiya [Edwards-shaped elliptic curves and cryptography. Monograph],* "Politekhnika", Kyiv, P.272, 2017.

[4] A.V. Bessalov, "Unikalnyje kriptograficheskie svoistva necyklicheskikh skruchennykh krivykh Edvardsa [The unique cryptographic properties of Edwards' non-cyclic twisted curves]", *Prikladnaya radioelektronika: nauchno-tekhn. zhurnal,* vol. 17, no. 1,2, pp.49-54, 2018.

[5] A.V. Bessalov, K.A. Oleshko, D.N. Porechnaya, O.V. Tsygankova, O.N. Chornyi, "Kriptostoikiye skruchennyie krivyie Edvardsa s minimalnoy slozhnostyu gruppovykh operacii [Crypt-Resistant Edwards Curved Curves with Minimal Complexity of Group Operations]",*Prikladnaya radioelektronika: nauchno-tekhn. zhurnal,* vol. 15, no. 3, pp.141–150, 2016.

[6] A.V. Bessalov, O.V. Tsygankova, "Vzaimosvyaz' semeistv tochek bolshikh poryadkov krivoy Edvardsa nad prostym polem [Interrelation of families of high-order points of the Edwards curve over a simple field]", *Problemy peredachi informacii,* vol. 51, no. 4, pp. 92-98, 2015.

[7] A.V. Bessalov, O.V. Tsygankova, "Chislo krivykh v obobtshchennoy forme Edvardsa s minimalnym chetnym kofaktorom poryadka krivykh [The number of curves in the generalized Edwards form with a minimal even cofactor of the order of the curve]", *Problemy peredachi informacii,* vol. 53 (1), pp. 101-111, 2017.

[8] A.V. Bessalov, O.V. Tsygankova, "Proizvoditelnost' gruppovykh operacii na skruchennoy krivoy Edvardsa nad prostym polem [Performance of group operations on a twisted Edwards curve over a simple field]", *Radiotekhnika,* no. 181, pp. 58-63, 2015.