Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves

Anatoly Bessalov[1], Serhii Abramov[1], Volodymyr Sokolov[1], Pavlo Skladannyi[1], and Oleksii Zhyltsov[1]

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

Abstract

A multifunctional cryptosystem RCNIE on isogenies of non-supersingular Edwards curves is proposed, which solves the problems of Diffie-Hellman secret sharing, digital signature, and public key encryption. The problems of choosing the parameters of non-supersingular Edwards curves forming pairs of quadratic twist with orders $p+1\pm t\equiv 0 \bmod 8$ over a prime field F_p are considered. Encryption algorithms with mutual authentication of Alice and Bob based on the sharing of their secrets are given, while the length of the key and the size of the digital signature are minimally short and do not exceed the size of the field F_p element. An illustration is given of the operation of the cryptosystem model on 4 degrees of isogenies {3,5,7,37} over the field F_{863} for a pair of quadratic twist curves with orders 840 and 888. It is shown that for non-supersingular curves there are main and dual cryptosystems, each of which has also an isomorphic cryptosystem. This allows you to perform parallel computing and speed up algorithms. A comparative evaluation of the arithmetic and properties of CSIDH and RCNIE is given. It is noted that we have not found strong arguments for the slow implementation of the CRS scheme in comparison with CSIDH. Taking into account the peculiarities of each of them, both schemes are certainly promising.

Keywords

Curve in generalized Edwards form, complete curve, twisted curve, quadratic curve, non-supersingular curve, curve order, point order, isomorphism, isogeny.

1. Introduction

The presentation [1] of the authors of the PQC CSIDH algorithm names the CRS scheme (Couveignes-Rostovtsev-Stolbunov) known since the beginning of the 21st century as the first proposed scheme on isogenies of non-supersingular elliptic curves [2–4]. Its remarkable properties are the commutativity of isogenic transitions, the flexibility, and simplicity associated with the use of prime field F_p arithmetic [5–7].

Further, the appearance of the PQC SIDH (2011) and CSIDH (2018) algorithms already uses the technology of supersingular elliptic curves over the fields F_{p^2} and F_p, respectively, which is justified by the relatively faster implementation of the algorithms [8]. In [1] it is noted that CRS encryption is unacceptably slow and can take several minutes at a security level of 128 bits.

Being engaged in recent years in the problems of modeling and modifying CSIDH [9–12], we became interested in the reasons for the above fact, which is not substantiated by anything. One of the goals of this paper is to try to compare the difficulties that hinder the execution of the CSIDH algorithm and our simple CRS-like model on non-cyclic Edwards curves. The main difference from CRS [2] in this work is, as in CSIDH, the use of pairs of quadratic twist curves, which uses the property of isogeny bi-directionality. It should be noted that the set of

CQPC-2023: Classic, Quantum, and Post-Quantum Cryptography, August 1, 2023, Kyiv, Ukraine

EMAIL: a.bessalov@kubg.edu.ua (A. Bessalov); s.abramov.asp@kubg.edu.ua (S. Abramov); v.sokolov@kubg.edu.ua (V. Sokolov); p.skladannyi@kubg.edu.ua (P. Skladannyi); o.zhyltsov@kubg.edu.ua (O. Zhyltsov)
ORCID: 0000-0002-6967-5001 (A. Bessalov); 0000-0002-5145-2782 (S. Abramov); 0000-0002-9349-7946 (V. Sokolov); 0000-0002-7775-6039 (P. Skladannyi); 0000-0002-7253-5990 (O. Zhyltsov)

non-supersingular elliptic curves is wider than the corresponding set of supersingular curves with a rough estimate by a factor of $\sqrt{p}$, and, as a result, contains many potentialities. We managed to find some of them, which are discussed in this article.

In [1] and early implementations of CSIDH, supersingular curves in the Montgomery form [1] were used, but soon in [13] using the (W: Z)-coordinates [14] of curves in the Edwards form, a gain of 20% was obtained in comparison with [1] in the speed of calculations. Further, generalizing the formulas for calculating isogenies for Edwards curves [15] to twisted Edwards curves in [9], we illustrated the implementation of CSIDH models on non-cyclic quadratic and twisted Edwards curves [10–12]. The last curves were first defined in the fundamental work [16], but with unfortunate terminology, so we use the classification of curves in the Edwards form [17, 18]. An analysis of the properties of supersingular Edwards curves of all classes is given in [19, 20]. In this paper, we use non-supersingular Edwards curves of two classes with the same constraint $p \equiv$ 3mod4. This allows one to express the equations of curves of a quadratic twist pair using additively inverse parameters.

A well-known problem of the CSIDH algorithm is the vulnerability to a side channel attack based on the measurement of the computation time of the chain of isogenies of each degree, which is proportional to the secret exponent e_k of the key. In a large number of articles [21–24], the solution to this problem is proposed by increasing the exponents by fictitious ones to a known maximum (Constant time CSIDH). It is clear that such redundancy significantly reduces the speed of the algorithm. In [11], we proposed randomization of the CSIDH algorithm as a method to counter side-channel attacks. It is also used in this article.

The key encapsulation algorithms [12, 25–27] are now preferred to the classic Diffie-Hellman secret sharing scheme. Such an algorithm can also be constructed using the CRS scheme.

The order of an elliptic curve E over a prime field F_p is defined as $\#E = p + 1 - t$, where t is the trace of the Frobenius endomorphism equation. For a quadratic twist curve E^t, respectively, this order $\#E^t = p + 1 + t$ is symmetric concerning the mean value $p + 1$. For a supersingular curve, $t = 0$ and the orders of both curves $p + 1$ coincide, and the sets of isogeny degrees are the same, but the signs of the exponents of the degrees are inverse to each other, as in CSIDH. In the case of non-supersingular curves, the orders of quadratic twist pairs differ by $2t$, then there are different degrees of isogenies on curves of two classes related as quadratic twist pairs with different orders. This is the main specificity of non-supersingular curves. The exponents of the isogeny degrees of these two curves, as in CSIDH, have opposite signs. The alternation of degrees of isogenies according to the randomization method is random, and the simplicity of transitions of the chain of isogenies from one class of curves to another is achieved by the fact that their parameters are additively inverse: $(a, d) \leftrightarrow (-a, -d)$.

In Section 1, a brief review of the properties of quadratic and twisted Edwards curves [18] is given, and methods and options for choosing the parameters of a pair of these curves as a pair of quadratic twists are proposed. Section 2 presents algorithms of the Randomized Commutative Non-supersingular Isogeny Encryption (RCNIE) scheme on quadratic and twisted non-supersingular Edwards curves (NECs). In Section 3 an illustration of the computation of isogenic chains in the corresponding algorithms on a model with degrees {3,5,7,37} over the field F_{863} is given. Here we discuss the existence of isomorphic and dual cryptosystems on isogenies of non-supersingular curves, expanding their possibilities and applications. Finally, Section 4 compares the CSIDH algorithm and the RCNIE scheme.

2. Choice of Non-Supersingular Non-Cyclic Edwards Curves Parameters

The elliptic curve $E_{a,d}$ the equation in the generalized Edwards form [17] with two parameters a and d is written as

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

For the first time, such a curve was proposed in the fundamental work [12] with the coefficient a at x^2 and the term “*twisted Edwards curve*.” For the correct division of curves in the Edwards form into non-intersecting classes, we use our classification [17].

If the quadratic character is $\chi(ad) = -1$, then curve (1) is isomorphic to the complete Edwards curve [16] with one parameter d, $\chi(d) = -1$, $a = 1$. Another case $\chi(ad) = 1$ generates 2 classes of non-cyclic curves: quadratic and twisted Edwards curves. In particular, if $\chi(a) = \chi(d) = 1$, curve (1) is isomorphic to the quadratic Edwards curve [17] with one parameter

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

The twisted Edwards curve is defined in [17] as a special case of the curve (1) with $\chi(a) = \chi(d) = -1$. The introduction of the second parameter a into equation (1) in [16] is necessary only for these conditions.

In [16], curve (2) together with the complete curve are called Edwards curves. At the same time, their properties and structure are cardinally different [17, 18]. The controversial terminology in [16] sometimes leads to misunderstandings and errors in scientific articles, which is discussed in [10]. In this paper, in particular, the following theorem is proved.

Theorem 2 [10]. For a curve $E_{a,d}$ (1) in generalized Edwards form $x^2 + ay^2 = 1 + dx^2y^2$ defined over a prime field F_p, there exists a unique quadratic twist curve $E_{\bar{a},\bar{d}}{}^t$ with parameters $\bar{a} = ca,\ \bar{d} = cd,\ c \in F_p{}^*$.

Its proof is given in [10]. From it, in particular, it follows that in the class of complete Edwards curves, the quadratic twist curve $E_d^t = E_{d^{-1}}$ lies inside this class, while for the quadratic curve (2), quadratic twist gives a twisted curve $E_{a,d}^t = E_{ca,cd}$,$\chi(c) = -1$. Each of the 3 classes contains equal sets $\frac{p-3}{2}$ curves ($d \neq 0, \pm1$). Then the replacement of the class of complete Edwards curves by 2 classes of non-cyclic Edwards curves doubles the space of pairs of quadratic twist curves in the CSIDH algorithm.

We define a quadratic and twisted Edwards curve as a pair of quadratic twists with parameters $\chi(ad) = 1, \bar{a} = ca,\ \bar{d} = cd,\ \chi(c) = -1$. Since we accept the condition $p \equiv 3 \bmod 4$, we can accept $c = -1,\ \bar{a} = -a = -1,\ \bar{d} = -d,$ where $a = 1, and\ d$ are the parameters of the quadratic curve (2), respectively $\bar{a}, \bar{d}$ are twisted curves. In other words, the transition from quadratic to twisted curve and vice versa can be defined as $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Then the twisted Edwards curve equation (1) can be written as

$$E_{-1,-d}: x^2 - y^2 = 1 - dx^2y^2,\quad d \in F_p^*,\ d \neq 1,\ \chi(d) = 1. \tag{3}$$

The orders of quadratic (2) and twisted (3) Edwards curves are comparable to 0mod8, then $p \equiv -1\text{mod}8$ [17]. Note that equation (3) has a fixed parameter $a = -1$ after which all curves (3) are determined by one parameter $(-d)$. Quadratic residues of parameters ($a = 1$ and d) of curve (2) become quadratic non-residues ($a = -1, -d$) of curve (3). This property of additively inverse parameters simplifies the illustration of the operation of cryptosystems on the isogenies of these curves. Equation (1) can be written in a different form with the change *d*→*ad* and fixing *a*.

It is interesting that in equation (2), as well as for the complete Edwards curve with one parameter, one can single out the parameter *d*

$$d = (x^{-2} + y^{-2} - x^{-2}y^{-2}).$$

This means that using the multiplicative inversion of the coordinates of eight known points of the curve *P* = (±*x*, ±*y*), *Q* = (±*y*, ±*x*) it is easy to calculate the unique parameter *d* of the curve. This is useful in cryptanalysis and should be taken into account in algorithms to protect against such an attack.

By analogy with CSIDH, it is easy to form the general parameters of a CRS-like cryptosystem on isogenies of Non-supersingular Edwards Curves (NECs). Let $n_0 = \prod_{k=1}^{K} l_k$ and N = $8n_0$ be the order of a quadratic supersingular Edwards curve over a field with modulus $p_0 = N - 1$. By setting the values of the Frobenius trace $t = \pm 8m, m = 1,2,3, \ldots$ we determine the sum $p_0 \pm 8m = p$ equal to the prime number *p*. Then over the field F_p there exists a quadratic NEC (2) of order #E_d = $8n_0$ and a twisted curve (3) of order $\#E_{-1,-d}$ $= N \pm 16m = 8n_1$.

Example 1. For a set of isogeny degrees $\{l_k\} = \{3,5,7\}, n_0 = 105, \mathrm{N} = 840, p_0 = 839,$ for *m* = 3 we get a prime number *p* = 839 + 24 = 863. Then the orders of the curves of the quadratic twist pair are #E_d =840 $= 8 \cdot 3 \cdot 5 \cdot 7$ and $\#E_{-1,-d}$ $= N + 48 = 888 = 8 \cdot 3 \cdot 37, n_1 = 111$.

Another method is possible, not always lead to success. You can set two sets of degrees that differ by one or more elements and calculate the arithmetic mean of the products of the elements of these sets *u*. If 8*u*−1= *p* is a prime number, it is the desired modulus of *p*.

Example 2. Let $\{l_k\} = \{5,7\}, n_0 = 35, 8n_0 = 380$. In the second set $\{l_k\}^t = \{3,11\},\ n_1 = 33, 8n_1 = 364$. The mean of orders is 8u = 372, but 372 – 1 = 371 is not a prime number. However, $16u - 1$ = 743 is a prime number, and over the field F_{743} one can obtain, with double redundancy, pairs of quadratic twist curves with orders 760 and 728, containing isogeny kernels of degrees $\{5,7\}$ and $\{3,11\}$.

Example 3. Let $\{l_k\} = \{3,5,7,11\}, n_0 = 1155, 8n_0 = 9240$. In the second set $\{l_k\}^t = \{3,5,7,13\}$ we change element 11 of the first sets by 13 and calculate $n_1 = 1365, 8n_1 = 10920$. The average value of the orders of the two curves is 10080 = $p + 1$, since p = 10079 is a prime number. Here the trace of the Frobenius equation is $t = 840$, and the orders of the curves of the quadratic twist pair are $\#E_{\mathrm{d}}$ = $9240, \#E_{-1,-d} = 10920$. Note that for p = 9239, it is possible to build CSIDH, for p = 10079 only CRS, and the number 10919 is not prime.

An approach can be considered rational if the sets of isogenies degrees of pair curves of quadratic twist intersect as much as possible. For example, in the second curve with the preservation of all lower degrees, the highest degree l_{max1} can be replaced by a higher one $l_{\max 2}$, then the orders of the two curves differ by a factor $l_{\max 1}/l_{\max 2}$. This difference cannot exceed the allowable limits of the Hasse boundaries. For real cryptosystems, this is impossible. The orders of the pair of quadratic twist curves $p + 1 - t\ and\ p + 1 + t$ for $t < 2\sqrt{p}$ differ for large p with an estimate of $1 - \frac{2}{\sqrt{p}}$. Meanwhile, for CSIDH, for example, the ratio of the maximum orders $l_{\max 1}/l_{\max 2}$ differs little from 0.99, which is less than 1 on about 1%. In the alternative case, for non-intersecting two sets of degrees, there are also no such sets that would give practically equal products. It is more pragmatic to specify the first non-supersingular curve with minimal isogeny degrees, followed by an appropriate factorization of the order of the twist curve (Example 1). It will only add new degrees of isogenies with a smaller number of them. The number of isogenies degrees in both curves can be made approximately equal by selecting from a table of primes with alternating numbers for the first and second curves (as in Example 2). The problem of choosing the parameters of quadratic twist pairs of non-supersingular curves still needs to be studied.

Quadratic and twisted NEC as a pair of quadratic twists have different orders and different structures. Except for the two points (0, ±1), all their points are different. Both curves are non-cyclic concerning points of even order (contain 3 points of the 2nd order each, two of which are singular points $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ [17]). Quadratic NEC, in addition, contains 2 singular points of the 4th order $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$. The presence of 3 points of the 2nd order limits the number 8 to the minimum even cofactor of the order Ord E = 8n (n is odd) of twisted and quadratic Edwards curves [17]. The maximum order of the points of these curves is Ord E/2. Points of even orders mustn't be involved in the calculation of isogenies of odd degrees (the first multiplication by four of a random point P gives a random point R of odd order n or a divisor of n).

The choice of two classes of non-cyclic NECs for cryptosystems on isogenies is justified by their advantages over complete NECs:

1. The number of all quadratic and twisted Edwards curves $(p - 3)$ is twice the number $\frac{p-3}{2}$ of all complete Edwards curves, the corresponding proportion is also valid for the number of isogenic NECs and, therefore, the security of the cryptosystem.
2. The transition to the curve of quadratic twist $E_d \leftrightarrow E_{-1,-d}$ does not require the laborious inversion of the parameter $d \leftrightarrow d^{-1}$, which is necessary for a complete NEC.

Along with isogenic curves (with different J-invariants), there are isomorphic curves with equal J-invariants, which are defined [16, 28]

$$J(a,d) = \frac{16(a^2 + d^2 + 14ad)^3}{ad(a-d)^4}, \qquad (4)$$
$$ad(a-d) \neq 0.$$

This parameter, in particular, recognizes isomorphic curves with different values of the parameter d. As a result of calculations of chains of isogenies, one usually makes the change $d \rightarrow J(d)$. This parameter is also used in the ElGamal encryption scheme. For quadratic and twisted Edwards curves $J(d) = J(d^{-1})$, i.e. inverting the parameters d gives an isomorphic curve.

3. Algorithms of the RCNIE Scheme on Quadratic and Twisted Edwards Curves

Instead of supersingular ones, we start here with non-supersingular Edwards curves (NECs) of two classes (2) and (3), connected as pairs of quadratic twist with orders $p + 1 \pm t \equiv 0 \mathrm{mod} 8$.

A nonzero value of t by a factor of $\sqrt{p}$ expands the set of curves and offers interesting new applications.

In contrast to the CRS scheme [2] on curves in the Weierstrass form with two parameters, which does not use pairs of quadratic twist, we build encryption algorithms on the fastest today Edwards curves quadratic twist pairs with one variable parameter d. Another important factors in speeding up our algorithms are the rejection of the very laborious calculation of the isogenic function $\varphi(R)$ of point R and randomization of algorithms [10].

In this paper, we propose a PQC RCNIE scheme. It is distinguished from the known ones by the existence of four parallel cryptosystems (with the addition of dual and two isomorphic ones) and, most importantly, multi-functionality.

The PQC CSIDH [1] algorithm is based on the CGA (class group action) encryption function over a prime field F_p. The CGA function defines an isogenic mapping Θ of a supersingular elliptic curve E of order #E = p + 1 into a curve $E' = E * \Theta$ of the same order of the form $\Theta = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$, where l_k are odd prime degrees of isogenies and e_k are isogeny exponents (number of isogenic transitions). The sign of the exponent is $e_k > 0$ for the original curve, and $e_k < 0$ for the quadratic twist curve. The mapping Θ is commutative and is equally valid for all elliptic curves over the field F_p regardless of their order.

A pair of non-supersingular quadratic twist curves have different orders and different sets of degrees $\{l_k\}$ and $\{l_k\}^t$, which may partially intersect. For the intersection $\{l_k\} \cap \} \{l_k\}^t$, as in CSIDH, each l-isogeny has both signs and then $[{l_k}^{e_k}]$*$[{l_k}^{-e_k}]$ = 1. This means that chains of l-isogenies of different signs are built in reverse order and cancel each other out. Therefore, the keys in CSIDH give for each degree l_k an exponent e_k of only one sign. For non-supersingular curves, the union of sets $\{l_k\} \cup \{l_k\}^t$ is constructed, and the signs of the exponents e_k are determined by whether the isogeny belongs to one of the curves of the quadratic twist pair. One should strive for the equiprobable use of both curves, which is true for sets $\{l_k\}$and $\{l_k\}^t$ of equal power. Since isogeny curves of corresponding degrees exist in the classes of curves (2) and (3) connected as pairs of quadratic twist, to construct commutative chains of isogenies we use the CGA encryption function $\Theta = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$ [1]. A specific feature of the application of this function for non-supersingular curves is the cardinal complication of the multiplicative inversion operation for some of the isogeny degrees that are different in the sets $\{l_k\}$and $\{l_k\}^t$. For our tasks, this does not violate the efficiency of encryption algorithms, while at the same time complicating the tasks of cryptanalysis. We will return to this problem in Section 3.

In all algorithms, the CGA encryption function $\Theta(\Omega)$ encrypts the secret key $\Omega = (e_1, e_2, .., e_K)$ using the mapping $\Theta = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$ and the starting curve E_0 into an isogenic curve $E' = E_0 * \Theta$, whose parameter is taken either as the corresponding public key or as a new short secret key. The parameters of the quadratic NEC $\#E_d^{(0)}= p + 1 - t = 2^m \prod_{k=1}^{K} l_k$, $m \geq 3$ and the prime field modulus $p \equiv t - 1\, mod\, 8$ are given. The $\#E_{-1,-d}^{(0)}= p + 1 + t$ and the factorization of degrees $\{l_k\}^t$ of twisted NEC are determined. A randomized algorithm for calculating Alice's public key d_A using the secret key $\Omega_A = (e_1, e_2, \ldots e_K)$ on the isogenies of curves (2) and (3) [11] is given below.

Randomized algorithm 1:
Evaluating encryption function on quadratic and twisted NEC

```
    Input: $d_A \in E_A, \chi(d) = 1$ and a secret key $\Omega_A = (e_1, e_2, \ldots e_K)$.
    Output: $d_B$ such that $[{l_1}^{e_1}, {l_2}^{e_2}, \ldots {l_K}^{e_K}] * E_A = E_B$, where $E_{A,B}$:   $x^2 + y^2 = 1 + d_{A,B} x^2 y^2$,
1.  Let $S_0 = \{k | e_k > 0\}$ , $S_1 = \{k | e_k < 0\}$, $n_0 = \prod_{k \in S_0} l_k$ , $n_1 = \prod_{k \in S_1} l_k$ ,
2.  While some $e_k \neq 0$ do
    3. Sample a random $x \in F_p$,
    4. Set  $a \leftarrow 1, \lambda \leftarrow 0$ ,  $E_A$: $x^2 + y^2 = 1 + d_A x^2 y^2$ If $\chi((x^2 - 1)/(dx^2 - 1) = 1$,
    5. Else $a \leftarrow -1, \lambda \leftarrow 1$   $E_A$: $x^2 - y^2 = 1 - d_A x^2 y^2$,
    6. Compute $y$-coordinate of the point $P = (x, y) \in E_A$,
    7. Compute $R \leftarrow [4]P$,
    8. Sample a random $l_k|, k \in S_\lambda$,
        9.  Compute $Q \leftarrow [n_\lambda / l_k]R$,
        10. If $Q \neq (1,0)$ computes kernel $G$ of $l_k$-isogeny $\varphi: E_B \leftarrow E_A$,
        11. Else start over to line 3,
        12. Compute $d_B$ of curve $E_B$, $d_A \leftarrow d_B$, $e_k \leftarrow e_k - a$ ,
        13. Skip $k$ in $S_\lambda$ and set $n_\lambda \leftarrow (n_\lambda / l_k)$ If $e_k = 0$,
14. Return $d_A$.
```

This algorithm has important differences from the original algorithm 2 [1], which are discussed in [11]. In addition to modifications related to the randomization method of the CSIDH algorithm, here we refuse the redundant isogenic function φ(R) of a random point *R*, which radically speeds up the algorithm.

The idea of randomization is that for any random value of the variable *x* (*xy* ≠ 0, ∞), the point *P* = (*x*,*y*) with a known parameter *d* always belongs to one of the two curves (2) or (3). This makes it possible to double the speed ap selection of a random point P and complicate the side channel attack. This is also facilitated by a random choice of isogeny degrees (as they are exhausted). Also, if P is not well chosen, moving to a new degree often fixes the problem faster than varying *x*.

At the beginning of Algorithm 1, two subsets $S_{\lambda}, \lambda = 0{,}1$, with degree numbers l_k, are formed, together with two factors n_0 and n_1 of the number $n = n_0 n_1$: the index λ=0 ($e_k > 0$) corresponds to the choice of a quadratic NEC, and λ = 1 is twisted NEC ($e_k < 0$). Since the order of the curve is #E_d= 8n_0, then in line 7 of the algorithm for the curve E_d the point $R = 4n_1P$ of odd order n_0 is calculated, and the curve $E_{-1,-d}$ the point $R = 4n_0P$ of odd order $n_1$is calculated. This minimizes the cost of the next scalar multiplication, which determines the point Q of the isogeny kernel of the degree l_k (line 9). Further, in line 10 of the algorithm, by doubling the points, $s = (l_k - 1)/2$ *x*-coordinates of the points of the kernel <*Q*> are calculated.

In line 7 of Algorithm 1, double doubling the random point *P* immediately allows you to get rid of points of an even order (including special points of the 2nd and 4th order) and then the calculation of scalar multiplications in subgroups of points of an odd order of the curve. Their task is to find $\frac{(l_k-1)}{2}$ of *x*-coordinates α_i of the kernel points <Q> of prime order l_k. As a result, according to the formula [15]

$$d^{'} = d^{l}A^{8}, A = \prod_{i=1}^{s}\alpha_{i}, \text{ s} = (l_k - 1)/2 \qquad (5)$$

the parameter $d^{'}$ of the l_k-isogenic quadratic NEC is calculated. Twisted NEC parameters (3) $a^{'} = -1, d^{'} \to -d^{'}$. We emphasize that the concept of RCNIE is the construction of chains of isogenic curves as Abelian groups, and not isogenic functions $\varphi(R)$ of a random point R. The labor-intensive calculations of the latter in [1] are redundant.

3.1. Diffie-Hellman Non-Interactive Secret Sharing Algorithm

1. Choice of parameters. For odd primes l_k, compute $\prod_{k=1}^{K} l_k$, choose an appropriate field modulus $p = 2^m \prod_{k=1}^{K} l_k - 1,\ m \geq 3$ and start the elliptic curve $\boldsymbol{E_0}$.

2. **Calculation of public keys**. Alice and Bob use secret keys in the form of vectors $\Omega_{A,B} = (e_1, e_2, .., e_K)$ construct isogenic maps $\Theta_{A,B} = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$ and calculate the isogenic curves $E_{A,B} = \Theta_{A,B} * E_0$ as their public keys. These curves are determined by their parameters up to isomorphism.

3. Key exchange. Here the protocol is similar to item 2 with the replacement $E_0 \to E_B$ for Alice and $E_0 \to E_A$ for Bob. Knowing Bob's public key, Alice calculates $E_{BA} = \Theta_A * E_B = \Theta_A * \Theta_B * E_0$. Similar actions Bob gives the result $E_{AB} = \Theta_B * E_A = \Theta_B * \Theta_A * E_0$ which coincides with the first one due to the commutativity of the group operation. The J-invariant of the curve E_{AB} (E_{BA}) is taken as a shared secret [1].

3.2. Digital Signature Algorithm

The tasks of the digital signature are to authenticate the sender of message *M* and to verify the integrity of the transmitted message by the recipient. Alice usually uses her private key for this, and Bob uses her public key for verification. In the previous secret-sharing problem, both of these functions are performed: Alice encrypts Bob's public key E_B with the secret key $\Omega_{A,}$ and computes the shared secret $E_{\mathrm{B}A}$. Bob uses Alice's public key E_{A} and his secret $\Omega_{\mathrm{B},}$ to calculate the same curve $E_{A\mathrm{B}}$. The fact that $E_{AB} = E_{\mathrm{B}A}$ means that the task of authenticating Alice by Bob has been completed.

When checking, it remains for Bob to make sure that together with the equality $E_{A\mathrm{B}} = E_{\mathrm{B}A}$ for the sent *M* and received *M'* messages, the hash codes are identical: *H*(*M*') = *H*(*M*). Both qualities can be easily combined by concatenation into one with the secret of the first of them preserved. The most secure from a quantum computer for this is hashing the combined equalities above. These symmetric procedures are included in the digital signature algorithm below.

Precomputation

Based on each other's public keys E_A and E_B and their private keys $\Omega_{A,B} = (e_1, e_2, .., e_K)$ Alice and Bob perform calculations of the previous Diffie-Hellman secret-sharing scheme and find curves E_{BA}= E_{AB}=E_{κ}. Next, Alice respectively forms, and Bob verifies the digital signature *DS*:

A. *DS* formation

1. Calculation $h = H(M) < p$.
2. Calculation $\mathrm{J}(\kappa) = \mathrm{J}(E_{BA})$.
3. Calculation $DS = H[\mathrm{J}(\kappa) || h] <$ p.
4. Dispatch $(M, DS) \rightarrow B$.

B. *DS* Verification

1. Calculation $h' = H(M')$.
2. Calculation $\mathrm{J}(\kappa) = \mathrm{J}(E_{AB})$.
3. Calculation $DS' = H[\mathrm{J}(\kappa) || h'] < p$.
4. Checking $DS' = DS$. In the case of $DS' \neq DS$, the signature is incorrect.

It is a non-standard signature in the sense that in the asymmetric scheme, it is generated by Alice's private key and verified by Bob with her public key, and Bob's corresponding keys are not required. This is because a non-interactive Diffie-Hellman scheme was adopted as a basis, equalizing the conditions for Alice and Bob: both parties use their secret keys and the public keys of the other party to form a shared secret. Such conditions mean that they work in the scheme of mutual trust of symmetric cryptography, although on the technology of asymmetric cryptography. Perhaps this is permissible since Bob can write to Alice with the same rights, and she is obliged to believe him. To do this, they created a shared secret. The main thing is that a multifunctional cryptosystem works on this basis.

This original signature does not exceed the size of a prime field module and is rather concise. The signature algorithm is closer to RSA and half as long as the ElGamal signature. Here, only hashing and field operations are performed on both sides, with element inversions as the most complex operations. The algorithm can equally rely on CSIDH. The level of quantum security of finding the secret curve E_K in the Diffie-Hellman secret sharing problem is estimated as $\sqrt[4]{p}$. Calculations in the procedures for generating and verifying a digital signature have the maximal security level for a quantum computer.

3.3. ElGamal Encryption Algorithm

This asymmetric cryptography algorithm was proposed in [2] without using quadratic twist curves. Interestingly, it is also based on a secret-sharing scheme. In the staging part, of the public keys, only the recipient's key is—the E_{B} curve. Alice, on the other hand, calculates her public key $E_{A,}$ in the encryption process and transmits each session to Bob along with the ciphertext. In essence, this means that she uses a one-time secret $\Omega_{A,}$, which forms her one-time public key $E_{A,}$. The combination of Alice's one-time keys $\Omega_{A,}$, $E_{A,}$, and Bob's long-term keys $\Omega_{B,}$, $E_{B,}$ allows both parties to compute the one-time shared secret $E_{BA,} = E_{AB,}$ It is used by Alice to encrypt the short message $M \epsilon F_p$, and by Bob to decrypt it. We describe the algorithm from [2] with the notations adopted here.

General system parameters:

- F_p is a prime field.
- $l_k, k = 1,2, .., K$ are isogeny degrees.
- e_k is integers $m \leq e_k \leq m$-exponents of isogenies.
- m is the boundary value of the exponent.
- E_0 is starting the elliptic curve and its equation.
- E_{B} is Bob's public key.
- $M \epsilon F_p$ is plain text.

A. Encryption

1. Setting a random secret key $\Omega_{A,} = (e_1, e_2, .., e_K)$ and generating the function CGA $\Theta_A = [l_1{}^{e_1}, l_2{}^{e_2}, .., l_K{}^{e_K}]$.
2. Calculation of Alice's public key $E_{A,} = E_{0,} * \Theta_A$.
3. Calculation of the shared Diffie-Hellman secret $E_{BA,} = E_{B,} * \Theta_A = E_{\kappa}$.
4. Calculation of the J-invariant of the curve $E_{BA,}$: $J_{\kappa} = J(E_{BA,})$.
5. Calculation of the ciphertext S = $(M \cdot J_{\kappa})$ mod p.
6. Sending $(E_{A,}, S)$ to Bob.

B. Decryption

1. Based on the secret key $\Omega_{B,} = (e_1, e_2, .., e_K)$ function form $\Theta_B = [l_1{}^{e_1}, l_2{}^{e_2}, .., l_K{}^{e_K}]$.
2. Calculation of the shared Diffie-Hellman secret $E_{AB,} = E_{A,} * \Theta_B = E_{\kappa}$.
3. Calculation of the J-invariant of the curve $E_{AB,}$: $J_{\kappa} = J(E_{AB,})$.
4. Calculation of the plain text $M = (S/J_{\kappa})$ mod p.

The use of one-time secrets in such a scheme makes it more secure than a non-interactive Diffie-Hellman key exchange.

All three of the above algorithms solve the main problems of asymmetric cryptography. The last two algorithms include the first one, which becomes the base one. As a result, we can state that in this paper we propose a multifunctional cryptosystem PQC RCNIE on isogenies of non-supersingular Edwards curves. Comparative evaluations of its properties are discussed in the next section.

4. Modeling RCNIE

As in the works [2, 29, 30], whose authors concluded the theoretical provisions of a cryptosystem on isogenies of elliptic curves, resistant to quantum attacks, with examples of encryption of messages on odd degrees of isogenies, in our works [9–12] we use modeling as a way to easily illustrate the properties of algorithms. Understanding these properties opens the way for something new and better. Sometimes the new is the well-forgotten old, as is the case with curves in the Edwards form.

Based on the data of Example 1 of Section 1, we obtain four degrees of isogenies $\{l_k\} = \{3,5,7,37\}$, the first three of which are factors of order 840 of the quadratic curve (2), and degrees 3 and 37 divide order 888 of the twisted curve (3) over the field F_{863} and the trace of the Frobenius equation *t* =24. For the first curve (2) the signs of the isogeny exponents $e_k > 0$, and for curve (3) $e_k < 0$. Here degree 3 is bidirectional (allows both signs), and degrees 5 and 7 ($e_k > 0$) and 37 ($e_k < 0$) are unidirectional. Below we discuss these features of the isogenies of non-supersingular curves.

With a relatively small field modulus *p* = 863, it is not difficult to find estimated $\sqrt{p}$ of the parameters d of all curves (2) with order 840. Since they are squares, then a full enumeration modulo *p* of all $\mathrm{c} = 2,3, \ldots ,431$, and $d = c^2$ gives the set of all 62 values of the parameters *d* of the NEC (2) and (3), shown in Table 1. All the curves together, respectively, are 124. In the class of complete Edwards curves, there would be 62 of them. Here the number of parameters is even, so for each curve, there is an isomorphic curve with the parameter $d \leftrightarrow d^{-1}$ and the same J-invariant (4). For example, $169^{-1} = 623, J(169) = J(623) = 826$. Then there are 31 non-isomorphic curves (2), and the same number of curves (3). Isogenies of all degrees have a prime period π = 31.

Table 1
An array of values of 62 quadratic and twisted NEC parameters *d* at *p* = 863, #*E* = 840, #*E*^{t}=888 (*t* = 24)

169	400	729	161	818	210	436	309	43	665	840
19	779	111	308	253	116	705	503	32	573	472
71	616	618	444	302	192	486	318	852	231	728
300	113	311	858	673	725	589	75	684	551	307
688	843	339	623	706	281	181	27	186	632	130
835	409	345	283	596	326	236				

All values of the parameters in Table 1 can be found by calculating the chains of any isogeny of degrees {3,5,7,37}. For example, let us calculate the 3-isogeny chain of a quadratic curve (2) in the same way as in [11] for CSIDH on supersingular curves of order 840 over the field F_{839}. Choosing the first curve in Table 1 as the starting one, we obtain

$$\frac{d^{(0)} = 169}{(3)} \xrightarrow{1} \frac{503}{(3)} \xrightarrow{1} \frac{318}{(3)} \xrightarrow{1} \frac{652}{(3)} \xrightarrow{1} \frac{181}{(3)} \xrightarrow{1} \frac{551}{(3)} \xrightarrow{1} \frac{326}{(3)} \xrightarrow{1} \frac{161}{(3)} \xrightarrow{1} \frac{618}{(3)} \xrightarrow{1} \frac{436}{(3)}$$
$$\xrightarrow{1} \frac{302}{(3)} \xrightarrow{1} \frac{186}{(3)} \xrightarrow{1} \frac{665}{(3)} \xrightarrow{1} \frac{400}{(3)} \xrightarrow{1} \frac{43}{(3)} \xrightarrow{1} \frac{858}{(3)} \xrightarrow{1} \frac{835}{(3)} \xrightarrow{1} \frac{210}{(3)} \xrightarrow{1} \frac{705}{(3)} \xrightarrow{1} \frac{311}{(3)} \qquad (6)$$
$$\xrightarrow{1} \frac{27}{(3)} \xrightarrow{1} \frac{728}{(3)} \xrightarrow{1} \frac{616}{(3)} \xrightarrow{1} \frac{840}{(3)} \xrightarrow{1} \frac{472}{(3)} \xrightarrow{1} \frac{283}{(3)} \xrightarrow{1} \frac{444}{(3)} \xrightarrow{1} \frac{113}{(3)} \xrightarrow{1} \frac{673}{(3)} \xrightarrow{1} \frac{852}{(3)}$$
$$\xrightarrow{1} \frac{253}{(3)} \xrightarrow{1} \frac{169 = d^{(31)}}{(3)}$$

The number above arrow 1 means one step of the 3-isogeny chain of the quadratic NEC curve (2) with the exponent $e_k > 0$. Under the value of the parameter $d^{(i)}$ we write the degree of isogeny in brackets. For the twisted curve (3) with $e_k < 0$, there is also a 3-isogeny chain of period π = 31

$$\frac{d^{(0)} = 169}{(3)} \xrightarrow{-1} \frac{253}{(3)} \xrightarrow{-1} \frac{852}{(3)} \xrightarrow{-1} \frac{673}{(3)} \xrightarrow{-1} \frac{113}{(3)} \xrightarrow{-1} \frac{444}{(3)} \xrightarrow{-1} \frac{283}{(3)} \xrightarrow{-1} \frac{472}{(3)} \xrightarrow{-1}$$
$$\frac{840}{(3)} \xrightarrow{-1} \frac{616}{(3)} \xrightarrow{-1} \frac{728}{(3)} \xrightarrow{-1} \frac{27}{(3)} \xrightarrow{-1} \frac{311}{(3)} \xrightarrow{-1} \frac{705}{(3)} \xrightarrow{-1} \frac{210}{(3)} \xrightarrow{-1} \frac{835}{(3)} \xrightarrow{-1}$$
$$\frac{858}{(3)} \xrightarrow{-1} \frac{43}{(3)} \xrightarrow{-1} \frac{400}{(3)} \xrightarrow{-1} \frac{665}{(3)} \xrightarrow{-1} \frac{186}{(3)} \xrightarrow{-1} \frac{302}{(3)} \xrightarrow{-1} \frac{436}{(3)} \xrightarrow{-1} \frac{618}{(3)} \xrightarrow{-1}$$
$$\frac{161}{(3)} \xrightarrow{-1} \frac{326}{(3)} \xrightarrow{-1} \frac{551}{(3)} \xrightarrow{-1} \frac{181}{(3)} \xrightarrow{-1} \frac{652}{(3)} \xrightarrow{-1} \frac{318}{(3)} \xrightarrow{-1} \frac{503}{(3)} \xrightarrow{-1} \frac{169 \; = \; d^{(31)}}{(3)}$$

having a reverse order of alternation of isogenic curves (the last chain and (6) are read in reverse or opposite order). The number above the arrow (–1) means one step of the isogeny of the curve (3) with negative parameters. Here the remarkable property of the twofold finding of the multiplicative inversion of an element of an isogenic chain arises. On the one hand, it's true:

$$\begin{aligned} &E^{(0)} * E^{(1)} * E^{(2)} * \dots * E^{(\pi)} = E^{(0)} \;\Rightarrow \\ &\left[E^{(0)}\right] * \left[E^{(0)}\right]^{-1} = 1, \qquad (7) \\ &\left[E^{(0)}\right]^{-1} = E^{(1)} * E^{(2)} * \dots * E^{(\pi)}. \end{aligned}$$

On the other hand, for bidirectional *l*-isogenies of a pair of quadratic twist curves with exponents ±1, we have

$$E^{(1)} * E^{(-1)} = 1 \;\Rightarrow\; \left[E^{(1)}\right]^{-1} = E^{(-1)} \qquad (8)$$

In other words, to multiplicatively reverse one step of an isogenic chain, it is required in the general case to find a chain of period π (see (6) and (7)). The same problem for bidirectional isogenies is solved in one step instead of π steps (8). The opposite signs of the exponents of such isogenies cancel each other out: [l^{+1}]*[l^{-1}] = 1.

The above case takes place in CSIDH, which distinguishes it favorably from CRS. But in CSIDH, the isogeny of each degree in the keys is used as a unidirectional exponent, which is understandable, since different signs of the exponent only neutralize each other [31]. Property (8) is only useful for protection against side-channel attacks [11], and in the CSIKE problem [12, 32]. Together with non-supersingular curves, the inversion of a unidirectional isogeny element according to (7) requires knowledge of the isogeny period and computation time, which is unrealizable for real cryptosystems. In these cryptosystems, handling tasks should be avoided.

Characteristically, for the starting curve ${E_d}^{(0)} = E_{169}$, the sequence $d^{(i)}$ (6) does not contain the element $169^{-1} = 623$ with the same J-invariant. It follows that this is also true for all elements of this sequence of period 31, any of which can be taken as the starting element with the corresponding cyclic shift (as in a cyclic code of length 31). All J-invariants of parameters (6) are different. Isogenic curves of other degrees 5, 7, and 11 contain the same parameters and the same period as (6), alternating in a different order. Next, we will see that the same operating parameters contain all the calculations in the secret sharing scheme. If you invert the starting curve $169^{-1} \to 623$, you do not need to build new isogenic chains, it is enough to invert the results. In this case, the other half of the parameters of Table 1, not included in (6), will be working. Thus, there are two isomorphic cryptosystems with different mutually inverse parameters *d* and coinciding sets of *J*-invariants. If the starting curve is given and does not change all parameters $d^{(i)}$ of isogenic chains are unique and there is no need to pass to the J-invariant of the resulting curve. An isomorphic cryptosystem can solve other problems in parallel, which doubles the performance of such a system. Further, we will see that in addition to the isomorphic cryptosystem, there is also a dual cryptosystem, which also has its isomorphic one. Overall, there is the potential to quadruple the performance of the RCNIE scheme.

4.1. Implementation of the Diffie-Hellman Secret Sharing Algorithm

In our model with isogenies of degrees {3,5,7,37}, to equalize the probabilities of choosing the curves of a pair of quadratic torsion, we will take all the degrees to be unidirectional, then in the secret keys the degrees {5,7} will be assigned to the quadratic curve ($e_k > 0$), and the degree $\{3,37\}^t$ to twisted ($e_k < 0$). Let’s take the secret keys of Alice $\Omega_A = (-2,5,1,-4)$ and Bob $\Omega_B = (-1,3,3,-5)$. Let's compute each of their public keys in 12 randomly chosen isogeny steps.

Alice’s public key with a random choice of curves and degrees is defined as

$$\frac{d^{(0)} = 169}{(5)} \xrightarrow{1} \frac{840}{(3)} \xrightarrow{-1} \frac{616}{(5)} \xrightarrow{1} \frac{43}{(5)} \xrightarrow{1} \frac{326}{(5)} \xrightarrow{1} \frac{852}{(3)} \xrightarrow{-1} 673 = d^{(6)}$$

$$\frac{d^{(6)} = 673}{(37)} \xrightarrow{-1} \frac{472}{(7)} \xrightarrow{1} \frac{551}{(37)} \xrightarrow{-1} \frac{503}{(5)} \xrightarrow{1} \frac{472}{(37)} \xrightarrow{-1} \frac{27}{(37)} \xrightarrow{-1} 835 = d^{(12)} \Rightarrow d_A = 835.$$

Bob’s analogous calculations give:

$$\frac{d^{(0)} = 169}{(3)} \xrightarrow{-1} \frac{253}{(5)} \xrightarrow{1} \frac{616}{(5)} \xrightarrow{1} \frac{43}{(7)} \xrightarrow{1} \frac{444}{(7)} \xrightarrow{1} \frac{161}{(5)} \xrightarrow{1} 253 = d^{(6)}$$

$$\frac{d^{(6)} = 253}{(7)} \xrightarrow{1} \frac{186}{(37)} \xrightarrow{-1} \frac{161}{(37)} \xrightarrow{-1} \frac{652}{(37)} \xrightarrow{-1} \frac{253}{(37)} \xrightarrow{-1} \frac{444}{(37)} \xrightarrow{-1} 616 = d^{(12)} \Rightarrow d_B$$

As a result, public keys d_A =835, d_B=616. are available to two parties. Next, Alice calculates the E_{BA} curve using her secret key $\Omega_A = (-2, 5, 1, -4)$:

$$\frac{d^{(0)} = 616}{(3)} \xrightarrow{-1} \frac{728}{(3)} \xrightarrow{-1} \frac{27}{(5)} \xrightarrow{1} \frac{665}{(5)} \xrightarrow{1} \frac{181}{(5)} \xrightarrow{1} \frac{113}{(5)} \xrightarrow{-1} 311 = d^{(6)}$$

$$\frac{d^{(6)} = 311}{(5)} \xrightarrow{-1} \frac{186}{(7)} \xrightarrow{1} \frac{840}{(37)} \xrightarrow{-1} \frac{311}{(37)} \xrightarrow{-1} \frac{858}{(37)} \xrightarrow{-1} \frac{186}{(37)} \xrightarrow{-1} 161 = d^{(12)} \Rightarrow d_{BA} = 161$$

Bob’s symmetric calculation with $\Omega_B = (-1, 3, 3, -5)$:

$$\frac{d^{(0)} = 835}{(5)} \xrightarrow{1} \frac{618}{(3)} \xrightarrow{-1} \frac{161}{(5)} \xrightarrow{1} \frac{253}{(5)} \xrightarrow{1} \frac{616}{(7)} \xrightarrow{1} \frac{652}{(7)} \xrightarrow{1} 858 \ = d^{(6)}$$

$$\frac{d^{(6)} = 858}{(7)} \xrightarrow{1} \frac{113}{(37)} \xrightarrow{-1} \frac{840}{(37)} \xrightarrow{-1} \frac{311}{(37)} \xrightarrow{-1} \frac{858}{(37)} \xrightarrow{-1} \frac{186}{(37)} \xrightarrow{-1} d^{(12)} \Rightarrow d_{AB} = 161$$

give the same result due to the commutativity of the isogenies $d_{AB} = d_{BA} = 161$ which determines the quadratic curve $\boldsymbol{E_{161}}$ of the shared secret. As noted above, this value is unique (for a given starting curve) and here it is not required to pass to the *J*-invariant in the shared secret $\boldsymbol{\kappa} = 161$.

4.2. Implementation of the Digital Signature Algorithm

The previous problem is solved at the pre-computation stage and also performs mutual authentication of Alice and Bob. They calculated the shared secret key $\boldsymbol{\kappa}$ =161.

A. *DS* formation

1. Calculation $h = H(M)$. Let $h = 852 < \text{p}$.
2. Calculation of $\text{J}(\boldsymbol{\kappa}) = 583$.
3. Calculation $DS = H(852||583) = 796$.
4. Sending $(M, DS) \to \text{B}$, $DS = 796$.

B. *DS* Verification

1. Calculation $h' = H(M')$. Let $h' = 852 < p$.
2. Calculation of $J(\boldsymbol{\kappa}) = 583$.
3. Calculation $DS' = H(852||583) = 796$.
4. Verification: $DS' = DS = 796$. DS is correct.

In conclusion of this section, we note that the example of the implementation of the encryption algorithm here is redundant since with other conditions it is given by the CRS co-authors in [2]. We will only comment on this example.

In [2], an example was constructed for 6 unidirectional isogenies of degrees {3,5,7,11,13,17} with their product 255255 over a prime field with modulus $p = 2038074743$ and the order $\#E = 2038078635$ of the curve in the Weierstrass form with two parameters A and B. There is a typo in the last number in the article since it is not divisible by all degrees except 3 and 5. It is not clear why the model required a redundancy of approximately 10^4 times for the field modulus and curve order. In the corresponding number of times, the calculations become more complicated, and both parameters A and B of the curve increase (these are ten-digit decimal numbers instead of the necessary six-digit ones). In addition, two Weierstrass curve parameters can now be easily replaced with one Edwards curve parameter d and double the computational speed. Perhaps, here and in other algorithms [29, 30, 33], the reasons for the slowness of the CRS scheme are associated with excessive redundancy of parameters, which can be eliminated. But this is not a reason to consider the CRS scheme unacceptable. We will return in the next section to a discussion of this issue.

5. Comparative Evaluations of Properties CSIDH and RCNIE

In [11], we proposed a randomized CSIDH model with bidirectional isogenies of degrees {3.5.7} on curves (2) and (3) above the field F_{839}. These parameters are close to the parameters of non-supersingular curves (2) and (3) over the field F_{863} with different orders 840 and 888 and a trace of Frobenius equation $t = 24$. These two models are most convenient and correctly compared.

It can already be argued that with the transition from CSIDH to a non-supersingular curve, one or more new degrees of isogenies always appear (in our case, $l = 37$). Their insignificant disadvantage is unidirectional isogenies, and for large cryptosystems, it is practically the inability to inverse the isogenic chains and such tasks should be avoided in algorithms. Here we see mutual advantages and disadvantages.

If we now turn to problems related to speed, then we have not found any new reasons inhibiting the execution of the algorithm. Usually, when choosing a random point *P* at the beginning of each step in calculating the isogenic curve, the point *P* may be unsuccessful with a certain degree l_k. This means that the order of point *P* does not contain a factor l_k. The probability of such an event $l_k^{-1}$the more, the lower the degree and reaches the maximum value of 1/3. We do not recommend taking too small degrees in cryptosystems, they are the most problematic. In the described case, randomization allows random transitions to other degrees of isogenies. From our experience, unsuccessful random points arise with the same frequency, regardless of whether the curve is supersingular or not. As noted in the previous section, the slowness of the implementation of the calculations of the isogenies is most likely associated with the exorbitant redundancy of the characterization of the prime field F_p and the curve order in the models used. The reason for this redundancy [2] remains unclear.

For NEC, there is a unique ability to build not only a pair of quadratic twists with the orders $p + 1 \pm t$ but also inside each class to find a pair of curves with the same order as in a quadratic twist curve. We will call the corresponding curves *dual*. Their existence allows you to replace quadratic curves with twisted ones and vice versa. For example, the degree of isogenies of $l = 37$ in our model belongs to the twisted curves $E_{-1,-d}$ of power 64 and order 888. Over the field F_{863}, there is a curve E_d of order 888 with a minimum parameter $d = 6$. Calculate for curves E_d parameters $d^{(i)}$ chains of 37-isogenic curves on the period $\pi = 31$:

$$\frac{d^{(0)}=6}{(37)}\xrightarrow{1}\frac{678}{(37)}\xrightarrow{1}\frac{703}{(37)}\xrightarrow{1}\frac{212}{(37)}\xrightarrow{1}\frac{611}{(37)}\xrightarrow{1}\frac{420}{(37)}\xrightarrow{1}\frac{248}{(37)}\xrightarrow{1}\frac{159}{(37)}\xrightarrow{1}\frac{821}{(37)}\xrightarrow{1}\frac{562}{(37)}$$

$$\xrightarrow{1}\frac{538}{(37)}\xrightarrow{1}\frac{546}{(37)}\xrightarrow{1}\frac{12}{(37)}\xrightarrow{1}\frac{581}{(37)}\xrightarrow{1}\frac{136}{(37)}\xrightarrow{1}\frac{654}{(37)}\xrightarrow{1}\frac{464}{(37)}\xrightarrow{1}\frac{428}{(37)}\xrightarrow{-1}\frac{313}{(37)}\xrightarrow{1}\frac{361}{(37)}$$

$$\xrightarrow{1}\frac{191}{(37)}\xrightarrow{1}\frac{392}{(37)}\xrightarrow{1}\frac{837}{(37)}\xrightarrow{1}\frac{29}{(37)}\xrightarrow{1}\frac{199}{(37)}\xrightarrow{1}\frac{246}{(37)}\xrightarrow{1}\frac{683}{(37)}\xrightarrow{1}\frac{695}{(37)}\xrightarrow{1}\frac{751}{(37)}\xrightarrow{1}\frac{24}{(37)}$$

$$\xrightarrow{1}\frac{553}{(37)}\xrightarrow{1}\frac{6}{(37)}.$$

Here we see half of the dual curves E_d parameters of order 888. As in (6), in this sequence, no element d has the inverse d^{-1}. The second half of the parameters $d^{(i)}$) is calculated by the inversion (for isomorphic curves) of the above. The corresponding twisted curves have order 840. The existence of dual curves makes it possible to build two cryptosystems over the same field of F_{863}: the main and dual, the signs of the exponent isogenies of which change places. These cryptosystems can work independently, and, therefore, double the number of tasks to be solved. If you add isomorphic to each of the two cryptosystems mentioned, four parallel cryptosystems are formed with different sets of parameters d that allow parallel independent calculations. It is still unclear whether there is a simple (as for pairs of quadratic twist) relationship between the parameters of the main and dual curves. This question remains open. In any case, the existence of dual cryptosystems, unique for non-supersingular curves, promises a 4-fold expansion of the capabilities of cryptosystems on the isogenies of elliptic curves. This prospect requires further research.

The results of the implementation of the Edwards-CSIDH model [13] in projective coordinates $(W\colon Z)$ claim that it is faster than the Montgomery-CSIDH models in coordinates $(X\colon Z)$ by 20%. Note that this model in [13] is built on the complete Edwards curves E_d with the order $\#E_d$ = p+1 = 4n (n- odd) and the inversion of the parameter $d \leftrightarrow d^{-1}$ when the transition to the curve of quadratic twist. [9–12] use the fastest arithmetic of quadratic (2) and twisted curves (3) with additive inversion to the parameters of a pair of quadratic twists. The main advantage of these classes of Edwards curves over a prime field F_p is the doubling of several curves in the algorithm with the corresponding increase in safety.

6. Conclusion

A multifunctional cryptosystem RCNIE on isogenies of non-supersingular Edwards curves is proposed, which solves the problems of Diffie-Hellman secret sharing, digital signature, and public key encryption. It is built on two classes of non-cyclic Edwards curves forming pairs of quadratic twists.

The basic RCNIE algorithm is a secret sharing algorithm that also serves to mutually authenticate users.

A model for the execution of crypto-algorithms on isogenies of 4 degrees {3,5,7,37} is constructed and an analysis of its properties is given. Examples of calculations of curve parameters in crypto-algorithms using the randomization method are given.

The existence of the main and dual cryptosystems on non-supersingular curves is illustrated, for each of which there are isomorphic cryptosystems with inverted parameters. The possibility of parallel computing algorithms in these cryptosystems allows you to quadruple the performance of a complex cryptosystem, or use some of them for redundancy and updating.

A comparative evaluation of the arithmetic of cryptosystems on isogenies of supersingular and non-supersingular elliptic curves is given. It is noted that the authors found no reason to consider the latter technology to be slower than that adopted in CSIDH. Since the number of all non-supersingular curves is estimated to be $\sqrt{p}$ times greater than the number of supersingular ones, it is reasonable to use a number of their advantages mentioned above in future applications.

We believe that CSIDH and CRS technologies should not be opposed, but should be developed as promising, taking into account the features and advantages of each of them.

Further studies, it is planned to study new approaches to the formation of sets of isogeny degrees in RCNIE, as well as the digital signatures algorithm.

7. References

[1] W. Castryck, et al., CSIDH: An Efficient Post-Quantum Commutative Group Action, Advances in Cryptology (ASIACRYPT) (2018) 395–427. doi: 10.1007/978-3-030-03332-3_15

[2] A. Rostovtsev, A. Stolbunov, Public-Key Cryptosystem based on Isogenies, IACR Cryptology ePrint Archive 2006/145 (2006). https://ia.cr/2006/145

[3] P. W. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, in: 35th Annual Symposium on Foundations of Computer Science (1994) 124–134. doi: 10.1109/SFCS.1994.365700

[4] J. M. Couveignes, Hard homogeneous spaces, IACR Cryptology ePrint Archive 2006/291 (2006). https://ia.cr/2006/291

[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), vol. 2631 (2020) 30–39.

[6] A. Bessalov, et al., Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves, Cybersecurity Providing in Information and Telecommunication Systems (CPITS), vol. 2746 (2020) 1–13.

[7] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics (2009). doi: 10.1007/978-0-387-09494-6

[8] A. V. Sutherland, Identifying Supersingular Elliptic Curves, LMS Journal of Computation and Mathematics 15 (2012) 317–325. doi: 10.1112/s1461157012001106

[9] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Eurves, Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 1–11.

[10] A. Bessalov, How to Construct CSIDH on Quadratic and Twisted Edwards Curves. Cybersecurity: Education, Science, Technique 3(15) (2022) 148–163. doi: 10.28925/2663-4023.2022.15.148163

[11] A. Bessalov, L. Kovalchuk, S. Abramov, Randomization of CSIDH Algorithm on Quadratic and Twisted Edwards Curves, Cybersecurity: Education, Science, Technique 1(17) (2022) 128–144. doi: 10.28925/2663-4023.2022.17.128144

[12] 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.

[13] S. Kim, et al., Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves, Advances in Cryptology (ASIACRYPT) (2019) 273–292. doi: 10.1007/978-3-030-34621-8_10

[14] R. Farashahi, S. Hosseini, Differential Addition on Twisted Edwards Curves, Lecture Notes in Computer Science (2017) 366–378. doi: 10.1007/978-3-319-59870-3_21

[15] D. Moody, D. Shumow, Analogues of Vélu's Formulas for Isogenies on Alternate Models of Elliptic Curves, Mathematics of Computation 85(300) (2015) 1929–1951. doi: 10.1090/mcom/3036

[16] D. J. Bernstein, et al., Twisted Edwards Curves, Lecture Notes in Computer Science, vol. 5023 (2008) 389–405. doi: 10.1007/978-3-540-68164-9_26

[17] A. Bessalov, Elliptic Curves in Edwards Form and Cryptography (2017) (In Russian).

[18] A. Bessalov, O. Tsygankova, Number of Curves in the Generalized Edwards Form with Minimal Even Cofactor of the Curve Order, Problems of Information Transmission 53(1) (2017) 92-101. doi: 10.1134/S0032946017010082

[19] A. Bessalov, L. Kovalchuk, Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 123, Cybernetics and Systems Analysis 55(3) (2019) 347–353. doi: 10.1007/s10559-019-00140-9

[20] A. Bessalov, L. Kovalchuk, Supersingular Twisted Edwards Curves over Prime Fields.* II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 663, Cybernetics and Systems Analysis 55(5) (2019) 731–741. doi: 10.1007/s10559-019-00183-y

[21] H. Onuki, et al., A Faster Constant-Time Algorithm of CSIDH Keeping Two Points. Lecture Notes in Computer Science (2019) 23–33. doi: 10.1007/978-3-030-26834-3_2

[22] A. Jalali, et al., Towards Optimized and Constant-Time CSIDH on Embedded Devices, Lecture Notes in Computer Science (2019) 215–231. doi: 10.1007/978-3-030-16350-1_12

[23] M. Meyer, S. Reith, A Faster Way to the CSIDH, Lecture Notes in Computer Science, vol. 11356 (2018) 137–152. doi: 10.1007/978-3-030-05378-9_8

[24] M. Meyer, F. Campos, S. Reith, On Lions and Elligators: An Efficient Constant-Time Implementation of CSIDH, Cryptology ePrint Archive 2018/1198 (2018). https://ia.cr/2018/1198

[25] D. Jao, et al., Supersingular Isogeny Key Encapsulation (NIST Round 2) (2019). doi: 10.13140/RG.2.2.26543.07847

[26] National Institute of Standards and Technology. Post-quantum cryptography standardization (2016). https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

[27] M. Qi., An Efficient Post–Quantum KEM from CSIDH, Journal of Mathematical Cryptology 16(1) (2022) 103-113. doi: 10.1515/jmc-2022-0007

[28] L. C. Washington, Elliptic Curves (2008). doi: 10.1201/9781420071474

[29] A. Stolbunov, Constructing Public-Key Cryptographic Schemes based on Class Group Action on a Set of Isogenous Elliptic Curves, Advances in Mathematics of Communications 4(2) (2010) 215–235. doi: 10.3934/amc.2010.4.215

[30] A. Stolbunov. Cryptographic Schemes Based on Isogenies, PhD Thesis (2011). doi: 10.13140/RG.2.2.20826.44488

[31] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, Cybersecurity Providing in Information and Telecommunication Systems (CPITS-II), vol. 3187 (2022) 302–309.

[32] A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Cybersecurity Providing in Information and Telecommunication Systems (CPITS), vol. 3421 (2023) 36–45.

[33] J. Kieffer, Accelerating the Couveignes Rostovtsev Stolbunov key exchange protocol, Rapport de stage de Master 2 Mathématiques fondamentales, Université Paris VIUniversité Paris VI (2017) (In French). doi: 10.48550/arXiv.1804.10128