Hindawi
Security and Communication Networks
Volume 2018, Article ID 5747642, 11 pages
https://doi.org/10.1155/2018/5747642

Research Article

Efficient Isogeny Computations on Twisted Edwards Curves

Suhri Kim,[1] Kisoon Yoon,[2] Jihoon Kwon,[1] Seokhie Hong,[1] and Young-Ho Park[3]

[1] *Center for Information Security Technologies (CIST), Korea University, Seoul, Republic of Korea*
[2] *NSHC Inc., Uiwang, Republic of Korea*
[3] *Sejong Cyber University, Seoul, Republic of Korea*

Correspondence should be addressed to Young-Ho Park; youngho@sjcu.ac.kr

Received 6 April 2018; Accepted 26 June 2018; Published 15 July 2018

Academic Editor: Mun-Kyu Lee

The isogeny-based cryptosystem is the most recent category in the field of postquantum cryptography. However, it is widely studied due to short key sizes and compatibility with the current elliptic curve primitives. The main building blocks when implementing the isogeny-based cryptosystem are isogeny computations and point operations. From isogeny construction perspective, since the cryptosystem moves along the isogeny graph, isogeny formula cannot be optimized for specific coefficients of elliptic curves. Therefore, Montgomery curves are used in the literature, due to the efficient point operation on an arbitrary elliptic curve. In this paper, we propose formulas for computing 3 and 4 isogenies on twisted Edwards curves. Additionally, we further optimize our isogeny formulas on Edwards curves and compare the computational cost of Montgomery curves. We also present the implementation results of our isogeny computations and demonstrate that isogenies on Edwards curves are as efficient as those on Montgomery curves.

1. Introduction

The security of public key cryptosystems is mostly based on a number of theoretic problems such as the hardness of factoring large numbers or solving discrete logarithms over the finite field. However, due to Shor's algorithm, these problems can be solved in polynomial time by the quantum adversary, consequently threatening the security of current public key cryptosystems [1]. Therefore, demands for quantum-secure cryptographic primitives are inevitable.

Postquantum cryptography (PQC) is alternative cryptographic primitives that are safe against the quantum adversary. Numerous studies have been made on PQC in order to substitute or interoperate with existing systems. The main categories of PQC are multivariate-based cryptography, code-based cryptography, lattice-based cryptography, hash-based digital signature, and isogeny-based cryptography. Although isogeny-based cryptography is the most recent field in PQC, it is considered as one of the prominent candidates due to its short key sizes and the reason that it can be implemented over currently used elliptic curve primitives.

The security of isogeny-based cryptography is based on the hardness of finding isogeny between given two elliptic curves. The first isogeny-based cryptosystems using ordinary elliptic curves were proposed by Couveignes and later by Stolbunov [2, 3]. The proposed scheme was extremely inefficient and even suffered from the quantum subexponential algorithm proposed by Childs et al. [4]. In 2011, Jao and De Feo presented a new cryptosystem based on the difficulty of constructing isogenies between supersingular elliptic curves, which is still infeasible against the known quantum attacks [5]. In 2016, Azarderakhsh et al. proposed a key compression method for supersingular isogeny key exchange, which was later improved by Costello et al. [6, 7]. Azarderakhsh et al. also implemented key exchange protocol on ARM-NEON and FPGA devices [8, 9]. Costello et al. proposed faster computation methods and library for supersingular isogeny key exchange [10]. In 2017, isogeny-based digital signature schemes were proposed by Galbraith et al. and Yoo et al., which brought diversity in the isogeny-based cryptography [11, 12]. Additionally, after the National Institute of Standards and Technology (NIST) announced a standardization project for PQC, Supersingular Isogeny Key Encapsulation (SIKE) was submitted as one of the candidates [13]. As stated above, extensive researches have been done in isogeny-based cryptography.

Since any curve in isogeny-based cryptosystem has group structure $(\mathbb{Z}/(p \mp 1)\mathbb{Z}))^2$, for prime p, either the curve or its twist has a point of order four [5]. As a result, it is isomorphic to a twisted Edwards curve and to a Montgomery curve [14]. Moreover, as coefficients of the elliptic curves change randomly in the isogeny-based cryptosystem, Montgomery curves are used in the state-of-the-art implementations. This is due to the fact that Montgomery ladder reduces the cost of point operations on Montgomery curves compared with any other forms of elliptic curves. However, whether other forms of elliptic curves are efficient as Montgomery curves is still unclear. Costello et al. proposed explicit formulas for 3 and 4 isogenies and also remarked that there might exist savings to be gained in Supersingular Isogeny Diffie–Hellman (SIDH) twisted Edwards version [15]. Meyer et al. proposed the hybrid SIDH scheme which exploits the fact that arithmetic in Edwards curves are efficient in certain cases [16]. Their method uses Edwards curves for point operations and Montgomery curves for isogeny computation. Independent from isogeny-based cryptosystem, Moody and Shumow were the first to propose isogeny formula on elliptic curves other than Weierstrass form [17]. They applied Vélu's formula on twisted Edwards curves and Huff curves. However, isogeny construction on these curves for cryptographic usage has not been done.

The aim of this work is to identify whether (twisted) Edwards curves are as efficient as Montgomery curves for isogeny-based cryptosystems. The following list details the main contributions of this work.

(i) We propose the optimized 3- and 4-isogeny formulas on twisted Edwards curves to be applied in the isogeny-based cryptography. Previous works on constructing isogenies on alternate curves are mostly for the theoretical foundations. To the best of our knowledge, we are the first to propose 4-isogeny formula on (twisted) Edwards curves, given an arbitrary subgroup. The details of our isogeny formulas on twisted Edwards curves are presented in Section 3.

(ii) We propose the optimized 3- and 4-isogeny formulas on Edwards curves. The proposed 3- and 4-isogeny formulas on Edwards curves require 6**M**+5**S** and 7**M**+5**S**, respectively, where **M** (resp., **S**) refers to field multiplication (resp., a field squaring). All of our formulas are given in terms of projective YZ-coordinates, which can later combine with YZ-coordinates only point operations on Edwards curves. The details of our isogeny formulas on Edwards curves are presented in Section 4.

(iii) We present the implementation results of our isogeny formulas and comprehensive analysis of their performance. We demonstrate that implementation results of isogenies on Edwards curves are similar to Montgomery curves. Therefore, the current isogeny-based cryptosystem can also work with Edwards curves.

This paper is organized as follows: A review of some special forms of elliptic curves is provided in Section 2. The description of isogeny of elliptic curves and Vélu's formula to compute isogeny is also presented in Section 2. Specifically, we introduce an existing application of Vélu's formula on Montgomery curves and twisted Edwards curves. In Section 3, we present our method to compute isogenies in twisted Edwards curves. Our optimized formulas for isogeny on Edwards curves and their implementations are given in Section 4. We draw our conclusions and future work in Section 5.

2. Preliminaries

In this section, we introduce the definition of special forms of elliptic curves. There are various forms of elliptic curves, but we will focus on twisted Edwards curves and Montgomery curves in this paper. Next, an isogeny of elliptic curves and Vélu's formulas are introduced. Due to the work of Vélu, isogeny can be constructed given a finite subgroup. We describe a previous method that applied Vélu's formula on twisted Edwards curves and Montgomery curves [5, 17].

2.1. Models of Elliptic Curve. Let K be a field with the characteristic not equal to 2 or 3. An *elliptic curve* defined over K is a smooth, projective algebraic curve of genus 1 with a distinguished point. It is well known that the points of an elliptic curve form an additive group with the distinguished point as the identity element. From the Riemann–Roch theorem, every elliptic curve can be defined by a cubic polynomial equation in two variables. For example, an elliptic curve can be defined by a short Weierstrass equation

$$\begin{aligned} W_{\alpha,\beta}: \quad & y^2 = x^3 + \alpha x + \beta, \\ & 4\alpha^3 + 27\beta^2 \neq 0, \end{aligned} \tag{1}$$

or by a Montgomery equation

$$\begin{aligned} M_{A,B}: \quad & By^2 = x^3 + Ax^2 + x, \\ & B\left(A^2 - 4\right) \neq 0. \end{aligned} \tag{2}$$

The j-invariants of the above curves are defined as $j(W_{\alpha,\beta}) = 1728 \cdot 4\alpha^3/(4\alpha^3 + 27\beta^2)$ and $j(M_{A,B}) = 256(A^2 - 3)^3/(A^2 - 4)$, respectively.

Two algebraic curves are said to be *birationally equivalent* if their function fields are isomorphic to each other. The representative of a birational class is called a *model*. An elliptic curve expressed in Montgomery equation is called *Montgomery model* and *Weierstrass model* if it is expressed in Weierstrass equation. Two models play important roles in the implementation of elliptic curves for cryptographic usage. Note that $M_{A,B}$ has either three rational points of order two or a rational point of order four (possibly both) [19, 20].

Another important model is the *Edwards model* defined by the equation

$$E_d : x^2 + y^2 = 1 + dx^2y^2, \quad d \in K \setminus \{0, 1\}. \tag{3}$$

In fact, E_d is not an elliptic curve as it has singular points $(1 : 0 : 0)$ and $(0 : 1 : 0)$ at infinity. In Edwards curves, the point $(0, 1)$ is the identity element, and the point $(0, -1)$ has order two. The points $(1,0)$ and $(-1,0)$ have order four. The condition that E_d always has a rational point of order four restricts the use of elliptic curves in the Edwards model. To overcome this deficiency, Bernstein et al. proposed *twisted Edwards curves* which are defined by the equation

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2, \tag{4}$$

for distinct nonzero elements $a, d \in K$ [14]. Clearly, $E_{a,d}$ is isomorphic to an Edwards curve over $K(\sqrt{a})$. Later in this paper we demonstrate that it is efficient to work with both projective coordinates and projective curve coefficients. Let $(A, B, C) \in \mathbb{P}^2(K)$ where $C \in \overline{K}^{\times}$ such that $a = A/C$ and $d = D/C$. Then $E_{a,d}$ can be expressed as

$$E_{A:D:C} : Ax^2 + Cy^2 = C + Dx^2y^2. \tag{5}$$

The addition law on twisted Edwards curve is defined as follows, and doubling can be performed with exactly the same formula.

$$\begin{aligned}&(x_1, y_1) + (x_2, y_2)\\&= \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right).\end{aligned} \tag{6}$$

Bernstein et al. showed the following cryptographically interesting relations on the above three models of elliptic curve [14].

Theorem 1. *Let E be an elliptic curve defined over a field K with the characteristic not equal to 2. The group of rational points $E(K)$ has an element of order 4 if and only if E is birationally equivalent over K to an Edwards curve.*

Theorem 2. *Let K be a field with* $\#K \equiv 3 \pmod 4$*; then every Montgomery curve over K is birationally equivalent over K to an Edwards curve.*

As Theorem 2 is used to compute 4-isogeny formula in Edwards curves, we shall define K with $\#K \equiv 3 \bmod 4$ in the remainder of this paper, unless otherwise specified.

2.1.1. Relation between Twisted Edwards Curves and Montgomery Curves. In [14], Bernstein et al. proved that every twisted Edwards curve over K is birationally equivalent over K to a Montgomery curve. Since this relation is used later in this paper, we shall describe it briefly. Let a and d be nonzero elements in K. Then every twisted Edwards curve $E_{a,d}$ is birationally equivalent to a Montgomery form $M_{A,B}$ via

$$(x, y) \longrightarrow (u, v) = \left(\frac{1+y}{1-y}, \frac{1+y}{(1-y)x}\right), \tag{7}$$

where $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$. The inverse of the map from $M_{A,B}$ to $E_{a,d}$ is defined as

$$(u, v) \longrightarrow (x, y) = \left(\frac{u}{v}, \frac{u-1}{u+1}\right). \tag{8}$$

The first coordinate in map (7) is computed by using only y-coordinate and the second coordinate in map (8) uses only u-coordinate. In projective coordinates, this map becomes remarkably simple [21]. A point $(X_M : Z_M)$ on a Montgomery curve can be transformed to the corresponding Edwards YZ-coordinates $(Y_E : Z_E)$ and vice versa:

$$\begin{aligned}(X_M : Z_M) &\longrightarrow (Y_E : Z_E) = (X_M - Z_M : X_M + Z_M),\\(Y_E : Z_E) &\longrightarrow (X_M : Z_M) = (Y_E + Z_E : Z_E - Y_E).\end{aligned} \tag{9}$$

Therefore, the point conversion between these two curves costs only two additions.

2.2. Isogeny and Vélu's Formulas. An *isogeny* between two elliptic curves E_1 and E_2 is a surjective group homomorphism with a finite kernel. Two elliptic curves E_1 and E_2 are said to be *isogenous* over K if there exists an isogeny $\phi : E_1 \longrightarrow E_2$ defined over K. If the degree of the isogeny ϕ is equal to the order of the kernel of ϕ, then ϕ is called a *separable* isogeny. An isogeny of degree ℓ is called an ℓ-isogeny. Throughout this paper, an ℓ-isogeny is a separable isogeny, unless otherwise stated.

For every isogeny $\phi : E_1 \longrightarrow E_2$, there exists an isogeny $\widehat{\phi} : E_2 \longrightarrow E_1$ such that

$$\phi \circ \widehat{\phi} = [\deg \phi]. \tag{10}$$

The isogeny $\widehat{\phi}$ is called the dual isogeny of ϕ. By using this fact, the relation of isogeny is an equivalence relation. Moreover, E_1 and E_2 are isogenous over K if and only if the group of the rational points $E_1(K)$ and $E_2(K)$ has the same cardinality. If ϕ is a separable isogeny of degree 1, then ϕ is an isomorphism. An isomorphism class of elliptic curves is uniquely represented by the j-invariant. That is, two elliptic curves are isomorphic over $\overline{K}$ if and only if they have the same j-invariant. Moreover, the kernel of an isogeny is finite. Conversely, if a finite subgroup G of an elliptic curve E is given, then there exists an elliptic curve $E' \cong E/G$ and a separable isogeny $\phi : E \longrightarrow E'$, with $\ker \phi = G$.

There are two methods to construct isogeny between elliptic curves. Vélu gave the explicit formulas to construct an isogeny with a given elliptic curve and a given finite subgroup as the kernel [22]. Later, Kohel proposed that isogeny ϕ can be computed from the kernel polynomial [23]. In this paper, we focus on Vélu's method to construct isogenies. Vélu's formulas are based on the transformation

$$\begin{aligned}(x_P, y_P) \longrightarrow \Bigg(&x_P + \sum_{Q \in G \setminus \{O\}} (x_{P+Q} - x_Q), y_P\\&+ \sum_{Q \in G \setminus \{O\}} (y_{P+Q} - y_Q)\Bigg),\end{aligned} \tag{11}$$

which is invariant under the translation by the points in the kernel G. In order to compute rational functions given by Vélu, let E be an elliptic curve with short Weierstrass form as in (1) for the simplicity. For a finite subgroup G, partition $G \setminus \{O\}$ into two sets, G^+ and G^-, such that $G \setminus \{O\} = G^+ \cup G^-$

and Q ∈ G^+ if and only if $-Q \in G^-$. For each point $Q \in G$, define the following equations:

$$\begin{aligned} g_Q^x &= 3x_Q^2 + a, \\ g_Q^y &= -2y_Q, \\ v_Q &= 2g_Q^x, \\ u_Q &= \left(g_Q^y\right)^2, \\ v &= \sum_{Q \in G^+} v_Q, \\ w &= \sum_{Q \in G^+} u_Q + x_Q v_Q. \end{aligned} \tag{12}$$

Then, the isogeny ϕ is given by

$$\begin{aligned} \phi(x, y) \longrightarrow \Bigg(& x + \sum_{Q \in G^+} \frac{v_Q}{x - x_Q} - \frac{u_Q}{(x - x_Q)^2}, y \\ & - \sum_{Q \in G^+} \frac{2u_Q y}{(x - x_Q)^3} + v_Q \frac{y - y_Q - g_Q^x g_Q^y}{(x - x_Q)^2} \Bigg). \end{aligned} \tag{13}$$

The order of the isogeny is equal to the order of the subgroup G. The equation of the image curve is

$$E' : y^2 = x^3 + (\alpha - 5v)x + (\beta - 7w). \tag{14}$$

2.2.1. Vélu's Formulas on Montgomery Curves. In this section, we describe how even-degree isogenies are induced on Montgomery curves. This method was proposed by Jao and De Feo and later optimized by Costello et al. [5, 10]. The main processes for deriving 4-isogeny are illustrated in projective coordinates. For odd-degree isogenies, refer to [10].

Let $M_{A,B}$ be a Montgomery curve defined in (2). It has a point of order two $P_2 = (0, 0)$ and a point of order four $P_4 = (1, \sqrt{(A + 2)/B})$, either defined over a quadratic extension, such that $[2]P_4 = P_2$. The isogeny—which has degree 2 and maps P_4 to $(0, 0)$—is defined as

$$\begin{aligned} & \phi : M_{A,B} \longrightarrow F \\ & (X : Y : Z) \longrightarrow \left(X(X - Z)^2 : Y\left(X^2 - Z^2\right) : X^2 Z\right), \end{aligned} \tag{15}$$

where $x = X/Z$ and $y = Y/Z$ for $(x, y) \in M_{A,B}$. The corresponding image curve is given as

$$F : By^2 = x^3 + (A + 6)x^2 + 4(2 + A)x. \tag{16}$$

Since the image curve is not in Montgomery form, computing square roots is unavoidable in order to transform F back to Montgomery form. To overcome such problem, consider the isogeny ψ with $\langle(0, 0)\rangle$ as a kernel, given by

$$\begin{aligned} & \psi : F \longrightarrow M_{A',B'} \\ & (X : Y : Z) \longrightarrow \left(X' : Y' : Z'\right), \end{aligned} \tag{17}$$

where $X' = -X(AZ + X + 2Z)(X + 4Z)$, $Y' = Y(4AZ^2 - X^2 + 8Z^2)$, and $Z' = (A - 2)X^2 Z$ in the above equation. The equation of the image curve is given as in Montgomery form:

$$M_{A',B'} : \frac{B}{2 - A} y^2 = x^3 - 2\frac{A + 6}{2 - A} x^2 + x. \tag{18}$$

Then, $\phi_1 = \psi \circ \phi$ is an isogeny of degree four that maps $M_{A,B}$ to $M_{A',B'} = M_{A,B}/\langle P_4\rangle$. However, this formula cannot be applied twice to obtain isogeny of degree 4^2. Instead, it would only induce multiplication by 4-isogeny when ϕ_1 is computed twice. In order to apply 4-isogeny successively for 4^ℓ-isogeny, ϕ_1 must be combined with isomorphism of Montgomery curves that maps 4-torsion point to some specific coordinate. This is already apparent as we have computed ϕ with point P_4 of a specific form. Let $P \neq \pm P_4$ be a point of order four in $M_{A,B}$. Let $P = (X_M : Y_M : Z_M)$ and $[2]P = (X_0 : Y_0 : Z_0)$ be the projective coordinates of P and $[2]P$, respectively. The isomorphism ι defined below maps $[2]P$ to $(0, 0)$ and P to point of the form $(1, \ldots)$.

$$\begin{aligned} & \iota : M_{A,B} \longrightarrow E \\ & (X : Y : Z) \longrightarrow (Z_M(XZ_0 - ZX_0) : YZ_M Z_0 : \\ & \quad Z(X_M Z_0 - Z_M X_0)), \end{aligned} \tag{19}$$

with the corresponding curve equation defined below.

$$\begin{aligned} E : \frac{BZ_M Z_0}{X_M Z_0 - Z_M X_0} y^2 \\ = x^3 + \frac{Z_M(3X_0 + AZ_0)}{X_M Z_0 - Z_M X_0} x^2 + x. \end{aligned} \tag{20}$$

Combining ϕ_1 with ι, we are able to compute 4-isogeny successively.

2.2.2. Vélu's Formulas on Twisted Edwards Curves. As denoted in the previous section, there exist birational maps from Edwards curves to Weierstrass curves. Let ψ be the transformation from a twisted Edwards curve to a Weierstrass curve W and ϕ be isogeny from W to another curve W'. Let ψ^{-1} be the transformation from a Weierstrass curve W' back to a twisted Edwards curve. The intuitive approach toward computing the isogeny between twisted Edwards curves is to combine these maps. However, the transformation from Weierstrass curves to twisted Edwards curves is complicated if the corresponding Weierstrass curve is not of the form below.

$$W'_{\alpha',\beta'} : y^2 = x^3 + 2(a + d)x^2 + (a - d)^2 x \tag{21}$$

Moreover, one needs to compute square roots in order to transform back to twisted Edwards form. To solve this issue, Moody and Shumow proposed compact formulas for odd-degree isogenies on twisted Edwards curves [17]. The isogeny of order $\ell = 2s + 1$ on twisted Edwards curves can be computed by using the following theorem.

Theorem 3. *Suppose G is a subgroup of the twisted Edwards curve $E_{a,d}$ with odd order $\ell = 2s + 1$ and points $G = \{(0, 1), (\pm\alpha_1, \beta_1), \ldots, (\pm\alpha_s, \beta_s)\}$. Then a normalized ℓ-isogeny from $E_{a,d}$ to $E_{\widehat{a},\widehat{d}}$, where $\widehat{a} = A^4/B^4a^\ell$ and $\widehat{d} = A^4B^4d^\ell$, with $A = \prod_{i=1}^{s}\alpha_i$, $B = \prod_{i=1}^{s}\beta_i$, is given by*

$$\Psi(x, y) = \left((-1)^s \frac{x}{A^2}\prod_{i=1}^{s}\frac{\beta_i^2x^2 - \alpha_i^2y^2}{1 - d^2\alpha_i^2\beta_i^2x^2y^2}, \frac{y}{B^2}\right. \\ \left.\cdot\prod_{i=1}^{s}\frac{\beta_i^2y^2 - a^2\alpha_i^2x^2}{1 - d^2\alpha_i^2\beta_i^2x^2y^2}\right). \tag{22}$$

The idea of the above formula comes from the fact that the map

$$(x_P, y_P) \longmapsto \left(\prod_{Q\in G}\frac{x_{P+Q}}{x_Q}, \prod_{Q\in G}\frac{y_{P+Q}}{y_Q}\right), \tag{23}$$

is invariant under the translation by an element in G. Note that this idea does not apply for even-degree isogenies since either the abscissa or the ordinate of every 2-torsion point vanishes.

3. The Proposed Isogeny Computations on Twisted Edwards Curves

In this section, we propose optimized formulas for 3-isogeny and 4-isogeny on twisted Edwards curves, which are commonly used degrees in the isogeny-based cryptosystem. For 3-isogeny, we use Moody and Shumow's result as a base formula and optimize it by using projective coordinates, projective curve coefficients, and division polynomial [17]. For even-degree isogeny computation, we exploit the efficiency of computing a birational map between twisted Edwards curves and Montgomery curves. The 4-isogeny formula on twisted Edwards curves can be obtained by composing the birational map and isogeny on Montgomery curves.

3.1. 3 Isogenies on Twisted Edwards Curves. Let $P = (\alpha, \beta)$ be a 3-torsion point on twisted Edwards curve $E_{a,d}$ defined in (4). Let ϕ be the 3-isogeny with kernel $\langle P\rangle$ that maps $E_{a,d}$ to the twisted Edwards curve $E_{a',d'}$, where $E_{a',d'} = E_{a,d}/\langle P\rangle$. Then, by using the formula proposed by Moody and Shumow [17], ϕ is given by

$$\phi(x, y) \\ = \left((-1)\frac{x}{\alpha^2}\frac{\beta^2x^2 - \alpha^2y^2}{1 - d^2\alpha^2\beta^2x^2y^2}, \frac{y}{\beta^2}\frac{\beta^2y^2 - \alpha^2a^2x^2}{1 - d^2\alpha^2\beta^2x^2y^2}\right), \tag{24}$$

with the curve parameters a' and d' such that

$$a' = \frac{\alpha^4}{\beta^4}a^3, \\ d' = \alpha^4\beta^4d^3. \tag{25}$$

From the curve equation, x^2 and α^2 can be expressed as $x^2 = (1 - y^2)/(a - dy^2)$ and $\alpha^2 = (1 - \beta^2)/(a - d\beta^2)$, respectively. By substituting x^2 and α^2, the y-coordinate in equation (24) is given by

$$\frac{y}{\beta^2}\frac{\beta^2y^2 - \alpha^2a^2x^2}{1 - d^2\alpha^2\beta^2x^2y^2} = \frac{y}{\beta^2} \\ \cdot\frac{\beta^2y^2 - \left(\left(1 - \beta^2\right)/\left(a - d\beta^2\right)\right)a^2\left(\left(1 - y^2\right)/\left(a - dy^2\right)\right)}{1 - d^2\left(\left(1 - \beta^2\right)/\left(a - d\beta^2\right)\right)\beta^2\left(\left(1 - y^2\right)/\left(a - dy^2\right)\right)y^2}. \tag{26}$$

To prevent inversions when computing isogeny and curve coefficients, we utilize projective coordinates and projective curve coefficients. Let $P = (X_3 : Y_3 : Z_3)$ be the projective representation of P such that $\alpha = X_3/Z_3$ and $\beta = Y_3/Z_3$. Let $(Y : Z)$ be the additional input and $(Y' : Z')$ be its corresponding image. By substituting the projective coordinates in (26) and simplifying the equation, we can obtain

$$\frac{Y'}{Z'} = \frac{YZ_3^2}{ZY_3^2}\cdot\frac{Y_3^2Y^2\left(aZ_3^2 - dY_3^2\right)\left(aZ^2 - dY^2\right) - Z_3^2Z^2\left(Z_3^2 - Y_3^2\right)a^2\left(Z^2 - Y^2\right)}{Z_3^2Z^2\left(aZ^2 - dY^2\right)\left(aZ_3^2 - dY_3^2\right) - d^2Y_3^2Y^2\left(Z_3^2 - X_3^2\right)\left(Z^2 - Y^2\right)} \\ = \frac{YZ_3^2}{ZY_3^2}\cdot\frac{aY_3^2Z^2 - dY_3^2Y^2 + aZ_3^2Y^2 - aZ_3^2Z^2}{dY_3^2Y^2 - dY_3^2Z^2 + aZ_3^2Z^2 - dZ_3^2Y^2}. \tag{27}$$

Since $y = Y_3/Z_3$ is a root of the 3-division polynomial $\psi_3(y) = (a - d)^3(a + 2ay - 2dy^3 - dy^4)/2^4(1 - y)^4$, we can express $d = aZ_3^3(Z_3 + 2Y_3)/Y_3^3(2Z_3 + Y_3)$. Then, we have

$$\frac{Y'}{Z'} = \frac{Y\left(Z^2Y_3^2 + 2Z^2Y_3Z_3 + Y^2Z_3^2\right)}{Z\left(Z^2Y_3^2 + 2Y^2Y_3Z_3 + Y^2Z_3^2\right)}. \tag{28}$$

In summary, from the additional input $(Y : Z)$, projective version of (26) gives

$$\left(Y' : Z'\right) = \left(Y\left(Z^2Y_3^2 + 2Z^2Y_3Z_3 + Y^2Z_3^2\right) :\right. \\ \left.Z\left(Z^2Y_3^2 + 2Y^2Y_3Z_3 + Y^2Z_3^2\right)\right). \tag{29}$$

Now, let a' and d' be the curve coefficients of the image curve. Substituting $\alpha^2 = (Z_3^2 - Y_3^2)/(aZ_3^2 - dY_3^2)$ and $d = aZ_3^3(Z_3 + 2Y_3)/Y_3^3(2Z_3 + Y_3)$ in (25) represented in projective coordinates, we have

$$\begin{aligned} a' &= \frac{a\left(Y_3 + 2Z_3\right)^2}{Y_3^2}, \\ d' &= \frac{aZ_3\left(Z_3 + 2Y_3\right)^3}{Y_3^3\left(2Z_3 + Y_3\right)}. \end{aligned} \tag{30}$$

To avoid inversions, projective versions of (30) are

$$\begin{aligned} A' &= AY_3\left(Y_3 + 2Z_3\right)^3, \\ D' &= AZ_3\left(Z_3 + 2Y_3\right)^3, \\ C' &= C^2Y_3^3\left(2Z_3 + Y_3\right), \end{aligned} \tag{31}$$

where $a' = A'/C'$ and $d' = D'/C'$ for $a = A/C$ and $d = D/C$.

3.2. 4 Isogenies on Twisted Edwards Curves. Computing 4 isogenies is more complicated than odd-degree isogenies in twisted Edwards curves. There exist roughly two approaches for computing 4 isogenies in twisted Edwards curves. The first method is to transform twisted Edwards curve to corresponding Weierstrass form and apply Vélu's formula. However, transforming back to twisted Edwards form from Weierstrass form is complicated as square root computations might be required in some cases. The other approach is to use the birational relation between twisted Edwards curves and Montgomery curves. As the transformation between twisted Edwards curves and Montgomery curves costs only two additions, we can compute 4-isogeny on a Montgomery curve and transform back to a twisted Edwards curve. However, when applying the 4-isogeny formula on Montgomery curves proposed by Jao and De Feo, the isomorphism ι that maps 4-torsion point to a specific point must be combined to compute 4-isogeny consecutively [5]. Therefore, after transforming a twisted Edwards curve into a Montgomery curve, the isomorphism must be combined with 4-isogeny.

In summary, the composition we used is as follows:

$$E_{a,d} \xrightarrow{\psi} M_{A,B} \xrightarrow{\iota} M_{A',B'} \xrightarrow{\phi_1} M_{A'',B''} \xrightarrow{\psi'^{-1}} E_{a',d'}, \tag{32}$$

where ψ and ψ'^{-1} are birational maps and ϕ_1 is an isogeny obtained using Vélu's formulas.

Let $P = (X_4 : Y_4 : Z_4)$ be a 4-torsion point on twisted Edwards curve $E_{a,d}$, represented in projective coordinate. The birational map ψ that maps twisted Edwards curve $E_{a,d}$ to Montgomery curve $M_{A,B}$ sends P as follows:

$$\psi\left(Y_4 : Z_4\right) \longrightarrow \left(X_M : Z_M\right) = \left(Y_4 + Z_4 : Z_4 - Y_4\right), \tag{33}$$

where

$$\begin{aligned} A &= \frac{2\left(a + d\right)}{a - d}, \\ B &= \frac{4}{a - d}. \end{aligned} \tag{34}$$

Let $P' = (X_M : Z_M)$ be the corresponding 4-torsion point on $M_{A,B}$. The evaluation of 4-isogeny $\phi = \phi_1 \circ \iota$ on $M_{A,B}$ with kernel $\langle P' \rangle$ is defined as in [10].

$$\begin{aligned} \left(X' : Z'\right) = \Big(&X\left(2X_MZ_MZ - X\left(X_M^2 + Z_M^2\right)\right) \\ &\cdot \left(X_MX - Z_MZ\right)^2 : \\ &Z\left(2X_MZ_MX - Z\left(X_M^2 + Z_M^2\right)\right)\left(Z_MX - X_MZ\right)^2\Big). \end{aligned} \tag{35}$$

Note that this formula is already combined with the isomorphism ι so that additional transform is not necessary. Finally, the birational map ψ'^{-1}, which maps the Montgomery curve back to the twisted Edwards curve $E_{a',d'}$, is defined as follows:

$$\psi'^{-1}\left(X' : Z'\right) \longrightarrow \left(Y' : Z'\right) = \left(X' - Z' : X' + Z'\right). \tag{36}$$

The curve coefficients a' and d' of the image curve $E_{a',d'}$ are given by

$$\begin{aligned} a' &= \frac{A + 2}{B}, \\ d' &= \frac{A - 2}{B}. \end{aligned} \tag{37}$$

Combining the three maps ψ, ϕ, and ψ'^{-1} yields 4-isogeny from $E_{a,d}$ to $E_{a',d'}$. The equation below is the evaluation of the 4-isogeny by computing $(Y' : Z')$, given the additional point $(Y : Z)$ on $E_{a,d}$.

$$\begin{aligned} Y' &= X\left(2X_MZ_MZ - X\left(X_M^2 + Z_M^2\right)\right) \\ &\quad \cdot \left(X_MX - Z_MZ\right)^2 \\ &\quad - Z\left(2X_MZ_MX - Z\left(X_M^2 + Z_M^2\right)\right) \\ &\quad \cdot \left(Z_MX - X_MZ\right)^2, \\ Z' &= X\left(2X_MZ_MZ - X\left(X_M^2 + Z_M^2\right)\right) \\ &\quad \cdot \left(X_MX - Z_MZ\right)^2 \\ &\quad + Z\left(2X_MZ_MX - Z\left(X_M^2 + Z_M^2\right)\right) \\ &\quad \cdot \left(Z_MX - X_MZ\right)^2. \end{aligned} \tag{38}$$

Simplifying the above equations by substituting $X_M = Y_4 + Z_4$ and $Z_M = Z_4 - Y_4$, we have

$$\begin{aligned} Y' &= \left(Z^2Y_4^2 + Y^2Z_4^2\right)YZ\left(Y_4 + Z_4\right)^2, \\ Z' &= \left(Z^2Y_4^2 + Y^2Z_4^2\right)^2 + 2Y^2Z^2Y_4Z_4\left(Y_4^2 + Z_4^2\right). \end{aligned} \tag{39}$$

We now describe the evaluation of the curve coefficients of the image curve. For the 4-torsion point $P = (X_4 : Y_4 : Z_4)$ on the twisted Edwards curve $E_{a,d}$, birational map is used to transform into the Montgomery form $M_{A,B}$. The curve coefficients, as well as the image of P and $[2]P$, are as given below.

$$\begin{aligned} A &= \frac{2(a+d)}{a-d}, \\ B &= \frac{4}{a-d}, \\ \psi(P) &= (X_M : Z_M), \\ \psi([2]P) &= (X_0 : Z_0). \end{aligned} \tag{40}$$

Here $X_M = Y_4 + Z_4$, $Z_M = Z_4 - Y_4$, $X_0 = (X_M + Z_M)^2 (X_M - Z_M)^2$, and $Z_0 = 4X_M Z_M ((X_M - Z_M)^2 + ((A+2)/4)(4X_M Z_M))$ in the above equation. Next, the isomorphism ι sends $\psi(P)$ to a point of the form $(1, \dots)$ and $\psi([2]P)$ to $(0,0)$. The coefficients of the corresponding image curve $M_{A',B'}$ are

$$\begin{aligned} A' &= \frac{Z_M (3X_0 + AZ_0)}{X_M Z_0 - Z_M X_0}, \\ B' &= \frac{BZ_M Z_0}{X_M Z_0 - Z_M X_0}. \end{aligned} \tag{41}$$

Then, by combining the isogeny ϕ_1, coefficients of the image curve are given below.

$$\begin{aligned} A'' &= \frac{-2(A'+6)}{2-A'} \\ &= \frac{2(AZ_M Z_0 - 3Z_M X_0 + 6X_M Z_0)}{AZ_M Z_0 + 5Z_M X_0 - 2X_M Z_0}, \end{aligned} \tag{42}$$

$$B'' = \frac{B'}{2-A'} = \frac{-BZ_M Z_0}{AZ_M Z_0 + 5Z_M X_0 - 2X_M Z_0}. \tag{43}$$

Finally, by applying the birational map to transform back to the twisted Edwards curve, we obtain the coefficients of the 4-isogeny twisted Edwards curve. Let $E_{a',d'} = E_{a,d}/\langle P \rangle$ be the image curve. Then we have

$$a' = \frac{A''+2}{B''} = \frac{-4(AZ_M Z_0 + Z_M X_0 + 2X_M Z_0)}{BZ_M Z_0}, \tag{44}$$

$$d' = \frac{A''-2}{B''} = \frac{-16(Z_M X_0 - X_M Z_0)}{BZ_M Z_0}. \tag{45}$$

Since X_M/Z_M is a root of the 4-division polynomial $\phi_4 = x^4 + 2Ax^3 + 6x^2 + 2Ax + 1$ of a Montgomery curve $M_{A,B}$, we can express A in terms of X_M and Z_M. Simplifying the above equation with expression in terms of Y_4 and Z_4, we have

$$\begin{aligned} A' &= A(Y_4 + Z_4)^4, \\ D' &= 8AY_4 Z_4 (Y_4^2 + Z_4^2), \\ C' &= CY_4^4. \end{aligned} \tag{46}$$

4. The Proposed Isogeny Computations on Edwards Curves

In this section, we present 3- and 4-isogeny formulas on Edwards curves. Recall that 2-isogeny on twisted Edwards curves requires square root computation when transforming back to twisted Edwards curves [17]. Hence, we assumed twisted Edwards curves to have a 4-torsion point by restricting the order of the field. However, every elliptic curve having a 4-torsion point is birationally equivalent to Edwards curves [14]. Therefore, twisted Edwards curves having a 4-torsion point are in fact Edwards curves, with the curve coefficient $a = 1$. Since the number of curve coefficients is reduced, the proposed isogeny formulas can further be optimized.

4.1. 3 Isogenies on Edwards Curves. Let $P = (\alpha, \beta)$ be a 3-torsion point on Edwards curve E_d, where $\beta = Y_3/Z_3$. Let $\phi : E_d \longrightarrow E_{d'}$ be a 3-isogeny generated by a kernel $\langle P \rangle$, so that $E_{d'} = E_d/\langle P \rangle$. Since (29) is independent of the curve coefficients, 3-isogeny formula on Edwards curve is identical to 3-isogeny on twisted Edwards curves. The curve coefficient of the isogenous curve $E_{d'}$ is

$$\begin{aligned} d' = \beta^8 d^3 &= \left(\frac{Y_3}{Z_3}\right)^8 \left(\frac{Z_3^3 (Z_3 + 2Y_3)}{Y_3^3 (2Z_3 + Y_3)}\right)^3 \\ &= \frac{(Z_3 + 2Y_3)^3 Z_3}{(2Z_3 + Y_3)^3 Y_3}. \end{aligned} \tag{47}$$

Therefore, in projective coordinates,

$$\begin{aligned} D' &= (Z_3 + 2Y_3)^3 Z_3, \\ C' &= (2Z_3 + Y_3)^3 Y_3. \end{aligned} \tag{48}$$

4.2. 4 Isogenies on Edwards Curves. Similar to the case for computing 3-isogeny on Edwards curves, only the formula for computing image curve coefficient is changed when computing 4-isogeny on Edwards curves. By setting $a = 1$ and starting from (34), we have

$$\begin{aligned} D' &= 8Y_4 Z_4 (Y_4^2 + Z_4^2), \\ C' &= (Y_4 + Z_4)^4. \end{aligned} \tag{49}$$

To conclude, note that all of our formulas are given in terms of projective YZ-coordinates. Since point operations such as doubling and tripling on Edwards curves can be performed by YZ-coordinates, our formulas are well-adjusted to the isogeny-based cryptosystem.

4.3. Algorithms for Computing Isogenies on Edwards Curves. This section presents an efficient way to compute three and four isogenies on Edwards curves. In order to evaluate 3-isogeny efficiently, consider the difference between Y and Z

```
Require: 3-torsion point $P = (Y_3 : Z_3)$ and a curve point $Q = (Y : Z)$ on $E_d$
Ensure: Image point $Q' = (Y' : Z')$ on $E_{d'}$ and curve coefficients $C', D'$ of the image curve $E_{d'}$ where $d' = D'/C'$
$t_0 \longleftarrow Z \cdot Y_3$          // $t_0 = ZY_3$
$t_1 \longleftarrow Y \cdot Z_3$          // $t_1 = YZ_3$
$t_2 \longleftarrow t_0 + t_1$            // $t_2 = ZY_3 + YZ_3$
$t_3 \longleftarrow Y + Z$                // $t_3 = Y + Z$
$t_2 \longleftarrow t_2^2$                // $t_2 = (ZY_3 + YZ_3)^2$
$t_2 \longleftarrow t_2 \cdot t_3$        // $t_2 = (ZY_3 + YZ_3)^2(Y + Z)$
$t_0 \longleftarrow t_0 - t_1$            // $t_0 = ZY_3 - YZ_3$
$t_0 \longleftarrow t_0^2$                // $t_0 = (ZY_3 - YZ_3)^2$
$t_1 \longleftarrow Y - Z$                // $t_1 = Y - Z$
$t_0 \longleftarrow t_0 \cdot t_1$        // $t_0 = (ZY_3 - YZ_3)^2(Y - Z)$
$Y' \longleftarrow t_0 + t_2$             // $Y' = 2Y(Z^2Y_3^2 + 2Z^2Y_3Z_3 + Y^2Z_3^2)$
$Z' \longleftarrow t_2 - t_0$             // $Z' = 2Z(Z^2Y_3^2 + 2Y^2Y_3Z_3 + Y^2Z_3^2)$
$c_0 \longleftarrow Y_3 + Z_3$            // $c_0 = Y_3 + Z_3$
$c_0 \longleftarrow c_0^2$                // $c_0 = (Y_3 + Z_3)^2$
$c_1 \longleftarrow Y_3^2$                // $c_1 = Y_3^2$
$c_2 \longleftarrow Z_3^2$                // $c_2 = Z_3^2$
$c_3 \longleftarrow c_0 - c_1 - c_2$      // $c_3 = 2Y_3Z_3$
$t_0 \longleftarrow c_1 + c_1$            // $t_0 = 2Y_3^2$
$t_0 \longleftarrow t_0 + c_1$            // $t_0 = 2Y_3^2 + Y_3^2$
$t_1 \longleftarrow c_0 + c_3$            // $t_1 = (Y_3 + Z_3)^2 + 2Y_3Z_3$
$t_1 \longleftarrow t_1 + t_0$            // $t_1 = Z_3^2 + 4Y_3Z_3 + 4Y_3^2$
$t_0 \longleftarrow c_2 + c_3$            // $t_0 = Z_3^2 + 2Y_3Z_3$
$D' \longleftarrow t_0 \cdot t_1$         // $D' = (Z_3 + 2Y_3)^2(Z_3^2 + 2Y_3Z_3)$
$t_0 \longleftarrow c_1 - c_2$            // $t_0 = Y_3^2 - Z_3^2$
$t_1 \longleftarrow c_3 + c_3$            // $t_1 = 4Y_3Z_3$
$t_1 \longleftarrow c_0 - t_1$            // $t_1 = (Y_3 - Z_3)^2$
$t_0 \longleftarrow t_0 \cdot t_1$        // $t_0 = (Y_3^2 - Z_3^2)(Y_3 - Z_3)^2$
$C' \longleftarrow D' + t_0$              // $C' = (2Z_3 + Y_3)^3Y_3$
return $Y', Z', C', D'$
```

Algorithm 1: Computing 3-isogeny on Edwards curves.

coordinates. Let $F = Y' + Z'$ and $G = Y' - Z'$, where Y' and Z' are defined as in (29). Then, F and G are given by

$$F = (ZY_3 + YZ_3)^2 (Y + Z), \qquad G = (ZY_3 - YZ_3)^2 (Y - Z). \tag{50}$$

Therefore, Y' and Z' can be obtained alternatively by computing $Y' = F + G$ and $Z' = F - G$. To compute the coefficients of the image curve, (48) can be rewritten as

$$\begin{aligned} D' &= (Z_3 + 2Y_3)^3 Z_3 \\ &= \left(Z_3^2 + 4Y_3Z_3 + 4Y_3^2\right)\left(Z_3^2 + 2Y_3Z_3\right), \\ C' &= (2Z_3 + Y_3)^3 Y_3 = D' + \left(Y_3^2 - Z_3^2\right)(Y_3 - Z_3)^2. \end{aligned} \tag{51}$$

Hence, when values $Z_3^2, Y_3^2, (Y_3 + Z_3)^2$, and $2Y_3Z_3$ are computed, D' and C' can be computed with two field multiplications. Algorithm 1 shows an efficient way to compute 3-isogeny and its corresponding curve coefficients. The total cost for Algorithm 1 is 6**M**+5**S**.

Next, to compute 4-isogeny formula on Edwards curves, let $F' = Y' + Z'$ and $G' = Y' - Z'$, where Y' and Z' are defined as in (39). Then F' and G' can be written as

$$\begin{aligned} F' &= \left(YZ\left(Y_4^2 + Z_4^2\right) + \left(Y^2Z_4^2 + Z^2Y_4^2\right)\right)(ZY_4 + YZ_4)^2, \\ G' &= \left(YZ\left(Y_4^2 + Z_4^2\right) - \left(Y^2Z_4^2 + Z^2Y_4^2\right)\right)(ZY_4 - YZ_4)^2. \end{aligned} \tag{52}$$

Therefore, Y' and Z' can be obtained alternatively by computing $Y' = F' + G'$ and $Z' = F' - G'$. Also, note that D' in (49) equals to

$$D' = (Y_4 + Z_4)^4 - (Y_4 - Z_4)^4 = C' - (Y_4 - Z_4)^4. \tag{53}$$

The coefficients of the image curve can be computed more efficiently using the above equation. The algorithm for computing 4-isogeny and its corresponding curve coefficients is described in Algorithm 2. The total cost for Algorithm 2 is 7**M**+5**S**.

```
**Require**: 4-torsion point $P = (Y_4 : Z_4)$ and curve point $Q = (Y : Z)$ on $E_d$
**Ensure**: Image point $Q' = (Y' : Z')$ on $E_{d'}$ and curve coefficients $C', D'$ of the image curve $E_{d'}$ where $d' = D'/C'$
$t_0 \longleftarrow Z \cdot Y_4$          // $t_0 = ZY_4$
$t_1 \longleftarrow Y \cdot Z_4$          // $t_1 = YZ_4$
$t_2 \longleftarrow t_0 \cdot t_1$        // $t_2 = YZY_4Z_4$
$t_2 \longleftarrow t_2 + t_2$            // $t_2 = 2YZY_4Z_4$
$t_3 \longleftarrow t_0 + t_1$            // $t_3 = YZ_4 + ZY_4$
$t_3 \longleftarrow t_3^2$                // $t_3 = (YZ_4 + ZY_4)^2$
$t_5 \longleftarrow t_3 - t_2$            // $t_5 = Y^2Z_4^2 + Z^2Y_4^2$
$t_4 \longleftarrow Y \cdot Z$            // $t_4 = YZ$
$c_0 \longleftarrow Y_4 + Z_4$            // $c_0 = Y_4 + Z_4$
$c_0 \longleftarrow c_0^2$                // $c_0 = (Y_4 + Z_4)^2$
$t_4 \longleftarrow t_4 \cdot c_0$        // $t_4 = YZ(Y_4 + Z_4)^2$
$t_4 \longleftarrow t_4 - t_2$            // $t_4 = YZ(Y_4^2 + Z_4^2)$
$Y' \longleftarrow t_4 + t_5$             // $Y' = YZ(Y_4^2 + Z_4^2) + (Y^2Z_4^2 + Z^2Y_4^2)$
$Z' \longleftarrow t_4 - t_5$             // $Z' = YZ(Y_4^2 + Z_4^2) - (Y^2Z_4^2 + Z^2Y_4^2)$
$t_0 \longleftarrow Y' \cdot t_3$         // $t_0 = F'$
$t_3 \longleftarrow t_5 - t_2$            // $t_3 = (YZ_4 - ZY_4)^2$
$t_1 \longleftarrow Z' \cdot t_3$         // $t_1 = G'$
$Y' \longleftarrow t_0 + t_1$             // $Y' = 2(Z^2Y_4^2 + Y^2Z_4^2)YZ(Y_4 + Z_4)^2$
$Z' \longleftarrow t_0 - t_1$             // $Z' = 2(Z^2Y_4^2 + Y^2Z_4^2)^2 + 4Y^2Z^2Y_4Z_4(Y_4^2 + Z_4^2)$
$C' \longleftarrow c_0^2$                 // $C' = (Y_4 + Z_4)^4$
$c_0 \longleftarrow Y_4 - Z_4$            // $c_0 = (Y_4 - Z_4)$
$c_0 \longleftarrow c_0^2$                // $c_0 = (Y_4 - Z_4)^2$
$c_0 \longleftarrow c_0^2$                // $c_0 = (Y_4 - Z_4)^4$
$D' \longleftarrow C' - c_0$              // $D' = 8Y_4Z_4(Y_4^2 + Z_4^2)$
return $Y', Z', C', D'$
```

Algorithm 2: Constructing 4-isogeny on Edwards curves.

4.4. Implementation Results. To evaluate the performance of the proposed formulas, the algorithms are implemented in C language. We used the isogeny formula implemented in SIDH library version 3.0 for isogenies on Montgomery curves. Moreover, to make an exact comparison with isogenies on Montgomery curves, the field operations implemented in SIDH library were used for both curves. The field operations in SIDH library are written in x64 assembly [18]. As a result, the difference in performance lies purely in the computation of isogenies. All cycle counts were obtained on one core of an Intel Core i7-6700 (Skylake) at 3.40 GHz, running Ubuntu 16.04 LTS. For compilation, we used GNU GCC version 5.4.0.

In this section, the field K is fixed as $K = \mathbb{F}_{p^2}$, where p is prime, and $\mathbb{F}_{p^2} = \mathbb{F}_{p^2}[X]/(X^2 + 1)$. For the prime p, we used 503-bit prime $p_{503} = 2^{250} \cdot 3^{159} - 1$ and 751-bit prime $p_{751} = 2^{372} \cdot 3^{239} - 1$, presented in [13, 18]. The base field operations were tested in order to visualize the ratio between field operations. To this end, each field operation was repeated 10^8 times for each prime field. Table 1 summarizes the average cycle counts of field operations over $\mathbb{F}_{p^2}$.

As in Table 1, 1**S** equals approximately 0.8**M**, for both 503-bit prime and 751-bit prime. Based on the above result, Table 2 shows the computational cost and corresponding cycle counts of 3 and 4 isogenies, when using Montgomery curves and Edwards curves. For each isogeny computation, we report the average cycles of 10^8 times. Note that the number of field multiplications and squarings are same for 3-isogeny. Therefore, to better represent the results, we also counted field additions and subtractions. In Table 2, **a** (resp., **s**) refers to field addition (resp., subtraction).

Note that the base field operations in [18] run in constant time to protect against timing attacks [24]; field additions cost more cycles than field subtractions. Therefore, 3-isogeny on Edwards curves are slightly faster than on Montgomery curves. Overall, because the proposed algorithms used field subtractions more than field additions, the performance gap between Montgomery curves and Edwards curves is small.

5. Conclusion and Future Work

In this paper, we proposed 3- and 4-isogeny formulas on twisted Edwards curves that can be applied in isogeny-based cryptography. For 3-isogeny, we optimized Moody and Shumow's formula by applying projective coordinates, projective curve coefficients, and division polynomials [17]. For even-degree isogeny, we combined bilinear map between twisted Edwards curves and Montgomery curves and isogeny on Montgomery curves. We further optimized our isogeny formulas by working on with Edwards curves. The computational costs for 3 and 4 isogenies on Edward curves are 6**M**+5**S** and 7**M**+5**S**, respectively. We also implemented our formulas and demonstrated that isogenies on Edwards curves are as efficient as isogenies on Montgomery curves. For the future work, we plan to implement our isogeny formulas on

Table 1: Cycle counts of the field operations over $\mathbb{F}_{p^2}$.

Field size	Addition	Subtraction	Multiplication	Squaring
p_{503}	79	62	795	640
p_{751}	120	102	1593	1260

Table 2: Implementation results of 3 and 4 isogenies on Montgomery curves and Edwards curves (cc represents the number of clock cycles).

	3-isogeny		4-isogeny	
	p_{503}	p_{751}	p_{503}	p_{751}
Montgomery curves [18]	$6\mathbf{M}+5\mathbf{S}+14\mathbf{a}+5\mathbf{s}$		$6\mathbf{M}+6\mathbf{S}+7\mathbf{a}+4\mathbf{s}$	
	8,931 cc	17,833 cc	9,146 cc	16,375 cc
Edwards curves (This Work)	$6\mathbf{M}+5\mathbf{S}+11\mathbf{a}+7\mathbf{s}$		$7\mathbf{M}+5\mathbf{S}+4\mathbf{a}+7\mathbf{s}$	
	8,843 cc	17,644 cc	9,363 cc	16,542 cc

isogeny-based cryptosystem and measure its performance. Additionally, we plan to consider isogeny formulas on other forms of elliptic curves and report the best isogeny degree for isogeny-based cryptography.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (no. NRF-2017R1A2B4011599).

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[2] J. M. Couveignes, "Hard homogeneous spaces," *IACR Cryptology ePrint Archive*, vol. 291, 2006.

[3] A. Stolbunov, "Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves," *Advances in Mathematics of Communications*, vol. 4, no. 2, pp. 215–235, 2010.

[4] A. Childs, D. Jao, and V. Soukharev, "Constructing elliptic curve isogenies in quantum subexponential time," *Journal of Mathematical Cryptology*, vol. 8, no. 1, pp. 1–29, 2014.

[5] D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *Post-quantum cryptography*, vol. 7071 of *Lecture Notes in Comput. Sci.*, pp. 19–34, Springer, Heidelberg, 2011.

[6] R. Azarderakhsh, D. Jao, K. Kalach, B. Koziel, and C. Leonardi, "Key compression for isogeny-based cryptosystems," in *Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography*, pp. 1–10.

[7] C. Costello, D. Jao, P. Longa, M. Naehrig, J. Renes, and D. Urbanik, "Efficient compression of sidh public keys," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 679–706, Springer, 2017.

[8] R. Azarderakhsh, B. Koziel, and S. H. F. Langroudi, "Fpga-sidh: High-performance implementation of supersingular isogeny diffie-hellman key-exchange protocol on fpga," *IACR Cryptology ePrint Archive*, vol. 672, 2016.

[9] B. Koziel, A. Jalali, R. Azarderakhsh, D. Jao, and M. Mozaffari-Kermani, "Neon-sidh: efficient implementation of supersingular isogeny diffie-hellman key exchange protocol on arm," in *International Conference on Cryptology and Network Security*, pp. 88–103, Springer, 2016.

[10] C. Costello, P. Longa, and M. Naehrig, "Efficient algorithms for supersingular isogeny diffie-hellman," in *Annual Cryptology Conference*, pp. 572–601, Springer, 2016.

[11] S. D. Galbraith, C. Petit, and J. Silva, "Identification protocols and signature schemes based on supersingular isogeny problems," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 3–33, Springer, 2017.

[12] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, and V. Soukharev, "A post-quantum digital signature scheme based on supersingular isogenies," in *Financial cryptography and data security*, vol. 10322 of *Lecture Notes in Comput. Sci.*, pp. 163–181, Springer, Cham, 2017.

[13] R. Azarderakhsh, M. Campagna, C. Costello et al., "Supersingular isogeny key encapsulation. submission to the nist post-quantum standardization project," 2017.

[14] D. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, "Twisted Edwards curves," in *International Conference on Cryptology in Africa*, vol. 5023, pp. 389–405, Springer, 2008.

[15] C. Costello and H. Hisil, "A simple and compact algorithm for sidh with arbitrary degree isogenies," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 303–329, Springer, 2017.

[16] M. Meyer, S. Reith, and F. Campos, On hybrid sidh schemes using edwards and montgomery curve arithmetic,.

[17] 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.

[18] C. Costello, P. Longa, and M. Naehrig, "Sidh library," 2016.

[19] K. Okeya, H. Kurumatani, and K. Sakurai, "Elliptic curves with the Montgomery-form and their cryptographic applications," in *Public key cryptography (MELbourne, 2000)*, vol. 1751 of *Lecture Notes in Comput. Sci.*, pp. 238–257, Springer, Berlin, 2000.

[20] I. E. Shparlinski and A. V. Sutherland, “On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average,” *LMS Journal of Computation and Mathematics*, vol. 18, no. 01, pp. 308–322, 2015.

[21] R. R. Farashahi, I. E. Shparlinski, and J. F. Voloch, “On hashing into elliptic curves,” *Journal of Mathematical Cryptology*, vol. 3, no. 4, 2009.

[22] J. Vélu, “Isogénies entre courbes elliptiques,” *Comptes Rendus Mathematique Academie des Sciences, Paris*, vol. 273, pp. 238–241, 1971.

[23] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields [Ph.D. Thesis]*, University of California, Berkeley, Calif, USA, 1996.

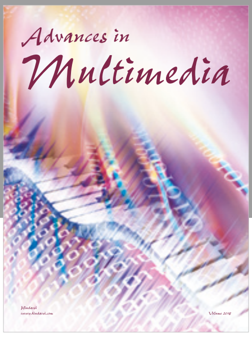
[24] P. C. Kocher, “Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems,” in *Annual International Cryptology Conference*, pp. 104–113, Springer, 1996.

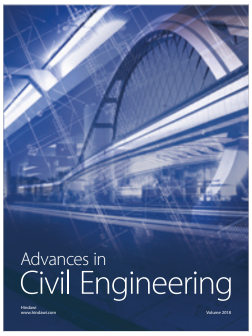
Journal of
Engineering

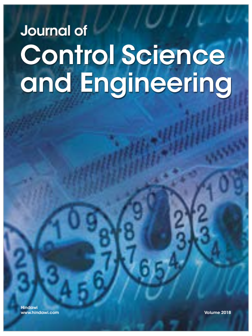
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

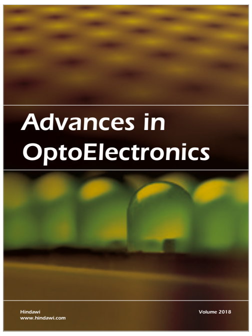

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

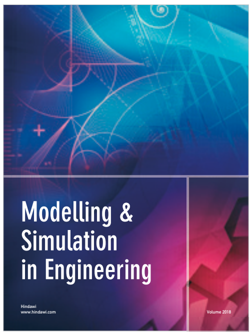
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

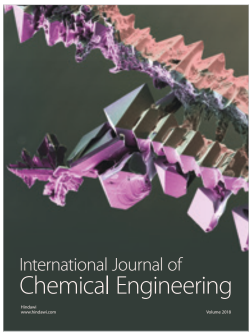

Advances in
OptoElectronics

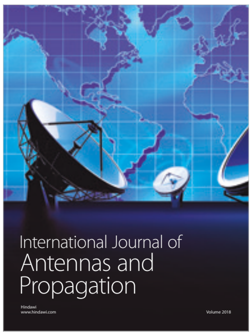
VLSI Design

International Journal of
Navigation and
Observation

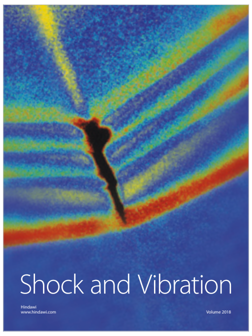

Modelling &
Simulation
in Engineering

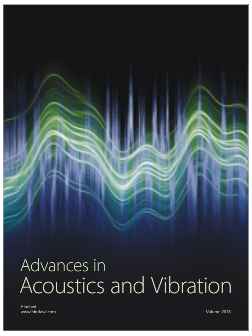
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration