Research of the graphic model of the points of the elliptic curve in the Edward form

Serhii Abramov[1,†], Volodymyr Sokolov[1,*,†] and Vadym Abramov[1,†]

[1] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudryavska str., 04053 Kyiv, Ukraine

Abstract

Elliptic curves in Edwards form, known for their speed and efficiency, are highly promising for asymmetric cryptosystems. The CSIDH protocol is particularly notable for post-quantum cryptography. Recent studies classify these curves and demonstrate CSIDH's implementation on quadratic and twisted Edwards curves, highlighting their unique properties through graphical models like the wheel representation of point exponentiation. The model in the form of a graph of points of an elliptic curve in the form of Edwards was studied. The algorithm for the reconstruction of the series of points kP of all groups of points of the Edwards curve without the use of a group operation for 1/8 of the known points has been refined. The possibility of reconstructing the order of these points is also shown.

Keywords

post-quantum cryptography, elliptic curve, point exponentiation, exponentiation graph, point reconstruction, reconstruction pattern

1. Introduction

Elliptic curves in Edwards's form [1], which have been studied and modernized by the authors of the work [2], today are the fastest and most promising in asymmetric cryptosystems. One of the promising protocols for post-quantum cryptography is CSIDH [3]. In work [4] a new classification of these curves is proposed, and in works [5, 6] the implementation of the CSIDH algorithm on quadratic and twisted Edwards's curves is substantiated and illustrated with examples. In works [7, 8] an analysis of the special properties of quadratic and twisted Edwards supersingular curves is carried out and a graphic model of the process of exponentiation of curve points in the form of a wheel is used. In [8], a method for finding all points of the scalar product kP of a point P is proposed if a segment of 1/8 of all points is known. Additional studies of the method of reconstruction of the points of these curves make it possible to further simplify and speed up the finding of these points and their orders.

An elliptic curve in the generalized Edwards form is defined by the equation [4]

$$E_{a,d}: x^2 + ay^2 = 1 + dx^2y^2, \quad \{a,d\} \in F_p^*, a \neq d, d \neq 1. \tag{1}$$

In case $\chi(ad) = 1, \chi(a) = \chi(d) = 1$ there is an isomorphism of the curve (1) with the *quadratic Edwards curve* [4]. The curve has a parameter d, which is defined as a quadratic excess, in addition, and for these curves, it is usually accepted $a = 1$. According to the classification [4], the quadratic curve is described by the equation:

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \chi(d) = 1, d \neq 1. \tag{2}$$

The modified law of adding curve points (1) is defined as [4]:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1y_1x_2y_2}, \frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2}\right). \tag{3}$$

The law of doubling the point (x_1, y_1), accordingly, has the form

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}\right). \tag{4}$$

Quadratic Edwards's curves (2) have a noncyclic subgroup of the 4th order, which includes three points of the 2nd order and a neutral element of the group of points O. Two of these points are special and have an infinite second coordinate. Curves (2) also have two singular points of the 4th order.

Special points of the second order

$$D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right) \text{ at } \frac{ad}{p} = 1.$$

Special points of the 4th order

$$\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right) \text{ at } \frac{d}{p} = 1.$$

When implementing crypto algorithms, it is necessary to know the order of the used points of the curve. The order of the point P is determined in the process of exponentiation of the point by multiplication by a scalar number k ($k = 1 \dots KP$) and construction of the exponentiation group $GK(P) = \{P, 2P, 3P, \dots, kP, \dots, KP\}$, where the K-order of the point if $KP = O(1,0)$, and numbers $P, 2P, \dots, KP$ form a group of curve points $GK = \{kP | k = 1 \dots KP\}$ [4].

Curve (2) with a minimum cofactor of 8 has an order $N_E = 8n$ (n is odd), while the maximum order of the point is equal

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine

* Corresponding author.
† These authors contributed equally.
s.abramov.asp@kubg.edu.ua (S. Abramov);
v.sokolov@kubg.edu.ua (V. Sokolov);
v.abramov@kubg.edu.ua (V. Abramov)

0000-0002-5145-2782 (S. Abramov);
0000-0002-9349-7946 (V. Sokolov);
0000-0002-8026-1475 (V. Abramov)

to $4n$. Let $P = (x_1, y_1)$, Ord $P = 4n$. Then, for example, a subgroup $\langle P \rangle = \{kP | k = 1 \dots 4n\}$ is cyclic and runs through all points kP where $k = 1 \dots 4n$. At the same time, there are 4 basis points $nP = F_1, 2nP = D_0, 3nP = -F_1, 4nP = O = (1,0)$. It is convenient to represent the cyclic subgroup of the curve (2) in the form of a wheel of exponentiation points (Bessalov's wheel) [4].

The exponentiation of curve points is carried out using expressions (3,4), which are quite complex, and therefore the creation of methods for simplifying and accelerating exponentiation is relevant for research [9–13]. In work [8], based on the interconnection of families of high-order points, the kP points of the Edwards curve are reconstructed without the use of group operations, reducing the number of point calculations to 1/8 of the order of the group.

2. Method description

This paper considers some features of the exponentiation process that can further simplify calculations.

Consider an example from work [14], which uses the Edwards quadratic curve (2) with parameters $a = 1, d = 5^2 \bmod 23 = 2$. At $p = 23$, it is supersingular and has an order $N_E = 24, n = 3$. The curve has base points $\pm F_1 = (0, +1), D_0 = (-1,0), O = (1,0)$, special points $(9, \infty), (-9, \infty), (\infty, 9), (\infty, -9)$ and two families of 8 non-basic points of high order in each $(\pm 5, \pm 10), (\pm 10, \pm 5), (\pm 6, \pm 11), (\pm 11, \pm 6)$. Table 1 shows the coordinates of the points of all its subgroups of orders $4n = 12$ and $2n = 6$.

A family of points of high order is eight points of a curve $(\pm x, +y)$, $(\pm y, \pm x)$ which lie on a plane x—y on one circle with a radius not equal to one (wheel of points). Fig. 1 shows an example of placing a family of points of high order in affine coordinates x, y. The family includes four points $(\pm x, \pm y)$ and four points where x and y coordinates are interchanged $(\pm y, \pm x)$. For convenience, the first 4 points can be called the initial subfamily, and the last four points can be called swap points (swap subfamily). Each family is located symmetrically for both the x-axis and the y-axis. We will call each family modulo the coordinates of the first point, which we will call the initial point.

Curve (2) of order $N_E = 24$ at $p = 23$ has four families of non-basis points of order 3, 6, and 12. These points are generators of cyclic exponentiation subgroups (rows). Table 1 shows these points and subgroups of their exponentiation. The curve under consideration has the following families: (5,10) it includes starting points (5,10) and swap points (10,5) (where the coordinates x, y have changed places), return points $(5, -10)$ and $(10, -5)$, as well as a mirror $(-5,10)$ and $(-10, 5)$. Similarly, the family $(6,11) = (6,11) + (11,6)$.

In Table 2, we can observe interesting features, for example, all doubling points of all groups (column 2P) are exclusively points of the family (5, 10) and then the points of this family also completely occupy columns 4P, 8P, and 10P.

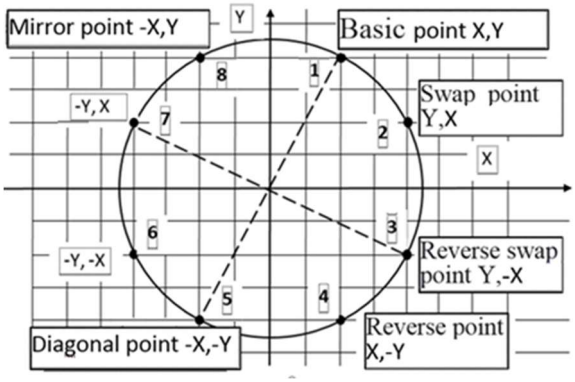

Figure 1: Symmetrical Location of the family of high-order points (x, y) on the affine plane

Table 1
Basic and special points

Point #	Group order	1P	2P	3P	4P
1	0	(1,0)			
2	1	$(-1,0)$	(1,0)		
Point order		2			
3	4	(0,1)	$(-1,0)$	$(0,-1)$	(1,0)
4	4	$(0,-1)$	$(-1,0)$	$(0,-1)$	(1,0)
Point order		4	2	4	
5	2	$(9,\infty)$	(1,0)		
6	2	$(-9,\infty)$	(1,0)		
Point order		2			
7	4	$(\infty,9)$	$(-1,0)$	$(\infty,-9)$	(1,0)
8	4	$(\infty,-9)$	$(-1,0)$	$(\infty,9)$	(1,0)
Point order		4	2	4	

In Table 2, the order of points is the same in all groups of the same order.

3. Wheel of exponentiation

For clarity and convenience of working with cyclic groups, all their points are offered $1P, 2P, \dots, KP$ arranged in a circle—Bessalov's exponentiation wheel [4] (Fig. 2).

The points of the wheel show the scalar coefficients multiplied by the point P is the generator of the group $< P >$. The coordinates of the points of the group are located on the outside of the wheel, and the order of the corresponding points is on the inside. The difference from Fig. 1 is that the points of the curve in Bessalov's wheel are in the order of their location in the exponentiation group and their number is equal to the order of the corresponding group. At the same time, the properties related to symmetry are similar. To construct each group of order K, it is necessary to carry out K operations of multiplication by a scalar coefficient $k = 1 \dots K$ [4].

Table 2
Families of high-order points

Point #	Group order	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$
1	6	(5,10)	(−5,10)	(−1,0)	(−5,−10)	(5,−10)	(1,0)
2	6	(5,−10)	(−5,−10)	(−1,0)	(−5,10)	(5,10)	(1,0)
Point order		6	3	2	3	6	
3	3	(−5,10)	(−5,−10)	(1,0)			
4	3	(−5,−10)	(−5,10)	(1,0)			
Point order		3	3				
5	12	(10,5)	(5,10)	(0,1)	(−5,10)	(−10,5)	(−1,0)
6	12	(10,−5)	(5,−10)	(0,−1)	(−5,−10)	(−10,−5)	(−1,0)
7	12	(−10,5)	(5,−10)	(0,1)	(−5,−10)	(10,5)	(−1,0)
8	12	(−10,−5)	(5,10)	(0,−1)	(−5,10)	(10,−5)	(−1,0)
9	12	(6,11)	(5,−10)	(∞,9)	(−5,−10)	(−6,11)	(−1,0)
10	12	(6,−11)	(5,10)	(∞,−9)	(−5,10)	(−6,−11)	(−1,0)
11	12	(−6,11)	(5,10)	(∞,9)	(−5,10)	(6,11)	(−1,0)
12	12	(−6,−11)	(5,−10)	(∞,−9)	(−5,−10)	(6,−11)	(−1,0)
Point order		12	6	4	3	12	2
13	6	(11,6)	(−5,−10)	(−9,∞)	(−5,10)	(11,−6)	(1,0)
14	6	(11,−6)	(−5,10)	(−9,∞)	(−5,−10)	(11,6)	(1,0)
15	6	(−11,6)	(−5,10)	(9,∞)	(−5,−10)	(−11,−6)	(1,0)
16	6	(−11,−6)	(−5,−10)	(9,∞)	(−5,10)	(−11,6)	(1,0)
Point order		6	3	2	3	6	
Point #	Group order	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$
5	12	(−10,−5)	(−5,−10)	(0,−1)	(5,−10)	(10,−5)	(1,0)
6	12	(−10,5)	(−5,10)	(0,1)	(5,10)	(10,5)	(1,0)
7	12	(10,−5)	(−5,10)	(0,−1)	(5,10)	(−10,−5)	(1,0)
8	12	(10,5)	(−5,−10)	(0,1)	(5,−10)	(−10,5)	(1,0)
9	12	(−6,−11)	(−5,10)	(∞,−9)	(5,10)	(6,−11)	(1,0)
10	12	(−6,11)	(−5,−10)	(∞,9)	(5,−10)	(6,11)	(1,0)
11	12	(6,−11)	(−5,−10)	(∞,−9)	(5,−10)	(−6,−11)	(1,0)
12	12	(6,11)	(−5,10)	(∞,9)	(5,10)	(−6,11)	(1,0)
Point order		12	3	4	6	12	

All of them are connected with the help of three basic points $D_i, \pm F_i$ form a symmetrical structure [4].

$$P \pm F = (x_1, y_1) + (0, \pm 1) = (\pm(-y_1), \pm x1).$$

Central symmetry relative to turning the wheel at 180° has diametrical points P and P^* located at the ends of the wheel diameter:

$$P + D = (x_1, y_1) + (-1,0) = (-x_1, -y_1) = P^*.$$

Vertical (mirror) symmetry is formed by points symmetrical about the vertical axis. These points are from the same family with the same y coordinate, and the x coordinate changes sign: these are points (x, y) and $(-x, y)$.

The points of the lower semicircle are determined similarly using the reverse (inverse) point at which the sign of the coordinate changes y: $-P = (x_1, -y_1)$.

In Table 2, point families $(10, 5)$ and $(6, 11)$ generate subgroups of maximum order 12 and $3P = F_1 = (\infty, 9)$ a singular point of the 4th order. Point $D = (9, \infty)$ is a singular point of the 2nd order. Consider the family $(10, 5)$ without singular points, its points are of order 12, and the wheel of points is presented in Fig. 2.

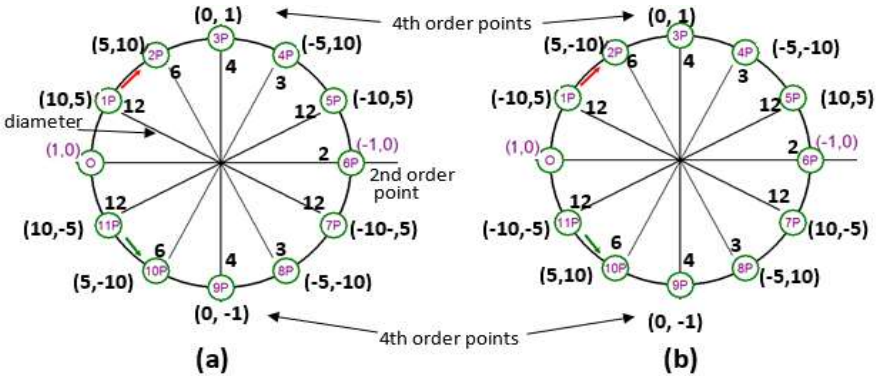

Figure 2: Model of 12 order of cyclic groups of points (a) $(10, 5), (10, -5)$ and (b) $(-10, 5), (-10, -5)$

The coordinates of the points are located near the corresponding scalar coefficient when going around the wheel clockwise from the generator point $1P = (10,5)$. The group of the inverse point—the generator $(10, -5)$ begins when going around counter-clockwise from point $11P$.

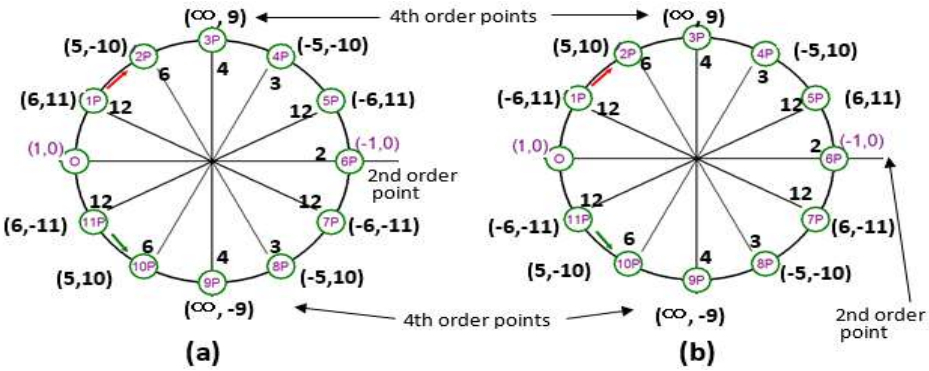

Figure 3: Model 12 of the order of cyclic groups of points (a) $(6,11), (6,-11)$ and (b) $(-6,11), (-6,-11)$

Inverse points with different signs of the y coordinate are located symmetrically on the horizontal axis, and points from the same family but different groups are located symmetrically on the vertical axis, i.e., they have the same y coordinate and the x coordinate has a different sign. Opposite points are located at the ends of the diagonal, where all coordinates have different signs.

Other groups of this family can be presented in the form of a transformed first wheel. The transformation consists of the fact that at odd points $(1P, 3P, \dots)$ we invert the sign of the X coordinate, and at even points $(2P, 4P, \dots)$ is the Y coordinate (Figs. 2b, 3b).

4. Wheel template of a cyclic group

The wheel in Fig. 2 shows the exponentiation of the points $(10,5)$ and $(10,-5)$, the other two groups (Fig. 2b) of this family, formed by the points $(-10,5)$ and $(-10,-5)$, can be presented in the form of a wheel that can be built by transforming the first wheel. The family at each point remains the same as in the previous wheel. It is possible to create (reconstruct) the wheel of other groups of this family based on the first group of the family without a table and complex calculations. Each of the 4 points of any subfamily (initial or swap) is located in different sectors. In each sector, there are points from different subfamilies, one from each, and the subfamilies themselves are not repeated. The wheel of all cyclic groups of the same order has the same arrangement of points. (Figs. 2, 3). This is convenient to use to create a wheel template of a given order. At the same time, you need to know the order of the exponentiation group. Fig. 4 shows a 12-order wheel template. Inside the wheel, the order of points is shown, valid for any group of this order. A more convenient view of the wheel of a large order is presented in the form of Fig. 5.

As with the wheel, Fig. 5 presents the points of the curve, the exponentiation factor k, and the order of the points r. To construct the entire group, as it was said in [4], it is enough to find the points of the first half-sector (1/8 part of all points of the wheel). Next, you should fill out the template according to certain rules.

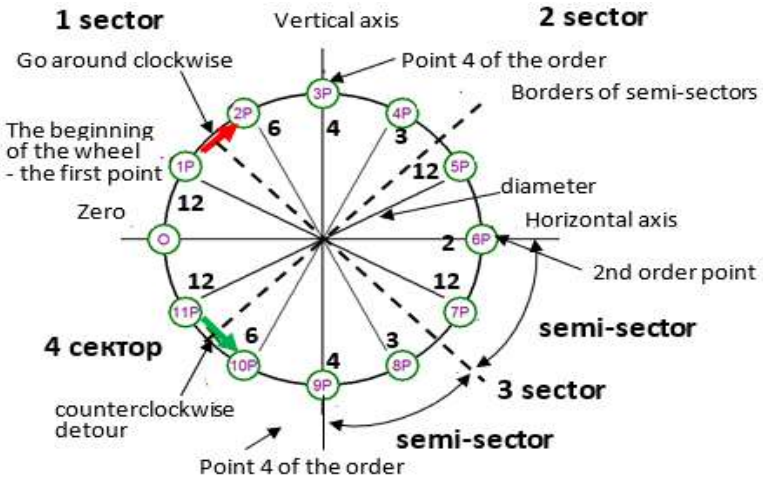

Figure 4: Exponentiation wheel template for group 12 order

0	1	2	3	4	5	6		Column number
1,0	10,5	5,10	0,1	-5,10	-10,5	-1,0		Point coordinates
12P	1P	2P	3P	4P	5P	6P		Points
1	12	6	4	3	12	2		Order of points
12P	11P	10P	9P	8P	7P	6P		Points
1,0			0, -1			-1,0		Point coordinates

Figure 5: The exposure wheel template for the 12-order group

5. Example of constructing the wheels of all cyclic groups of the Edwards curve

Consider an example from work [7], this is an Edwards curve of order $N_E = 28, d = 8, p = 19$.

From the solution of the equation, we get a complete set of curve points. In Table 3, the points are arranged in ascending order of the X coordinate. For ease of consideration, we write the $X > 9$ coordinate as $X = X - p = x - 19$.

Table 3

Calculation of curve points $N_E = 28, d = 8, p = 19$

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$X - P$	—	—	—	—	—	—	—	—	—	—	−9	−8	−7	−6	−5	−4	−3	−2	−1
X^2	0	1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1
Y^2	1	0	5	6	7	9	8	13	16	4	4	16	13	8	9	7	6	5	0
Y	1	0	±9	±5	±8	±3	—	—	±4	±2	±2	±4	—	—	±3	±8	±5	±9	0

There are base points $(0,1), (0,-1), (1,0), (-1,0)$ and 6 families of non-base points with 4 points each: $(2,9), (9,2), (3,5), (5,3), (4,8), (8,4)$.

Basic points 4, non-basic 24 (6 families of 4 points each), 28 points in total, curve order 28. It is convenient to use cyclic subgroups to find the order of points. Consider the cyclic subgroup formed by the point $(2,9)$, which is shown in Table 4 (Nt is the order of the point). Each point of the table is equal to the point $P(2,9)$ multiplied by k, i.e., equal kP. First, the subgroup order can be determined by calculating the first half-sector of the table (points $P, 2P, 3P$). As soon as we reached the point $F_1 = 7P(0,1)$ of order 4, it becomes clear that there is also point 2 of order $14P(-1,0)$, point 4 of order $21P(0,-1)$, and point $O(1,0)$. Total $7 \times 4 = 28$ points.

Table 4

All points of the curve

kP	P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$
X	2	−8	−3	−5	−4	−9	0	9	4	5	3	8	−2	−1
Y	9	4	5	3	8	−2	1	−2	8	3	5	4	9	0
Nt	28	14	28	7	28	14	4	7	28	14	28	7	28	2
kP	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$	$23P$	$24P$	$25P$	$26P$	$27P$	$28P$
X	−2	8	3	5	4	9	0	−9	−4	−5	−3	−8	2	1
Y	9	−4	−5	3	8	−2	−1	2	−8	−3	−5	−4	−9	0
Nt	28	7	28	14	28	7	4	14	28	7	28	14	28	1

The subgroup has order 28 and includes all points of the curve. The table has base points with a known order: points $7P$ and $21P$ order 4, $14P$ order 2, and neutral point $(1,0)$. Non-base points can have an order of 28, 14, and 7, you can find their orders using a minimum number of calculations. There are 28 points in the table and it ends with the point (1, 0), so the order of the generator point $(2,9)$ will be 28. The doubled point $2P$ has order 14, i.e., the point $2P$ must be multiplied by 14 to get the point $O(1,0) = 28P$ because 2 is a divisor 28, a $s = 28/k = 14$. Point $4P$ is transformed into point 28P by multiplying by 7 (7 steps), i.e., regardless of the order of point P, point $4P$ has order 7, since $28 = 4 \times 7$. From the points where k is a divisor of 28, you can reach zero in s steps by going through r cycles subgroups $28r = ks$, that is, when the integer $s = 28r/k$. Here K is the divisor of $28r$. In this equation, for a given and minimal r, we have an integer s.

For example, for the third point $3P$ we have to 3 then $s = N \times r/k = 28 \times r/3 = 2 \times 2 \times 7 \times r/3$. There are no common factors and the integer s can be at $r = k = 3$, then the order of this point is $s = 28$. For point $6P$ we have $K = 6 = 2 \times 3$ then $s = 2 \times 2 \times 7 \times r/2 \times 3$, we reduce by a common factor of 2 and get $s = 14$.

Applying this rule further, we will get a suitable template for each order of the group, for example, the following template for the point of order 28. Here the wheel is shown in the form of a table, the cells of the table are more convenient for filling with data (Fig. 6).

кP	1P	2P	3P	4P	5P	6P	7P	8P	9P	10P	11P	12P	13P
X													
Y													
N	28	14	28	7	28	14	4	7	28	14	28	7	28
28P													14P
1													-1
0													0
1													2
кP	27P	26P	25P	24P	23P	22P	21P	20P	19P	18P	17P	16P	15P
X													
Y													
N	28	14	28	7	28	14	4	7	28	14	28	7	28

Figure 6: Exponentiation Wheel template for points of order 28

6. Rules for reconstruction of points

Now in this template, you need to place the points that depend on the first point of $1P$. Rules and formulas to simplify this process are developed in [4]:

For a curve of order N, there can be subgroups of order $R_i \mid N$, and the first point 4 of the order F_1, if any, will appear on the step $(R_i/4) \times$ P.

Algorithm for constructing the wheel of the cyclic subgroup of the point P of the N[th] order curve.

1. The point P of the curve is the input.
2. Using the expressions $(3,4)$, we find the points $2P, 4P, 8P, \dots, 2^k$, etc.
3. If the last dot appeared from a family that was already significant, we moved to the second sector of the wheel. And point F_1 is between the last k and penultimate $(k-1)$ points $k < (R_i|N) < k-1$.
4. Hence, the order R_i of the point P is determined.
5. Choose the appropriate wheel template and fill it with points accordingly [4].

7. Reconstruction of points of all curve groups

Let's consider some properties of the wheel.

Examining the points of various curves, it is possible to identify some regularities. Yes, points from the same family are not repeated in each sector.

If the group has points of orders 2 and 4, then the order of this group is a maximum of $4n$. Then, on the border of the half-sector, we get points from swap families. For example, in groups $(3,5)$ (Table 5), the boundary of the semi-sector passes between points 3 and 4, and these points of families $(4,8)$ and $(8,4)$, respectively. When the calculation reaches point $4P$, we can find the remainder [4] without calculation, and determine the order of the group and all points.

If the group does not have a point of order 4, then the order of this group is $2n$. For example, in groups $(5,3)$, the border of sectors 1 and 2 passes between points 3 and 4 (Table 6), where the first mirror point from the families appears $(8,4)$.

If there are no points of order 2 and 4, then the order of this group is n. For example, in groups $(9,2)$, the boundary between the upper and lower semicircle passes between points 3 and 4 (Table 7). These are also mirror points of the family $(5,3)$.

Points of the same family are not repeated within the sector.

Table 5
Point group (3, 5)

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
x	3	−9	−4	8	2	5	0	−5	−2	−8	4	9	−3	−1	-3	9	4	-8	-2	-5	0	5	2	8	−4	−9	3	1
y	5	2	8	−4	−9	3	1	3	−9	−4	8	2	5	0	-5	-2	-8	4	9	-3	-1	-3	9	4	−8	−2	-5	0

Table 6
Point group (5, 3)

K	1	2	3	4	5	6	7	8	9	10	11	12	13	14
X	5	9	−8	8	−9	−5	−1	−5	−9	8	−8	9	5	1
Y	3	2	4	4	2	3	0	−3	−2	−4	−4	−2	−3	0

Table 7
Point group (9, 2)

K	1	2	3	4	5	6	7
X	9	8	−5	−5	8	9	1
Y	2	4	3	−3	−4	−2	0

Regularities are also preserved in curves of a higher order. For example, a curve $N_e = 80, a = 1, d = 2, p = 79$ its exponentiation table has the form presented in Fig. 7. If we choose the initial families as shown in the following Table 8.

Table 8
Initial families

x	2	34	23	13	6	20	30	37	15
y	24	14	12	18	19	27	29	8	22
	1	2	3	4	5	6	7	8	9

Then, about them, the swap families have the following form Table 9.

Table 9
Swap families

x	24	14	12	18	19	27	29	8	22
y	2	34	23	13	6	20	30	37	15
	1	2	3	4	5	6	7	8	9

The wheel for the generator (2,24) is shown in Fig. 7. The coordinates of the points are shown on the green background, the scalar exponentiation factor is on the yellow, and the orders of the points are on the gray *Pk*. All the properties described above are present. There is a neutral point $O(1,0)$, two special points of the 4th order $(\infty, \pm 35)$, and point 2 of the order. There is an opportunity for 1/8 of all points to reconstruct other points. Based on the obtained data, it is possible to reconstruct the rest of all groups of this family without even knowing 1/8 of its points.

For any group $P \times ki$ of order $\#G(x,y)$ regardless of the coordinates of the points, the orders are arranged in the same way. Of the order factors of the group $\#G(x,y) = g_1 \times g_2 \times \ldots \times g_s$ remove the elements that coincide with the multipliers of the scalar $ki = ki_1 \times ki_2 \times \ldots$, and the remaining factors give the value of the order of the points. For example, in our example with $\#G(x,y) = 40 = 2 \times 2 \times 2 \times 5$ for a point $8P = 2 \times 2 \times 2$ have $N(8P) = \underline{2 \times 2 \times 2} \times 5 = 5$. And for a symmetrical point $12P = 2 \times 2 \times 3$ have $\underline{2 \times 2} \times 2 \times 5 = 10$. The orders of the remaining symmetric points coincide.

X	2,	-34	23	-13	6	-20	-30	37,	-15,	∞,	15,	-37,	30,	20,	-6,	13,	-23,	34,	-2,	
Y	24	-14	12	18	19	-27	29	-8	-22	35	-22	-8	29	-27	19,	18	12	-14	24	
kP	P	2P	3P	4P	5P	6P	7P	8P	9P	10P	11P	12P	13P	14P	15P	16P	17P	18P	19P	
Ni	40	20	40	10	8	20	40	5	40	4	40	10	40	20	8	5	40	20	40	
(1,0)	First sector										Second sector									(-1,0)
40P																				20P
1	Fourth sector										Third sector									2
X	2,	-34	23	-13	6	-20	-30	37,	-15,	∞,	15,	-37,	30,	20.,	-6,	13,	-23,	34,	-2,	
Y	-24	14	-12	-18	-19	27	-29	8	22	-35	22	8	-29	27	-19,	-18	-12	14	-24	
kP	39P	38P	37P	36P	35P	34P	33P	32P	31P	30P	29P	28P	27P	26P	25P	24P	23P	22P	21P	
	40	20	40	10	8	20	40	5	40	4	40	10	40	20	8	5	40	20	40	

Figure 7: Exponentiation of order curve points $N_E = 80$

Consider one of the groups of maximal order, let its generator be the point $P(x_1, y_1)$. According to the rules (3,4), we calculate the first sector of its wheel. This includes points from half of all curve points, one point from each family, and points from it that are not repeated. Other points of the wheel belong only to these families.

The second half of the curve points includes the remaining swap points. The maximum order group is formed by the swap point generator $P(y_1, x_1)$, which is the first point of the group (and the wheel). Other points are taken from the wheel and changed according to the following rules:

1. Even points are taken from the initial families and odd ones from the swap families.
2. Coordinate signs are arranged as follows: at the second point, the sign of the x coordinate is inverted, at the 3rd point, both coordinates are inverted, at the 4th point, the coordinate is inverted, at the 5th point, the signs do not change, so the process is repeated until the sector is filled [15].

8. Conclusions

The considered properties make it possible to find all *kP* points of all groups of the curve by the value of 1/8 of the points of only one group (wheel). With the known order of the group, each exponentiation coefficient k corresponds to its order of the point, which does not depend on the coordinates of the point, but only on the order of the group and k. This can be used to create a template from which to reconstruct the exponentiation points and their orders, for example, when modeling algorithms.

In the future, we plan to continue to explore the properties of Edwards curves.

References

[1] H. Edwards, A Normal Form for Elliptic Curves, Bull. Amer. Math. Soc. 44(3) (2007) 393–422. doi: 10.1090/S0273-0979-07-01153-6.

[2] D. Bernstein, T. Lange, Faster Addition and Doubling on Elliptic Curves, Advances in Cryptology—ASIACRYPT'2007, Lect. Notes Comp. Sci. 4833 (2007) 29–50. doi: 0.1007/978-3-540-76900-2_3.

[3] W. Castryck, et al., CSIDH: An efficient post-quantum commutative group action, Advances in Cryptology—ASIACRYPT 2018. Lect. Notes Comp. Sci. 11274 (2018) 395–427. doi: 10.1007/978-3-030-03332-3_15.

[4] A. Bessalov, Elliptic curves in Edwards form and cryptography, Monograph, "Polytechnic" (2017).

[5] A. Bessalov, V. Sokolov, P. Skladannyi, Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves, in: 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), vol. 2631 (2020) 30–39.

[6] A. Bessalov, How to Construct Csidh on Quadratic and Twisted Edwards Curves, Cybersecur. Educ. Sci. Tech. 3(15) (2022) 148–163. doi: 10.28925/2663-4023.2022.15.148163.

[7] A. Bessalov, O. Tsygankova, Interrelation of families of points of high order on the Edwards curve over a

prime field, Probl. Inf. Transm. 4(51) (2015) 391–397. doi: 10.1134/S0032946015040080.
[8] A. Bessalov, O. Cigankova, Correlation of Big Order Points Sets of the Edwards Curves Over Prime Field, Ukrainian Inf. Secur. Res. J. 17(1) (2015) 73–80. doi: 10.18372/2410-7840.17.8327.
[9] V. Dolhov, A. Nelasaia, Methods for Increasing the Speed of Cryptographic Transformations on Elliptic Curves, Radioelectron. Inform. Manag. 2 (2004) 72–78.
[10] I. Dychka, M. Onai, T. Drozda, A Modified Windowed Method for Multiplying a Point of an Elliptic Curve by a Scalar in a Field GF(p), Radioelectron. Inform. Manag. 2 (2016).
[11] A. Bessalov, A Method for Finding the Order of the Point of a Twisted Edwards Curve, Radioengineering 186 (2016) 110–118.
[12] O. Tsygankova, R. Tsygankov, Animation of Exponentiation Points of Edwards Curve, in: XV All-Ukrainian Scientific and Practical Conference of Students, Aspirants and Young Scientists "Theoretical and Applied Problems of Physics, Mathematics and Informatics," VPI VPK "Politechnika" (2017) 114–116.
[13] E. Kachko, A. Svinarev, S. Golovashich, Methods and Algorithms for Accelerating Computations in Asymmetric Transformations on Elliptic Curves, Radiotekhnika, 114 (2000) 69–74.
[14] A. Bessalov, S. Abramov, Special Properties of the Law of Addition of Points of Non-Cyclic Edwards Curves, Cybern. Syst. Anal. 58(6) (2022) 3–14.
[15] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.