Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves

Anatoly Bessalov , Volodymyr Sokolov * , Sergey Abramov

Posted Date: 24 June 2024

doi: 10.20944/preprints202406.1600.v1

Keywords: post-quantum cryptography; isogeny-based cryptography; isogeny; supersingular Edwards curve; quadratic Edwards curve; twisted Edwards curve; complete Edwards curve; CSIDH; CSIKE; CRS

 doi:10.20944/preprints202406.1600.v1

Article

Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves

Anatoly Bessalov, Volodymyr Sokolov * and Serhii Abramov

Department of Information and Cyber Security named after Professor Volodymyr Buriachok, Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv 04053, Ukraine
* Correspondence: v.sokolov@kubg.edu.ua

Abstract: The article presents the author's works in the field of modifications and modeling of the PQC CSIDH algorithm on non-cyclic supersingular Edwards curves and its predecessor CRS scheme on ordinary non-cyclic Edwards curves are reviewed. Lower estimates of the computational speed gains of the modified algorithms over the original ones are obtained. The most significant results were obtained by choosing classes of non-cyclic Edwards curves connected as quadratic twist pairs instead of cyclic complete Edwards curves, as well as the method of algorithm randomization as an alternative to "constant time CSIDH." It is shown that in the CSIDH and CSIKE algorithms, there are two independent cryptosystems with the possibility of parallel computation, eliminating the threat of side-channel attacks. For the CRS scheme, there are four such cryptosystems. Integral lower bound estimates of the performance gain of the modified CSIDH algorithm are obtained at $1.5 \cdot 2^9$, and for the CRS scheme are $3 \cdot 2^9$.

Keywords: post-quantum cryptography; isogeny-based cryptography; isogeny; supersingular Edwards curve; quadratic Edwards curve; twisted Edwards curve; complete Edwards curve; CSIDH; CSIKE; CRS

1. Introduction

The announcement of the Post-Quantum Cryptography (PQC) Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) algorithm [1], based on the original CRS scheme [2], was accompanied by the author's statement that it has the smallest known key length of 512 bits with a security level of 128 bits. However, problems with vulnerability to side-channel attacks and fast performance were noted. To overcome the slowness of the implementation of the Couveignes-Rostovtsev-Stolbunov (CRS) scheme [3], the authors justified their choice of supersingular elliptic curves in Montgomery form instead of ordinary (non-supersingular) ones in [2], which speeds up the implementation by a factor of 2,000 [1].

A significant acceleration of CSIDH [1] implementation (20%) was achieved in [4] with Farashahi-Hosseini [5] calculations in projective coordinates $(W:Z)$. The CSIDH model [4] uses the Edwards isogenies of complete curves technique [6] with computations of isogenic curve parameters using formulas [7].

In our articles [8–15] we disagreed with the ambiguous terminology of curves in Edwards form in the pioneering [6] and proposed a more correct classification of them into three non-isomorphic classes [8]. The present article has two aims. First, we give an overview of our most promising modifications of the CSIDH algorithm, which improve the efficiency of the algorithm. Along with this, here for the first time we obtain an integral lower bound estimate of the gain in the speed of computation of isogenic chains $\gamma = 3 \cdot 2^9$ in the speed of computing isogenic chains due to all proposed modifications.

Section 2 gives the rationale for the choice of non-cyclic classes of quadratic and twisted supersingular Edwards curves defined as a pair of quadratic twists over a prime field F_p, where $p \equiv 7 \bmod 8$ [8–11]. Their advantages over the class of complete supersingular Edwards curves are the doubling of the set of all curves and, most importantly, the elimination of the laborious operation of inversion of the d^{-1} parameter d in the transition to quadratic twist. In this article, we obtain the

 doi:10.20944/preprints202406.1600.v1

first partial estimate of the gain $\gamma_1\gamma_2 = 2^5$ in the speed of computation in CSIDH on non-cyclic supersingular Edwards curves compared to complete supersingular Edwards curves.

In Section 3, based on the estimates obtained in [10] of the computational cost in projective coordinates $(W:Z)$ Farashahi-Hosseini [5] parameter d of the isogenic curve and isogenic function $\phi(x,y)$ we obtained an estimate of the gain in computational speed in CSIDH $\gamma_3 = 2.235$ due to the refusal of the redundant calculation of the function $\phi(x,y)$.

In Section 4, we consider the method of randomization of the CSIDH algorithm [12] and justify estimates of the speed gain of its implementation. We emphasize the existence of two isomorphic cryptosystems with parallel computation capability, which removes the threat of side-channel and doubles the performance of the algorithm. Here, the partial estimate of the speed gain of the algorithm is $\gamma_4\gamma_5\gamma_6 = 2^3$.

Section 5 is devoted to the optimization of the distribution of isogeny degrees in CSIDH [14], which is not dense and has discontinuities in the table of prime numbers. It is shown that, while preserving the security parameters, it is possible to reduce the degree of the senior isogeny and obtain a linear estimate of the CSIDH acceleration by a factor of 1.5.

The original and fast key encapsulation algorithm Commutative Supersingular Isogeny Key Encapsulation (CSIKE) [13] and its model implementation are discussed in Section 6. Here a single public key of the recipient is used instead of two in CSIDH, which gives a security gain.

In Section 7, we consider aspects of the CRS model implementation of the Diffie-Hellman secret sharing scheme on 4-degree isogenies {3,5,7,37} of ordinary non-cyclic Edwards curves. An important advantage of these curves is the existence of 4-independent cryptosystems with the possibility of parallel computation and performance quadrupling (or doubling compared to CSIDH). Other interesting problems and modifications of cryptosystems are considered in [15].

2. Selection of Classes and Types of Edwards Curves

Depending on the quadratic properties of the parameters a and d we in [8] also propose a more correct classification of curves into three non-intersecting classes than in [6]:

A. Complete Edwards curves: $\chi(a) = 1, \chi(d) = -1$;

B. Quadratic Edwards curves: $\chi(a) = \chi(d) = 1$;

C. Twisted Edwards curves: $\chi(a) = \chi(d) = -1$.

The well-known implementation of the CSIDH algorithm [4] is based on complete Edwards curves **A** in the Farashahi-Hosseini $(W:Z)$ coordinate system, which accelerated its performance by 20% compared to Montgomery curves in the $(X:Z)$ coordinate system. We have justified and utilized non-cyclic curves of classes **B** and **C** as quadratic twist pairs in [9–15]. They have two important advantages over the complete Edwards curves **A**:

1. Doubling the number of all curves in the algorithm over a single class **A** doubles the set of all isogenic curves of classes **B** and **C** with a corresponding gain in security. This can be exchanged for a gain in computational speed $\gamma_1 = 2$;
2. For half of all computable isogenic curves with negative exponents e_i given by the secret key Ω (see Section 4), no time-consuming inversion of the parameter d of the class **A** isogenic curve is required. The corresponding gain in speed γ_2 in computational speed should be estimated.

Let us define curves **B** and **C** as a pair of quadratic twists at $p \equiv 7 \bmod 8$ by the equations:

$$E_{1,d}: x^2 + y^2 = 1 + dx^2y^2, a, d \in F_p^*, a = 1, \chi(d) = 1, \quad (1)$$

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

In the twisted curve (2), both parameters of the curve are multiplied by (-1) and become non-square. The orders of all supersingular Edwards curves are equal to $\#E = p + 1 = 8n$, where for the CSIDH algorithm $n = \prod_{i=1}^{K} l_i$, where l_i are the degrees of prime odd isogenies (see Section 4). The maximum order of a point of a non-cyclic curve is $4n$, so it is sufficient to multiply any random point by four to obtain odd-order points.

 doi:10.20944/preprints202406.1600.v1

It follows from (1) and (2) that the transition to quadratic twist for classes **B** and **C** is practically free, whereas within class A such a transition is achieved by inversion of the parameter d, which according to a known estimate [16] requires (10..50)M, where M is the cost of multiplication in the group F_p^*. Taking conditionally the complexity of the transition between curves (1) and (2) as $1M$, we obtain a conditional average estimate of the gain $\gamma_2 \approx 2^5$ in computational speed compared to complete curves **A**. Since in the CSIDH algorithm the transition to quadratic twist is required for approximately half of the isogenic curves, we can use a conditional lower estimate of the gain $\gamma_2 \approx 2^4$.

By curve type here we mean supersingular curves with trace $t = 0$ or ordinary curves with order $\#E = p + 1 - t$, where t is the trace of the Frobenius equation, $t \neq 0$. Since the set of the former is $\sqrt{p}$ times wider than the set of supersingular curves, interesting unique applications of this type of Edwards curves are discussed in [15] and Section 7.

An important tool in analyzing isogenies is the *J*-invariant [6]

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

This parameter distinguishes between isogenic (with different *J*-invariants) and isomorphic (with equal *J*-invariants) curves. Since the *J*-invariant retains its value for all isomorphic curves and quadratic twist pairs [17], it is the same for a pair of quadratic and twisted supersingular Edwards curves ($a = \pm 1$), so we will use the invariant $J(d)$. It is useful both in finding supersingular curves and in constructing isogeny chain graphs. One of the properties of *J*-invariant is $J(d) = J(d^{-1})$.

For the considered classes of supersingular Edwards curves the substitution $d \to d^{-1}$ gives an isomorphism, and for complete Edwards curves a quadratic twist.

3. Computation of Odd-Degree Isogenies on Edwards Curves and Complexity Estimation

Isogenies of an elliptic curve $E(K)$ over the field K into a curve $E'(K)$ is a homomorphism $\phi: E(\bar{K}) \to E'(\bar{K})$given by rational functions. This means that there exists a rational function [17]

$$\phi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{f(x)}{g(x)}\right) = (x', y'), \quad (4)$$

mapping the points of the curve E to the points of the curve E', and for all $P, Q \in E(K)$ $\phi(P+Q) = \phi(P) + \phi(Q)$. The isogeny degree is the maximum of the degrees $l = \deg \phi\,(x,y) = \max\{\deg p\,(x), \deg q\,(x)\}$and its kernel $\ker \phi = G$ is the subgroup $G \subseteq E$ whose points are mapped by the function $\phi(x,y)$ into a neutral element O of the group E'. The degree of the separable isogeny is equal to the ordering l of its kernel. The isogeny compresses the set of points of the curve E в l times (l curve points E are mapped to a single point on the curve E').

The computation of isogenies of Edwards curves of classes **A** and **B** of odd powers is performed according to Theorem 2 [7]. In [9] we generalized it to curves of class **C** in the following theorem.

Theorem 1. *Let* $G = \{(1,0), \pm Q_1, \pm Q_2, \dots, \pm Q_s\}$ *is a subgroup of odd order of* $l = 2s + 1$ *points of* $\pm Q_i = (\alpha_i, \pm\beta_i)$ *curve* E_d *over the field* F_p.

Let's determine

$$\phi(P) = (x', y') = \left(\prod_{Q \in G} \frac{x_{P+Q_i}}{x_{Q_i}} \frac{x_{P-Q_i}}{x_{-Q_i}}, \prod_{Q \in G} \frac{y_{P+Q_i}}{x_{Q_i}} \frac{y_{P-Q_i}}{x_{-Q_i}}\right). \quad (5)$$

Then $\phi(x,y)$ there is *l*-isogeny with the kernel *G* from the curve $E_{a,d}$ into a curve $E'_{a',d'}$ with parameters $a' = a^l d' = A^8 d^l$, where $A = \prod_{i=1}^{s} \alpha_i$, and the mapping function

$$\phi(x,y) = \left(\frac{x}{A^2}\prod_{i=1}^{s} \frac{(\alpha_i x)^2 - a^2(\beta_i y)^2}{1 - (d\alpha_i\beta_i xy)^2}, \frac{y}{A^2}\prod_{i=1}^{s} \frac{(\alpha_i y)^2 - (\beta_i x)^2}{1 - (d\alpha_i\beta_i xy)^2}\right) \quad (6)$$

or

 doi:10.20944/preprints202406.1600.v1

$$\phi(x,y)=\left(\frac{x}{A^2}\prod_{i=1}^{s}\frac{x^2-a{\beta_i}^2}{1-d\beta_i x^2},-\frac{y}{A^2}\prod_{i=1}^{s}\frac{x^2-{a_i}^2}{a-d\alpha_i x^2}\right). \quad (7)$$

Proof of Theorem 1. Its proof is given in [9]. It is important to note that the isogenic function (7) includes the parameter a, which is absent in the original Theorem 2 [7]. □

The parameters of the isogenic curve according to Theorem 2 [7] are calculated by the formulas

$$a'=a^l d'=A^8 d^l,\ A=\prod_{i=1}^{s}\alpha_i. \quad (8)$$

The task of this section is a comparative evaluation of the complexity of computing the isogenic function $\phi(x,y)$ and the parameter d' of the isogenic curve $E'_{a',d'}$. This will allow us to estimate the gain in computational speed in the CSIDH algorithm when giving up the computation of the function $\phi(x,y)$ (justified in Section 4).

The fastest results today for curve isogenies in Edwards form are obtained in projective coordinates $(W:Z)$ with the introduction of a generalized Farashahi-Hosseini variable $w=dx^2y^2$ [5]. For isogenies of degree l are calculated $s=(l-1)/2$ points $Q_i=(\alpha_i,\beta_i)$ of the isogeny kernel together with the coordinates $w_i=d\alpha_i^2\beta_i^2$, then according to Theorem 2 [4]

$$w(\phi)=w\prod_{i=1}^{s}\frac{w-w_i}{1-ww_i}. \quad (9)$$

Let M complexity of multiplication in the field F_p, S is the complexity of squaring, and let us use the results of [4]. Taking into account the complexity of calculating the coordinates of the kernel points, the complexity of calculating the function $\phi(x,y)$ is equal to

$$C_\phi=s(8M+2S)+S-2M. \quad (10)$$

The cost of calculating the parameter d' of the isogenic curve E', respectively,

$$C_d=s(6M+2S)+5S-4M. \quad (11)$$

Let's take the known estimate $S=\frac{2}{3}M$ [6]. Then we have

$$C_\phi=\frac{28}{3}sM-\frac{4}{3}M,\ C_d=\frac{22}{3}sM-\frac{2}{3}M. \quad (12)$$

The gain in computing speed without taking into account C_ϕ equals

$$\gamma_3=\frac{C_d+C_\phi}{C_d}=1+\frac{C_\phi}{C_d}=1+\frac{14s-2}{11s-1}. \quad (13)$$

For l at the maximum $s\approx 300$ and minimum $s=1$ this gain is equal to 2.27 and 2.20, respectively. On average, we obtain $\gamma_3=2.235$. Thus, the acceleration of the CSIDH algorithm when refusing the redundant calculation of the function $\phi(x,y)$ is estimated by the coefficient $\gamma_3=2.235$.

4. Randomization of the CSIDH Algorithm on Non-Cyclic Edwards Curves

The PQC CSIDH algorithm is proposed by the authors [1] to solve the classical Diffie-Hellman key exchange problem. Isogenic curve mapping E of order $\#E$ over a prime field F_p into a curve E' is defined as the class-group action and is commutative. Compared to the known original CRS scheme (Couveignes [18] and Rostovtsev et al. [2]) on ordinary curves, the use of isogenies of supersingular curves allowed us to speed up the algorithm and obtain the smallest known key size (512 bits with a security level of 128 bits in [1]).

Let the curve E of order $\#E$ contain points of small odd orders $l_k, k=1,2,\dots,K$. Then there exists an isogenic curve E' of the same order $\#E$ as a mapping of degree $l_k: E\to E'=[l_k]*E$. Repetition of this operation e_k times is denoted as $[{l_k}^{e_k}]*E$. The values of the exponents of the isogenies $e_k\in Z$ determine the length of the chain of isogenies of degree l_k. In [1] the interval of

 doi:10.20944/preprints202406.1600.v1

exponent values is adopted $[-m \le e_k \le m]$, $m = 5$, $K = 74$, which provides a security level of 128 bits during attacks on a quantum computer. Negative values of the exponent e_i mean transition to the supersingular curve of quadratic twist.

Non-interactive key exchange using the Diffie-Hellman scheme involves steps [1]:

1. *Parameter selection*. For small prime odd l_k is calculated $n = \prod_{k=1}^{K} l_k$ where the value K is determined by the security level, a suitable field modulus $p = 2^m \prod_{k=1}^{K} l_k - 1, m \ge 3$, and the starting elliptic curve E_0 are chosen;
2. *Public key computation*. Alice uses her secret key $\Omega_A = (e_1, e_2, \dots, e_K)$ constructs an isogenic mapping $\Theta_A = [{l_1}^{e_1}, {l_2}^{e_2}, \dots, {l_K}^{e_K}]$ and computes the isogenic curve $E_A = \Theta_A * E_0$ as her public key. Bob, based on the secret key Ω_B and function Θ_B performs the same computation and obtains his public key $E_B = \Theta_B * E_0$ These curves are defined by their parameters with exact isomorphism;
3. *Key exchange*. The protocol here is similar to Step 2 with a change $E_0 \to E_B$ for Alice and $E_0 \to E_A$ for Bob. Knowing Bob's public key, Alice calculates $E_{BA} = \Theta_A * E_B = \Theta_A \Theta_B * E_0$. Bob's similar action gives the result $E_{AB} = \Theta_B * E_A = \Theta_B \Theta_A * E_0$, coinciding with the first one due to the commutativity of the group operation. As a shared secret we take J-invariant of the curve E_{AB} (E_{BA}).

Below we give a modification of Alice's computation algorithm according to Section 3 [1] using isogenies of quadratic and twisted supersingular Edwards curves.

Algorithm 1. *Evaluation of the class-group action on quadratic and twisted supersingular Edwards curves.*

Input: $d_A \in E_A, \chi(d) = 1$ and a list of integers $\Omega_A = (e_1, e_2, \dots, e_K)$.
Output: d_B such that $[{l_1}^{e_1}, {l_2}^{e_2}, \dots, {l_K}^{e_K}] * E_A = E_B$, where $E_{A,B}: x^2 + ay^2 = 1 + ad_{A,B}x^2y^2$.

1. WHILE some $e_i \neq 0$ DO
2. Sample a random $x \in F_p$;
3. Set $a \leftarrow 1$, $E_A: x^2 + y^2 = 1 + d_A x^2 y^2$ IF $\frac{1-x^2}{1-dy^2}$ is a square in F_p;
4. ELSE $a \leftarrow -1$, E_A: $x^2 - y^2 = 1 - d_A x^2 y^2$;
5. Let $S = \{i | ae_i > 0\}$. IF $G = \emptyset$ then start over to Line 2 while $a \leftarrow -a$;
6. Let $n = \prod_{i \in S} l_i$ and compute $R \leftarrow \frac{p+1}{2n} P, P \leftarrow P(x, y)$;
7. FOR each $i \in S$ DO
8. Compute $Q \leftarrow \frac{k}{l_i} R$;
9. IF $Q \neq (1,0)$ compute an isogeny $\phi: E_A \to E_B$ with $\ker \phi = Q$;
10. Set $d_A \leftarrow d_B$, $R \leftarrow \phi(R)$, $e_i \leftarrow e_i - a$;
11. Skip i in S and $n \leftarrow \frac{n}{l_i}$ IF $e_i = 0$;
12. RETURN d_{A}. □

Compared to Algorithm 2 in [1], Algorithm 1 adapted to quadratic and twisted supersingular Edwards curves, makes modifications that are discussed in [11]. In this section, we present an analysis of the speed gains of the randomized algorithm [12] compared to the algorithm [1].

The CSIDH algorithm [1] is constructed in such a way that the computation of isogenic chains according to functions $\Theta_{A,\mathrm{B}} = [{l_1}^{e_1}, {l_2}^{e_2}, \dots, {l_K}^{e_K}]$ are performed in two stages: first the set is formed S with key exponents e_k of one sign, then, after zeroing of all e_k, of the other. At each stage, the kernels and parameters of exactly $|e_k|$ of isogenic curves of isogenies of degrees l_k constructed on curves of the same class (E_d or $E_{-1,-d}$). This gives rise to the threat of a side-channel attack based on measuring the time of these computations, proportional to the length of the $|e_k|$ and degree l_k of each chain $[{l_k}^{e_k}]$. In this regard, most articles on this topic [19,20] consider different variants of "constant time CSIDH" in which the secret exponents are e_k are built up to an upper bound m by fictitious chains of isogenies. Such protection is achieved by significant redundancy and slowing down the algorithm by half.

We propose in [12] another method for solving the problem is the randomization of the path of isogenic chains. The idea is that any random coordinate of the x of an elliptic curve always generates

 doi:10.20944/preprints202406.1600.v1

a random point $P=(x,y)$ of one of the two curves of a pair of quadratic twist pair (1) or (2). Then instead of trying (unsuccessfully with probability ½) to find a point of a curve of a given class and succeeding with probability 1, we determine the class of curve (in our case it is the curve E_d (1) or $E_{-1,-d}$ (2), one of which the point belongs to $P=(x,y)$). Then we calculate the first isogenic curve in this class $E^{(1)}=[l_k]*E^{(0)}$ isogeny degree l_k corresponding to the sign of the exponent e_k. The selection l_k is randomized, and the value $|e_k|$ is decreased by one. In the next step with a new value of the parameter $d^{(1)}$ the random point $P=(x,y)$ of one of the curves E_d or $E_{-1,-d}$, the isogeny kernel of the randomly chosen degree is determined l_k and the parameter $d^{(2)}$ of the chain. The process continues until all $e_k=0$. The corresponding randomized CSIDH Algorithm 2 is given below.

Algorithm 2. *Randomized evaluation of the class-group action on quadratic and twisted supersingular Edwards curves.*

Input: $d_A\in E_A, \chi(d)=1$ and a list of integers $\Omega_A=(e_1,e_2,\dots,e_K)$.
Output: d_B such that $[{l_1}^{e_1},{l_2}^{e_2},\dots,{l_K}^{e_K}]*E_A=E_B$, where $E_{A,B}: x^2+y^2=1+d_{A,B}x^2y^2$.

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 $a\leftarrow 1$, $s\leftarrow 0$, $E_A: x^2+y^2=1+d_Ax^2y^2$ IF $\chi\left(\frac{x^2-1}{dx^2-1}\right)=1$;
5. ELSE $a\leftarrow -1$, $s\leftarrow 1$, $E_A: x^2-y^2=1-d_Ax^2y^2$;
6. Compute y-coordinate of the point $P=(x,y)\in E_A$;
7. Compute $R\leftarrow\frac{p+1}{2n_s}P$;
8. Sample a random $l_k|k\in S_s$;
9. Compute $Q\leftarrow\frac{n_s}{l_k}R$;
10. IF $Q\neq(1,0)$ compute kernel G of l_k-isogeny $\phi: E_A\to E_B$;
11. ELSE start over to Line 3;
12. Compute d_B of curve E_B, $d_A\leftarrow d_B$, $e_k\leftarrow e_k-s$;
13. Skip k to V_s and set $n_s\leftarrow\frac{n_s}{l_k}$ IF $e_k=0$;
14. RETURN d_A. □

Here instead of one set S in Algorithm 1 two sets S_0 and S_1 are formed, in which the numbers of isogeny degrees corresponding to the key positions are recorded Ω_A with positive and negative exponents e_k, respectively. At any random choice of x is coordinate we obtain a random point $P=(x,y)$, belonging to the curve (1) or (2). Its multiplication by four in Step 7 gives a point of R of odd order. The scalar multiplication in Step 9 calculates the point of the Q of the isogeny kernel, then the coordinates of all points of the kernel G.are calculated. Finally, in Step 12, according to (8), we calculate the parameter d' of the isogenic curve E'.

Note that in classical CSIDH there is already a guaranteed level of protection against the type of side channel attack described above. It is determined by the sign of the secret exponent$e_k$of the key. Since each component of $[l_k]$ function Θ computation time $[{l_k}^{+1}]$ and $[{l_k}^{-1}]$ is the same, the probability of the analyst's success even in the conditions of error-free values of l_k is equal to $2^{-K}=2^{-74}$ (for the data of [1]). For the average length of $\frac{m+1}{2}=3$ chain of isogenies of each degree l_k the total length of the chain of isogenies of the function is $\Theta=3\cdot 74=222$ steps. Let p_1 be the probability of error-free determination of degree l_k by the analyst at one step of the randomized CSIDH protocol, then its probability of success can be estimated by the value $2^{-74}{p_1}^{222}, p_1<1$. For example, at $p_1=\frac{1}{2}$ the analyst's probability of success is 2^{-296}, and at $p_1=\frac{3}{4}$ this probability is close to the value 2^{-165} that is well below the safety level 2^{-128}. Various modifications of the proposed randomization method are possible with insertions of single dummy exponents into the sample components of the $[l_k]$ functions Θ that will not introduce redundancy into the calculations. Note that one mistake of an analyst destroys all his labor-intensive work.

 doi:10.20944/preprints202406.1600.v1

Algorithm 2 does not include the computation of the isogenic function $\phi(x,y)$, which gives an estimate of the speed gain of Algorithm 2 $\gamma_3 = 2.235$. The following gain $\gamma_4 = 2$ randomization method provides that instead of choosing one of the curves (1) or (2) with probability ½ in Algorithm 2, any choice is good. There is also an approximate gain $\gamma_5 = 2$ compared to "constant time CSIDH" in which close to half of the isogenies are fictitious, which is not the case in Algorithm 2.

Finally, we'll justify the gain $\gamma_6 = 2$ due to parallel computations in two cryptosystems with isomorphic curves. This article is described for the first time. The idea is that in classes **B** and **C** for any Edwards curve (1) and (2) with parameter d there exists an isomorphic curve with parameter d^{-1}. Fixing the starting curve E_0, we construct chains of isogenies of all degrees of the first cryptosystem with the secret key Ω_1. The second cryptosystem with the secret key Ω_2 can be easily constructed on the set of all curves isomorphic to the first one. For this purpose, another starting curve is chosen by inverting the parameter d of any curve of the first cryptosystem. These two sets of curves do not intersect, and it is possible to solve two problems simultaneously instead of one, which doubles the computational performance. In addition, parallel computing removes the threat of side-channel attacks altogether and makes the "constant time CSIDH" redundancy meaningless.

Reducing for simplicity the estimate γ_3 and taking $\gamma_3 = 2$, we obtain from the results of this section a partial estimate of the computational speed gain of the CSIDH algorithm $\gamma_3\gamma_4\gamma_5\gamma_6 = 2^4$. Thus, the final lower speedup estimate of the CSIDH algorithm modified in [9–15] is no less than $\prod_{k=1}^{6}\gamma_k \geq 2^9$. In the following sections, we consider further modifications of CSIDH and their performance evaluations.

5. Optimization of Isogeny Degree Set in CSIDH

In this section, we optimize the distribution of isogeny degrees $\{l_k\}$ in [14] and evaluate the gains γ_7 of this optimization in comparison with the CSIDH model [1].

We found that 74 degrees l_k isogenies in [1] with the value of $l_{\max} = 587$ runs only a fraction of all minimal prime numbers from 3 to 587, the total number of which is 106. In other words, 32 values of prime numbers are not included in the list of degrees l_k in the model [1], which means discontinuities (gaps) in the set of $\{l_k\}$. With an average cost of each degree of 8 bits, a rough estimate of the cost of the removed degrees is $32 \cdot 8 = 256$ bits. These losses are unnecessary and generate a slowdown of the algorithm at excessively high degrees of isogenies.

We set a task to analyze possible distributions of sets of prime numbers of the set $L = \{l_k\}^K$ with size K and to find variants of optimization (compaction) of this distribution. According to the table of prime numbers up to 587, the complete set $L = \{l_k\}^N = \{3,5,7,\dots,587\}$ contains $N = 106$ all prime numbers.

Let's call the set of prime numbers ordered in ascending order $\{l_k\}^K$ is optimal if at known $l_{\min} = l_m$ and K product $\prod_{k=m}^{K+m-1} l_k = \max$. It follows from the definition that the optimal set of prime numbers is dense (without skips) with elements $\{l_m, l_{m+1}, \dots, l_{K+m-1}\} \in L$. It is constructed as a segment of length K of ordered prime numbers. Removing at least one number (except the extreme numbers) from the middle of the segment gives a non-optimal set $\{l_k\}^K \notin L$. Removal of one of the extreme numbers l_m, l_{max} of the segment gives two different optimal sets of size $K-1$. Any subset (segment of length K) of the complete set L is an optimal set. A non-optimal set contains skips that violate the condition $\prod_{k=m}^{K+m-1} l_k = \max$.

The complete set $L = \{l_k\}^{106} = \{3,5,7,\dots,587\}^{106}$ is optimal by definition. Removing 32 numbers from it gives a set $\{l_k\}^{K=74}$ that is far from optimal. This set $\{l_k\}$ in [1]. We associate the notion of optimality exclusively with the maximization of the product of elements of the set.

Let's divide L into subsets $Lh = \{l_k\}^{K_h}, h = 1,\dots,6$ which includes prime numbers in the hundreds of numbers with numbers h. For the first hundred, for example, we have the subset $L1 = \{3,5,7,\dots,97\}^{K_1}$, where $K_1 = 24$. For all six subsets Lh these numbers K_h are given in the second row of Table 1.

 doi:10.20944/preprints202406.1600.v1

Table 1. Distribution of the number K_h prime numbers in subsets Lh and their products B_h within hundreds with numbers h.

h	1	2	3	4	5	6
K_h	24	21	16	16	17	12
B_h	119.795	151.245	127.623	135.192	149.782	109.134

Each degree l_k in binary form has a $\log(l_k)$ bit. For all products of numbers l_k in subsets Lh we calculate the bit length $B_h = \sum_{l_k \in Lh} \log(l_k)$ of the degrees of isogenies. The values B_h are given in the third row of Table 1. These results allow us to draw interesting conclusions. First, the sum of all bits of the third row $\sum_{h=0}^{6} B_h = 792.772 = 793$ bits, defining the product of all 106 prime numbers $\{3, \dots, 587\}$, has a redundancy of 283 bits compared to the minimum lower threshold of 510 bits ($4n > 2^{512}$) [1] security requirements. Second, prime numbers in the 5th and 6th hundreds ($L5$ and $L6$) can be removed, since $\sum_{h=1}^{4} B_h = 533.855 = 534$ bits, which satisfies with a margin of 24 bits the requirement $4n > 2^{512}$. Ignoring the last two columns of Table 1, we obtain 77 values of the elements of the optimal set of $\{l_k\}^{K=77} = \{3, \dots, 397\}$ of prime numbers. Further, we propose to remove the 3 lowest degrees in the first hundred $\{3,5,7\}$ and construct the optimal set of isogeny degrees $Lopt = \{11,13, \dots, 397\}^{74}$ of the same size 74 as in [1]. This preserves the length $K = 74$ of the secret key. Given the equality $\log(3 * 5 * 7) = 6.714$, the product n of all l_k of the optimal set $Lopt$ is evaluated by a binary number of length 528 bits. Adding 2 bits, we obtain the estimate $\log p = 530$ bit. For the distribution $Lopt$ we can adjust Table 1: in column $h = 1$ of the table we should put the values of $K_1 = 21, B_1 = 113.081$ and the last two columns of the table should be deleted. Then $\sum_{h=1}^{4} K_h = 74, \sum_{h=1}^{4} B_h = 527.141 = 528$ bits, $\log p = 530$ bit. Such an optimal distribution of degrees $\{l_k\}$ isogenies ensures that the minimal security threshold of 512 bits of the algorithm is exceeded by 18 bits.

Note that the reserve of 18 bits can be used up by removing the two maximum isogeny degrees 397 and 389 for a total cost of 18 bits and taking $l_{\max} = 383$. However, this requires reducing the length $K \leftarrow K - 2$ of the secret key by two.

The main advantage of the set of isogeny degrees proposed here $Lopt$ over the one used in [1] is a significant (by a factor of 1.5) decrease of $l_{\max} = 587$ up to $l_{\max} = 397$ with an optimal distribution of prime numbers. The real gain requires experimental estimation of the complexity of CSIIDH implementation at such a radical reduction of the value of $l_{\max}$.

So, a linear estimate of the gain in computational speed due to the optimization of the isogeny degree distribution is equal to $\gamma_7 = 1.5$. Together with the total gain of the previous sections, we obtain a speedup of the CSIIDH algorithm by a factor of $1.5 * 2^9 \cong 770$ times.

6. CSIKE Algorithm

The classical non-interactive Diffie-Hellman algorithm is based on the use of two public keys. The same problem of generating a shared secret can be solved in a protocol with one transmission session and one recipient's public key, which is more secure. To do this, Alice generates a shared secret, encrypts it with Bob's public key, and sends him the encrypted key. On receipt, Bob decrypts it with his secret key. This protocol is called key encapsulation. It involves the steps [21]:

1. *Secret key generation* k. Alice uses a random number sensor to find the secret encapsulation vector $\Omega_k = (e_1, e_2, \dots, e_K)$, constructs the class function of the class group action $\Theta_k = [{l_1}^{e_1}, {l_2}^{e_2}, \dots, {l_K}^{e_K}]$ and computes an isogenic curve $E_k = \Theta_k * E_0$, whose parameter d_k is taken as the secret key $d_k = k$.
2. *Key encapsulation.* It's Alice's procedure for encrypting the key k with Bob's public key E_B. To do this, Alice computes an isogenic curve $\Theta_k * E_B = E_{kB}$. The parameter d_{kB} of this curve is sent to Bob.
3. *Key decapsulation.* Bob's decryption of the curve E_{kB} with his secret key Ω_B is reduced to his computation of an isogenic curve $\overline{\Theta_B} * E_{kB} = E_k$ where the mapping $\overline{\Theta_B}$ is constructed by inversion of all signs of the exponents of Bob's secret key $\Omega_B \to (-\Omega_B)$.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 June 2024 doi:10.20944/preprints202406.1600.v1

In [13], we propose the original CSIKE algorithm as a modification of CSIDH, replacing Alice's secret key with a secret vector Ω_k, with which she computes a curve $E_k = \Theta_k * E_0$ and the shared secret key $d_k = k$. Alice then encrypts it with Bob's public key E_B. and computes the curve $E_{kB} = \Theta_k * E_B = \Theta_k * \Theta_B * E_0$. Bob decapsulates his cipher using a multiplicative inverse function $\overline{\Theta_B}$ (such that $\Theta_B * \overline{\Theta_B} = \mathbf{I}$, where $\mathbf{I} = [1,1,\dots,1]|_K$), thereby restoring the curve $E_k = \Theta_k * E_0$. As the key of encapsulation by both parties, we can take *J*-invariant of the curve E_k.

We consider a simple model of the implementation of the CSIKE algorithm on quadratic and twisted supersingular Edwards curves that form pairs of quadratic twist curves with order $p+1$. Such curves exist only at $p \equiv -1 \bmod 8$ and have order $\#E = \#E^t = p+1 = cn(n-odd), c \equiv 0 \bmod 8$. Let such a pair of curves contain kernels of order 3, 5, and 7. At the value $n = 105$ of the minimal prime $p = 8n-1 = 839$, then the order of these curves $\#E = 8n = 840$. The parameter d of the whole family of 418 quadratic Edwards curves can be taken as squares $d = r^2 \bmod p, r = 2,\dots,419$. Of these, 66 pairs of quadratic and twisted supersingular Edwards curves are found with parameters $a = \pm 1$ and $\chi(ad) = 1$. Table 2 summarizes the values of the parameter d for pairs of quadratic E_d and twisted $E_{-1,-d}$ supersingular Edwards curves. They are written as squares $d = r^2 \bmod p, r = 2,\dots,419$ in ascending order r. In this example, the relative proportion of supersingular Edwards curves is close to 16%. Note that for each curve in Table 2, there is at least one isomorphic curve with a parameter d^{-1} and the same *J*-invariant (2).

Table 2. Values of 66 parameters d of quadratic and twisted supersingular Edwards curves ($a = \pm 1$) at $p = 839$ and $\#E = 840$.

144	*	289	*	784		2	*	61	*	258	*	508	*	365		488	*	30		705		
742		56		259	*	180	*	329		135		640		32		38	*	28	*	90		
564		772	*	286	*	40		610		98		475		63		511		43	*	795		
414	*	76	*	752	*	800		405	*	666	*	112	*	413		200		236	*	433	*	
15	*	683	*	293	*	750		808		578	*	288		636	*	514	*	276		773	*	
243	*	45		788	*	172	*	777		427		21	*	810		552		420		230		

* A set of 33 parameters that have mutually inverse pairs of parameters for parallel computing.

For the first quadratic curve $E_d^{(0)} = E_{144}$ from Table 2, we can construct 3-, 5-, and 7-isogenies and find the parameters $d^{(i)}$ of a chain of isogenic curves $E_d^{(i)}, i = 0,1,2,\dots,\mathrm{T}$ such that $d^{(T)} = d^{(0)}$. Period T of the chain of isogenies divides the number $66 = 2 \cdot 3 \cdot 11$ of all supersingular Edwards curves. The calculations of the parameters of $d^{(i)}$ chains of respectively 3-, 5-, and 7-isogenies quadratic supersingular Edwards curves are useful only for illustrating the properties of chains of isogenies of quadratic twist pair curves and we omit them in this article. We only note that the period of the 3-isogeny $T_3 = 33$, and the other two $T_5 = T_7 = 11$. The fragments of isogenic chains of quadratic supersingular Edwards curves in the tables are read from left to right, for twisted ones—from right to left. At each step i isogeny of degree $l = 2s+1$ coordinates $\alpha_1,\dots,\alpha_s, s = (l-1)/2$ points of the kernel, after which the parameter of the $d^{(i+1)}$ of the isogenic curve $E_d^{(i+1)}$ according to (8) is calculated. Calculation of the isogenic function $\phi(x,y)$, according to Algorithm 1 of Section 5 is not necessary.

Example 5.1. *Suppose Alice has generated a secret vector* $\Omega_k = (7,-5,8)$, *which by isogenic mapping* $\Theta_k = [3^7, 5^{-5}, 7^8]$ *at the first stage transforms it into a shared secret key* k *i.e., calculates the curve* $E_k = \Theta_k * E_0$.

Then at the second stage, she encrypts this key with Bob's public key. d_B. Let Bob's secret $\Omega_B = (-8,6,-5)$, respectively, its function of the class-group action $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$. Let us perform their key computations k, d_B. As the starting curve of the chain of isogenies, we take the curve $E_d^{(0)} = E_{144}$. Then $E_k = E_0 * \Theta_k$, $E_B = E_0 * \Theta_B$.

To simplify the record in the algorithm for calculating the isogenic curve $E_k = E_0 * \Theta_k$ we will use only the parameters $d^{(i)}$ which completely defines the curves $E_d^{(i)}(e_k > 0)$ and $E_{-1,-d}^{(i)}(e_k < 0)$ as pairs of quadratic twists. In the parameter chain $d^{(i)}$ below we write in parentheses the degree of

 doi:10.20944/preprints202406.1600.v1

isogeny, above the arrow the number of steps with the exponent sign e_k. For example, according to the function $\Theta_k = [3^7, 5^{-5}, 7^8]$ and the curve $E_d^{(0)} = E_{144}$ without resorting to the randomization method (see Section 4), Alice computes a chain of

$$\frac{d_0 = 144}{(7)} \xrightarrow{8} \frac{258}{(5)} \xrightarrow{-5} \frac{112}{(3)} \xrightarrow{7} 286 = k. \quad (14)$$

So, the shared secret key $k = 286$. Similarly, Bob calculates his public key based on the curve E_{144} and a function $\Theta_B = [3^{-8}, 5^6, 7^{-5}]$

$$\frac{d_0 = 144}{(5)} \xrightarrow{6} \frac{788}{(7)} \xrightarrow{-5} \frac{258}{(3)} \xrightarrow{-8} 514 = d_B. \quad (15)$$

So Bob's public key $d_B = 514$. Then, in the second encapsulation step, Alice encrypts Bob's public key with the secret key $k = 286$ and calculates $E_{Bk} = E_B * \Theta_k$.

$$\frac{d_B = 514}{(3)} \xrightarrow{7} \frac{683}{(5)} \xrightarrow{-5} \frac{38}{(7)} \xrightarrow{8} 259 \Rightarrow d_{Bk} = 259. \quad (16)$$

Finally, in the third step of decapsulation, Bob from the curve $d_{Bk} = 259$ removes his secret key using the inverse function $\overline{\Theta_B} = [3^8, 5^{-6}, 7^5]$

$$\frac{d_0 = 259}{(7)} \xrightarrow{5} \frac{578}{(5)} \xrightarrow{-6} \frac{38}{(3)} \xrightarrow{8} 286 \Rightarrow d_k = 286. \quad (17)$$

He ends up with a shared secret key $k = 286$ calculated for him by Alice. To avoid ambiguity when obtaining isomorphic curves, J-invariant (3) is taken as the encapsulation key by both parties $J(d_k) = 525$ curve E_{286}.

The above example gives a concise illustration of the CSIKE algorithm. Its efficiency increases significantly after using the randomization method (see Section 4). For example, Alice's computation of the encapsulation key k. based on the secret vector $\Omega_\kappa = (7, -5, 8)$ can be realized by a pseudo-random chain of isogenic curves in 20 steps

$$\frac{d_0 = 144}{(3)} \xrightarrow{2} \frac{405}{(5)} \xrightarrow{-1} \frac{15}{(7)} \xrightarrow{1} \frac{488}{(5)} \xrightarrow{-1} \frac{43}{(7)} \xrightarrow{2} \frac{508}{(5)} \xrightarrow{-1} \frac{289}{(3)} \xrightarrow{2} \frac{43}{(7)} \xrightarrow{3}$$
$$\xrightarrow{3} \frac{405}{(5)} \xrightarrow{-1} \frac{15}{(3)} \xrightarrow{1} \frac{243}{(5)} \xrightarrow{-1} \frac{293}{(7)} \xrightarrow{3} \frac{636}{(3)} \xrightarrow{1} 286 \Rightarrow d_k = k = 286. \quad (18)$$

This result is, understandably, the same as the first result above. In Table 2, exactly half of the parameters d are marked with asterisks. These 33 values are included in the period $T = 33$ 3-isogeny and form a set of parameters d^* of the first cryptosystem with the starting curve E_{144} (or any other curve of this set d^*). In our example, all isogenic curves belong to this set. The parameters not labeled in Table 2 form the set of 33-parameter d^{-1} isomorphic curves, on which we can build a second cryptosystem independent of the first one with the possibility of parallel computation. For example, from the starting curve with $d^* = 144$ parameter inversion we come to an isomorphic curve E_{705} of the second cryptosystem (see Table 2). Further, by specifying different secrets Ω_{k1} and Ω_{k2} in the two cryptosystems, we can double the key length (512 → 1024 bit in CSIDH). Parallel computation, moreover, makes a side-channel attack hopeless. Note also that this possibility arises when only classes of non-cyclic Edwards curves (1) and (2) are used. □

We can conclude that the CSIKE algorithm and modifications of the CSIDH algorithm proposed in our works [13] on quadratic and twisted supersingular Edwards curves provide an efficient and secure alternative to various variants of "Constant time CSIDH" [19,20] with lower estimates in computational speed up to $1.5 \cdot 2^9$. Computation of odd degree isogenies in coordinates $(W:Z)$ [4], allows us to realize the fastest computations to date in the construction of PQC protocols CSIDH, CSIKE, and similar. Examples of such implementation for simple models of CSIDH and CSIKE algorithms are given in [9–15]. The possibility of refusing to compute the isogenic function $\phi(R)$ of a random point R, which more than doubles the speedup of the algorithm, is justified. The above results cast doubt on the assertion of the author of [22] about the insufficient efficiency of the CSIDH algorithm. The largest computational costs in the algorithms are associated with scalar multiplications of random points, the costs of which require rather experimental evaluation.

 doi:10.20944/preprints202406.1600.v1

7. CRS Encryption Scheme on Isogenies of Ordinary Non-Cyclic Edwards Curves

The presentation of Castryck et al. [1] of the PQC CSIDH algorithm cites the CRS scheme as the first proposed scheme on isogenies of ordinary elliptic curves [2]. Its remarkable properties are the commutativity of isogenic transitions, flexibility, and simplicity due to the use of prime field arithmetic F_p. The CSIDH algorithm already uses the technology of supersingular elliptic curves, which is justified by the relatively faster implementation of the algorithms. For example, it is noted that CRS encryption is prohibitively slow and can take several minutes at a security level of 128 bits [1].

In [15], we attempted to find reasons for the slowness of the CRS scheme compared to CSIDH and found only immeasurable redundancy in the choice of cryptosystem parameters [2,3]. Then, dealing with the modeling and modification problems of CSIDH, we constructed a prime 4-isogenous model of the CRS scheme with degrees {3,5,7,37} with our modifications [15]. Since the set of ordinary elliptic curves is approximately $\sqrt{p}$ times wider than the set of supersingular curves, we should expect that their advantages would be discovered as well. Indeed, such advantages turned out to be the growth of the number of degrees of isogenies at a given or close modulus of the p field, and the presence of four parallel independent cryptosystems instead of two in CSIDH, which doubles the speed of the CRS scheme algorithm comparably to CSIDH.

In this survey article, we only consider aspects related to the encryption model and omit the multifunctionality of the scheme described in the original article [15].

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 $|t| \le 2\sqrt{p}$. For a curve of quadratic twist E^t this order $\#E^t = p + 1 + t$ is symmetric concerning the mean value $p + 1$. For the 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 reversed, as in CSIDH. In the case of ordinary curves, the orders of the quadratic twist pairs differ by $2t$, then there exist different degrees of isogenies on curves of two classes related as quadratic twist pairs with different orders. This is the main specificity of ordinary curves. The exponents of the degrees of isogenies of these two curves, as in CSIDH, have opposite signs. The alternation of the degrees of isogenies according to the randomization method is random, and the simplicity of the transitions of the chain of isogenies from one class of non-cyclic Edwards curves (1) and (2) to another is achieved by the fact that their parameters are additively inverse: $(a, d) \leftrightarrow (-a, -d)$ (see Section 2).

By analogy with CSIDH, it is not difficult to form general parameters of CRS—similar cryptosystem on isogenies of ordinary Edwards curves of order $\#E \equiv 0 \bmod 8$ over a field with modulus $p \equiv 7 \bmod 8$. Let $n_0 = \prod_{k=1}^{K} l_k$ and $N = 8n_0$ is the order of a quadratic supersingular Edwards curve over a field with modulus $p_0 = N - 1$. 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 a prime number p. Then over the field F_p there exists a quadratic ordinary Edwards curve (1) of order $\#E_d = 8n_0$ and a twisted curve (2) of order $\#E_{-1,-d} = N \pm 16m = 8n_1$.

For example, for the set of degrees of isogenies $\{l_k\} = \{3,5,7\}, n_0 = 105, N = 840, p_0 = 839$, then at $m = 3$ we obtain a prime number $p = 839 + 24 = 863$. Thus the orders of the curves of the pair of quadratic twists are $\#E_d = 840 = 8 \cdot 3 \cdot 5 \cdot 7$ and $\#E_{-1,-d} = N + 48 = 888 = 8 \cdot 3 \cdot 37$, $n_1 = 111 = 3 \cdot 37$.

Other variants of calculating the ordinary Edwards curve parameters are given in [15]. Thus, we have four degrees of isogenies $\{l_k\} = \{3,5,7,37\}$, the first three of which are factors of order 840 of the quadratic curve (1), and degrees 3 and 37 share order 888 of the twisted curve (2) over the field F_{863} and the trace of the Frobenius endomorphism equation $t = -24$. For the first curve (1), the signs of the exponents of the isogenies are $e_k > 0$, and for the curve (2) $e_k < 0$. Here degree 3 is bidirectional (admits both signs), and degrees 5 and 7 ($e_k > 0$) and 37 ($e_k < 0$) are unidirectional.

With a relatively small field modulus $p = 863$ it is not difficult to find the estimated $\sqrt{p}$ parameters d of all curves (1) with order 840. Since they are squares, a complete search modulo p of all $c = 2,3, \ldots, 431$, and $d = c^2$ yields the set of all 62 values of the parameters d of the ordinary Edwards curves (1) and (2) given in Table 3. All curves together, respectively, are 124. Here the

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 June 2024 doi:10.20944/preprints202406.1600.v1

number of parameters is even since for each curve there exists an isomorphic curve with parameter $d \leftrightarrow d^{-1}$ and the same J-invariant (3). For example, $169^{-1} = 623$, $J(169) = J(623) = 826$. Then there are 31 non-isomorphic curves (1), the same number of curves (2). Isogenies of all degrees have a prime period $\pi = 31$.

Table 3. The array of 62-parameter values of d quadratic and twisted ordinary Edwards curves ($a = \pm 1$) at $p = 863$, $\#E_d = 840$, $\#E_{-1,-d} = 888$ ($t = 24$).

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	*	652	*	130	
835	*	409		345		283	*	596		326	*	236									

* A set of 31 parameters that have mutually inverse pairs of parameters for parallel computing.

All parameter values of Table 3 can be found by computing chains of any degree isogeny {3,5,7,37} in period $\pi = 31$. For example, let us compute the chain of 3-isogenies of the quadratic curve (1) in the same way as in [10] for CSIDH on supersingular curves of order 840 over the field F_{839}. Choosing the first curve in Table 3 as the starting curve, we obtain for the curve (1)

$$\underset{(3)}{d^{(0)} = 169} \xrightarrow{1} \underset{(3)}{503} \xrightarrow{1} \underset{(3)}{318} \xrightarrow{1} \underset{(3)}{652} \xrightarrow{1} \underset{(3)}{181} \xrightarrow{1} \underset{(3)}{551} \xrightarrow{1} \underset{(3)}{326} \xrightarrow{1} \underset{(3)}{161} \xrightarrow{1} \underset{(3)}{618} \xrightarrow{1} \underset{(3)}{436} \xrightarrow{1} \underset{(3)}{302} \xrightarrow{1}$$
$$\xrightarrow{1} \underset{(3)}{186} \xrightarrow{1} \underset{(3)}{665} \xrightarrow{1} \underset{(3)}{400} \xrightarrow{1} \underset{(3)}{43} \xrightarrow{1} \underset{(3)}{858} \xrightarrow{1} \underset{(3)}{835} \xrightarrow{1} \underset{(3)}{210} \xrightarrow{1} \underset{(3)}{705} \xrightarrow{1} \underset{(3)}{311} \xrightarrow{1} \underset{(3)}{27} \xrightarrow{1} \underset{(3)}{728} \xrightarrow{1} \quad (19)$$
$$\xrightarrow{1} \underset{(3)}{616} \xrightarrow{1} \underset{(3)}{840} \xrightarrow{1} \underset{(3)}{472} \xrightarrow{1} \underset{(3)}{283} \xrightarrow{1} \underset{(3)}{444} \xrightarrow{1} \underset{(3)}{113} \xrightarrow{1} \underset{(3)}{673} \xrightarrow{1} \underset{(3)}{852} \xrightarrow{1} \underset{(3)}{253} \xrightarrow{1} \underset{(3)}{169 = d^{(31)}}.$$

The number above Arrow 1 denotes one step of the 3-isogeny chain of the quadratic ordinary Edwards curve (1) with exponent $e_k > 0$. Under the value of the parameter $d^{(i)}$ in parentheses, we write the degree of isogeny.

For the curved curve (2) with $e_k < 0$ there also exists a 3-isogeny of the same period π =31

$$\underset{(3)}{d^{(0)} = 169} \xrightarrow{-1} \underset{(3)}{253} \xrightarrow{-1} \underset{(3)}{852} \xrightarrow{-1} \underset{(3)}{673} \xrightarrow{-1} \underset{(3)}{113} \xrightarrow{-1} \underset{(3)}{444} \xrightarrow{-1} \underset{(3)}{283} \xrightarrow{-1} \underset{(3)}{472} \xrightarrow{-1} \underset{(3)}{840} \xrightarrow{-1}$$
$$\xrightarrow{-1} \underset{(3)}{616} \xrightarrow{-1} \underset{(3)}{728} \xrightarrow{-1} \underset{(3)}{27} \xrightarrow{-1} \underset{(3)}{311} \xrightarrow{-1} \underset{(3)}{705} \xrightarrow{-1} \underset{(3)}{210} \xrightarrow{-1} \underset{(3)}{835} \xrightarrow{-1} \underset{(3)}{858} \xrightarrow{-1} \underset{(3)}{43} \xrightarrow{-1}$$
$$\xrightarrow{-1} \underset{(3)}{400} \xrightarrow{-1} \underset{(3)}{665} \xrightarrow{-1} \underset{(3)}{186} \xrightarrow{-1} \underset{(3)}{302} \xrightarrow{-1} \underset{(3)}{436} \xrightarrow{-1} \underset{(3)}{618} \xrightarrow{-1} \underset{(3)}{161} \xrightarrow{-1} \underset{(3)}{326} \xrightarrow{-1} \quad (20)$$
$$\xrightarrow{-1} \underset{(3)}{551} \xrightarrow{-1} \underset{(3)}{181} \xrightarrow{-1} \underset{(3)}{652} \xrightarrow{-1} \underset{(3)}{318} \xrightarrow{-1} \underset{(3)}{503} \xrightarrow{-1} \underset{(3)}{169 = d^{(31)}},$$

having a reverse order of alternation of isogenic curves (the last chain and (19) are read in reverse order). The number above the arrow (–1) means one step of the isogenic curve (1) with negative parameters. Do not forget that the pair of twist curves E_d and $E_{-1,-d}$ here are orders of 840 and 888, respectively. For any other degree of isogeny, we can construct similar (19) and (20) chains of isogenic curves of period $\pi = 31$ with the same set of parameters $d^{(i)}$, but with different orders of alternation. In Table 3, these 31 parameters d are marked with asterisks. This is the set of parameters d of the first cryptosystem. Inverting each parameter d^* we get unlabeled 31 parameters d of the second cryptosystem. As in Section 6 when describing CSIKE (CSIDH), here we also have two isomorphic cryptosystems with the possibility of parallel computation.

A remarkable property of ordinary curves in comparison with supersingular curves is the existence of two more isomorphic cryptosystems. The idea is prime: we can swap the orders of the

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 June 2024 doi:10.20944/preprints202406.1600.v1

quadratic (1) and twisted (2) ordinary Edwards curves. The corresponding cryptosystem will be called dual.

Let the orders of the curves (1) and (2) over the field F_{863} $\#E_d = 888$, $\#E_{-1,-d} = 840$. For a dual cryptosystem, we can compute an array of parameter values d instead of the brute-force method for Table 3. Let us find just one curve (1) with an order $\#E_d = 888$ and parameter $d = 6$. Let us compute a 37-isogeny chain like (19) with a starting value $d = 6$, and its values marked with an asterisk are entered in the first three rows of Table 4. In the same sequence, in the next three rows of the array, we will write the inverted values of the d^{-1} of the isomorphic curves (not marked with an asterisk). The upper and lower parts of Table 4 form equal-sized sets of the parameters of the d of two isomorphic dual cryptosystems.

Table 4. The grouped array of 62-parameter values of d quadratic and twisted ordinary Edwards curves $(a = \pm 1)$ at $p = 863$, $\#E_d = 888$, $\#E_{-1,-d} = 840$ $(t = 24)$.

6	*	678	*	703	*	212	*	611	*	420	*	248	*	159	*	821	*	562	*	538	*	
546	*	12	*	581	*	136	*	654	*	464	*	438	*	313	*	361	*	191	*	392	*	
837	*	29	*	199	*	246	*	683	*	695	*	751	*	24	*	553	*					
144		849		685		460		613		150		87		38		226		453		470		
49		72		254		514		128		478		664		670		153		122		284		
697		744		425		214		513		488		732		36		103						

* A set of 31 parameters that have mutually inverse pairs of parameters for parallel computing.

So, using an ordinary instead of supersingular Edwards curve, we get four independent cryptosystems instead of two, which in parallel computing provides a 4-fold gain in cryptosystem performance compared to classical CSIDH. Parallel computation must make it impossible to realize side channel attack and redundancy in "constant time CSIDH" meaningless. Redundant cryptosystems can be used both for the 4-fold increase of key length in encapsulation algorithms and for simplification of the algorithm (reducing the number of isogeny degrees at fixed key length).

Let us consider an example of the implementation of the Diffie-Hellman secret-sharing algorithm on the first cryptosystem with 31 parameters d^* from Table 4. In our model with isogenies of degrees {3,5,7,37}, to equalize the selection probabilities of the quadratic twist pair curves, we assume all degrees are unidirectional, then in the secret keys of degrees {5,7} we attribute the quadratic curve $(e_k > 0)$ and degrees $\{3,37\}^t$ to the twisted curve $(e_k < 0)$. Let's take Alice's secret keys $\Omega_A = (-2,5,1,-4)$ and Bob's $\Omega_B = (-1,3,3,-5)$ Let's compute for 12 randomly chosen isogeny steps for each of their public keys.

Alice's public key with randomly chosen curves and degrees is defined as

$$\frac{d^{(0)} = 169}{(5)} \xrightarrow{1} \frac{840}{(3)} \xrightarrow{-1} \frac{616}{(5)} \xrightarrow{1} \frac{43}{(5)} \xrightarrow{1} \frac{326}{(5)} \xrightarrow{1} \frac{852}{(3)} \xrightarrow{-1} 673 = d^{(6)}, \quad (21)$$

$$\frac{d^{(6)} = 673}{(37)} \xrightarrow{-1} \frac{472}{(7)} \xrightarrow{1} \frac{551}{(37)} \xrightarrow{-1} \frac{503}{(5)} \xrightarrow{1} \frac{472}{(37)} \xrightarrow{-1} \frac{27}{(37)} \xrightarrow{-1} 835 = d^{(12)} \Rightarrow \quad (22)$$

$$\Rightarrow d_A = 835.$$

Bob's similar calculations give

$$\frac{d^{(0)} = 169}{(3)} \xrightarrow{-1} \frac{253}{(5)} \xrightarrow{1} \frac{616}{(5)} \xrightarrow{1} \frac{43}{(7)} \xrightarrow{1} \frac{444}{(7)} \xrightarrow{1} \frac{161}{(5)} \xrightarrow{1} 253 = d^{(6)}, \quad (23)$$

$$\frac{d^{(6)} = 253}{(7)} \xrightarrow{1} \frac{186}{(37)} \xrightarrow{-1} \frac{161}{(37)} \xrightarrow{-1} \frac{652}{(37)} \xrightarrow{-1} \frac{253}{(37)} \xrightarrow{-1} \frac{444}{(37)} \xrightarrow{-1} 616 = d^{(12)} \Rightarrow \quad (24)$$

$$\Rightarrow d_B = 616.$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 24 June 2024 doi:10.20944/preprints202406.1600.v1

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

$$\frac{d^{(0)} = 616}{(3)} \xrightarrow{-1} \frac{728}{(3)} \xrightarrow{-1} \frac{27}{(5)} \xrightarrow{1} \frac{665}{(5)} \xrightarrow{1} \frac{181}{(5)} \xrightarrow{1} \frac{113}{(5)} \xrightarrow{-1} 311 = d^{(6)}, \quad (25)$$

$$\frac{d^{(6)} = 311}{(5)} \xrightarrow{-1} \frac{186}{(7)} \xrightarrow{1} \frac{840}{(37)} \xrightarrow{-1} \frac{311}{(37)} \xrightarrow{-1} \frac{858}{(37)} \xrightarrow{-1} \frac{186}{(37)} \xrightarrow{-1} 161 = d^{(12)} \Rightarrow \quad (26)$$

$$\Rightarrow d_{BA} = 161.$$

Bob's symmetric calculus

$$\frac{d^{(0)} = 835}{(5)} \xrightarrow{1} \frac{618}{(3)} \xrightarrow{-1} \frac{161}{(5)} \xrightarrow{1} \frac{253}{(5)} \xrightarrow{1} \frac{616}{(7)} \xrightarrow{1} \frac{652}{(7)} \xrightarrow{1} 858 = d^{(6)}, \quad (27)$$

$$\frac{d^{(6)} = 858}{(7)} \xrightarrow{1} \frac{113}{(37)} \xrightarrow{-1} \frac{840}{(37)} \xrightarrow{-1} \frac{311}{(37)} \xrightarrow{-1} \frac{858}{(37)} \xrightarrow{-1} \frac{186}{(37)} \xrightarrow{-1} d^{(12)} \Rightarrow \quad (28)$$

$$\Rightarrow d_{AB} = 161$$

give the same result due to the commutativity of isogenies $d_{AB} = d_{BA} = 161$, which defines the quadratic curve E_{161} of the shared secret. As noted above, this value is unique (for a given starting curve). It is not required here in the shared secret $k = 161$ to go to the J-invariant. Similar calculations with other starting curves and keys can be performed in parallel in other 3-independent cryptosystems to solve different problems.

9. Discussion

Let us summarize the main and composite results of the present and previous [9–15] works:

1. The results obtain a lower estimate of the computational speed gain of the modified CSIDH algorithm on non-cyclic supersingular Edwards curves by a $\gamma = 1.5 \cdot 2^9$ times;
2. The transition from the class of complete Edwards curves to the classes of quadratic and twisted Edwards curves double the set of curves and does not require inversion of the parameter d of the Edwards curves, which is evaluated by a partial gain estimate of a 2^5 times;
3. The method of randomization of the CSIDH algorithm and avoiding the computation of the isogenic function $\phi(x, y)$ in the projective coordinates $(W:Z)$ of Farashahi-Hosseini speeds up the algorithm more than 2^3 times;
4. Optimizing the isogeneity degrees of the CSIDH algorithm reduces the maximum isogeneity degree with a linear estimate of the algorithm speedup by a factor of 1.5;
5. For every non-cyclic Edwards curve, there exists an isomorphic Edwards curve with an inverted parameter, which gives rise to the existence of two independent cryptosystems with parallel computation capability. This doubles the performance of the CSIDH algorithm and eliminates the threat of side-channel attacks. The CSIKE scheme also allows doubling the length of the secret key to 1024 bits;
6. An original CSIKE key encapsulation scheme with one public key instead of two in CSIDH is proposed and modeled, which provides improved security of the algorithm;
7. A model of Diffie-Hellman secret sharing on isogenies of degrees {3,5,7,37} of non-cyclic Edwards curves is constructed for the CRS scheme of ordinary curves. It is shown that instead of two isomorphic cryptosystems in the CSIDH algorithm, the transition to a set of ordinary Edwards curves gives rise to four independent cryptosystems with parallel computation capability. This can double the above estimate of the computational speed gain up to $\gamma = 3 \cdot 2^9$.

Although in [22] it is stated that a drawback of CSIDH is that it is still considered to be inefficient when compared to other algorithms, taking into account the optimization data of the algorithm, it can be assumed that the algorithm can be used on an equal basis with other PQC algorithms.

 doi:10.20944/preprints202406.1600.v1

9. Conclusions

Based on the results of these calculations, we can conclude that the integral improvement of the characteristics of PQC algorithms allows us to significantly increase the speed of the algorithm (about 1,500 times). Taking into account the short key length and the increased speed of the algorithm, it is promising to use it to ensure secure exchange in embedded systems and systems with limited computing resources. In addition, the parallelization of computations allows for minimizing the exploitation of side-channel vulnerabilities. We believe that CSIDH and CRS technologies should not be contrasted but should be developed as promising technologies, taking into account the features and advantages of each of them.

Future research is planned to investigate new approaches to form isogeny degree sets in CRS encryption and digital signature schemes.

Author Contributions: Conceptualization, A.B.; methodology, A.B.; software, S.A.; validation, A.B. and V.S.; formal analysis, V.S.; investigation, S.A.; resources, V.S.; original draft preparation, V.S.; review and editing, V.S.; visualization, V.S.; funding acquisition, V.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Castryck, W.; Lange, T.; Martindale, C.; Panny, L.; Renes, J. CSIDH: An efficient post-quantum commutative group action. In 24th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), Brisbane, QLD, Australia, 2–6 December 2018, vol. 11274, 395–427. [https://doi.org/10.1007/978-3-030-03332-3_15]
2. Rostovtsev, A.; Stolbunov, A. Public-key cryptosystem based on isogenies. *Cryptology ePrint Archive, Paper 2006/145, 2006 (preprint)*. [https://eprint.iacr.org/2006/145]
3. Stolbunov, A. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications* **2010**, *4(2)*, 215–235. [https://doi.org/10.3934/amc.2010.4.215]
4. Kim, S.; Yoon, K.; Park, Y.-H.; Hong, S. Optimized method for computing odd-degree isogenies on Edwards curves. In 25th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), Kobe, Japan, 8–12 December 2019, part II, vol. 11922, 273–292. [https://doi.org/10.1007/978-3-030-34621-8_10]
5. Farashahi, R.R.; Hosseini, S.G. Differential addition on twisted Edwards curves. In 22nd Australasian Conference (ACISP), Auckland, New Zealand, 3–5 July 2017, part II, vol. 10343, 366–378. [https://doi.org/10.1007/978-3-319-59870-3_21]
6. Bernstein, D.J.; Birkner, P.; Joye, M.; Lange, T.; Peters, C. Twisted Edwards curves. In 1st International Conference on Cryptology in Africa (AFRICACRYPT), Casablanca, Morocco, 11–14 June 2008, vol. 5023, 389–405. [https://doi.org/10.1007/978-3-540-68164-9_26]
7. Moody, D.; Shumow, D. Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves. *Mathematics of Computation* **2015**, *85(300)*, 1929–1951. [https://doi.org/10.1090/mcom/3036]
8. Bessalov, A. Elliptic Curves in Edwards Form and Cryptography; Polytechnic: Kyiv, Ukraine, 2017 (in Russian).
9. Bessalov, A.; Sokolov, V.; Skladannyi, P. Modeling of 3- and 5-isogenies of supersingular Edwards curves. In 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS), Lviv-Shatsk, Ukraine, 2–3 June 2020, vol. 2631(I), 30–39.
10. Bessalov, A. On correctness of conditions for the CSIDH algorithm implementation on Edwards curves. *Radiotekhnika* **2022**, *208*, 16–27. [https://doi.org/10.30837/rt.2022.1.208.02]
11. Bessalov, A.; Sokolov, V.; Skladannyi, P.; Mazur, N.; Ageyev, D. Implementation of the CSIDH algorithm model on supersingular twisted and quadratic Edwards curves. In Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), Kyiv, Ukraine, 26 October 2021, vol. 3187(1), 302–309.
12. Bessalov, A.; Kovalchuk, L.; Abramov, S. Randomization of CSIDH algorithm on quadratic and twisted Edwards curves. *Cybersecurity: Education, Science, Technique* **2022**, 1(17), 128–144. [https://doi.org/10.28925/2663-4023.2022.17.128144]

13. Bessalov, A.; Sokolov, V.; Skladannyi, P.; Abramov, S.; Zhyltsov, O. Modeling CSIKE algorithm on non-cyclic Edwards curves. In Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), Kyiv, Ukraine, 13 October 2022, vol. 3288, 1–10.
14. Bessalov, A.; Abramov, S.; Sokolov, V.; Mazur, N. CSIKE-ENC combined encryption scheme with optimized degrees of isogeny distribution. In Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), Kyiv, Ukraine, 28 February 2023, vol. 3421, 36–45.
15. Bessalov, A.; Abramov, S.; Sokolov, V.; Skladannyi, P.; Zhyltsov, O. Multifunctional CRS encryption scheme on isogenies of non-supersingular Edwards curves. In Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC), Kyiv, Ukraine, 1 August 2023, vol. 3504, 12–25.
16. Koblitz, N.; Menezes, A. A riddle wrapped in an Enigma. *IEEE Security & Privacy* **2016**, *14(6)*, 34–42. [https://doi.org/10.1109/msp.2016.120]
17. Washington, L.C. *Elliptic Curves: Number Theory and Cryptography*, 2nd ed.; Chapman & Hall / CRC: Boca Raton, USA, 2008.
18. Couveignes, J.-M. Hard homogeneous spaces. *Cryptology ePrint Archive, Paper 2006/291, 2006 (preprint)*. [https://eprint.iacr.org/2006/291]
19. Onuki, H.; Aikawa, Y.; Yamazaki, T.; Takagi, T. A faster constant-time algorithm of CSIDH keeping two points. In 14th International Workshop on Security (IWSEC), Tokyo, Japan, 28–30 August 2019, vol. 11689, 23–33. [https://doi.org/10.1007/978-3-030-26834-3_2]
20. Jalali, A.; Azarderakhsh, R.; Kermani, M.M.; Jao, D. Towards optimized and constant-time CSIDH on embedded devices. In 10th International Workshop (COSADE), Darmstadt, Germany, 3–5 April 2019, vol. 11421, 215–231. [https://doi.org/10.1007/978-3-030-16350-1_12]
21. Yoneyama, K. Post-quantum variants of ISO/IEC standards. In 5th ACM Workshop on Security Standardisation Research Workshop (SSR), London, United Kingdom, 11 November 2019, 13–21. [https://doi.org/10.1145/3338500.3360336]
22. Galbraith, S.D.; Perrin, D.; Voloch, J.F. CSIDH with level structure. *Cryptology ePrint Archive, Paper 2023/1726, 2023 (preprint)*. [https://eprint.iacr.org/2023/1726]