Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves

Anatoly Bessalov[1[0000-0002-6967-5001]], Lyudmila Kovalchuk[2[0000-0003-2874-7950]], Volodymyr Sokolov[1[0000-0002-9349-7946]], Pavlo Skladannyi[1[0000-0002-7775-6039]], and Tamara Radivilova[3[0000-0001-5975-0269]]

[1] Borys Grinchenko Kyiv University, Ukraine
[2] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," Ukraine
[3] Kharkiv National University of Radio Electronics, Ukraine
v.sokolov@kubg.edu.ua

Abstract. The analysis of the 2-isogeny existence conditions of generalized Edwards form curves over a prime field, including complete, quadratic, and twisted Edwards curves, is presented. An overview of the properties of these three classes of curves is given. Generalization of the results known for the classes of complete and quadratic curves to the class of twisted Edwards curves is obtained. A modified law of point's addition is used to correctly determine the isogeny degree.

Keywords: Generalized Edwards Form Curve, Complete Edwards Curve, Twisted Edwards Curve, Quadratic Edwards Curve, Curve Order, Points Order, Addition of Points, Isomorphism, Isogeny.

1 Introduction

One of the well-known prospects of post-quantum cryptography (PQC) is the isogeny of supersingular elliptic curves with as many subgroups of their points as possible. The discrete logarithm problem (DLP) of classical elliptic cryptography is replaced by the problem of finding one of the isogenies of a large number of subgroups of such a noncyclic curve, which is sufficiently resistant to the attacks of a virtual quantum computer. To date, the growing interest in isogenies is associated with the shortest key length in the proposed algorithms in comparison with other known candidates for PQC at a given level of security [1].

Sect. 2 provides a brief review of the literature on this topic. Sect. 3 of the article gives the basic definitions of isomorphic curves in Montgomery and Edwards forms, the laws of the point's addition, and doubling with a modification adapted to the horizontal symmetry of inverse points. A brief overview of the properties of three classes of generalized Edwards form curves following the classification is given. Sect. 4 summarizes the results of one of the methods for obtaining 2-isogeny for two classes of complete and quadratic Edwards curves [3] to the class of twisted Edwards curves, analyzes the existence conditions for the 2-isogeny in three classes of Edwards curves over a prime field, and includes examples.

2 Review of the Literature

The properties of isogenies for Weierstrass curves are well studied. Effective methods for constructing and isogenies properties of promising classes of curves in the Edwards form are much less known. The Edwards curves with one parameter, defined in [2], have very attractive advantages for cryptography: fastest exponentiation of a point [2], completeness and universality of the law of point's addition, affine coordinates of a neutral element of a points group, enhanced security against side-channel attacks [2–4]. 3- and 5-isogenies are considered in previous works [5] and [6].

The programming of group operations is accelerated due to the absence of a singular point at infinity as a neutral element of an Abelian group of points. The introduction of the second curve parameter in [7] extended the class of curves in the Edwards form and gave rise to classes of quadratic and twisted curves with new properties of interest to cryptographic applications. In this paper, the known results for the 2-isogeny of complete and quadratic Edwards curves [3, 8] are generalized to the class of twisted Edwards curves [9, 10]. In particular, an analysis of the existing conditions of such curves over a prime field is given.

3 Isomorphism and Properties of Classes of Generalized Edwards Form Curves

The analysis of isogenies of Edwards curves is often based on Weierstrass and their special cases of isomorphic curves in Montgomery or Legendre form. Let's describe the curve of the Montgomery form over the field F_q, $q = p^m$ by the equation [7]

$$M_{C,D}: Dv^2 = u^3 + Cu^2 + u, C = 2\frac{a+d}{a-d}, D = \frac{4}{a-d}, a = \frac{C+2}{D}, d = \frac{C-2}{D}, C^2 \neq 4. \quad (1)$$

This curve is by a rational transformation of coordinates

$$y = \frac{u}{v}, x = \frac{u-1}{u+1} \Longrightarrow u = \frac{1+x}{1-x}, v = \frac{u}{v} \quad (2)$$

is mapped into a birationally equivalent in the generalized Edwards form curve of [7, 10] with the equation

$$E_{a,d}: x^2 + ay^2 = 1 + dx^2y^2, a, d \in F_p^*, d \neq 1, a \neq d, p \neq 2. \quad (3)$$

Unlike the original equation of this curve in [7] here we multiply the parameter a by y^2 instead of x^2. If the quadratic character $\chi(ad) = -1$, the curve (3) is isomorphic to the complete Edwards curve [2] $E_{1,d} = E_d$ with one parameter d

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \chi(d) = -1, d \neq 0,1. \quad (4)$$

In the case of $\chi(ad) = 1$ and $\chi(a) = \chi(d) = 1$ the curve (1) is isomorphic with the quadratic Edwards curve [10]

$$E_d: x^2 + y^2 = 1 + dx^2y^2, \chi(d) = 1, d \neq 0,1 \quad (5)$$

having, in contrast to (4), the parameter *d* defined as a square. This difference leads to radically different properties of curves (4) and (5) [10], which are summarized below. Despite this, in the pioneering work [7], these classes of curves are united by the general term "Edwards curves."

In [10], we proposed to swap the coordinates *X* and *Y* in the form of an Edwards curve. Then the modified universal law of addition of points has the form

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - ay_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}\right). \quad (6)$$

If two points coincide, we obtain from (6) the law of points doubling

$$2(x_1, y_1) = \left(\frac{x_1^2 - ay_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}\right). \quad (7)$$

The use of modified laws (6), (7) allows us to preserve the generally accepted horizontal symmetry (relative to the axis *X*) of the inverse points.

Let's define now the inverse point as $-P_1 = (x_1, -y_1)$ we will acquire according to (6) the coordinates of the neutral element of the group of points $O = (x_1, y_1) + (x_1, -y_1) = (1,0)$. Except for the neutral element *O* on the axis *x*, there is also the point of the *second order*, for which by (7) $2D_0 = (1,0) = O$. Depending on the properties of the parameters *a* and *d* we can get also two singular points of the 2nd order and two singular points of the 4th order.

As follows from (3), the axis Y can also contain non-singular points $\pm F_0 = \left(0, \pm 1/\sqrt{a}\right)$ of the 4th order, for which $\pm 2F_0 = D_0 = (-1,0)$. These points exist over the primary field F_p if the parameter a is a square (quadratic residue). The law of points addition (6) of the curve (3), in contrast to the original, retains the definition of the degree of isogeny adapted to curves in the Weierstrass form. In addition to the above, points of the 4th order can exist as non-singular for nonzero coordinates *x* and *y* [10]. The order of the Edwards curve is $N_E = 2^m \cdot n, m \geq 2, n$ is odd.

Justification of the new classification of generalized Edwards form curves is given in papers [10, 11]. Below are definitions of three classes of these curves and a list of fundamental properties of curves of different classes.

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

- Complete Edwards curves with the condition C1: $\chi(ad) = -1$.
- Twisted Edwards curves with the condition C2.1: $\chi(a) = \chi(d) = -1$.
- Quadratic Edwards curves with the condition C2.2: $\chi(a) = \chi(d) = 1$.

The main properties of these classes of curves [8–10]:

1. For points of the second order, the first class of complete Edwards curves over a prime field is the class of cyclic curves, while twisted and quadratic Edwards curves form classes of non-cyclic curves. The maximum order of points of curves of the last 2 classes does not exceed $N_E/2$.

2. The class of complete Edwards curves does not contain singular points. The order of these curves is $N_E \equiv 4 \bmod 8$ or $N_E \equiv 0 \bmod 8$.

3. The twisted Edwards curves contain only two singular points of the 2nd order $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}; \infty\right)$. The order of these curves is $N_E \equiv 4 \bmod 8$ or $N_E \equiv 0 \bmod 8$.

4. Quadratic Edwards curves contain two singular points of the 2nd order $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}; \infty\right)$ and two singular points of the 4th order $\pm F_1 = \left(\infty; \pm\frac{1}{\sqrt{d}}\right)$. The order of these curves is $N_E \equiv 0 \bmod 8$.

5. Twisted and quadratic Edwards curves form pairs of quadratic torsion based on the transformation of parameters: $\tilde{a} = ca, \tilde{d} = cd, \chi(c) = -1$.

6. In the classes of twisted and quadratic Edwards curves, the replacement $a \leftrightarrow d$ gives the isomorphism $E_{a,d} \sim E_{d,a}$.

7. Complete and quadratic Edwards curves are isomorphic to curves with parameter $a = 1$: $E_{a,d} \sim E_{1,d/a}$. The introduction of the parameter into the equation of curve (3) is justified only for the class of twisted Edwards curves.

8. Twisted Edwards curves under $p \equiv 1 \bmod 4$ do not have the points of the 4th order and have the order $N_E = 4n, n$ is odd.

9. For points of odd order, the law of addition of points (6) is always complete (i. e., the sum of any pair of points does not give a singular point).

4 2-Isogeny for the Classes of Complete, Quadratic, and Twisted Edwards Curves

The isogeny of the elliptic curve $E(K)$ over a field K into a curve $E'(K)$ is a homomorphism $\phi: E(\overline{K}) \to E'(\overline{K})$ over an algebraic closure $\overline{K}$ given by rational functions. This means that for all points $P, Q \in E(K), \phi(P + Q) = \phi(P) + \phi(Q)$ and there exist rational functions [12]

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{f(x)}{g(x)}\right) = (x', y'),$$

mapping points of the curve E at the points of the curve E'. The degree of isogeny is the maximum of the degrees $\alpha = \deg \phi(x, y) = \max\{\deg p(x), \deg q(x)\}$, and its kernel is subgroup $G \subseteq E$ of the order α (separable isogeny), the points of which are mapped by the function $\phi(x, y)$ into a neutral element of the group O.

Isogeny compresses the points of the curve E at α times and is a surjection (α points of the curve E are mapped to one point of the curve E'). When $G = O$, isogeny becomes isomorphism ($\alpha = 1$).

The calculation of isogenies is usually carried out using the Velu formulas [12] for curves in the Weierstrass form. In paper [3] isogeny formulas of the second (2-isogeny) and odd degrees are obtained, adapted, in particular, to curves in the form of Edwards (4) and (5) with one parameter d (complete and quadratic Edwards curves).

Let us analyze and extend some of their results to curves (3) with the emphasis on the analysis of the existing conditions for 2-isogeny over a prime field.

The construction of 2-isogeny in [3] is carried out in three stages:

1. Isomorphic transformation $\psi_1(x,y)=(u,v)$ of the Edwards curve into the Montgomery form.

2. The construction of 2-isogeny $\psi_2(u,v)=(U,V)$.

3. Reverse transformation $\psi_3(U,V)=(x,y)$ of the isogenous curve in the Montgomery shape to the Edwards shape.

As a result, the composition $\phi(x,y)=\psi_1\circ\psi_2\circ\psi_3$ of three mappings between the curve E and the isogenic curve E' is found.

At the first stage, the Edwards curve (3) $x^2+ay^2=1+dx^2y^2$ by a rational transformation (2)

$$\psi_1(x,y)=\left((a-d)\frac{1+u}{1-u},(a-d)\frac{2u}{v}\right)$$

is transformed into the birationally equivalent Montgomery form

$$v^2=u^3+2(a+d)u^2+(a-d)^2u. \tag{8}$$

The point (0,0) is the second-order point of this curve, which, together with the point at infinity as a neutral element of the group, forms the kernel of the 2-isogeny. It is required to find parameters $\bar{a}$ and $\bar{d}$ of the isogenous curve with equation (8) and the rational function $\psi_2(u,v)=(U,V)$.

For the Montgomery curve of the general view

$$M_{c,b}: v^2=u^3+cu^2+bu, \tag{9}$$

finding 2-isogeny is well known [12]. Based on the Velu formulas, using the laws of the addition of the points of the curve in the general Weierstrass form, for the curve (9) one can obtain the 2-isogeny ([12], the example 12.4)

$$\psi_2(u,v)=\left(\frac{u^2+cu+b}{u},\frac{u^2-b}{u^2}v\right)=(U,V) \tag{10}$$

and the equation of the isogenous curve

$$V^2=U^3-2cU^2+(c^2-4b)U. \tag{11}$$

The discriminant of the quadratic equation on the right-hand side of (11) is $\Delta=16b$, and depending on the meaning of $\chi(b)$, the curve (11) has one or three points of the 2nd order. In the first case, one can construct one 2-isogeny, in the two-three points (for three kernels as subgroups of the second-order).

The main question in this work is the question of the existence of 2-isogeny in three classes of Edwards curves. As follows from (8) and (9), only those curves (9) of general form can be reduced to the Montgomery form (1) or (8) (and, accordingly, to the Edwards form), the parameter b of which is the square ($\chi(b)=1$). This is connected with the existence on the curve (9) the points of the 4th order $F=(u_1,v_1)$, such that $2F=(0,0)$. Then, taking $b=u_1^2$, equation (9) after replacement $c\to Cu_1$ is reduced to the form

$$v^2=u^3+Cu_1u^2+u_1^2u, \tag{12}$$

or to isomorphic (1) (or its quadratic torsion) curve

$$v^2 = u^3 + Cu^2 + u, C = 2\frac{a+d}{a-d}. \quad (13)$$

This curve is birationally equivalent to the generalized Edwards form curve (3) when $v^2 \to Dv^2$. The equation (12) is equivalent to (8) when $u_1^2 = (a-d)^2$ and $Cu_1 = 2(a+d)$.

Thus, the 2-isogenic curve (11) with the discriminant $\Delta = 16u_1^2$ in this case, has three points of the 2nd order, and corresponding isogenies can be found only in the classes of quadratic and twisted Edwards curves forming pairs of quadratic torsion. At the time the curve E, for which isogeny is built, can have one point of the 2nd order and two points of the 4th order (the class of complete Edwards curves), or belong to other classes of Edwards curves with three points of the second order. For example, with $p \equiv 3\mathrm{mod}4$ supersingular curve $v^2 = u^3 + u$ (for which $\chi(c^2 - 4b) = -1$) has one point of the second-order and two points of the 4th order and is isomorphic to the complete Edwards curve. Its 2-isogenous curve (11) $V^2 = U^3 - 4U$ has three points of the second-order and falls into the classes of quadratic and twisted Edwards curves with the same order $p+1$ of these curves. However, the element (–4) is a quadratic nonresidue, and the Edwards curve, isomorphic to a curve of the form $V^2 = U^3 - 4U$, does not exist over a prime field (see equation (12)). However, taking $U \to U - 2$, we obtain an isomorphic curve $V^2 = U^3 + 6U^2 + 8U$, for which isomorphism with the Edwards curve over a prime field with $p \equiv 7\mathrm{mod}8$ exists. Thus, the original curve E of the form (8) with the adaptation to Edwards curves can have one or three points of the second-order and, therefore, over a prime field belongs to one of the classes of complete, twisted, or quadratic Edwards curves. All these curves in the extension F_{p^2}, in which all the elements of the subfield F_p become squares, become quadratic Edwards curves. Of course, in the extension F_{p^n}, we can also build complete as well as twisted Edwards curves.

The equations (8) and (9) are identical for $c = 2(a+d), b = (a-d)^2$, then $c^2 - 4b = 16ad$ and the isogenic curve equation (11) in the Montgomery form has the form

$$M_1: V^2 = U^3 - 4(a+d)U^2 + 4adU. \quad (14)$$

Its discriminant is $\Delta = 16(1-d)^2$, and the corresponding roots are defined as $2(a+d) \pm 2(a-d) = \{4a, 4d\}$. Therefore, it can be written as follows:

$$M_1: V^2 = U(U-4a)(U-4d). \quad (15)$$

Linear coordinate offset $U \to \{U-4a, U-4d\}$ to other values of the cubic roots in (15) leads to two alternative equations (14) of isogenous curves in the Montgomery form:

$$M_2: V^2 = U^3 - 4(d-2a)U^2 + 16a(a-d)U, \quad (16)$$

$$M_3: V^2 = U^3 + 4(2d-a)U^2 - 16d(a-d)U. \quad (17)$$

The curve (16), up to isomorphism, coincides with the isogenic curve in the form (8), but with the parameters $\bar{a}$ and $\bar{d}$

$$V^2 = U^3 + 2(\bar{a} + \bar{d})U^2 + (\bar{a} - \bar{d})^2 U. \quad (18)$$

From this equation and (12)–(14) one can obtain the equalities

$$2\frac{\bar{a}+\bar{d}}{\bar{a}-\bar{d}}U_1 = -4(a+d), U_1^2 = 16ad.$$

Hence, after the substitution $U_1 = \pm 4\sqrt{ad}$ we obtain

$$\frac{\bar{a}+\bar{d}}{\bar{a}-\bar{d}} = \frac{\mp(a+d)}{2\sqrt{ad}} \Rightarrow \bar{d}_1^{\pm 1} = \bar{a}_1 \left(\frac{\sqrt{a}+\sqrt{d}}{\sqrt{a}-\sqrt{d}}\right)^2. \quad (19)$$

So, for curve (8), two isogenous curves (14) in the form (18) have two mutually inverse parameters $\bar{d}_1^{\pm 1}$ of isomorphic quadratic or twisted Edwards curves.

According to property 5 of Sect. 2, the twisted Edwards curve is the quadratic torsion of the quadratic Edwards curve $E_{1,d} = E_d$ with the offset $c = a$ of the parameters $\tilde{a} = a,\ \tilde{a} = ad, \chi(a) = -1$, where d is the parameter of the quadratic Edwards curve ($\chi(d) = 1$). In this case, the parameter a can be considered as a fixed factor of the variable parameter d, moreover $\tilde{a} \pm \tilde{d} = a(1 \pm d)$. For example, with $p \equiv 3 \bmod 4$ for a twisted curve, we can take $a = -1$ and with $p \equiv 1 \bmod 4$ as the smallest value of the quadratic nonresidue.

Further, instead of the curve $E_{a,d}$ we will use the curve $E_{a,ad}$ that leads to the substitution $d \to ad$. This simplifies the formulas for the isogenic curve parameters.

The formula (19) is valid only for one of the three points of the 2nd order (0,0) of the curve (15). Based on (12), (13), (16)–(18) one can obtain two more formulas for the parameter $\bar{d}_{2,3}$ of isogenic curves, which are given below in Theorem 1.

The inverse transformation of isogenous curves in the Montgomery form (M_1, M_2, and M_3) into the Edwards form $E_{a,ad}$ is performed based on rational functions (2) taking into account different values of coordinates of points of the 4th order $\pm U_1 \in \{4a\sqrt{d}, 4a\sqrt{1-d}, 4a\sqrt{d(d-1)}\}$ or $\pm U_1 = \bar{a} - \bar{d}$ with the help of rational function

$$\psi_3(U, V) = \left(\frac{U-U_1}{U+U_1}, \frac{2U}{V}\sqrt{\frac{U_1}{\bar{a}-\bar{d}}}\right) = (x, y).$$

Substitution of these rational functions of the form (2) into the equations of the curve in the Montgomery form gives the isogenic Edwards curve $x^2 + \bar{a}y^2 = 1 + \bar{d}x^2y^2$.

The composition $\phi(x, y) = \psi_1 \circ \psi_2 \circ \psi_3$ of three transformations leads to the 2-isogeny formulas for curves in the Edwards form, which are given below in Theorem 1.

In [3], the theorem was proved that is valid for complete and quadratic Edwards curves ($a = 1$). We generalize this theorem to all generalized Edwards form curves (3). Besides, we give its formulation taking into account the modification of the law of points addition (6) of Edwards curves and the replacement ($x \leftrightarrow y$) [10].

Theorem 1. Let's take the generalized Edwards form curve $E_{a,ad}$ and the elements (possibly in extension) of the field $K: \delta^2 = d, \gamma^2 = 1 - d, i^2 = -1$. Then there exist three pairs of 2-isogeny $E_{a,ad} \to E'_{a,a\bar{d}}$, set by the functions ϕ_1, ϕ_2, and ϕ_3

$$\phi_1(x,y) = \left(\frac{ad \mp \delta}{ad \pm \delta}\frac{a\delta x^2 \pm 1}{a\delta x^2 \mp 1}, i(a\delta \mp 1)\frac{y}{x}\frac{1 - a^2dx^2}{1 - a^2d}\right),$$

mapping $E_{a,ad} \to E'_{\bar{a},\bar{a}\bar{d}}$ with the parameters $\bar{d}_1^{\pm 1} = \bar{a}\left(\frac{1-\delta}{1+\delta}\right)^2$;

$$\phi_2(x,y) = \left(\frac{(a\gamma \mp 1)x^2 \pm 1}{(a\gamma \pm 1)x^2 \mp 1}, (a\gamma \mp 1)xy\right),$$

mapping $E_{a,ad} \to E'_{\bar{a},\bar{a}\bar{d}}$ with the parameters $\bar{d}_2^{\pm 1} = \bar{a}\left(\frac{1-\gamma}{1+\gamma}\right)^2$;

$$\phi_3(x,y) = \left(-\frac{\delta x^2 \mp i\gamma - \delta}{\delta x^2 \pm i\gamma - \delta}, (i\gamma \pm \delta)\frac{y}{x}\right),$$

mapping $E_{a,ad} \to E'_{\bar{a},\bar{a}\bar{d}}$ with the parameters $\bar{d}_3^{\pm 1} = \bar{a}\left(\frac{i\gamma-\delta}{i\gamma+\delta}\right)^2$.

The proof of the theorem for the case $a = 1$ is given in [3]. Let us adapt its formulas for the curve (3).

Taking into account the accepted designations, equations (16), (18), (19) of isogenic curves can be written

$$M_1: V^2 = U^3 - 4a(1 + \delta^2)U^2 + (4a\delta)^2U;$$
$$M_2: V^2 = U^3 + 4a(1 + \gamma^2)U^2 + (4a\gamma)^2U;$$
$$M_3: V^2 = U^3 + 4a(\delta^2 + (i\gamma)^2)U^2 + (4ai\delta\gamma)^2U.$$

The first coordinates of the points (U_1, V_1) of the 4th order of these curves (for them $2(U_1, V_1) = (0,0)$) are respectively equal to $U_1^{(1)} = \pm 4a\delta$, $U_1^{(2)} = \pm 4a\gamma$, and $U_1^{(3)} = \pm 4ai\delta\gamma$. Equating the coefficients at U^2 in (15), (20), and the equations of isogenic curves, we obtain

$$2\frac{\bar{a} + \bar{d}}{\bar{a} - \bar{d}}U_1^{(1)} = -4a(1 + \delta^2),$$
$$2\frac{\bar{a} + \bar{d}}{\bar{a} - \bar{d}}U_1^{(2)} = 4a(1 + \gamma^2),$$
$$2\frac{\bar{a} + \bar{d}}{\bar{a} - \bar{d}}U_1^{(3)} = 4a(\delta^2 + (i\gamma)^2).$$

Hence, for each pair of isogenic curves, we find the values of the parameters:

$$\bar{d}_1^{\pm 1} = \bar{a}\left(\frac{1 - \delta}{1 + \delta}\right)^2,$$
$$\bar{d}_2^{\pm 1} = \bar{a}\left(\frac{1 - \gamma}{1 + \gamma}\right)^2,$$
$$\bar{d}_3^{\pm 1} = \bar{a}\left(\frac{\delta - i\gamma}{\delta + i\gamma}\right)^2.$$

We emphasize that for the curve $E_{a,ad}$ they do not depend on the parameter a, but they depend on the parameter $\bar{a}$.

The proof of formulas for mapping rational functions ϕ_1, ϕ_2, and ϕ_3 is based on the composition $\phi(x,y) = \psi_1 \circ \psi_2 \circ \psi_3$ of three transformations: from an Edwards curve

to a Montgomery shape, an isogenous transformation of a Montgomery curve, and finally the inverse transformation of the latter to an Edwards curve. It repeats the corresponding proof in [3] with the replacement $\delta \to a\delta, \gamma \to a\gamma$.

It should be noted that the generally accepted definition of the degree of isogeny is the highest of the degrees of the polynomials of the first rational function $\frac{p(x)}{q(x)}$ of the transformation $\phi(x, y)$ [11]. It is valid for Weierstrass curves. If we turn to the original Theorem 1 [3], then we come to a paradoxical result: the degree of 2-isogeny is equal to 1. The modified law of Edwards curve points addition (6) with horizontal symmetry of inverse points $\pm(x_1, y_1) = (x_1, \pm y_1)$ adopted by us removes this paradox: the degree of isogeny is $\alpha = \deg(\phi) = 2$.

Let's consider some properties of 2-isogeny of Edwards curve $E_{a,ad}$ over a prime field.

Proposition 2. The complete Edwards curve with the order $N_E \equiv 0 \bmod 8$ has a unique mapping $\phi_2(x, y)$ over the primary field F_p at $\chi(\gamma) = 1$ to the quadratic Edwards curve.

Proof. By doing $\chi(\gamma) = 1$ the complete curve has points of the 8th order and its order is $N_E \equiv 0 \bmod 8$ [10]. At $\chi(\gamma) = 1$ there exist elements $\pm\gamma$ of the field F_p and the parameter $\bar{d}_2^{\pm 1} = \bar{a}\left(\frac{1-\gamma}{1+\gamma}\right)^2$ of the quadratic ($\bar{a} = 1$) or twisted ($\chi(\bar{a}) = -1$) Edwards curve. At $\bar{a} = 1$ there exists a 2-isogeny $\phi_2(x, y)$ and the corresponding quadratic curves are isomorphic to each other with parameters $\bar{d}_2^{\pm 1}$. The transformation from a quadratic curve to a twisted curve as a quadratic torsion change all points of the curve (except $O = (1,0)$ and $D_0 = (-1,0)$), therefore, an isogeny $\phi_2(x, y)$ from a complete curve exists only in a pair of quadratic curves ($\bar{a} = 1$). On the other hand, for the complete Edwards curve over the field F_p there are no elements of the field $\delta = \pm\sqrt{d}$, because $\chi(d) = -1$ and 2-isogeny $\phi_1(x, y)$ and $\phi_3(x, y)$ over the field F_p do not exist. This proves the uniqueness of the mapping $\phi_3(x, y)$ as one of three functions defined in Theorem 1.

Consequence. The complete Edwards curve with the order $N_E \equiv 0 \bmod 4$ does not have 2-isogeny over the field F_p in all classes of generalized Edwards form curves.

Proof. From Proposition 2 it follows that the complete Edwards curves are mapped exclusively to the quadratic Edwards curves. But the order of quadratic Edwards curves is $N_E \equiv 0 \bmod 8$ [10], that's why complete Edwards curves with the order $N_E \equiv 0 \bmod 4$, according to the Tate theorem [12], do not have 2-isogeny over the field F_p.

Proposition 3. The quadratic Edwards curve has the only mapping $\phi_2(x, y)$ over the prime field F_p to the quadratic Edwards curve at any values p and $\chi(\gamma) = 1$, and mappings $\phi_1(x, y)$ and $\phi_3(x, y)$ at $p \equiv 1 \bmod 4$ and $\chi(\gamma) = 1$.

Proof. Similarly to Proposition 2, there is a unique mapping of the Edwards quadratic curve over the prime field to the Edwards quadratic curve; at $\chi(\gamma) = 1$ the only mapping $\phi_2(x, y)$ of the Edwards quadratic curve over the prime field F_p to the Edwards quadratic curve takes place. By doing $p \equiv 1 \bmod 4$ and $\chi(\gamma) = 1$ for quadratic curves there exist the elements of the field $\delta = \pm\sqrt{d}$, $\gamma = \pm\sqrt{1-d}$, and $i = \pm\sqrt{-1}$, and, respectively, mappings $\phi_1(x, y)$ and $\phi_3(x, y)$.

Proposition 4. The twisted Edwards curve has the only mapping $\phi_2(x,y)$ over the primary field F_p to the Edwards twisted curve at $p \equiv 3\mathrm{mod}4$ and $\chi(\gamma) = 1$.

Proof. According to property 8 of the Sect. 1 [10], at $p \equiv 1\mathrm{mod}4$ the twisted Edwards curve over the primary field F_p does not have points of the 4th order, therefore, the corresponding 2-isogeny does not exist in this class of curves. At $p \equiv 3\mathrm{mod}4$ over the field F_p there do not exist elements $i = \pm\sqrt{-1}$ and, respectively, mappings $\phi_1(x,y)$ and $\phi_3(x,y)$. The only 2-isogeny in this class at $p \equiv 3\mathrm{mod}4$ and $\chi(\gamma) = 1$ is the function $\phi_2(x,y)$.

Let's consider examples of the 2-isogeny of complete and quadratic Edwards curves over the field F_p.

Example 1. Let $p = 11$ and the complete Edwards curve $E = E_7: x^2 + y^2 = 1 + 7x^2y^2$ where $\chi(d = 7) = -1$, $\chi(1 - d = 4) = 1$ with the order $N_E = 16$ is given. According to Theorem 1, there exists only a pair of 2-isogeny Edwards quadratic curves $E' = E_4$ and $E' = E_3$ with the parameters $d_{1,2} = \bar{d}^{\pm 1} = \{4,3\}$ and the mapping $\phi_2(x,y)$. They have the same order $N_E = 16$ (which corresponds to the well-known Tate theorem [11]), are isomorphic to each other, but instead of one they already have 3 points of the 2nd order (the curves are noncyclic) and 12 points of the 4th order. There are two singular points of the 2nd and 4th order. The points of the original complete curve E are denoted as P_i , and the points of two isogenic curves E' is as Q_i. As with the doubling of points, the mapping $\phi_2(x,y)$ compresses the preimage (curve E) in half, i.e. maps a pair of points of curve E to one point of curve E'. Unlike doubling, 2-isogeny does not necessarily halve the order of a point of even order.

On the curve E, we have points $(\pm 1,0)$, $(0,\pm 1)$, $(\pm 2,\pm 4)$, $(\pm 3,\pm 3)$, $(\pm 4,\pm 2)$. Let $P_1 = (2,4)$ is the point of the 16th order of the curve. $P_2 = (3,3) = 6P_1$ is the point of the 8th order, $P_3 = (4,2) = 11P_1$. On the isogenous curve $E' = E_4$, except points $O = (1,0)$, $D_0 = (-1,0)$, $\pm F_0 = (0,\pm 1)$, we have singular points $D_{1,2} = (\pm 5,\infty)$, $\pm F_1 = (\infty,\pm 5)$, and points of the 4th order $(\pm 2,\pm 3)$ and $(\pm 3,\pm 2)$. Let's denote $Q_1 = (2,3)$, $Q_2 = (3,2)$, $P^* = P + D_0 = (-x_1,-y_1)$. Using the first function value $\phi_2(x,y)$ we calculate

$$\pm\phi_2(P_1,P_1^*)^{(1)} = (3,\pm 2) = \pm Q_2,$$
$$\pm\phi_2(P_2,P_2^*)^{(1)} = (\infty,\pm 5) = \pm F_1,$$
$$\pm\phi_2(P_3,P_3^*)^{(1)} = (-3,\pm 2) = \mp Q_2^*,$$
$$\phi_2(\pm F_0)^{(1)} = (-1,0) = D_0,$$
$$\phi_2(D_0,O)^{(1)} = (1,0) = O.$$

The second isogenic curve $E' = E_3$ with the parameter $d = 3$, except points O, D_0, $\pm F_0$, has singular points $D_{1,2} = (\pm 2,\infty)$, $\pm F_1 = (\infty,\pm 2)$, and the points of the 4th order $(\pm 4,\pm 4)$ and $(\pm 5,\pm 5)$. Let $R_1 = (4,4)$ and $R_2 = (5,5)$. According to the second value of the function $\phi_2(x,y)^{(2)}$ we obtain

$$\pm\phi_2(P_1,P_1^*)^{(2)} = (4,\mp 4) = \mp R_1,$$
$$\pm\phi_2(P_2,P_2^*)^{(2)} = (0,\pm 1) = \pm F_0,$$
$$\pm\phi_2(P_3,P_3^*)^{(2)} = (-4,\mp 4) = \pm R_1^*,$$
$$\phi_2(\pm F_0)^{(2)} = (-1,0) = D_0,$$
$$\phi_2(D_0,O)^{(2)} = (1,0) = O.$$

So, the function $\phi_2(x,y)$ maps a pair of points of the same order of the curve to one point of the curve E' (i.e. the function $\phi_2(x,y)$ is a surjection), and one complete Edwards curve is mapped to two isomorphic quadratic curves.

Example 2. Let's construct the isogeny for the quadratic curve $E = E_3$ from example 1 with the parameters $d = 3$, $1 - d = 9$, $\gamma = 3$. One of the isogenic curves when mapping $\phi_2(x,y)$ has the same parameter $d = 3$ and the same points $R_1 = (4,4)$, $R_2 = (5,5)$, $D_{1,2} = (\pm 2, \infty)$, $\pm F_1 = (\infty, \pm 2)$, $\pm F_0 = (\infty, \pm 1)$, D_0, O. The mapping $\phi_2(x,y)^{(2)}$ of this curve gives us the points of the curve E'

$$\pm\phi_2(R_1, R_1^*)^{(2)} = (\infty, \mp 2) = \pm F_1,$$
$$\pm\phi_2(R_2, R_2^*)^{(2)} = (0, \mp 1) = \mp F_0,$$
$$\phi_2(\pm F_0)^{(2)} = (-1,0) = D_0,$$
$$\phi_2(\pm F_1)^{(2)} = (2, \infty) = D_1,$$
$$\phi_2(D_1, D_2)^{(2)} = (-2, \infty) = D_2,$$
$$\phi_2(D_0, O)^{(2)} = (1,0) = O.$$

If you reapply the function $\phi_2(x,y)^{(2)}$ to the points of the isogenous curve E', we obtain the points of the curve E''

$$\phi_2(\pm F_0)^{(2)} = (-1,0) = D_0,$$
$$\phi_2(\pm F_1)^{(2)} = (2, \infty) = D_1,$$
$$\phi_2(D_1, D_2)^{(2)} = (-2, \infty) = D_2,$$
$$\phi_2(D_0, O)^{(2)} = (1,0) = O.$$

Thus, the second isogeny returns us to the points of the original curve ($E'' = E$), and for two steps the mapped points of the curve E are doubled (multiplied by α: points of the 4th order are mapped into points of the 2nd order, and points of the 2nd order are to the point O). This is an example of dual 2-isogeny $\hat{\phi}_2 = \phi_2(x,y)^{(2)}$ for a quadratic curve over a prime field.

Consider the isogenies of twisted Edwards curves over the field F_p. According to Proposition 3, they exist only at $p \equiv 3 \bmod 4$ and $\chi(\gamma) = 1$, at the same time it is possible to accept $a = \bar{a} = -1$.

Example 3. Let $p = 19$ and the twisted curve $E_{-1,-9}$ with the parameters $a = -1$, $ad = -9$, $\gamma = \sqrt{11} = \pm 7$ is given. Its order is $N_E = 16$. It has the points O, D_0, $D_{1,2} = (\pm 6, \infty)$, and the points of the first quadrant $P_1 = (2,1)$, $P_2 = (3,6)$, $P_3 = (5,5)$ (total of 12 points of the 4th order with the coordinates $(\pm x, \pm y)$). One of the isogenous curves $E'_{-1,-16}$, when mapped $\phi_2(x,y)$, has the parameter $\bar{d}_2 = \left(\frac{1-7}{1+7}\right)^2 = 16$, the points O, D_0, $D'_{1,2} = (\pm 5, \infty)$, and the points of the 4th order of the first quadrant $Q_1 = (2,3)$, $Q_2 = (7,8)$, $Q_3 = (9,9)$ (total of 12 points of the 4th order with the coordinates $(\pm x, \pm y)$). The mapping $\phi_2(x,y)^{(1)}$ of the curve $E_{-1,-9}$ gives the points of the first isogenous curve $E'_{-1,-16}$

$$\pm\phi_2(P_1, P_1^*)^{(1)} = \pm\left(\frac{(-7-1)2^2+1}{(-7+1)2^2-1} = 2, (-7-1)2 = 3\right) = \pm Q_1,$$
$$\pm\phi_2(P_2, P_2^*)^{(1)} = \pm(-7,8) = \mp Q_2^*,$$
$$\pm\phi_2(P_3, P_3^*)^{(1)} = \pm(-9,9) = \mp Q_3^*,$$
$$\phi_2(D_1, D_2)^{(1)} = (5, \infty) = D'_1,$$
$$\phi_2(D_0, O)^{(1)} = (1,0) = O.$$

The second isogenous curve $E'_{-1,13}$ with the reverse meaning of the parameter $\bar{d}_2^{-1} = 3^{-1} = 13$ is isomorphic to the first one and contains the points O, D_0, $D''_{1,2} = (\pm 4, \infty)$, $R_1 = (2,2)$, $R_2 = (8,6)$, $R_3 = (9,7)$. The mapping $\phi_2(x,y)^{(2)}$ of the curve $E_{-1,-9}$ gives the points of the 2nd isogenous curve $E'_{-1,-6}$

$$\pm\phi_2(P_1, P_1^*)^{(2)} = \pm\left(\frac{(-7+1)2^2-1}{(-7-1)2^2+1} = -9, (-7+1)2 = 7\right) = \mp R_3^*,$$
$$\pm\phi_2(P_2, P_2^*)^{(2)} = \pm(8,6) = \pm R_2,$$
$$\pm\phi_2(P_3, P_3^*)^{(2)} = \pm(2,2) = \pm R_1,$$
$$\phi_2(D_1, D_2)^{(2)} = (4, \infty) = D'_1,$$
$$\phi_2(D_0, O)^{(2)} = (1,0) = O.$$

In contrast to the isogenies of quadratic curves over a prime field, for twisted Edwards curves that do not have singular 4th order points, pairs of 4th order points of the curve E are mapped to one point of the same order of the curve E'. Halving the number of singular points is an advantage of the class of twisted Edwards curves over quadratic ones (when programming isogenies).

For isogeny $\phi: E \to E'$ there exists dual isogeny $\hat{\phi}: E' \to E$, in such way that $\phi^{\circ}\hat{\phi} = [\deg(\phi) = \alpha]$ [11]. The formulas of Theorem 2 prove that over the field F_p for the complete Edwards curves, dual isogeny does not exist, but it exists in the extension F_{p^2}. To find dual isogeny $\hat{\phi}: E' \to E$, for example to the function $\phi_1(x,y)$ with the values of the isogenic curve

$$\bar{d}_1^{\pm 1} = \bar{a}\left(\frac{1-\delta}{1+\delta}\right)^2.$$

It is necessary to solve the inverse problem: from the known value $\bar{d}_1$ of the curve E' it is necessary to calculate one of the suitable values of the parameter δ of the curve E, which is determined by a similar formula

$$\delta^{\pm 1} = \frac{1-\sqrt{\bar{a}^{-1}\bar{d}_1}}{1+\sqrt{\bar{a}^{-1}\bar{d}_1}}.$$

Hence we see that the dual mapping of the curve E' to the complete and twisted Edwards curves E exists only in the extension F_{p^2}, in which all curves defined over the field F_p, have the properties of quadratic curves.

5 Conclusions

Thus, over the field F_p there exists 2-isogenies $\phi: E \to E'$ from the complete curves to the quadratic Edwards curves, from the quadratic curves to the quadratic Edwards curves, and also from the twisted curves to the twisted Edwards curves. In the extension F_{p^2} all the curves defined over the field F_p become quadratic Edwards curve (their parameters a and d are the squares in the field F_{p^2}), and for any such curve, there is a pair of isogenic quadratic curves defined by Theorem 1. In practice, in this regard, the isogenies of curves given over F_p are calculated over the extension F_{p^2}. The implementation of one of the promising algorithms for PQC Supersingular Isogenies Diffie-Hellman (SIDH) [13] is based, as is known, on 2- and 3-isogeny of supersingular

elliptic curves. The use of fast twisted Edwards curve arithmetic will undoubtedly allow the construction of more efficient cryptosystems.

References

1. Komarova, A.: The analysis of existing post-quantum approaches and electronic signature schemes. Cybersecur. Issues **2**(30): 58–68 (2019). https://doi.org/10.21681/2311-3456-2019-2-58-68. [Publication in Russian]
2. Bernstein, D. J., Lange, T.: Faster addition and doubling on elliptic curves. Lect. Notes Comput. Sci. **4833**: 29–50 (2007). https://doi.org/10.1007/978-3-540-76900-2_3
3. Moody, D., Shumow, D.: Analogues of Velu's formulas for isogenies on alternate models of elliptic curves. Math. Computation **85**(300), 1929–1951 (2015). https://doi.org/10.1090/mcom/3036
4. Koblitz, N., Menezes, A.: A riddle wrapped in an Enigma. IEEE Secur. Priv. **14**(6): 34–42 (2016). https://doi.org/10.1109/msp.2016.120
5. Bessalov, A. V.: Calculation of parameters of cryptic curves Edwards over the fields of 5^{th} and 7^{th} characteristic. Cybersecur. Educ. Sci. Tech. **1**(1): 94–104 (2018). https://doi.org/10.28925/2663-4023.2018.1.94104. [Publication in Ukrainian]
6. Bessalov, A., Grubiyan, E., Sokolov, V., Skladannyi, P.: 3- and 5-isogenies of supersingular Edwards curves. Cybersecur. Educ. Sci. Tech. **4**(8): 6–21 (2020). https://doi.org/10.28925/2663-4023.2020.8.621
7. Bernstein, D. J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. Lect. Notes Comput. Sci. **5023**: 389–405 (2008). https://doi.org/10.1007/978-3-540-68164-9_26
8. Ahmadi, O., Granger, R.: On isogeny classes of Edwards curves over finite fields. J. Number Theory **132**(6), 1337–1358 (2012). https://doi.org/10.1016/j.jnt.2011.12.013
9. Bessalov, A. V.: Unique cryptographic properties of non-cyclic twisted Edwards curves. Appl. Radioelectr. **17**(1,2): 49–54 (2018). [Publication in Russian]
10. Bessalov, A. V.: Edwards Elliptic Curves and Cryptography (2017). [Publication in Russian]
11. Bessalov, A. V., Tsygankova, O. V.: Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. Probl. Inf. Transm. **53**(1): 92–101 (2017). https://doi.org/10.1134/s0032946017010082
12. Washington, L.: Elliptic Curves. Discrete Mathematics and Its Applications (2008). https://doi.org/10.1201/9781420071474
13. Jao, D., de Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Lect. Notes Comput. Sci. **7071**: 19–34 (2011). https://doi.org/10.1007/978-3-642-25405-5_2