CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution

Anatoliy Bessalov[1], Sergey Abramov[1], Volodymyr Sokolov[1], and Nataliia Mazur[1]

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

Abstract

For the PQC CSIDH and CSIKE algorithms, the advantages of two classes of quadratic and twisted supersingular Edwards curves over complete Edwards curves are justified. These classes form pairs of quadratic twist curves with order $p + 1 \equiv 0 \bmod 8$ over the prime field F_p and double the space of all curves in the algorithms. The randomized algorithms CSIDH and CSIKE are presented. An analysis of the degrees l_k isogenies distribution is given, and an optimal distribution within the given conditions is proposed with the degree $l_{max} = 397$ instead of $l_{max} = 587$ while maintaining the number $K = 74$ of all degrees. A probabilistic analysis of random odd order points R was carried out, probability estimates are obtained, and it is recommended to avoid isogenies with small values of the degrees l_k in algorithms. The features of the CSIKE algorithm with one public key of Bob in the problem of encapsulation by Alice of the secret key $\boldsymbol{\kappa}$, which Bob calculates at the stage of decapsulation with his secret key, are considered. A CSIKE-ENC scheme for combined encryption of the key κ and message M based on two asymmetric algorithms CSIDH and CSIKE with Alice's authentication and the well-known symmetric message encryption standard is proposed. The security aspects of the scheme are discussed.

Keywords

CSIKE, CSIKE-ENC, curve in generalized Edwards form, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, supersingular Edwards curve, curve order, point order, isogeny, isomorphism, class-group action, w-coordinates.

1. Introduction

One of the most promising PQC algorithms, which has generated a wide stream of scientific articles, is the CSIDH algorithm [1]. It solves the problem of non-interactive Diffie-Hellman secret sharing based on the construction of chains of isogenic supersingular elliptic curves with the set $\{l_k\}^K$ of K small odd prime degrees l_k isogenies over the prime field F_p. The binary length log p of the modulus p of the field determines the length of the key in the algorithm and the (log p)/2 security levels for attacks on a classical computer and (log p)/4 on a quantum computer (the notation "log" refers to the base-2 logarithm). The CSIDH algorithm has the smallest key length among known PQC algorithms.

This paper continues and develops the results of the previous one [2] in the problem of CSIKE key encapsulation with authentication and combined encryption by asymmetric and symmetric algorithms.

The first implementations of CSIDH were based on fast supersingular curves in the Montgomery form [1], but soon in [3–5] using the W: Z-coordinates of curves in the Edwards form, it was possible to obtain a gain of 20% in comparison with [1] in the computation speed. Further, generalizing the formulas for calculating isogenies for Edwards curves [6] to twisted Edwards curves in [7], we illustrated the implementation of CSIDH models on quadratic and twisted Edwards curves [2, 7, 9, 10]. The last curves were first defined in the fundamental work [11], but with unfortunate terminology, so we use the classification of curves in the Edwards form [12, 13]. An analysis of the properties of

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine

EMAIL: a.bessalov@kubg.edu.ua (A. Bessalov); s.abramov@kubg.edu.ua (S. Abramov); v.sokolov@kubg.edu.ua (V. Sokolov); n.mazur@kubg.edu.ua (N. Mazur)
ORCID: 0000-0002-6967-5001 (A. Bessalov); 0000-0002-5145-2782 (S. Abramov); 0000-0002-9349-7946 (V. Sokolov); 0000-0001-7671-8287 (N. Mazur)

supersingular Edwards curves of all classes is given in [14–18].

In most works related to the CSIDH algorithm, various variants of “constant time CSIDH” are proposed to counteract the well-known side channel attack [19, 20]. In [10], we proposed an alternative approach to solving the problem—randomization of the CSIDH algorithm. It also simplifies and speeds up the procedure for selecting random points and is used in this paper (Sections 2, 4).

As is known, one of the candidates for the NIST standardization process of PQC algorithms is SIKE [21]. This fact indicates its preference for the SIDH algorithm. In [2], we proposed a simple version of CSIKE as an original modification of CSIDH. It can be confidently stated that CSIDH and CSIKE provide a much simpler and more efficient implementation of solving the same problem as SIKE. Instead of the extended field F_{p^2} in SIKE, the prime field F_p arithmetic is significantly faster and halves the length of field elements and keys. A remarkable property of algorithms appears—the commutativity of isogenic mappings. The comparative simplicity of CSIDH and CSIKE is confirmed by the possibility to illustrate their work with examples within one paper [2, 7, 9, 10]. An important modification of our algorithm implementation models is the refusal to calculate the isogenic functions $\varphi(R)$ of a random point R, which makes the algorithm sufficiently fast. Note also that the CSIKE algorithm [2] is much simpler and more efficient than the CSIDH-KEM schemes [22, 23], which offer ElGamal-like public key encryption algorithms. In this paper, we analyze and optimize the important parameters of the CSIDH and CSIKE algorithms, propose a CSIKE-ENC scheme for combined message encryption with Alice’s authentication, and discuss some aspects of its security.

Section 1 of the paper gives definitions of 3 classes of curves in the Edwards form and a brief overview of the properties of Supersingular Edwards Curves (SEC) as a CSIDH and CSIKE tool. The advantages of classes of non-cyclic SEC over complete ones are substantiated. Section 2 discusses randomized versions of CSIDH and CSIKE and their features. In the 3rd section, an analysis of possible distributions of the degrees l_k of isogenies is carried out, a large redundancy of it is found in the basic work [1], and an optimal dense distribution *Lopt* is proposed within the constraints, in which instead of $l_{max} = 587$ [1] the maximum degree of isogenies is $l_{max} = 397$. This drastically simplifies and speeds up the algorithms. Probabilistic analysis of random points of maximum odd order *n* is given, and recommendations are given on the rational distribution of degrees l_k isogenies in a dense set $\{l_k\}^K$ of size *K*. Section 4 proposes an original CSIKE-ENC scheme for combined key and messages encryption with Alice’s authentication, security aspects are discussed, in addition to examples 1 and 2 [2], an example of calculations by Alice and Bob of simulated inserts according to the CSIDH algorithm is given.

2. Definitions in Classes of Elliptic Curves in the Edwards Form

The elliptic curve $E_{a,d}$ equation in the *generalized Edwards form* [12] with two parameters *a* and *d* is written as

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

For the first time, such a curve was proposed in [11] with the coefficient *a* at $x^2$and the term “twisted Edwards curves”. For the correct division of curves in the Edwards form into non-intersecting classes, we use our classification [12].

If the quadratic character χ(*ad*) = −1, curve (1) is isomorphic to the *complete Edwards curve* [11] with one parameter *d*

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

The existence condition of SEC of this class is $p \equiv 3\, mod\, 4$. Curve (2) is cyclic.

Another case χ(*ad*) = 1 generates 2 classes of non-cyclic curves: *quadratic and twisted Edwards curves*. In particular, if χ(*a*) = χ(*d*) = 1, curve (1) is isomorphic to the *quadratic Edwards curve* [12]

$$E_d: \quad x^2 + y^2 = 1 + dx^2y^2, \quad \chi(d) = 1, \quad d \neq 1. \tag{3}$$

Here, in contrast to (2), the parameter *d* is a square. For both curves (2) and (3) usually take *a* = 1.

The *twisted Edwards curve* is defined in [12] as a special case of the curve (1) with conditions χ(*a*) = χ(*d*) = −1. The introduction of the second parameter *a* into equation (1) in the pioneering work [11] is necessary only for these conditions.

In [11], curve (3) together with curve (2) are called *Edwards curves*. At the same time, their properties and structure Differ radically [12, 13]. The controversial terminology in [11] sometimes leads to misunderstandings and errors in scientific articles [8], which is discussed in [9]. In the last paper, in particular, the following theorem is proved.

Theorem 2 [9]. For a curve $E_{a,d}$ (1) in the generalized Edwards form

$$x^2 + ay^2 = 1 + dx^2y^2$$

over a prime field F_p, there is a unique quadratic twist curve $E_{\vec{a},\vec{d}}{}^t$ with parameters $\bar{a} = ca,\ \bar{d} = cd,\ c \in F_p{}^*$.

Its proof is given in [9]. From it, in particular, it follows that in the class of complete Edwards curves (2) the quadratic twist curve $E_d^t = E_{d^{-1}}$ lies inside this class, while for the quadratic curve (3) the quadratic twist is a twisted curve $E_{a,d}^t = E_{ca,cd}, \chi(c) = -1$. Each of the 3 classes contains equal sets (p−3)/2 curves ($d \neq 0$, ±1). 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 SEC exist only for $p \equiv 3\,mod\,4$ [14], we can take $c = -1,\ \bar{a} = -a = -1,\ \bar{d} = -d,$ where $a = 1, d$ are the quadratic curve (3) parameters, respectively, $\bar{a}, \bar{d}$ are twisted curve parameters. 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 SEC equation from (1) can be written as

$$E_{-1,-d}\colon\quad x^2 - y^2 = 1 - dx^2y^2, \\ d \in F_p^*,\quad d \neq 1,\ \chi(d) = 1. \tag{4}$$

The order of quadratic (3) and twisted (4) SEC $N_E = p+1 \equiv 0 \text{mod} 8$, then $p \equiv -1 mod 8$ [2]. Note that equation (4), like equation (3), has a fixed parameter $a = -1$, after which all curves (4) are determined by one parameter $(-d)$. Quadratic residues $a = 1\ and\ d$ of the curve (3) become quadratic non-residues $a = -1\ and\ (-d)$ of the curve (4). This simplifies the illustration of how the CSIDH algorithm works.

Quadratic and twisted SEC as a pair of quadratic twists have the same order $p + 1$, but a different structure. Except for the two points (0, ±1), all their points are different, so isogenies of the same degree have different kernels and are calculated independently. Both curves are non-cyclic concerning points of even order (contain 3 points of the 2nd order each, two of which are singular points $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}},\ \infty\right)$ [12]). Quadratic SEC, 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 $N_E = 8n$ (n-odd) of twisted and quadratic Edwards curves [12]. The maximum points order of these curves is $N_E/2$. Points of even orders mustn't be involved in the calculation of Scalar Multiplication (SM) of the CSIDH algorithm (the first multiplication by 4 of a random point P gives a random point R of odd order n or a divisor of n).

The choice of 2 classes of non-cyclic SEC for the CSIDH algorithm in our works [2, 7, 9, 10] is justified by their advantages over complete SEC:

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

Among isogenic curves (with different J-invariants) there are also isomorphic curves with equal J-invariants [11, 24]

$$J(a,d) = \frac{16(a^2 + d^2 + 14ad)^3}{ad(a-d)^4}, \\ ad(a-d) \neq 0. \tag{5}$$

This parameter, in particular, recognizes isomorphic curves with different curve parameters d. As a result of the calculation of isogenies chains, the substitution $d \to J(d)$ is usually made.

3. Randomized CSIDH and CSIKE Algorithms

The CSIKE-ENC protocol proposed in Section 4 includes the CSIDH algorithm as an authentication module, so below we briefly consider its randomized modification [2, 10] and discuss the problem of choosing isogeny degrees.

The PQC CSIDH algorithm was proposed by the authors of [1]. It is based on the CGA (class-group action) function over a prime field F_p. The CGA function defines an isogenic mapping Θ of a supersingular elliptic curve E of order $N_E = p + 1$ 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). This mapping is commutative.

The implementation of the CSIDH algorithm in [1] specifies the least isogeny degrees l_k,k = 1, 2,..., K, K = 74, l_K = 587, as well as an interval of 11 exponent values $[-m \leq e_k \leq m], m = 5$. Negative exponents mean the transition to a quadratic twist curve. Such parameters lead to a key length in CSIDH of 512 bits and a security level of 128 bits for quantum computer attacks.

Instead of supersingular curves in the Montgomery form [1] and complete Edwards curves [3], in [2, 7, 9, 10] we substantiate the advantages and build CSIDH models on noncyclic quadratic and twisted SEC, which form the quadratic twist pairs. They are of the order $N_E = 8n = p + 1,, \ n = \prod_{k=1}^{K} l_k$, while the modulus of a prime field is $p \equiv -1 \, mod \, 8$.

The non-interactive Diffie–Hellman secret sharing scheme includes the steps [1]:

1. **Choice of parameters.** For odd primes l_k, compute $n = \prod_{k=1}^{K} l_k$, select the 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. **Public keys Calculation**. 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 of $E_0 \to E_B$ 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.

For each function Θ there is a multiplicatively inverse $\overline{\Theta}$, such that $\Theta * \overline{\Theta} = I$, where $I = [1, 1, 1, ..., 1]^K$is the neutral element of CGA (K-dimensional vector of units). The mapping $\overline{\Theta}$is constructed by inverting the signs of all exponents e_k of the mapping Θ. It is used in our key encapsulation algorithm.

Below we present a randomized modification of Alice's calculation algorithm according to Section 2 of [10] using isogenies of quadratic and twisted SEC.

Randomized algorithm 1: Evaluating CGA function on quadratic and twisted SEC.

```
Input: $d_A \in E_A, \chi(d) = 1$ and a list of integers $\Omega_A = (e_1, e_2, \ldots e_K)$.
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 $R \leftarrow [(p + 1)/2n_\lambda]P$,
    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 $\varphi: E_A \to E_B$,
    11. Else start over to line 3,
    12. Compute $d_B$of curve $E_B$, $d_A \leftarrow d_B$, $e_k \leftarrow e_k - a$ ,
    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 [2]. 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.

At the beginning of Algorithm 1, two subsets S_λ, λ = 0,1, with degree l_k numbers 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 SEC, and λ = 1–to the choice twisted SEC ($e_k < 0$)). Since the order of the curve is p+1 = 8n, then in step 7 of the algorithm for the curve E_d the point $R = 4n_1 P$ of odd order n_0, is calculated, and for the curve $E_{-1,-d}$ the point $R = 4n_0 P$ of odd order n_1 is calculated. This minimizes the cost of the following scalar multiplication, which determines the point Q of the isogeny kernel of the degree l_k (Step 9). Further, in step 10 of the algorithm, by doubling the points, $s = (l_k - 1)/2$ of x-

coordinates of the kernel <Q> points are calculated.

In step 7 of Algorithm 1, double doubling the random point P immediately allows you to get rid of points of even order (including singular points of the 2nd and 4th order) and then the calculation of scalar multiplications in subgroups of odd order points are performed. Their task is to find $\frac{(l_k-1)}{2}$ of x-coordinates α_i of the kernel <Q> points of prime order l_k. As a result, according to the formula [6]

$$d' = d^l A^8, A = \prod_{i=1}^{s} \alpha_i, \quad s = (l_k - 1)/2 \qquad (6)$$

the parameter d' of the l_k-isogenic quadratic SEC is calculated. Twisted SEC parameters (4) $a' = -1, d' \to -d'$. We emphasize that the concept of CSIDH is the construction of chains of isogenic curves as Abelian groups, and not isogenic functions φ(R) of a random point R. The labor-intensive calculations of the latter [1] are redundant.

In our previous work [2], we proposed the original CSIKE algorithm as a modification of CSIDH. It is an algorithm for encapsulating the key **κ** as a shared secret between Alice and Bob (Commutative Supersingular Isogeny Key Encapsulation). Since it is the base for the combined encryption scheme (Section 4), we give a brief description of it. The algorithm includes 3 stages:

1. **Key κ generation** Alice generates random exponents $e_k \in [-m \ldots m]$ of small integers and finds the secret vector $\Omega_{\boldsymbol{\kappa}} = (e_1, e_2, .., e_K)$,, builds the CGA function $\Theta_{\boldsymbol{\kappa}} = [{l_1}^{e_1}, {l_2}^{e_2}, .., {l_K}^{e_K}]$ and calculates the isogenic curve $E_{\boldsymbol{\kappa}} = \Theta_{\boldsymbol{\kappa}} * E_0$, whose parameter $d_{\boldsymbol{\kappa}}$ is taken as $\boldsymbol{\kappa} \leftarrow d_{\boldsymbol{\kappa}}$.
2. **Key encapsulation**. This is the procedure for Alice to encrypt the key with Bob's public key E_B To do this, Alice calculates the isogenic curve $\Theta_{\boldsymbol{\kappa}} * E_B = E_{\boldsymbol{\kappa}B}$. The $d_{\boldsymbol{\kappa}B}$ parameter of this curve is sent to Bob.
3. **Key decapsulation**. Bob's decryption of the curve $E_{\kappa B}$ with his secret key $(-\Omega_B)$ reduces to his calculation of the isogenic curve $\overline{\Theta_B} * E_{\boldsymbol{\kappa}B} = \overline{\Theta_B} * \Theta_B * E_{\boldsymbol{\kappa}} = E_{\boldsymbol{\kappa}}$, where the inverse function $\overline{\Theta_B}$ is using Bob's additively inverse secret key: $\Omega_B \to (-\Omega_B)$.

So Alice and Bob have a shared secret $\boldsymbol{\kappa}$ instead of a shared secret d_{AB} in CSIDH. Usually, these parameters are replaced by the J-invariant (5), which is the same for isomorphic curves. Alice's private and public keys do not yet participate in this version of CSIKE. The analyst does not have any information about the key **κ** to organize the attack, which inevitably increases the security of the algorithm. The work [2] gives 2 examples of the operation of the four-isogenies CSIKE model with classical and randomized implementation. In Section 4, along with a modification of CSIKE in continuation of Example 2 [2], we will illustrate Alice's and Bob's calculations to authenticate Alice.

4. Analysis and Optimization of CSIDH and CSIKE Parameters

Below, we analyze and optimize the distributions of isogeny degrees $\{l_k\}$ and perform a statistical analysis of a good choice of a random point.

We found that 74 degrees $\{l_k\}$ isogenies in [1] with value $l_{max} = 587$ runs through only a fraction of all primes from 3 to 587, the total number of which is 106. In other words, 32 values of primes are not included in the list of degrees $\{l_k\}$ in the model [1], which means gaps in the set of all primes $\{l_k\}$. Such gaps reduce the product of all l_k, and form a reserve for its increase.

Let us pose the problem of analyzing possible distributions of sets of primes $\{l_k\}^K$ of size K to find options for optimizing this distribution. According to the table of primes up to 587, the complete set = $\{l_k\}^N$ = {3, 5, 7, …, 587}contains N = 106 of all primes.

Any segment of length K of the complete set $\{l_k\}^N$ of primes ordered in ascending order gives the product $\prod_{k=1}^{K} l_k = M(l_1, K)$. Removing one of the extreme elements l_1 or l_K reduces the value of M and $K \leftarrow K - 1$, but retains the segment density property (without gaps). Removing the element l_k from the middle of the segment (1<k<K) also reduces the value of M and $K \leftarrow K - 1$, but violates the density property (with a gap). Let us call an ascending set of primes $\{l_k\}^K$optimal if for known $l_{min} = l_1$ and K this set is dense. The optimal set has the following property: product $\prod_{k=1}^{K} l_k = \mathrm{M}(l_1, K) = max$.

Comment. In the product l_k, we take the removed element $l_d \leftarrow 1$. It is clear that such a replacement reduces the product by a factor l_d with the same K. In this sense, we write down the above maximization property. When removing the extreme elements of the segment, the property is preserved for the shortened segment $\{l_{2,..,} l_K\}^{K-1}$ or $\{l_{1\,,...,} l_{K-1}\}^{K-1}$.

In our problem, the complete set $L = \{l_k\}^{106} = \{3, 5, 7, \dots, 587\}^{106}$is optimal by definition. Removing 32 numbers from it in the middle gives the set $\{l_k\}^{K=74}$, which is far from optimal. The concept of optimality is associated exclusively with maximizing the product of elements of a set.

Let us divide the complete set $L = \{l_k\}^{N=106}$ ={3, 5, 7,…, 587} into subsets $Lh = \{l_k\}^{K_h}, h = 1..6$, including prime numbers in hundreds of natural numbers with numbers h. For the first hundred numbers, for example, we have the optimal subset $L1 = \{3, 5, 7, .., 97\}^{K_1}$, where $K_1 = 24$. For all 6 optimal subsets Lh, these numbers K_h are given in the second row of Table 1.

Table 1

Distribution of quantities K_h of primes and their products B_h within hundreds of natural numbers with numbers h (rounded to whole bits)

	1	2	3	4	5	6
K_h	24	21	16	16	17	12
B_h	119.7	151.2	127.6	135.1	149.7	109.1
	95	45	23	92	82	34

Each number l_k in binary form has log((l_k) bits (log to base 2). For all products of numbers $\{l_k\}$ in subsets, we calculate the bit length

$$B_h = \sum_{l_k \in Lh} log(l_k),$$

the values of which are given in the 3rd row of Table 1. These results allow us to draw interesting conclusions. Firstly, the sum of all bits of the 3rd row $\sum_{h=0}^{6} B_h = 792.772 = 793$ bits), which determines the product of all 106 prime numbers {3,…,587}, has a redundancy of 283 bits compared to the minimum lower threshold of 510 bits (4n>2^{512}, n>2^{510}) [1] security requirements. Secondly, the prime numbers in the 5th and 6th hundred (*L5* and *L6*) can be removed, since $\sum_{h=1}^{4} B_h = 533.855 = 534$ bits = 533.855 = 534 bits, which satisfies the requirement $n >$ 2^{510} with a margin of 24 bits. Ignoring the last 2 columns of Table 1, we obtain 77 values of elements of the optimal set $\{l_k\}^{K=77}$ = {3,..,397} of prime numbers.

Further, we propose to remove the 3 lower degrees {3, 5, 7} in the first hundred numbers and construct an optimal set of isogeny degrees *Lopt* = $\{11, 13, .., 397\}^{74}$ of the same size 74 as in [1]. This saves the length *K* = 74 of secret keys. Given the equality log(3*5*7) = 6.714, the product n of all l_k of the optimal set *Lopt* is estimated to be a binary number of length 528 bits. By adding 2 bits, we get the estimated *log p* = 530 bits. For the *Lopt* distribution, Table 1 can be corrected: in column h = 1 of the table, the values $K_1 = 21, B_1 = 113.081$ should be put, and the last 2 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, $logp = 530бит$. Such an optimal distribution of the isogenies degrees $\{l_k\}$ ensures that the minimal threshold *log p* = 512 bits of the algorithm is exceeded by 18 bits.

Note that the 18 bits reserve can be used up by removing the 2 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 2.

The main advantage of the set of isogeny degrees *Lopt* proposed here over that used in [1] is a significant (1.5 times) reduction of $l_{max} = 587$ to $l_{max} = 397$ with an optimal distribution of primes. The real gain requires an experimental assessment of the complexity of implementing the CSIIDH and CSIKE algorithms with such a radical decrease in the value of l_{max}.

It is possible to estimate other optimal distributions 〚$\{l_k\}^K$ based on Table 1 removing lower degrees of l_k and keeping *K*. It is clear that this only increases the security level of the algorithm and the value of l_{max}. For example, let's take $l_{min} = 101$, then the 24 degrees of the first hundred numbers must be replaced by 17 primes of the 5th hundred and the minimum 7 degrees of the 6th hundred ($l_{max} = 557$). We get the optimal set $\{l_k\}^{74} = \{101, 107, .., 557\}$.. The total sum log($l_k$) of this set is 627.161, which, with 2 bits added, gives the estimated *log p* = 630 bits. Compared to the first distribution discussed above, the length l*og p* of the key has increased by 100 bits. Here you can also exchange these 100 bits for a decrease in l_{max}, but this will significantly reduce the value of *K* (by an estimate of 11).

Let's move on to estimating the probability of a successful choice of a random point *P* at the start of each step of calculating the isogenic curve. In step 7 of Algorithm 1, we replace $n_\lambda \rightarrow n = \prod_{k=1}^{K} l_k$, then multiplication by 4 of a random point *P* gives a point *R* of maximum odd order ord(*R*) = *n* with probability

$$\Pr(R) = \frac{\varphi(n)}{n} = \prod_{k=1}^{K} (l_k - 1)/l_k = \prod_{k=1}^{K} \left(1 - l_k^{-1}\right). \qquad (7)$$

It is clear that adding any new isogeny to the algorithm only reduces this probability. It is also obvious that the smallest values of l_k, the decrease in probability (7) is more significant than for large ones. Already from this, we can conclude that to increase the probability (7) it is advisable to avoid very small values of l_k.

For a comparative estimate of probabilities (7), we consider two extreme options: 1. Filling in the set $\{l_k\}^K$ of size *K* from below; 2. Filling the set $\{l_k\}^K$ from above.

Option 1 is hypothetical since it immediately violates the given constraints. In the *Lopt* distribution, he requires replacing the removal of 3 lower degrees with the removal of higher ones: $\{l_k\}^K = \{3, 5, 7, \dots, 379\}$. However, these 3 high numbers add up to about 26 bits, which exceeds the maximum reserve of 24 bits concerning the minimum lower threshold of 510 bits. The specified security requirements are not met. If we ignore these insignificant 2 bits, we can calculate the overall probability estimate (7) for the optimal set $\{3, 5, 7, \dots, 379\}^{74}$ equal to Pr(*R*) = 0.194. Only for 24 degrees of isogenies of the first hundred numbers, this probability is equal 0.241. The greatest contribution to the reduction of this probability is made by the smallest degrees of 3 and 5: $\frac{2}{3} \cdot \frac{4}{5} = \frac{8}{15}$. The probability estimate of 0.194 for option 1 cannot be considered satisfactory.

Option 2 corresponds to the *Lopt* distribution proposed above exactly 74 primes lie densely in the set $\{11, 13, \dots, 397\}^{74}$. The probability estimate (7) for this set $\{l_k\}^K$ is Pr(R)2 = 0.407. Such an estimate for the *Lopt* set is maximally possible. It is twice as high as in option 1, it can be considered conditionally satisfactory.

On the other hand, it is almost obvious that the probability Pr(R\\$l_t$) that exactly one factor l_t of the number *n* is missing in the order of a random point *R* is equal to l_t^{-1}. Hence it follows that the most probable failures are in the search for subgroups of the curve of very small orders. For example, for the second optimal distribution $\{101, 103, 107, \dots, 557\}^{74}$ considered above, the probability of an unsuccessful selection of a random point with an order that does not contain the factor l_t does not exceed 1%. Here one can expect with great confidence a smooth process of calculating isogenic curves.

We do not know the elements of the set $\{l_k\}^K$ in the model from [1]. Random selection is difficult to justify. It is only known that the set of these degrees is determined by the security level and the fulfillment of the equality $4\prod_{k=1}^{K} l_k = p + 1 \cong 2^{512}$. Although the first distribution of *Lopt* degrees is much better than [1], its further improvement may involve resources that have not yet been used in the size *K* of the set and the values of the exponents e_k isogenies. Any algorithm has rich resources for modification.

An important conclusion of the probabilistic analysis of a successful choice of a random point is the recommendation to avoid using the lowest degrees of isogenies. They contribute the least to the security of the algorithm and the most to the problem of finding isogeny kernels.

5. Combined Encryption based on CSIKE-ENC Scheme

The disadvantage of the CSIKE algorithm proposed in [2] is the lack of sender authentication. At the same time, the information available to Bob—Alice's public key d_A—can be used by him to solve this problem using CSIDH. In addition, the extension and modification of the algorithm make it possible to perform the target function in one package—symmetric encryption of the message *M* of the sender. Such an extended algorithm can be called CSIKE-ENC (ENC-Encryption). It is a combined asymmetric-symmetric algorithm. Classical ECC protocols, it is similar to ECIES (one of the standards is ISO/IEC 1803-2-2009).

Let us introduce the notation:

1. C_o is the result of encrypting the secret key **κ** with Bob's public key (C_o < p);
2. *M*—message.
3. $C_{\boldsymbol{\kappa}} = ENC_{\kappa}$(M)—message *M* cipher with symmetric encryption key ***κ***.
4. $DEC_{\boldsymbol{\kappa}}(C_{\boldsymbol{\kappa}})$ is the result of decrypting the message *M* with the key ***κ***.
5. $Teg_{A,B}$—imitation inserts of Alice and Bob authentication.
6. *H(M)*—hash code of message *M*.

In this paper, we propose the following message transfer protocol *M*.

Pre Calculations

Alice and Bob, based on their public keys d_A, d_B and the non-interactive CSIDH algorithm, compute shared secrets $d_{BA} = Teg_A$ and $d_{AB} = Teg_B$, intended as imitation insets for Alice's authentication by Bob.

1. Encryption

Alice:

1. Generates secret vector $\Omega_\kappa = (e_1, e_2, \ldots, e_K)$, constructs CGA function $\Theta_\kappa = [l_1^{e_1}, l_2^{e_2}, \ldots, l_K^{e_K}]$ and calculates the isogenic curve $E_{\boldsymbol{\kappa}} = \Theta_\kappa * E_0$ whose parameter $d_{\boldsymbol{\kappa}}$ takes as $\boldsymbol{\kappa} \leftarrow d_{\boldsymbol{\kappa}}$.
2. During encapsulation, encrypts the key **κ** with Bob's public key and calculates the encrypted key $d_{\boldsymbol{\kappa} B} = C_0 < p$.
3. Expands the message M in the form $\widetilde{M} = (Teg_A, M)$.
4. Using the standard known to the parties encrypts the message $\widetilde{M}$ with the key **κ** of the symmetric cryptosystem: $C_{\boldsymbol{\kappa}} = ENC_{\boldsymbol{\kappa}}(\widetilde{M})$.
5. Sends to Bob a packet with two ciphers $DP = (C_0, C_{\boldsymbol{\kappa}})$.

2. Decryption

Bob:

1. Using its additive inverse key $(-\Omega_B)$ decrypts the first cipher C_0 ($C_0 < p$) and calculates the key **κ** (key decapsulation).
2. Decrypts the second cipher with the key $\boldsymbol{\kappa}$: $\widetilde{M} = DEC_{\boldsymbol{\kappa}}(C_\kappa) = (Teg_A, M)$.
3. Checks for equality $Teg_A = Teg_\mathrm{B}$. If they do not match, authentication fails and the message is rejected.

In the case of a successful test transmission of ciphers, both parties should make the replacement κ←H(κ) for the key $\boldsymbol{\kappa}$. This can radically increase the security level of a symmetric cryptosystem.

When using block symmetric encryption, any error or modification of the message is detected by chaotic decryption. In this case, the given protocol without a digital signature performs two of its functions—authentication and message integrity check (including transmission errors).

In the previous work [2], 2 examples of the implementation of the CSIKE model with input parameters $p = 9239$, $\{l_k\}^K = \{3,5,7,11\}$, $\Omega_\kappa = (4,-3,-3,2)$, $\Omega_B = (3,-2,2,-3)$, using 2 secret keys Ω_κ, Ω_B, without Alice's key Ω_A. To authenticate Alice in the above-combined encryption protocol, it is proposed to use this 3rd key to calculate the tags of Alice and Bob according to the CSIDH secret-sharing algorithm. They serve as an imitation insert that Bob checks for validity. In continuation of example 2 [2], below we illustrate an example of calculating randomized isogenic chains to determine the parameters d_{BA}, d_{AB}.

Example. Let Alice's secret key be $\Omega_\mathrm{A} = (2,-3,\ 1,-4)$ and the CGA function, respectively, $\Theta_\mathrm{A} = [3^2, 5^{-3}, 7^1, 11^{-4}]$. Then she computes her public key $E_A = \Theta_A * E_0$ with one of 2^{20} possible isogeny chains of length 10 [2]:

$$\frac{d^{(0)} = 2}{(11)} \xrightarrow{-1} \frac{6661}{(11)} \xrightarrow{-1} \frac{5469}{(5)} \xrightarrow{-1}$$

$$\frac{1548}{(7)} \xrightarrow{1} \frac{6482}{(3)} \xrightarrow{1} \frac{384}{(5)} \xrightarrow{-1}$$
$$7935 = d^{(6)}$$

$$\frac{d^{(6)} = 7935}{(5)} \xrightarrow{-1} \frac{7971}{(11)} \xrightarrow{-1}$$
$$\frac{5154}{(11)} \xrightarrow{-1} \frac{211}{(3)} \xrightarrow{1} 5308 = d^{(10)}.$$

So, Alice's public key is $d_\mathrm{A} = 5308$. In the Diffie–Hellman scheme, Alice encrypts with the CGA function $\Theta_\mathrm{A} = [3^3, 5^{-2}, 7^2, 11^{-34}]$ Bob's public key $d_B = 2504$ and obtains $E_{BA} = \Theta_A * E_B$ in 10 steps:

$$\frac{d^{(0)} = 2504}{(5)} \xrightarrow{-1} \frac{7430}{(5)} \xrightarrow{-1} \frac{5373}{(11)} \xrightarrow{-1}$$

$$\frac{50}{(3)} \xrightarrow{1} \frac{8935}{(7)} \xrightarrow{1} \frac{4468}{(5)} \xrightarrow{-1} 8001 = d^{(6)}$$

$$\frac{d^{(6)} = 8001}{(11)} \xrightarrow{-1} \frac{6813}{(11)} \xrightarrow{-1}$$
$$\frac{1908}{(3)} \xrightarrow{1} \frac{7761}{(11)} \xrightarrow{-1} 2384 = d^{(10)}.$$

So $d_{BA} = 2384 = Teg_A$.

Bob's encryption of Alice's public key $d_\mathrm{A} = 5308$ by the CGA function $\Theta_B = [3^3, 5^{-2}, 7^2, 11^{-3}]$ according to $E_{AB} = \Theta_B * E_A$ can be determined by a random chain of parameters $d^{(i)}$ isogenic curves

$$\frac{d^{(0)} = 5308}{(7)} \xrightarrow{1} \frac{7805}{(5)} \xrightarrow{-1}$$
$$\frac{4900}{(11)} \xrightarrow{-1} \frac{3466}{(3)} \xrightarrow{1} \frac{7327}{(5)} \xrightarrow{-1}$$
$$\frac{6250}{(11)} \xrightarrow{-1} 2723 = d^{(6)}$$

$$\frac{d^{(6)} = 2723}{(11)} \xrightarrow{-1} \frac{4550}{(3)} \xrightarrow{1}$$
$$\frac{5881}{(7)} \xrightarrow{1} \frac{6562}{(3)} \xrightarrow{1} 2384 = d^{(10)}.$$

It is clear that, due to the commutativity of CSIDH, $Teg_B = d_{AB} = 2384 = Teg_A$. These results are obtained by Alice and Bob at the pre-computation stage of the CSIKE-ENC scheme. Essentially, this step means inserting the CSIDH into the CSIKE-ENC.

The question may arise: if with the help of CSIDH the task of secrets sharing is solved easier and faster, what is the goal of CSIKE-ENC? The undoubted advantage of the latter is the increase in security. CSIDH includes 3 secret keys Ω_A, Ω_B, d_{BA} while CSIKE-ENC includes 5 secret keys Ω_A, $\Omega_B, d_{BA}, \Omega_\kappa, \boldsymbol{\kappa}$. The main argument of our assertion is that the attack on d_{BA} in CSIDH relies on the known public keys d_A and d_B of Alice and Bob, while in CSIKE-ENC the analyst for attacking the key $\boldsymbol{\kappa}$ has no information at all. Only Alice has the key $\Omega_{\boldsymbol{\kappa}}$ generating $\boldsymbol{\kappa}$. The above arguments complicate the task of cracking the key $\boldsymbol{\kappa}$. Different versions of the replacement κ←H(κ) proposed above to increase the entropy of the key and the security level. The question raised requires detailed analysis and quantitative assessments.

A good modification of CSIDH and CSIKE-ENC is to make the parameter d_0 secret of the original E_0 .This requires swapping Alice's and Bob's public keys but adds another private key and makes the analyst's task almost hopeless. When retransmitting an encrypted message based on CSIKE-ENC, for example, $d_0 \leftarrow \kappa$ can be received.

It should be noted that the security level of CSIDH is estimated by the size of the set of all SECs close to $\sqrt{p}$ [1]. Then for a module p with a length of 512 bits, as in [1], it is equal to 256 bits for a classical computer and 128 bits for a quantum one. We believe that hashing the key $\boldsymbol{\kappa} \in F_p$ will achieve the maximum level of security.

6. Conclusion

The paper presents an original CSIKE-ENC scheme for combined encryption of key $\boldsymbol{\kappa}$ and message $\widetilde{M}$ with sender authentication. The asymmetric algorithms CSIKE and CSIDH solve the problems of key encapsulation **κ** and Alice's authentication using imitation inserts, while the symmetric algorithm $ENC(\widetilde{M})_{\boldsymbol{\kappa}}$ with the key **κ** encrypts the message along with the secret imitation insert. The proposed scheme differs from the known KEM schemes in simplicity and efficiency. The security level in relation to the quantum computer of this scheme is estimated as (*log p*)/4. The increase in security in the key $\boldsymbol{\kappa}$ encapsulation scheme in comparison with Diffie–Hellman secret sharing is substantiated. A further increase in circuit security can be achieved by:

1. Classification of the starting curve E_0.
2. Hashing the key $\boldsymbol{\kappa}$.

Increased efficiency of the implementation of the scheme is achieved:

1. Using fast quadratic and twisted SECs and (*W*: *Z*) coordinates.
2. Rejection of redundant calculations of isogenic functions φ(*R*) of the point *R*.
3. Randomization of CSIKE and CSIDH algorithms.
4. Optimization of scalar multiplication of point *R* in (*W*: Z) coordinates.
5. Optimization of the distribution *Lopt* isogeny degrees and a significant (1.5 times) decrease in the maximum degree to l_{max}=397.
6. By avoiding small values of degrees in the set $\{l_k\}^K$.

In future work, we plan to continue the analysis of CSIKE modifications with the improvement of the model and the prospect of further standardization.

7. References

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

[2] A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10.

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

[4] R. R. Farashahi, S.G. Hosseini, Differential Addition on Twisted Edwards Curves, Inf. Secur. Privacy (2017) 366–378. doi:10.1007/978-3-319-59870-3_21

[5] S. Kim, et al., Efficient Isogeny Computations on Twisted Edwards Curves, Secur. Commun. Networks, (2018). doi:10.1155/2018/5747642

[6] D. Moody, D. Shumow, Analogues of Velus Formulas for Isogenies on Alternate Models of Elliptic Curves, Mathematics of Computation, 85(300) (2016) 1929–1951. doi:10.1090/mcom/3036

[7] A. Bessalov, et al., Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves, in: Workshop on

Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923 (2021) 1–11.

[8] T. Moriya, H. Onuki, T. Takagi, How to construct CSIDH on Edwards curves, Cryptographers' Track at the RSA Conference, CT-RSA 2020, (2020) 512–537. doi:10.1007/978-3-030-40186-3_22

[9] 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

[10] 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

[11] D. J. Bernstein, et al., Twisted Edwards Curves, AFRICACRYPT 2008, (2008) 389–405. doi:10.1007/978-3-540-68164-9_26

[12] A. Bessalov, Elliptic Curves in the Edwards Form and Cryptography, Monograph, 2017.

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

[14] A. Bessalov, L. Kovalchuk, Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Ed-wards Curves with j-Invariants Equal to Zero and 123, Cybernetics and Systems Analysist, 55(3) (2019) 347–353. doi:10.1007/S10559-019-00140-9

[15] 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 Analysist, 55(5) (2019) 731–741. doi:10.1007/s10559-019-00183-y

[16] A. Bessalov, et al., Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

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

[18] 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, no. I, vol. 2631 (2020) 30–39.

[19] H. Onuki, et al., A Faster Constant-time Algorithm of CSIDH keeping Two Points. ASI-ACRYPT, (2020).

[20] A. Jalali, et al., Towards Optimized and Constant-Time CSIDH on Embedded Devices. IACR Cryptology ePrint Archive, (2019) 297.

[21] R. Azarderakhsh, et al., Supersingular Isogeny Key Encapsu-lation—Submission to the NIST's Post-Quantum Cryptography Standardization Process, (2016).

[22] Mingping Qi. An efficient Post-Quantum KEM from CSIDH, J. Math. Cryptology, 16 (2022) 103–113. doi:10.1515/jmc-2022-0007.

[23] K. Yoneyama, Post-Quantum Variants of ISO/IEC Standards: Compact Chosen Ci-Pher Text Secure Key Encapsulation Mechanism from Isogeny, Proceedings of the 5th ACM Workshop on Security Standardization Research Workshop, (2019) 13–21. doi: 10.1145/3338500.3360336

[24] L. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition, CRC Press, (2008). doi: 10.1201/9781420071474