УДК

621.391.15: 519.7

A.V.BESSALOV

HOW TO CONSTRUCT CSIDH ON QUADRATIC AND TWISTED EDWARDS CURVES

In one of the famous works, an incorrect formulation and an incorrect solution of the implementation problem of the CSIDH algorithm on Edwards curves E_d is discovered. A detailed critique of this work with a proof of the fallacy of its concept is given. Specific properties of three non-isomorphic classes of supersingular curves in the generalized Edwards form is considered: complete, quadratic, and twisted Edwards curves. Conditions for the existence of curves of all classes with the order $p+1$ of curves over a prime field F_p are determined. The implementation of the CSIDH algorithm on isogenies of odd prime degrees based on the use of quadratic twist pairs of elliptic curves. To this end, the CSIDH algorithm can be construct both on complete Edwards curves with quadratic twist within this class, and on quadratic and twisted Edwards curves forming pairs of quadratic twist. In contrast to this, the authors of a well-known work are trying to prove theorems with statement about existing a solution within one class E_d of curves with a parameter d that is a square. The critical analysis of theorems, lemmas, and erroneous statements in this work is given. Theorem 2 on quadratic twist in classes of Edwards curves is proved. A modification of the CSIDH algorithm based on isogenies of quadratic and twisted Edwards curves is presented. To illustrate the correct solution of the problem, an example of Alice and Bob calculations in the secret sharing scheme according to the CSIDH algorithm is considered.

Keywords: curve in generalized Edwards form, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, curve order, point order, isomorphism, isogeny, w-coordinates, square.

INTRODUCTION

The reason for writing this article was the work of Japanese scientists [1]. Our attention was drawn to the title of this paper, which includes the keywords CSIDH (Commutative Supersingular Isogeny Diffie-Hellman [2]) and Edwards curves [3, 4]. This topic intersects, in particular, with works [5, 6, 7] and our research [8 - 14].

The most interesting results in this topic, in our opinion, were obtained in [5], which offers the fastest today arithmetic for computing odd-degree isogenies on complete Edwards curves [3] using the Farasakhi-Hosseini -coordinates [6] and the theorems of [7].

Since the term "Edwards curves", first defined in [4] for all curves E_d with one parameter d, is ambiguous (does not take into account the values of the quadratic character $\chi(d)$), the question arises: what kind of Edwards curves are we talking about in [1]? The authors of [1] removed this question with the new term "*purely* Edwards curves", meaning by it *all curves* E_d *with one parameter, except the complete Edwards curves*. For them obviously $\chi(d)=1, d\neq 1$.

The purpose of this article with a similar title [1] is a critical analysis of this work together with an illustration of the correct solution of the problem.

In our classification [11, 12], such curves are called “quadratic Edwards curves” (Section 1). Within this class of Edwards curves there are no quadratic twist pairs on which the CSIDH algorithm is based. Thus, we found a contradiction already in the title of [1], which proves its fallacy. The purpose of this article is a critical analysis of the incorrect statements and conditions of the theorems in [1], a

refutation of its concept, and, as a constructive, a proof and illustration of the correct solution of the problem.

In [8], we proved two theorems adapting formulas of odd degree isogenies for Edwards curves [7] to twisted Edwards curves and to their computing in Farasakhi-Hosseini $(W:Z)$-coordinates [6]. In the next paper [9], using a simple model, it was shown how the CSIDH algorithm works on the basis of supersingular quadratic and twisted Edwards curves connected as quadratic twist pairs, some estimates of the calculation cost in projective $(W:Z)$ Farasakhi-Hosseini coordinates were detailed.

This article is, to a certain extent, a continuation of the previous work [9]. Supersingular quadratic and twisted Edwards curves with the same order $N_E = p+1 = 2^m n,\ m \geq 3,$ (n – odd) exist only for $p \equiv 7 \bmod 8$. The minimum even cofactor of the order of such curves is 8, then for the CSIDH algorithm with an odd $n = \prod_{i=1}^{K} l_i$ the field modulus, we should choose $p = 8n-1.$ In order to adapt the definitions for the arithmetic of Edwards curves isogenies and curves in the Weierstrass form, we use the modified point addition law [11, 12] with the change of coordinates $x \leftrightarrow y$.

Section 1 gives a brief overview of the properties of complete, quadratic, and twisted supersingular Edwards curves (SEC) [13,14]. In Section 2, specific aspects of the implementation of the CSIDH algorithm model on quadratic and twisted SEC are considered, and a modification of the algorithm [2] is given. Since all the necessary calculations in the CSIDH algorithm are reduced only to field operations for calculating the isogenic curve parameter and scalar point multiplications, it is proposed to abandon the calculation of the isogenic function $\phi(R)$ of random point R. In section 3, we give critical analysis of theorems, lemmas and statements of article [1], their incorrectness and fallacy, substantiate the conclusion about the inconsistency of the concept and title of the article. The implementation of the CSIDH algorithm in [1] (section 6.2) relies on complete Edwards curves, which does not correspond to the problem posed in the paper. Instead of hypothetical curves $E_d[\pi-1]$ with one parameter in [1], one should actually use the known twisted SEC with two parameters and other existence conditions. The proof of Theorem 2 on quadratic twist of curves in the generalized Edwards form is given. In support of our conclusions, further in Section 4, an example of Alice and Bob's calculations in the Diffie-Hellman secret sharing scheme on quadratic and twisted SEC is given. Omitting the problem of computational cost, in this paper we mainly use affine coordinates.

1. PROPERTIES OF SUPERSINGULAR CURVES IN EDWARDS FORM

Let us consider some specific properties of supersingular Edwards curves (SEC) [13, 14]. An elliptic *curve in generalized Edwards form* [11] over a prime field F_p is defined by the equation

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

If a quadratic character $\chi(ad) = -1$, curve (1) is isomorphic to the *complete Edwards curve* [3, 4] with one parameter d

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

SECs of this class exist for $p \equiv 3 \bmod 4$, and their order is $N_E = p+1 \equiv 0 \bmod 4$.

Let $\chi(ad) = 1,\ \chi(a) = \chi(d) = 1$, then the curve (1) is isomorphic to the *quadratic Edwards curve* [11]

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

In contrast to (2), the parameter d of curve (3) is a square. SEC of class (3) have an order $N_E = p + 1 \equiv 0 \bmod 8$ and exist over a field F_p for $p \equiv -1 \bmod 8$. For both curves (2) and (3) we accept a parameter $a = 1$, and they are called as curves with one parameter. In [4], curve (3) together with curve (2) are defined as *Edwards curves*. At the same time, the difference in the quadratic characters of the parameters d leads to radically different properties of curves (2) and (3) [11, 12]. We discuss this below and in Section 3.

The *twisted Edwards curve* was defined in [11] as a particular case of curve (1) for $\chi(ad) = 1, \ \chi(a) = \chi(d) = -1.$

The new classification of curves in the generalized Edwards form (1) in [11, 12] divides them into 3 non-intersecting (non-isomorphic) classes of complete, quadratic, and twisted Edwards curves. This avoids the ambiguity and difficulties that arise in the still existing terminology, which allows the inclusion of one class of Edwards curves in another. In the pioneering work [4], in particular, authors define the twisted Edwards curve with two parameters as curve (1). As a result any curve in Edwards form can be called twisted Edwards curve. However, already in [4] itself, statistics are given for the number of complete, twisted Edwards curves and Edwards curves, which cannot be sorted out. Another example of ambiguous terminology is the work [1], the title of which contains the term "Edwards curves", but according to [4], it includes "complete Edwards curves". The question arises: what kind of curves are we talking about?

The logic of classification of curves in the generalized Edwards form (1) in [11, 12] is simple. Since the introduction of a new parameter into the equation (1) in the Edwards form is necessary only in one case: at $\chi(ad) = 1, \ \chi(a) = \chi(d) = -1$, it is logical to keep the term “twisted Edwards curves” [11] for curves with this condition. In this case, the class "twisted Edwards curves" becomes unique up to isomorphism (it has no curves in other classes). Another such unique class is the class of “complete Edwards curves” [3, 4] with the condition $\chi(ad) = -1$. Finally, the third unique class with the condition $\chi(ad) = 1, \ \chi(a) = \chi(d) = 1$ is the class of "*quadratic* Edwards curves". This term, proposed by us [11], is justified by the property $\chi(d) = 1$, which is different from the conditions of the other two classes. To a certain extent, it can also be justified by the term “quadratic twist”, which is exactly what the curves of the corresponding classes (quadratic and twisted curves) are connected. It is important that there are exactly three classes of curves (1), each with its own name, and no confusion.

In the application to the CSIDH algorithm on SECs, we define a pair of quadratic and twisted SEC [11] as a pair of quadratic twist with parameters $\chi(ad) = 1, \vec{a} = ca, \vec{d} = cd, \ \chi(c) = -1.$ (see Theorem 2 in Section 3). Since SEC exist only for $p \equiv 3 \bmod 4$ [13], we can take $c = -1, \ a = 1, \ \bar{a} = -1, \ \bar{d} = -d,$ where $a, d -$ are the parameters of a quadratic curve, and respectively, $\bar{a}, \bar{d} -$ of a twisted curve. In other words, the transition from a quadratic to a twisted curve and vice versa we can define $E_d = E_{1,d} \leftrightarrow E_{-1,-d}$. Then the twisted SEC equation for $p \equiv 7 \bmod 8$ from (1) we can written as

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

Here, the conditions for the modulus p and order of the curve $N_E = p+1 \equiv 0 \bmod 8$ are similar to curves (3). For $p \equiv 7 \bmod 8$, of course, also $p \equiv 3 \bmod 4$ holds.

Having fixed the parameter $a = -1$ and running through all admissible values of d, we can determine the set of cardinalities of all $\frac{p-3}{2}$ curves of each of the 3 classes of curves (1) (including isomorphic curves). Any twisted SEC one can reduce to the form (4).

The order $N_E = p+1-t$ of an elliptic curve over a prime field F_p is determined based on the trace t of the characteristic equation $\pi^2 + t\pi + p = 0$ of the Frobenius endomorphism, where for some point $P = (x.y)$ the Frobenius endomorphism $\pi(P) = (x^p, y^p)$. For a quadratic twist curve, the corresponding order will be $N_E{}^t = p+1+t$. An elliptic curve is supersingular if and only if, over any extension of a prime field F_p, the trace of the Frobenius equation is $t \equiv 0 \bmod p$, in this case $\pi^2 = -p,\ \pi = \pm\sqrt{-p}$ in an imaginary quadratic field [13, 15]. A pair of curves E and E^t is sometimes referred to $E[\pi+1],\ E[\pi-1]$ as two solutions of the quadratic Frobenius equation. In an algebraic closure $\overline{F}_p$, a supersingular curve does not contain points of order p. Over a prime field F_p, such a curve always has order $N_E = p+1$.

So, quadratic and twisted SEC as a pair of quadratic twist have the same order $N_E = p+1$ but different structure. All their points are different (except two points $(0,\pm 1)$), so isogenies of the same degree have different kernels. Both curves are non-cyclic with respect to points of the 2-nd order (contain 3 points of the 2-nd order each, two of which are exceptional points $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ [4, 11]). Quadratic SEC (3), in addition, contains two exceptional points of the 4-th order $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$. The presence of a noncyclic subgroup of the 4-th order containing 3 points of the 2-nd order limits the number 8 to the minimum even cofactor of the order $N_E = 8n\ (n - odd)$ of quadratic and twisted Edwards curves [11]. In general, their order is $N_E = 2^m n,\ m \geq 3$. The maximum order of points of these curves is $N_E / 2 = 4n.$ It is important that points of even orders are not involved in the calculations of the CSIDH algorithm (after the first multiplication of a random point P of maximum order by 4, we have a point of odd order n).

For the curve (1) J -invariant equal [4, 15]

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

This parameter distinguishes 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 [15], it is the same for a pair of twisted and quadratic SEC ($a = \pm 1$). It is a useful tool both in finding supersingular curves and in constructing isogeny chain graphs. One of the properties of the J −invariant is

$$J(d) = J(d^{-1}).$$

For the considered classes of SEC, the replacement $d \to d^{-1}$ gives an isomorphism, and for complete Edwards curves (2) it gives a quadratic twist.

2. MODIFICATION OF CSIDH ALGORITHM ON QUADRATIC AND TWISTED EDWARDS CURVES

The PQC CSIDH (Commutative SIDH) algorithm proposed by the authors of [2] for solving the same key exchange problem (SIDH), but based on isogenic mappings of supersingular elliptic curves as additive Abelian groups. Such a mapping over a prime field F_p as the class group action is defined [2] and is commutative. In comparison with the well-known original CRS scheme (Couveignes (1997), Rostovtsev, Stolbunov (2004)) on non-supersingular curves, the use of isogenies of supersingular curves made it possible to substantial speed up the algorithm and achieve the smallest known key size (512 bits in [2]).

Let the curve E of order $N_E = p+1$ contain points of small odd orders $l_i, i = 1,2,...,K.$ Then there is an isogenic curve E' of the same order as a l_i -degree map: $E \to E' = [l_i]^* E$. The repetition of this operation e_i times we denote $[l_i^{e_i}]^* E$. The values of the isogeny exponents $e_i \in Z$ determine the length $|e_i|$ of the chain of isogenies of degree l_i . In [2], an interval of exponential values $[-m \le e_i \le m]$ is accepted ($m = 5$), which provides a security level of 128 bits for a quantum computer attack. Negative values of the exponent mean a transition to a quadratic twist supersingular curve.

The implementation of the CSIDH algorithm mainly uses fast arithmetic of Montgomery elliptic curves $y^2 = x^3 + Cx^2 + x,\ C \neq \pm 2$ containing 2 points of the 4-th order and, accordingly, having an order $N_E = p+1 = 4n(n-odd).$ [2]. In [5], the CSIDH algorithm implemented on complete SEC of the same order. In this paper, we use quadratic and twisted SEC in the CSIDH algorithm, which have the same speed performance as complete Edwards curves [5]. In [8] we proved 2 theorems for implementation such possibility. With a minimum cofactor of 8, the order of twisted and quadratic SEC is $N_E = 8n$. Thus, for these SEC classes with order $N_E = 8n = p+1,\ n = \prod_{i=1}^{K} l_i.$ the field modulus in the CSIDH algorithm we chosen as $p = 8\prod_{i=1}^{K} l_i - 1 \equiv -1 \bmod 8$.

Non-interactive Diffie-Hellman key exchange includes the following steps [2]:

1. Choice of parameters. For small odd primes l_i , compute $n = \prod_{i=1}^{K} l_i$, where the value K is determined by the security level (in [2] $K = 74, l_{74} = 587$), and choose an appropriate field modulus $p = 2^m \prod_{i=1}^{K} l_i - 1,\ m \ge 3$ and a starting elliptic curve E_0 .

2. Calculation of public keys. Alice uses her private key $\Omega_A = (e_1, e_2, .., e_K)$ to build an isogenic mapping $\Theta_A = [l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ (class group action [2]) and calculates the isogenic curve $E_A = \Theta_A * E_0$ as her public key. Based on the secret key Ω_B and function Θ_B , Bob performs the same calculations and receives his public key $E_B = \Theta_B * E_0$. These curves are defined their parameters d_A, d_B up to isomorphism, which are accepted as public keys known to both parties.

3. Sharing secrets. Here the protocol is similar to item 2 with replacements $E_0 \to E_B$ 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 of Bob give a result $E_{AB} = \Theta_B * E_A = \Theta_B\Theta_A * E_0$ that coincides with the first one due to the commutatively of the group operation. The J-invariant of the curve $E_{AB}(E_{BA})$ is accepted the shared secret.

Below we present a modification of Alice's computational algorithm according to item 2 [2] using isogenies of quadratic and twisted SEC.

Algorithm 1: Evaluating the class-group action on quadratic and twisted SEC.

Input: $d_A \in E_A, \chi(d) = 1$ *and a list of integers* $\Omega_A = (e_1, e_2, ...e_K)$.

Output: d_B *such that* $[l_1^{e_1}, l_2^{e_2}, ...l_K^{e_K}] * E_A = E_B$, *where* $E_{A,B}$: $x^2 + y^2 = 1 + d_{A,B}x^2y^2$.

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** $(1 - x^2)/(1 - dx^2)$ *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* $S = \{i \mid ae_i > 0\}$. **If** $S = \varnothing$ *then start over to line 2 while* $a \leftarrow -a$,
   6. *Let* $k = \prod_{i \in S} l_i$, *and compute* $R \leftarrow [(p+1)/2k]P$, $P = (x, y)$,
   7. **For** e*ach* $i \in S$ **do**
      8. *Compute* $Q \leftarrow [k / l_i]R$
      9. **If** $Q \neq (1,0)$ *Compute the parameter* d_B *an isogeny* $\phi : E_A \to E_B$ *with* $\ker\phi = Q$ ***Set*** $d_A \leftarrow d_B$, $e_i \leftarrow e_i - a$ **,**
      10. *Skip* i *in* S *and* $k \leftarrow k / l_i$ **if** $e_i = 0$,

11. Return d_A.

In comparison with Algorithm 2 in [2], our Algorithm 1, adapted to twisted and quadratic SEC, has some modifications:

1. Checking the square in item 3 use the equation of the quadratic Edwards curve (3).

2. With the order of the twisted Edwards curve $N_E = 8n = p + 1$ with the maximum order $N_E / 2 = 4n$ of the point, to obtain a point of the order n, it is sufficient to double the random point twice. In item 6, this property lied's to reducing one doubling in the scalar product of the point P.

3. Item 9 has been corrected (you cannot reset the index i before zeroing e_i in item 10).

4. In item 9, only the parameter d_B of the isogenic curve is calculated and the function $\phi(R)$ point R is not calculated.

5. Updating the number $k \leftarrow k / l_i$ and reset i in item10 we perform after zeroing e_i.

According to item 10, exactly $|e_i|$ isogenies we calculate for each l_i until the exponent e_i is set to zero. Depending on its sign, isogenies are calculated in the class of quadratic ($e_i > 0$) or twisted SEC ($e_i < 0$).

The ultimate goal of the CSIDH secret sharing algorithm is to find the common curve parameter d_{AB} of curve E_{AB}. For each step in the chain of isogenies $E \to E'$, it is only necessary to calculate the parameter $d' = \psi(d, Q)$ based on the parameters d and the kernel $< Q >$ of the curve E. This calculation involves two SM (Scalar Multiplication) of random points R and $(s-1)$ recurrent doublings of points of kernel $< Q >$. Thus, the construction and calculation of a sufficiently complex function $\phi(R)$ is not necessary for the implementation of the CSIDH algorithm. Part of the calculations in the algorithm related to the calculation of the function $\phi(R)$ can be saved and significantly speed up the algorithm.

The construction of isogenies of odd prime degrees for quadratic Edwards curves based on Theorem 2 [7], and for twisted Edwards curves - Theorem 1 [8]. In the last work, for the first time, mapping $\phi(P)$ formulas for the curve (1) are given, depending on two parameters a and d. We formulate it below.

Theorem 1[1]. Let $G = \{(1,0), \pm Q_1, \pm Q_2, ..., \pm Q_s\}$ – subgroup of odd order $l = 2s+1$ of points $\pm Q_i = (\alpha_i, \pm\beta_i)$, of curve $E_{a,d}$ (1) over field F_p.

Define

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

Then $\phi(x, y)$ is l-isogeny with kernel G from the curve $E_{a,d}$ to the curve $E_{a',d''}$ with parameters

$$a' = a^l,\ d' = d^l A^8,\ \ A = \prod_{i=1}^{s} \alpha_i, \tag{6}$$

and the mapping function

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

or

$$\phi(x, y) = \left(\frac{x}{A^2} \prod_{ii=1}^{s} \frac{x^2 - a\beta_i^{\,2}}{1 - d\beta_i^{\,2} x^2}, \frac{-y}{A^2} \prod_{i=1}^{s} \frac{x^2 - \alpha_i^{\,2}}{a - d\alpha_i^{\,2} x^2} \right). \tag{8}$$

The proof of theorem in [8] is given.

Here, functions (7) and (8) include parameters a, d, which makes it possible to construct isogenies of twisted Edwards curves.

3. CRITICAL ANALYSIS OF INCORRECT IMPLEMENTATION CONDITIONS OF CSIDH ALGORITHM ON EDWARDS CURVES IN WORK [1]

Let us turn to the results of [1]. The main concept of this article is the construction of the CSIDH algorithm using one class - Edwards curves E_d (3) (the authors call it "*purely* Edwards curve", according to our classification [11] - "quadratic Edwards curve") over a prime field F_p. Since the

CSIDH algorithm is based on isogenies of supersingular curves using the quadratic twist of these curves, the question arises: is the problem posed in [1] solvable?

All theorems of this work use one Farashakhi-Hoseini coordinate $w(P) = dx_1^2 y_1^2$ for each point $P = (x_1, y_1)$. It is clear that the quadratic character $\chi(w(P)) = \chi(d)$. The neutral element $O = (1,0)$ of curve (3) in theorems [1] designated as 0_d, although for all curves (1) it does not depend on the parameter d.

The key theorem in [1] is Theorem 4. Let us formulate it according to the original.

Theorem 4[1]. *Let $p \equiv 3 \bmod 8$. Let P be a point on an Edwards curve E_d such that the P w-coordinate $w(P) \in F_p$, the order of P is not a power of 2, and $w(P)$ is square. If $w(2P)$ is square, there exists P' such that $P' \in E_d[\pi_p + 1]$, $w(2P) = w(P')$, and $\frac{p+1}{4} P' = 0_d$. If $w(2P)$ is not square, there exists P' such that $P' \in E_d[\pi_p - 1]$, $1/w(2P) = w(P')$ and $\frac{p+1}{4} P' = 0_d$.*

Formulation of the theorem. The first error in the formulation of the theorem: for $p \equiv 3 \bmod 8$ there are no curves E_d (3) that satisfied all conditions of the theorem. Indeed, in this case the order of the curve $N_E = p + 1 \equiv 4 \bmod 8$ is not divisible by 8. They exist only for $p \equiv 7 \bmod 8$ [13, 14]. The order of such curves with the minimum even cofactor 8 is $N_E = 8n = p + 1$, where $p \equiv -1 \bmod 8$. For example, $p = 11 \equiv 3 \bmod 8$ it sets a condition for the SEC of order $N_E = 12$, which does not contain the factor 8. It is clear that it is impossible to prove such a theorem.

On the proof of theorems [1]. In total, in Section 4 of [1], 10 lemmas and 7 theorems are proved. The condition $p \equiv 3 \bmod 8$ is specified in Lemmas 1,2,4, 5, 9, 10 and Theorems 3, 4, 5 and 7 with references to the lemmas and to the points of the curve (3), which does not exist under this condition, as well as its quadratic twist - twisted SEC (4). The proof of theorems and lemmas with incorrect conditions in the formulation does not make sense.

Further, the conditions of Theorem 4 define only one curve E_d (3) with the parameter d being a square ($\chi(d) = 1, d \neq 1$). For a random point $P = (x_1, y_1)$ and a point $2P$ on this curve, their respective w-coordinates are

$$w(P) = dx_1^2 y_1^2, \quad w(2P) = d\left(\frac{x_1^2 - y_1^2}{1 - dx_1^2 y_1^2}\right)^2 \left(\frac{2x_1 y_1}{1 + dx_1^2 y_1^2}\right)^2.$$

It follows that for $x_1 y_1 \neq 0, \infty$, the quadratic character $\chi(w(P)) = \chi(w(2P)) = \chi(d)$ is determined exclusively by the parameter d and, by the definition of curve E_d (3), is a square. This property is the same for both points P and $2P$, which contradicts the second assumption of the theorem. While the first assumption of the theorem is always true, the second assumption is always false for a given curve E_d (3), since it replaces $\chi(d) = 1$ with $\chi(d) = -1$. This means a transition to another class of SEC: complete Edwards curve (2) or twisted Edwards curve (4).

The transition to the class of complete SEC (2) with $\chi(d) = -1$ we exclude, since:

- The class (2) does not meet the first condition of Theorem 4 ($\chi(d) = 1$);
- All pairs of quadratic twist connected by parameters $d^{\pm 1}$ lie inside this class;
- Sets parameters d of SEC (2) and (3) are different (in the sense of $d_i^{(2)} \neq -d_k^{(3)}$);
- The class (2) does not contain points at infinity on which the proof of the theorem based.

Exceptional points (points at infinity) exist only in the classes of quadratic SEC (which are excluded by the second assumption of Theorem 4) and twisted SEC [4, 11]. Thus, instead of the curve $E_d[\pi_p - 1]$ in the statement of Theorem 4, there should be a twisted curve $E_{a,d}[\pi_p - 1]$ with conditions $\chi(a) = \chi(d) = -1$. It is important that this is no longer a curve E_d, but its quadratic twist $\chi(d) = 1$. Below we present our Theorem 2 with the proof of this assertion.

On SEC E_d (3) with order $N_E = 8n = p + 1$, $n = \prod_{i=1}^{K} l_i$ there is a unique subgroup $< Q >= G$ of points of prime order l_i as the kernel of a unique isogeny $[l_i]$. Over a prime field F_p, there is a unique SEC of the same order, defined as a quadratic twist $E_d^{\,t}$ of the curve (3), which has its own subgroup $< Q >^t$ of points of the order l_i as isogeny kernels $[l_i]^{-1}$. All points (except points $O = (1,0)$, $D_0 = (-1,0)$) the pair of curves E_d and $E_d^{\,t}$ are distinct, as are the corresponding kernels $< Q >$ and $< Q >^t$ l-isogenies. According to Theorem 2 $E_d^{\,t} = E_{a,ad}$, $\chi(a) = -1$. This is a twisted SEC, but not the Edwards curve, stated in the problem statement and in the title of the article [1]**.**

Exceptional points at infinity of the 2-nd and 4-th orders of the curve (1) we can written [11, 12]

$$D_{1,2} = \left(\pm \sqrt{\frac{a}{d}}, \infty \right), \quad \pm F_1 = \left(\infty, \frac{\pm 1}{\sqrt{d}} \right), \tag{9}$$

where the symbol "∞" we put when dividing by 0. Over a prime field F_p, all 4 points contain quadratic curves E_d (3), and the first 2 points of the 2-nd order are twisted curves (1) under the conditions $\chi(a) = \chi(d) = -1$. The latter generate a non-cyclic subgroup of points of the 2-nd order $G_4 = \{O = (1,0), D_0 = (-1,0), D_1, D_2\}$. According [11] the sums of a random point $P = (x_1, y_1) \notin G_4$ with exceptional points of the 2-nd order give the points

$$(x_1, y_1) + \left(\pm \sqrt{\frac{a}{d}}, \infty \right) = \left(\pm \sqrt{\frac{a}{d}} \cdot x_1^{-1}, \pm \frac{\pm 1}{\sqrt{ad}} \cdot y_1^{-1} \right)$$

From here

$$w(P + D_{1,2}) = \frac{1}{dx_1^2 y_1^2} = \frac{1}{w(P)} \quad . \tag{10}$$

For a similar sum with ordinary point of the 2-nd order $D_0 = (-1,0)$ we have

$$(x_1, y_1) + (-1,0) = (-x_1, -y_1) \quad \Rightarrow \quad w(P + D_0) = w(P) \qquad (11)$$

The sum of a random point $P = (x_1, y_1) \notin G_4$ with a 2-nd order point gives an even-order point, which on the curve order $N_E = 8n$ is at least 8 times greater than the number of odd-order points. Of these, for (2/3) points, the coordinate $w(P)$ is inverted according to (10), for the rest, according to (11), no. This is true for two classes - quadratic and twisted Edwards curves. However, this is not a reason to replace one curve with another [1], not forgetting that the quadratic characters $\chi(d)$ of their parameters are inverse. It also follows from this that the second assertion of Theorem 4 is valid only for twisted Edwards curves, but not for curves E_d (3) with one parameter. It is no less important that the condition $\chi(d) = -1$of this assertion is necessary but not sufficient. A condition $\chi(a) = -1$ and the connection between the parameters of the curves $E_{a,d}$ and $E^t{}_{a,d}$ should be determined (see our Theorem 2).

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

Proof. From equation (1) we have

$$y^2 = \frac{1 - x^2}{a - dx^2}. \qquad (12)$$

Let $\chi(d) = -1, \chi(a) = 1, a = d^2 = c^{-1}$. Quadratic twist (12) be given by transforming a square into a quadratic non-residue

$$dy^2 = \frac{1 - x^2}{d^2 - dx^2} \cdot d = \frac{1 - x^2}{1 - d^{-1}x^2} \cdot d^{-1} \quad \Rightarrow \quad \chi\left(\frac{1 - x^2}{1 - d^{-1}x^2}\right) = 1.$$

Then for the curve of quadratic twist we can write the equation

$$E_{\bar{a},\bar{d}}{}^t = E_{d^{-1}}: \quad x^2 + y^2 = 1 + d^{-1}x^2y^2, \quad \chi(d) = -1.$$

The above conditions are valid for the class of complete Edwards curves with one parameter for $a = d^2 = c^{-1}$, $\bar{a} = 1, \bar{d} = d^{-1}$. This result [3] is known.

Let now $\chi(a) = \chi(d) = 1$, $\chi(c) = -1$. In this case, quadratic twist (12) we can written as

$$c^{-1}y^2 = \frac{1 - x^2}{a - dx^2} \Rightarrow \quad y^2 = \frac{1 - x^2}{ca - cdx^2} = \frac{1 - x^2}{\bar{a} - \bar{d}x^2}.$$

This implies that the quadratic twist of a curve $E_{a,d}$ with parameters satisfying the condition $\chi(a) = \chi(d) = 1$ (a quadratic curve isomorphic to (3)) gives a curve of the class of twisted Edwards curves (1) after substituting $\bar{a} = ca, \bar{d} = cd. \chi(c) = -1.$ In other words, the quadratic twist of a curve E_d is a twisted Edwards curve $E_d^t = E_{c,cd}, \chi(d) = 1, \chi(c) = -1.$. The inverse mapping is given by multiplying both parameters by $c^{-1}: E_{c,cd}, {}^t = E_d \quad \chi(d) = 1, \chi(c) = -1.$ The theorem is proved.

Corollary 1. For quadratic Edwards curves E_d ($\chi(d)=1$) there are no quadratic twist curves within this class.

Corollary 2. For complete Edwards curves E_d ($\chi(d)=-1$) there exist quadratic twist curves $E_{d^{-1}}$ inside this class.

Corollary 1 is obvious from the uniqueness of the mapping of quadratic twist as a bijection. It eliminates the curves $E_d\ [\pi-1]$ in [1].

Note that this result is well known from [4] (hence the term twisted Edwards curves), but with a different proof from our proof of Theorem 2.

So, in the class of complete Edwards curves E_d (2), the quadratic twist pairs $E_d \leftrightarrow E^t{}_{d^{-1}}$ lies inside this class and has multiplicatively inverse parameters $d^{\pm 1}$. On the contrary, for the class of quadratic Edwards curves (3), for $p \equiv 3 \bmod 4$ and $c=-1$, quadratic twist $E_d{}^t \to E_{-1,-d}$ gives a curve from the class of twisted Edwards curves with additively opposite parameters a and d .

We consider it proved that for the class of SEC $E_d[\pi_p+1]$ defined in Theorem 4 [1], there are no curves of the same class $E_d[\pi_p-1]$ as quadratic twist pairs, the formulation of Theorem 4 is incorrect, and the concept of [1] is untenable. Strictly speaking, a unique transition of curve E_d (3) with the condition $\chi(d)=1$ to its quadratic twist is possible only in the class of twisted SEC with parameters $\bar{a}=ca,\ \bar{d}=cd,\ \chi(c)=-1$. Any SEC of this class is isomorphic to curve (4).

Interestingly, the implementation of the CSIDH algorithm in [1] (Section 6.2) uses the parameters of [2] for cyclic curves in the Montgomery form with one point of the 2-nd order and the field modulus $p=4\cdot l_{1i}\cdot l_2\cdot ...\cdot l_{74}-1, l_{74}=587,\ p\equiv 3 \bmod 4$, therefore the algorithm also works on complete Edwards curves E_d (2) , isomorphic to cyclic curves in the Montgomery form. This does not correspond to the task, and does not confirmed by theoretical results. In addition, such an implementation of the CSIDH, is known [5].

4. MODEL OF IMPLEMENTATION OF THE CSIDH ALGORITHM ON QUADRATIC AND TWISTED SEC

To illustrate the above conclusions, consider a simple model of the CSIDH algorithm on quadratic and twisted SEC that form quadratic twist pairs with the same order [9]. Let such a pair of curves contain kernels of the 3-rd and 5-th order at the smallest value $n=15$, then the minimum prime $p=239$ and the order of these curves $N_E=16n=240$. The parameter d of the entire family of 118 quadratic Edwards curves can be taken as squares $d=r^2 \bmod p, r=2..119.$. Of these, 30 pairs of quadratic and twisted SKE were found with parameters $a=\pm 1$ and $\chi(ad)=1.$ The quadratic SEC (3) is denoted by E_d, and the twisted SKE (4) is denoted as $E_{-1,-d}$. Table 1 shows the parameter d values for pairs of quadratic and twisted SEC. We written they as squares $d=r^2 \bmod p,, r=5..119.$

Table 1. Parameter d values of quadratic and twisted SEC $(a = \pm 1)$ for $p = 239$ and $N_E = 240$

25	64	121	196	50	183	5	10	87	176
24	153	11	110	48	187	120	193	27	160
213	44	2	201	61	3	206	192	80	62

In the CSIDH algorithm, an isogenic mapping $\Theta_A = [l_1^{e_1}, l_2^{e_2}, .., l_K^{e_K}]$ (class group action) from some base curve E_0 defines an isogenic curve $E_A = \Theta_A * E_0$. The sign of the degree e_i isogeny exponent specifies, in our case, a quadratic (e_i >0) or twisted (e_i < 0) SEC. At one step of the degree $[l_i^{e_i}]$, $e_i = \pm 1$ isogeny chain, the coordinates $\alpha_k, k = 1..s = (l-1)/2$ of the points of the curve (3) kernel or the curve (4) kernel of order l_i are calculated, then using formula (6) l_i - isogenic curve E' parameter d'. Two chains of isogenies with opposite signs of the exponents $\pm e_i$ give a neutral element of the mapping $[l_i^{e_i} \cdot l_i^{-e_i}] = [l_i^0]$, and then we get the original curve $E_0 = [l_i^0] * E_0$. For example, for a pair of quadratic twist (3), (4) at $e_i = \pm 1$, one can calculate a 3-isogeny curve $E_{25}^{(0)} \to E_{110}^{(1)}$, then a transition to quadratic twist (4) $E_{110}^{(1)} \to E_{-1,-110}^{(1)}$, then a 3-isogeny of curve (4) $E_{-1,-110}^{(1)} \to E_{-1,-25}^{(2)}$, and return to curve (3) $E_{-1,-25}^{(2)} \to E_{25}^{(0)}$. This implies an important property: the sequences of parameters $d^{(i)}$ of isogenic quadratic and twisted SEC on a period have a reverse character. In other words, if such a sequence is calculated for quadratic SEC, then for twisted SEC it is not required to recalculate it, but it is enough to reverse it on a period (in the opposite order).

Tables 2 and 3 show the results of calculation the parameters $d^{(i)}$ of chains of 3- and 5-isogenic quadratic SEC for module $p = 239$. For twisted SEC, the sequences $d^{(i)}$ should be read backwards on the period T. The period of 3-isogeny is $T = 5$, and 5-isogeny $T = 15$. To completeness in table 2 there are still 4 rows missing, and in table 3 - 2 rows with the parameters of table 1, however, the given data is sufficient for an example.

Table 2. Parameter $d^{(i)}$ values of two chains of 3-isogenic quadratic SEC ($a = 1$) for $p = 239$ (period $T = 5$)

i	**0**	**1**	**2**	**3**	**4**	**5**
$d^{(i)}$	25	110	50	10	3	25
$d^{(i)}$	193	62	61	2	5	193

Table 3. Parameter $d^{(i)}$ values of the chain of 5-isogenic quadratic SEC ($a=1$) for $p=239$, (period $T=15$)

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
$d^{(i)}$	25	201	62	10	121	5	110	183
i	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
$d^{(i)}$	61	3	187	193	50	11	2	25

Let us take the secret keys of the exponents $\{e_i\}$ isogenies of Alice and Bob's $\Omega_A=(3,-4)$, $\Omega_B=(-4,5)$, their functions of isogenic mappings, respectively $\Theta_A=[3^3,5^{-4}],\Theta_B=[3^{-4},5^5]$, Let's calculate their public keys d_A,d_B . As the starting curve of the chain of isogenies, we will take the curve $E^{(0)}=E_{25}$. Alice calculates the parameters of 7 isogenic curves $E^{(i)}$: three 3-isogenuc quadratic SEC and 4 5-isogenic twisted SEC in an arbitrary order. According to tables 2 and 3, her calculations generate a chain of length 7 isogeny curves

$$E^{(0)}=E_{25}\to E_{110}\to E_{50}\to E_{10}\Rightarrow E_{-1,-10}\to E_{-1,-62}\to E_{-1,-201}\to E_{-1,-25}\to E_{-1,-2}\Rightarrow E_2.$$

So, Alice's public key $d_A=2.$. Similar calculations of Bob with a secret key $\Omega_B=(-4,5)$ form a chain of length 9 isogeny curves

$$E_{25}\to E_3\to E_{10}\to E_{50}\to E_{110}\Rightarrow E_{-1,-110}\to E_{-1,-183}\to E_{-1,-61}\to E_{-1,-3}\to E_{-1,-187}\to E_{-1,-193}\Rightarrow E_{193},$$

which gives the value of its public key $d_B=193.$

Further, in the secret-sharing scheme, Alice, knowing Bob's public key, calculates the isogenic curve $E_{BA}=[3^3,5^{-4}]*E_{193}=E_{187}.$ Bob gets the same result using the function $E_{AB}=[3^{-4},5^5]*E_2=E_{187}.$ The shared secret is the parameter $d_{AB}=187.$ If we know the sum key of Alice and Bob $\Omega_A+\Omega_B=(-1,1),$ using tables 2, 3, it is easy to check this result: $d^{(0)}=25\to d^{(1)}=3\to d^{(2)}=187.$ Keys of opposite sign make the work of Alice and Bob fruitless.

In principle, the CSIDH algorithm can be perform with exponents $\{e_i\}$ of the same sign and doubling their values to preserve security, but such a prospect, which halves the number of curves in the algorithm, is hardly interesting.

The results of the implementation of the Edwards-CSIDH model [5] in projective coordinates $(W:Z)$ state that it is faster than the Montgomery-CSIDH model in coordinates $(X:Z)$ by 20%. Note that this model is construct on complete Edwards curves with order $N_E=4n(n-odd)$. On the basis of Theorems 1 and 2 in [8], in [9], and in this paper, we have shown how to implement such a model on quadratic and twisted SEC that form pairs of quadratic twist. The advantage of these 2 classes of curves over the complete Edwards curves is the doubling of the number of curves used in the CSIDH algorithm with a corresponding increase in security. In addition, the time-consuming inversion $d\to d^{-1}$ of the parameter is not required when going to the complete quadratic twist curve.

It can be concluded that the work [4], Theorem 2 and the illustration of the CSIDH model in this work will convince the authors of [1] of the erroneousness of their concept, that it is possible to implement the CSIDH algorithm using a single class "*purely* Edwards curves". In further research, we will consider the problems of constant-time CSIDH [16, etc.] and sampling of points.

References

1. Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. How to construct CSIDH on Edwards curves. In *Cryptographers' Track at the RSA Conference–CT-RSA 2020*, pages 512–537. Springer, 2020.
2. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology { ASIACRYPT 2018. pp. 395{427. Springer International Publishing, Cham (2018).
3. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29–50.
4. Bernstein Daniel J. , Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane. Twisted Edwards Curves.// IST Programme under Contract IST–2002–507932 ECRYPT, and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-1
5. Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves. In *Advances in Cryptology–ASIACRYPT 2019*, pages 273–292. Springer, 2019.
6. Farashahi, R.R., Hosseini, S.G.: Differential addition on twisted Edwards curves. In: Pieprzyk, J., Suriadi, S. (eds.) Information Security and Privacy. pp. 366{378. Springer International Publishing, Cham (2017).
7. Moody D., Shumow D. Analogues of Velus formulas for isogenies on alternate models of elliptic curves. Mathematics of Computation, vol. 85, no. 300, pp. 1929–1951,(2016).
8. Bessalov, A., Sokolov, V., Skladannyi, P., Zhyltsov, O. Computing of odd degree isogenies on supersingular twisted Edwards curves. CEUR Workshop Proceedings, 2021, 2923, pp. 1–11.(2021)
9. Бессалов А.В., Цыганкова О.В. Абрамов С.В. Оценка вычислительной сложности алгоритма CSIDH на суперсингулярных скрученных и квадратичных кривых Эдвардса. Радиотехника, 2021. – вып..207, С.40-51.
10. A. Bessalov, V. Sokolov, P. Skladannyi. Modeling of 3- and 5-Isogenies of Supersingular Edwards Curves // Proceedings of the 2nd International Workshop on Modern Machine Learning Technologies and Data Science (MoMLeT&DS'2020), June 2–3, 2020: abstracts. — No. I, vol. 2631. — Aachen: CEUR, 2020. — P. 30–39.
11. Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Монография. «Политехника», Киев, 2017. - 272с.
12. Bessalov A.V., Tsygankova O.V. Number of curves in the generalized Edwards form with minimal even cofactor of the curve order. Problems of Information Transmission, Volume 53, Issue 1 (2017), Page 92-101. doi:10.1134/S0032946017010082

13.. Bessalov, A.V., Kovalchuk, L.V. Supersingular Twisted Edwards Curves Over Prime Fields. I. Supersingular Twisted Edwards Curves with j-Invariants Equal to Zero and 12^3. Cybernetics and Systems Analysis, 2019, 55(3), Page 347–353.

14. Bessalov, A.V., Kovalchuk, L.V.Supersingular Twisted Edwards Curves over Prime Fields.* II. Supersingular Twisted Edwards Curves with the j-Invariant Equal to 66^3. Cybernetics and Systems Analysis, 2019, 55(5), Page 731–741.

15. Washington L,C.. Elliptic Curves. Number Theory and Cryptography. Second Edition. CRC Press, 2008.

16. A. Jalali, R. Azarderakhsh, M. M. Kermani, D. Jao.: Towards optimized and constant-time CSIDH on embedded devices. IACR Cryptology ePrint Archive 2019/297; https://eprint.iacr.org/2019/297. (to appear at COSADE 2019).

621.391.15 : 519.7

How to construct CSIDH on quadratic and twisted Edwards curves.

A.V. Bessalov,

In one of the famous works, an incorrect formulation and an incorrect solution of the implementation problem of the CSIDH algorithm on Edwards curves E_d was discovered. A detailed critique of this work with a proof of the inconsistency of its concept is given. Specific properties of three non-isomorphic classes of supersingular curves in the generalized Edwards form are considered: full, quadratic, and twisted Edwards curves. Conditions for the existence of curves of all 3 classes with the order $p+1$ of curves over a prime field F_p are determined. The implementation of the CSIDH algorithm on isogenies of odd prime degrees is based on the use of quadratic twist pairs of elliptic curves. To this end, the CSIDH algorithm can be built both on complete Edwards curves with quadratic twist within this class, and on quadratic and twisted Edwards curves forming pairs of quadratic twist. In contrast to this, the authors of a well-known work are trying to prove theorems that state that there is a solution within one class E_d of curves with a parameter d that is a square. The critical analysis of theorems, lemmas, erroneous statements in this work is carried out. Theorem 2 on quadratic twist in classes of Edwards curves is proved. A modification of the CSIDH algorithm based on isogenies of quadratic and twisted Edwards curves is presented. To illustrate the correct solution of the problem, an example of Alice and Bob calculations in the secret sharing scheme according to the CSIDH algorithm is considered for.

Keywords: curve in generalized Edwards form, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, curve order, point order, isomorphism, isogeny, w-coordinates, square, non square

621.391.15 : 519.7

Как построить CSIDH на квадратичных и скрученных кривых Эдвардса. А.В. Бессалов,

В одной из известных работ обнаружена некорректная постановка и неверное решение задачи имплементации алгоритма CSIDH на кривых Эдвардса E_d. Дана развернутая критика этой работы с доказательством несостоятельности ее концепции. Рассмотрены специфические свойства трех неизоморфных классов суперсингулярных кривых в обобщенной форме Эдвардса: полных, квадратичных и скрученных кривых Эдвардса. Определены условия существования кривых всех 3-х классов с порядком кривых $p+1$ над простым полем F_p. Имплементация алгоритма CSIDH на изогениях нечетных простых степеней базируется на использовании пар квадратичного кручения эллиптических кривых. С этой целью алгоритм CSIDH можно строить как на полных кривых Эдвардса с квадратичным кручением внутри этого класса, так и на квадратичных и скрученных кривых Эдвардса, образующих пары квадратичного кручения. В противовес этому авторы известной работы пытаются доказать теоремы, утверждающие о наличии решения внутри одного класса кривых E_d с параметром d, который является квадратом. Проведен критический анализ теорем, лемм, ошибочных утверждений в этой работе. Доказана теорема 2 о квадратичном кручении в классах кривых Эдвардса. Приведена модификация алгоритма CSIDH, построенного на изогениях квадратичных и скрученных кривых Эдвардса, Для иллюстрации корректного решения задачи рассмотрен пример вычислений Алисы и Боба в схеме разделения секретов согласно алгоритма CSIDH при $p = 239$.

Ключевые слова: кривая в обобщенной форме Эдвардса, полная кривая Эдвардса скрученная кривая Эдвардса, квадратичная кривая Эдвардса, порядок кривой, порядок точки, изоморфизм, изогения, w-координаты, квадратичный вычет, квадратичный невычет

621.391.15 : 519.7

Як побудувати CSIDH на квадратичних і скручених кривих Едвардса. А.В. Бессалов,

В одної з відомих робіт виявлені некоректна постановка і невірне рішення задачі імплементації алгоритму CSIDH на кривих Едвардса E_d. Дана розгорнена критика цієї роботи с доведенням неспроможності її концепції. Розглянуті специфічні властивості трьох неізоморфних класів суперсингулярних кривих в узагальненої формі Едвардса: повних, квадратичних та скручених кривих Едвардса. Визначені умови існування кривих усіх 3-х класів з порядком кривих $p+1$ над простим полем F_p. Імплементація алгоритму CSIDH на ізогеніях непарних простих степенів базується на застосуванні пар квадратичного кручення еліптичних кривих. З цією метою алгоритм CSIDH можна будувати як на повних кривих Едвардса з квадратичним крученням всередині цього класу, або на квадратичних і скручених кривих Едвардса, які створюють пари квадратичного кручення. В противагу до цього автори відомої роботи намагаються довести теореми, які стверджують о наявності рішення всередині одного класу кривих E_d з параметром d, який є квадратом. Проведено критичний аналіз теорем, лем, помилкових стверджень в цієї роботі. Доведено теорема 2 про квадратичне кручення в класах кривих Едвардса. Приведено модифікація алгоритму CSIDH, побудованого на ізогеніях квадратичних і скручених кривих Едвардса, Для ілюстрації коректного рішення задачі розглянуто приклад обчислень Аліси і Боба в схемі розподілу секретів згідно алгоритму CSIDH при $p = 239$.

Ключові слова: крива в узагальненій формі Едвардса, повна крива Едвардса скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, порядок точки, ізоморфізм, ізогенія, w--координати, квадратичний лишок, квадратичний не лишок

Сведения об авторе:

1. Бессалов Анатолий Владимирович, доктор технических наук, профессор, профессор Киевского университета имени Бориса Гринченко, Украина. ORCID ID 0000-0002-6967-5001.