www.czasopisma.pan.pl PAN www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 3, PP. 463–468
Manuscript received March 24, 2022; revised August, 2022. DOI: 10.24425/ijet.2022.139890

How to Compute an Isogeny on the Extended Jacobi Quartic Curves?

Łukasz Dzierzkowski, and Michał Wroński

***Abstract*—Computing isogenies between elliptic curves is a significant part of post-quantum cryptography with many practical applications (for example, in SIDH, SIKE, B-SIDH, or CSIDH algorithms). Comparing to other post-quantum algorithms, the main advantages of these protocols are smaller keys, the similar idea as in the ECDH, and a large basis of expertise about elliptic curves. The main disadvantage of the isogeny-based cryptosystems is their computational efficiency - they are slower than other post-quantum algorithms (e.g., lattice-based). That is why so much effort has been put into improving the hitherto known methods of computing isogenies between elliptic curves. In this paper, we present new formulas for computing isogenies between elliptic curves in the extended Jacobi quartic form with two methods: by transforming such curves into the short Weierstrass model, computing an isogeny in this form and then transforming back into an initial model or by computing an isogeny directly between two extended Jacobi quartics.**

***Keywords*—cryptology; post-quantum; elliptic curves; Jacobi quartics; isogenies**

I. Introduction

In the last few years, a threat from quantum computers has been rising, and the classical ECC may be at risk in some time. That is why cryptosystems, which are believed to be quantum-resistant, such as algorithms based on:

- lattices theory,
- **computing isogenies between elliptic curves**,
- codes theory,
- multivariate polynomials,
- hash functions

are becoming more important and more popular. In this paper, we will focus on the elliptic curve cryptography (ECC), which is prominent in public-key cryptography. It is used in number theory algorithms as well, e.g., for integer factorization or primality testing. Classic ECC algorithms are believed to be vulnerable to quantum computers but due to a large base of expertise, which was built up so far, it would be a pity to abandon this idea. That is the moment when the isogenies come to the rescue.

Isogenies are the morphisms between elliptic curves which preserve mappings between them. Finding these morphisms is hard. It requires many mathematical operations and resources. Therefore implementations efficiency leaves much to be desired, making searching for more efficient formulas worth the effort. Most of these equations use elliptic curves in the Weierstrass or Montgomery model, but there are many more such models that can be used, maybe even more efficiently. To compute isogeny between curves on an alternative model, one may transform the given elliptic curve, presented by an alternative model, via isomorphism to one of the standard models, then compute isogeny based on known formulas and finally transform obtained curve back into an alternative model.

There exist several methods for computing isogenies between elliptic curves. The first of them, which may be called „the basis" for any discussions about isogenies, was presented by Vélu in [1]. It allows calculating a morphism between two Weierstrass elliptic curves. The analogs of the primary formulas for isogenies on alternative models of elliptic curves were presented by Moody and Shumow in [2]. They gave equations for two other models: Edwards and general Huff's. As for the computing isogenies on the extended Jacobi quartics, two articles should be mentioned [3], [4] and they will be in one of the following parts.

This paper presents two new methods for computing isogenies between elliptic curves in an extended Jacobi quartic model. The first way is to transform such elliptic curve to Weierstrass model by formulas described in [5], then to compute isogeny with Vélu's formulas from [1] and at the end, to transform obtained curve into an extended Jacobi quartic model analogous to the first conversion. The second way is to compute an isogeny directly from one extended Jacobi quartic to another with formulas presented by us. Knowing the properties that must be met for the morphism to be an isogeny, we show new additive formulas which satisfy those properties. That allows obtaining equations for computing coefficients of an isogenous elliptic curve than known so far.

II. Vélu's formulas for isogenies

Any elliptic curve over a finite field K can be written in the Weierstrass form. There exist alternate models, such as Montgomery, Edwards, or Huff curves, and others. They differ in the equations and arithmetic formulas. In evaluating isogenies, the chosen elliptic curve model is not relevant from a conceptual point of view, but it is for the computational aspects. The first one, who gave explicit formulas for isogenies between Weierstrass curves, was Jacques Vélu in 1971 [1].

Ł. Dzierzkowski and M. Wroński are with Faculty of Cybernetics, Military University of Technology, Warsaw, Poland (e-mail: {lukasz.dzierzkowski, michal.wronski}@wat.edu.pl).

A. Isogenies

Elliptic curve over K can be presented by a smooth Weierstrass equation

$$E_{LW} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

or, if $\text{char}(K) \neq 2, 3$, in the short Weierstrass form

$$E_W : y^2 = x^3 + a_4x + a_6 \tag{2}$$

with coefficients $a_i \in K$, a point at infinity, denoted as $\mathcal{O}$ and a point of order two $P_{W,2} = (\theta, 0)$, if such exists on the particular curve [2].

Let F be a subgroup of E_W of an order l. Vélu's formulas show how to explicitly find the rational function form of an isogeny $\phi : E_W \to \tilde{E}_W$ with kernel F. For $P = (x_P, y_P) \in E_W$, ϕ is defined as

$$\phi(P) = \begin{cases} \left(x_P + \sum_{Q\in F-\{\mathcal{O}\}}(x_{P+Q} - x_Q), \right. \\ \left. y_P + \sum_{Q\in F-\{\mathcal{O}\}}(y_{P+Q} - y_Q)\right), & P \notin F, \\ \mathcal{O}, & P \in F, \end{cases} \tag{3}$$

where from [6] it is known, that

$$x_{P+Q} + x_{P-Q} = 2\frac{(x_P + x_Q)(x_Px_Q + a_4) + 2a_6}{(x_P - x_Q)^2} \tag{4}$$

Then if

$$t_P = \begin{cases} 3x_P^2 + a_4, & \text{P is of order two,} \\ 2(3x_P^2 + a_4), & \text{P is not of order two,} \end{cases} \tag{5}$$

and

$$u_P = 4x_P^3 + 4a_4x_P + 4a_6, \tag{6}$$

coefficients of a new curve $\tilde{E}_W$ are given by

$$\begin{aligned} \tilde{a}_4 &= a_4 - 5\sum_{P\in F-\{\mathcal{O}\}} t_P, \\ \tilde{a}_6 &= a_6 - 7\sum_{P\in F-\{\mathcal{O}\}} (u_P + x_Pt_P). \end{aligned} \tag{7}$$

Calculations based on the following formulas must be performed to find an image point $P' = (x', y')$ on the new curve

$$\begin{aligned} x' &= x + \sum_{P\in F-\{\mathcal{O}\}} \left(\frac{t_P(x-x_P)+u_P}{(x-x_P)^2}\right), \\ y' &= y - \sum_{P\in F-\{\mathcal{O}\}} \left(\frac{2yu_P+t_P(y-y_P)(x-x_P)+2y_P(3x_P^2+a_4)(x-x_P)}{(x-x_P)^3}\right). \end{aligned} \tag{8}$$

By computing isogenies between elliptic curves over a certain field, an isogeny graph can be drawn.

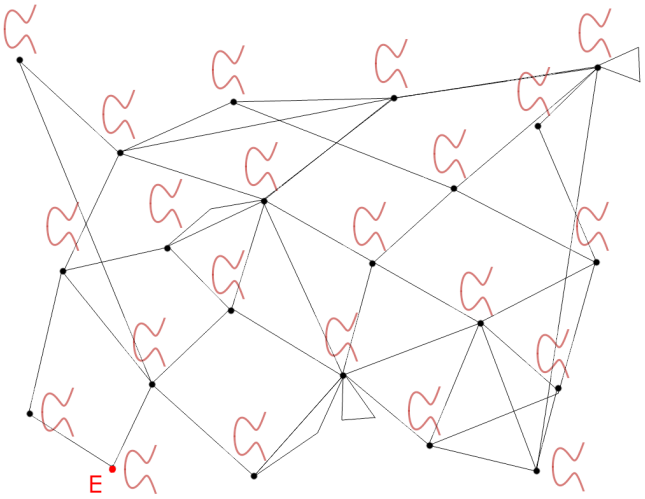

Fig. 1. An isogeny graph [7]

Since it is believed that the development of the quantum computer will not significantly affect the effectiveness of computing the isogenies between elliptic curves, such graphs as the above and the way of „navigating" through them are used in post-quantum cryptographic algorithms such as, for example, CSIDH.

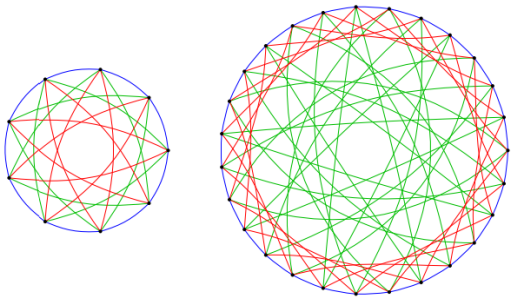

Fig. 2. Exemplary isogeny graphs that can be used in the CSIDH algorithm [8]

III. Extended Jacobi Quartics

Let K be a finite field with $\text{char}(K) \neq 2$. An extended Jacobi quartic [9] is an elliptic curve over K given by equation

$$E_J : y^2 = dx^4 + 2ax^2 + 1, \tag{9}$$

where coefficients $a, d \in K$ and $\Delta = 256d(a^2 - d)^2 \neq 0$.

All elliptic curves containing a point of order two [4], [5] can be represented in the form of the Equation (9)). Assume that E_W has a point of order two $P_{W,2} = (\theta, 0) \in E_W(K)$. Then, the Weierstrass elliptic curve from the Equation (2) is birationally equivalent to the extended Jacobi quartic from the Equation (9), where

$$\begin{aligned} d &= -\frac{3\theta^2+4a_4}{16}, \\ a &= -\frac{3}{4}\theta, \\ (x, y) &\to \left(\frac{2(3x-4a)}{3y}, \frac{54x^3-108ax^2+64a^3-27y^2}{27y}\right). \end{aligned} \tag{10}$$

The negation of a point $P = (x_P, y_P)$ on the extended Jacobi curve is given by $-P = (-x_P, y_P)$, the point at infinity

is represented as $\mathcal{O} = (0, 1)$ and the point's of order two coordinates are $P_{J,2} = (0, -1)$.

If coefficient d is not a square in K, then there exists complete arithmetic on the extended Jacobi curves, which means that addition formulas may be used for a point doubling. Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be points on the extended Jacobi curve E_J. The formulas [5] for points addition $P + Q = (x_{P+Q}, y_{P+Q})$ are given by

$$\begin{aligned} x_{P+Q} &= \frac{x_P y_Q + x_Q y_P}{1 - d x_P^2 x_Q^2}, \\ y_{P+Q} &= \frac{(y_P y_Q + 2a x_P x_Q)(d x_P^2 x_Q^2 + 1) + 2d x_P x_Q (x_P^2 + x_Q^2)}{\left(1 - d x_P^2 x_Q^2\right)^2}. \end{aligned} \tag{11}$$

IV. Isogenies on extended Jacobi quartics

In this section, we will recall previous articles about isogenies on the extended Jacobi quartic and present our two methods, which are presented in Graph 3.

The first method is a composition $\phi'_J = \pi^{-1} \circ \phi_W \circ \pi$ of three morphisms:

1) π - an isomorphism from an extended Jacobi curve to a Weierstrass curve,
2) ϕ_W - an isogeny between two Weierstrass curves,
3) π^{-1} - an inverse isomorphism to π, transforming a Weierstrass curve to an extended Jacobi quartic.

The second way to find an isogenous extended Jacobi quartic is to use formulas for the ϕ_J isogeny described below.

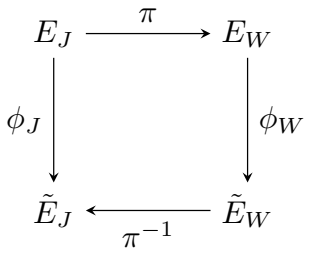

Fig. 3. Our two methods of computing isogeny between extended Jacobi quartics - direct and composite

A. Functions composition

The first method of finding an isogenous extended Jacobi quartic curve is performing three transformations, as described in the introduction to the current section.

In [4] Hu et al. presented an isomorphic transformation from the extended Jacobi quartic to the Weierstrass curve in two ways:

1) computing the isomorphisms from extended Jacobi quartic E_J to other Jacobi quartic $\tilde{E}_J$ and then to the Weierstrass curve $\tilde{E}_W$,
2) computing the isomorphisms from extended Jacobi quartic E_J to the Weierstrass curve E_W and then to other Weierstrass curve $\tilde{E}_W$,

as shown on a graph below.

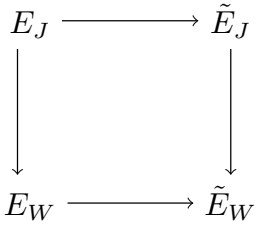

Fig. 4. Two methods of computing an isomorphic elliptic curve [4]

We partly drew from the above idea, but our goal was to obtain an isogenous extended Jacobi quartic. To conduct such calculations, three steps need to be followed.

1) Isomorphism from an extended Jacobi quartic curve to a short Weierstrass curve:

The composition begins with specifying the initial extended Jacobi quartic. It is in the same form as in the Equation (9)

$$E_J : y^2 = dx^4 + 2ax^2 + 1.$$

A purpose of the first transformation is a transition from an extended Jacobi quartic to a Weierstrass elliptic curve in the form as in the Equation (2)

$$E_W : y^2 = x^3 + a_4 x + a_6.$$

To compute Weierstrass coefficients a_4 and a_6, few modifications of the Equations (10) are necessary. Calculating a_4 is possible by changing the first formula from (10) and obtaining

$$a_4 = -\frac{3\theta^2 + 16d}{4}. \tag{12}$$

Knowing that $a = -\frac{3}{4}\theta$, Equation (12) may be modified as follows

$$a_4 = -\frac{4(a^2 + 3d)}{3}. \tag{13}$$

The second coefficient is calculable via using the point of order two on the short Weierstrass elliptic curve and the curve's equation. Because the point $P_{W,2} = (\theta, 0)$ lies on the curve, its coefficients must satisfy the curve's equation, which means that

$$\theta^3 + a_4\theta + a_6 = 0. \tag{14}$$

Being aware of the above formulas for converting a_4 and θ, the Equation (14) may be transformed to

$$a_6 = -\theta^3 - a_4\theta = \frac{16a(a^2 - 9d)}{27}. \tag{15}$$

As a result of the described modifications, the knowledge about an extended Jacobi quartic and its coefficients a and d is sufficient to obtain coefficients a_4 and a_6 of the isomorphic short Weierstrass curve.

To transform a point on an extended Jacobi quartic (x, y) to a point on a Weierstrass curve, the third formula from Equation (10) may be used.

2) Isogeny between short Weierstrass curves:

The second part of the composition is computing an isogeny between two Weierstrass curves. It is feasible to do by Vélu's formulas [1].

Conducting the second morphism may begin after receiving the Weierstrass curve E_W coefficients a_4 and a_6 from a previous section. Then the obtained curve may be transformed into

$$\tilde{E}_W : y^2 = x^3 + \tilde{a}_4 x + \tilde{a}_6. \tag{16}$$

Computing the isogenous curve's coefficients may be done with formulas from Equation (7) and transferring a point from E_W to $\tilde{E}_W$ may be done with Equation (8).

3) Isomorphism from a short Weierstrass curve to an extended Jacobi quartic curve:

The last part of the composition is finding an isogenous extended Jacobi quartic $\tilde{E}_J$, given by

$$\tilde{E}_J : y^2 = \tilde{d}x^4 + 2\tilde{a}x^2 + 1, \tag{17}$$

which is isomorphic to the short Weierstrass curve, computed during the previous morphism. To calculate coefficients $\tilde{d}$ and $\tilde{a}$, point $P_{\tilde{W},2} = \left(\tilde{\theta}, 0\right)$ of order two from the $\tilde{E}_W$ curve is required. Then, it is enough to use analogous formulas to described in Equation (10)

$$\begin{aligned} \tilde{d} &= -\tfrac{3\tilde{\theta}^2 + 4\tilde{a}_4}{16}, \\ \tilde{a} &= -\tfrac{3}{4}\tilde{\theta}, \end{aligned} \tag{18}$$

and an isogenous extended Jacobi quartic $\tilde{E}_J$ is given.

Transferring a point $P = (x_P, y_P)$ from the $\tilde{E}_W$ to $\tilde{E}_J$ requires completing computations based on the following formulas

$$(x_P, y_P) \to \left(-\frac{2(ax^2 - 3y - 3)}{3x^2}, -\frac{4(ax^2 - y - 1)}{x^3} \right). \tag{19}$$

4) Final composition: Having the above transformations, one can perform the whole process $\phi'_J = \pi^{-1} \circ \phi_w \circ \pi$. Computing the coefficients of the $\tilde{E}_J$ curve requires using a composition of the formulas given in Equations (13), (15), (7) and (18). Finding the coordinates of the point, transferred from the curve E_J to the curve $\tilde{E}_J$, consists of operations from Equations (10), (8) and (19).

B. Direct isogeny

Xu et al. [3] were the first to present the formulas for isogeny on the extended Jacobi quartic curve as

$$\phi(P) = \left(x_P \prod_{Q \in F-(0,1)} \frac{x_{P+Q}}{x_Q}, y_P \prod_{Q \in F-(0,1)} \frac{y_{P+Q}}{y_Q} \right). \tag{20}$$

The newer paper that contained other formulas for isogenies on the extended Jacobi quartic is the one presented by Hu et al. [4], whose formulas were given by

$$\phi(P) = \left(x_P \prod_{Q \in F-(0,1)} x_{P+Q}, y_P \prod_{Q \in F-(0,1)} \frac{y_{P+Q}}{y_Q} \right). \tag{21}$$

In this section, basing on the described above works, we present the second of our two methods of computing an isogenous extended Jacobi quartic.

Theorem 1: Let $F = \{(0,1), (\pm\alpha_1, \beta_1), \ldots, (\pm\alpha_s, \beta_s)\}$ be a subgroup of the extended Jacobi quartic curve E_J with odd order $l = 2s + 1$. Then ϕ_l, given by a formula

$$\phi_l(P) = \left(\sum_{Q \in F} x_{P+Q}, \frac{\sum\limits_{Q \in F} y_{P+Q}}{\sum\limits_{Q \in F} y_Q} \right) \tag{22}$$

is an l-isogeny with kernel F, from E_J to $\tilde{E}_J : y^2 = \tilde{d}x^4 + 2\tilde{a}x^2 + 1$, where

$$\tilde{d} = \frac{d}{\left(1 + 2\sum\limits_{i=1}^{s} y_i\right)^2} \tag{23}$$

and

$$\tilde{a} = \frac{a\left(1 + 2\sum\limits_{i=1}^{s} y_i\right) + 6d\left(\sum\limits_{i=1}^{s} y_i x_i^2\right)}{\left(1 + 2\sum\limits_{i=1}^{s} y_i\right)^3}. \tag{24}$$

Let $F^+ = \{(\alpha_1, \beta_1), \ldots, (\alpha_s, \beta_s)\}$, $F^- = \{(-\alpha_1, \beta_1), \ldots, (-\alpha_s, \beta_s)\}$ and $F^+ \cup F^- \cup \{\mathcal{O}\} = F$, then a point's coordinates maps are given by

$$\begin{aligned} \phi_l(x, y) = \Bigg(& x + \sum_{Q \in F^+} \frac{2xy_Q}{1 - dx^2x_Q^2}, \frac{1}{1 + 2\sum\limits_{Q \in F^+} y_Q} \\ & \cdot \left(y + \sum_{Q \in F^+} \frac{2yy_Q(dx^2x_Q^2 + 1)}{(1 - dx^2x_Q^2)^2} \right) \Bigg). \end{aligned} \tag{25}$$

Proof 1: At the beginning, it is easy to see that $\phi_l(0,1) = (0,1)$ and of course ϕ_l is invariant under the translation by any element of F, which means that $F \subseteq \ker(\phi_l)$. To prove that $F = \ker(\phi_l)$, the form of the given map can be considered. The formula for x-coordinate from Equation (25) may be transformed as follows

$$\begin{aligned} x_{\phi_l(P)} &= x_P + \sum_{Q \in F^+} \frac{2x_P y_Q}{1 - dx_P^2 x_Q^2} \\ &= \frac{x_P \prod\limits_{Q \in F^+} (1 - dx_P^2 x_Q^2) + \sum\limits_{Q \in F^+} \left(2x_P y_Q \prod\limits_{\substack{R \in F^+ \\ R \neq Q}} (1 - dx_P^2 x_Q^2) \right)}{\prod\limits_{Q \in F^+} (1 - dx_P^2 x_Q^2)} = \frac{N}{D}. \end{aligned}$$

For any point $P \in \ker(\phi_l)$ the value of $x_{\phi_l(P)}$ must be equal to 0, and therefore the value of the nominator N also. N may be expanded into a polynomial in the indeterminate x_P. The cardinality of the set F^+ is $|F^+| = s$. It means the degree of the polynomial N is $2s + 1$, so it may only have so many solutions. Due to the fact, that $|F| = 2s + 1$ as well, it is clear that only points from F belong to the kernel, therefore $F = \ker(\phi)$.

Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q) \neq (0,1)$ be points on E_J, then

$$x_{P+Q}+x_{P-Q} = \frac{x_Py_Q+x_Qy_P}{1-dx_P^2x_Q^2}+\frac{x_Py_Q-x_Qy_P}{1-dx_P^2x_Q^2} = \frac{2x_Py_Q}{1-dx_P^2x_Q^2},$$

$$\begin{aligned} y_{P+Q}+y_{P-Q} = & \frac{(y_Py_Q+2ax_Px_Q)(dx_P^2x_Q^2+1)+2dx_Px_Q(x_P^2+x_Q^2)}{\left(1-dx_P^2x_Q^2\right)^2} \\ & +\frac{(y_Py_Q-2ax_Px_Q)(dx_P^2x_Q^2+1)-2dx_Px_Q(x_P^2+x_Q^2)}{\left(1-dx_P^2x_Q^2\right)^2} \\ & = \frac{2y_Py_Q(dx_P^2x_Q^2+1)}{\left(1-dx_P^2x_Q^2\right)^2}. \end{aligned} \tag{26}$$

Knowing the coordinates of the point at infinity $\mathcal{O}=(0,1)$ and the inverse of the point $-Q=(-x_Q,y_Q)$, it is easy to obtain the formulas from Equation (25) basing on those from Equation (26).

The last part of the proof is to derive the formulas for coefficients $\tilde{d}$ and $\tilde{a}$ of the extended Jacobi quartic $\tilde{E}_J: y^2=\tilde{d}x^4+2\tilde{a}x^2+1$, where x and y are coordinates computed with formulas from Equation (25). Let $f(x,y)$ be a function given by

$$f(x,y)=(\tilde{d}x^4+2\tilde{a}x^2+1-y^2)\Big(\prod_{Q\in F^+}(1-dx_P^2x_Q^2)\Big)^4\Big(1+2\sum_{Q\in F^+}y_Q\Big)^2.$$

Because the extended Jacobi quartic equation was presented in such form, its value is zero, so we could multiply it by the denominators to eliminate the fractions without changing the value. Now, let us use formulas from Equation (25) to exchange x and y for the coordinates maps

$$\begin{aligned} f(x_{\phi_l(P)},y_{\phi_l(P)}) = & \left(\tilde{d}\left(x_P+\sum_{Q\in F^+}\frac{2x_Py_Q}{1-dx_P^2x_Q^2}\right)^4\right. \\ & +2\tilde{a}\left(x_P+\sum_{Q\in F^+}\frac{2x_Py_Q}{1-dx_P^2x_Q^2}\right)^2+1-\frac{1}{\left(1+2\sum\limits_{Q\in F^+}y_Q\right)^2} \\ & \left.\cdot y_P^2\left(1+\sum_{Q\in F^+}\frac{2y_Q(dx_P^2x_Q^2+1)}{(1-dx_P^2x_Q^2)^2}\right)^2\right) \\ & \Big(\prod_{Q\in F^+}(1-dx_P^2x_Q^2)\Big)^4\Big(1+2\sum_{Q\in F^+}y_Q\Big)^2. \end{aligned}$$

After expanding the equation and eliminating y_P by substituting a curve's equation for it, we get

$$\begin{aligned} f(x_{\phi_l(P)},y_{\phi_l(P)}) = & \tilde{d}\left(x_P\prod_{Q\in F^+}(1-dx_P^2x_Q^2)\right. \\ & \left.+\sum_{Q\in F^+}\left(2x_Py_Q\prod_{\substack{R\in F^+\\R\neq Q}}(1-dx_P^2x_Q^2)\right)\right)^4\Big(1+2\sum_{Q\in F^+}y_Q\Big)^2 \\ & +2\tilde{a}\prod_{Q\in F^+}(1-dx_P^2x_Q^2)^2\left(x_P\prod_{Q\in F^+}(1-dx_P^2x_Q^2)\right. \\ & \left.+\sum_{Q\in F^+}\left(2x_Py_Q\prod_{\substack{R\in F^+\\R\neq Q}}(1-dx_P^2x_Q^2)\right)\right)^2 \\ & \cdot\Big(1+2\sum_{Q\in F^+}y_Q\Big)^2+\Big(1+2\sum_{Q\in F^+}y_Q\Big)^2-(dx_P^4+2ax_P^2+1) \\ & \cdot\left(\prod_{Q\in F^+}(1-dx_P^2x_Q^2)^2+\sum_{Q\in F^+}\Big(2y_Q(dx_P^2x_Q^2+1)\right. \\ & \left.\cdot\prod_{\substack{R\in F^+\\R\neq Q}}(1-dx_P^2x_Q^2)^2\Big)\right)^2. \end{aligned}$$

Eventually, the equation has a form

$$\begin{aligned} f(x_{\phi_l(P)},y_{\phi_l(P)}) = & \left(\tilde{d}d^4\Big(1+2\sum_{Q\in F^+}y_Q\Big)^2-d^5\right)x_P^{8s+4} \\ & +\cdots+\left(2\tilde{a}\Big(1+2\sum_{Q\in F^+}y_Q\Big)^4-2a\Big(1+2\sum_{Q\in F^+}y_Q\Big)^2\right. \\ & \left.-12d\Big(\sum_{Q\in F^+}x_Q^2y_Q\Big)\Big(1+2\sum_{Q\in F^+}y_Q\Big)\right)x_P^2. \end{aligned}$$

Setting the cooefficients of x_P^{8s+4} and x_P^2 to zero allows to obtain formulas from Equations (23) and (24).

V. Further works and conclusions

Observing the pace of work on the quantum computer and on the improvements to Shor's algorithm, one can see that thinking about post-quantum cryptography is not unreasonable.

TABLE I. Number of qubits in IBM's quantum computer

year	number of quibits
2019	27
2020	65
2021	127
...	
2022	433
2023	1121
?	

In the last year (2021) IBM announced that a quantum computer with 127 qubits was ready. A company's roadmap predicts that in 2022 a computer with 433 qubits will be delivered and in 2023 a barrier of 1000 qubits will be broken. It is feasible but requires a lot of effort and implementing new ideas. The pace achieved nowadays should be a warning and a reason to think more seriously about threats resulting from the development of quantum technologies. Maybe some of them will be neutralised with the isogeny-based algorithms.

In this paper, we recalled a small part of the theory of elliptic curves and searching isogenies between them. We also presented two methods of computing isogenies between extended Jacobi quartics and the explicit formulas for conducting both of them.

Our first method allows finding an isogenous curve in a way that was never shown before and can be an alternative to classical isogeny computations. It allows computing an isogeny between two extended Jacobi quartic curves by an isomorphic transformation into the short Weierstrass curve, using Vélu's formulas to find an isogeny between two Weierstrass elliptic curves and then inverse transformation into the extended Jacobi quartic.

The second method, based on a direct morphism, gives simpler equations than known so far (e.g., in [4], which requires calculating roots). Our formulas allow computing an isogenous extended Jacobi quartic just with simple arithmetic operations.

Further works may be:

- checking other formulas for isogenies than given in Equation (22),
- examining a possibility to compute isogenies on other elliptic curve models with a composition method,
- verifying feasibility and effectiveness of the practical application of the methods described in this paper.

REFERENCES

[1] J. Velu, "Isogenies entre courbes elliptiques," *C. R. Acad. Sci. Paris Sér. A-B*, vol. 273, 1971.

[2] D. Moody and D. Shumow, "Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves," *Mathematics of Computation*, vol. 85, no. 300, pp. 1929–1951, 2016.

[3] X. Xu, W. Yu, K. Wang, and X. He, "Constructing Isogenies on Extended Jacobi Quartic Curves," in *Information Security and Cryptology*, K. Chen, D. Lin, and M. Yung, Eds. Cham: Springer International Publishing, 2017, pp. 416–427.

[4] Z. Hu, Z. Liu, L. Wang, and Z. Zhou, "Simplified isogeny formulas on twisted Jacobi quartic curves," *Finite Fields and Their Applications*, vol. 78, p. 101981, 2022. [Online]. Available: https://doi.org/10.1016/j.ffa.2021.101981

[5] O. Billet and M. Joye, "The Jacobi Model of an Elliptic Curve and Side-Channel Analysis," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, M. Fossorier, T. Høholdt, and A. Poli, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 34–42. [Online]. Available: https://doi.org/10.1007/3-540-44828-4_5

[6] I. Semaev, "Summation polynomials and the discrete logarithm problem on elliptic curves," Cryptology ePrint Archive, Report 2004/031, 2004.

[7] L. Dzierzkowski, "Analysis of the possibility of hardware implementation of SIDH key exchange scheme," Military University of Technology in Warsaw, 2020.

[8] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "CSIDH: an efficient post-quantum commutative group action," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2018, pp. 395–427. [Online]. Available: https://doi.org/10.1007/978-3-030-03332-3_15

[9] H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson, "Jacobi Quartic Curves Revisited," in *Information Security and Privacy*, C. Boyd and J. González Nieto, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 452–468. [Online]. Available: https://doi.org/10.1007/978-3-642-02620-1_31