The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography

Tomoki Moriya[1], Hiroshi Onuki[1], Yusuke Aikawa[2], and Tsuyoshi Takagi[1]

[1] Department of Mathematical Informatics, The University of Tokyo, Japan
{tomoki_moriya,onuki,takagi}@mist.i.u-tokyo.ac.jp
[2] Information Technology R&D Center, Mistubishi Electric Corporation, Japan
Aikawa.Yusuke@bc.mitsubishielectric.co.jp

Abstract. Isogeny-based cryptography is one of the main candidates of post-quantum cryptography. To realize efficient computations, one usually uses formulas of scalar multiplications and isogeny computations on elliptic curves using only one coordinate in isogeny-based cryptography. The x-coordinate of Montgomery curves is the most standard, and we sometimes use the x-coordinate of Montgomery$^-$ curves, the w-coordinate of Edwards curves, and the w-coordinate of Huff's curves.
In this paper, we define a novel function on elliptic curves called the generalized Montgomery coordinate that has the four coordinates described above as special cases. For a generalized Montgomery coordinate, we construct an explicit formula of scalar multiplication which includes the division polynomial, and both a formula of an image point under an isogeny and that of a coefficient of the codomain curve.
Finally, we expect numerous applications for the generalized Montgomery coefficient. As an experimental study, we present two applications of the theory of a generalized Montgomery coordinate. The first one is to construct a new efficient formula to compute isogenies on Montgomery curves. This formula is more efficient than the previous one for high degree isogenies as the $\sqrt{}$élu's formula in our implementation. The second one is to construct a new generalized Montgomery coordinate for Montgomery$^-$ curves used for CSURF.

Keywords: isogeny-based cryptography · Vélu's formulas · elliptic curves · generalized Montgomery coordinates

1 Introduction

In 1994, Shor revealed that the currently used public key cryptosystems can be broken by quantum computers [Sho94]. Therefore, we need to develop new cryptosystems that are resistant to cryptanalysis by both classical computers and quantum computers. Isogeny-based cryptography is considered as one of the important candidates of post-quantum cryptography due to its compactness. Indeed, isogeny-based key encapsulation, SIKE [ACC$^+$17], is listed in the NIST

Table 1. Previous results on one-coordinate arithmetic

Forms	Scalar multiplication	Isogeny computation
Montgomery	Montgomery [Mon87]	Renes [Ren18], Costello and Hisil [CH17]
Montgomery$^-$	Castryck and Decru [CD20]	
Edwards	Farashahi and Hosseini [FH17]	Kim *et al.* [KYPH19]
Huff	Huang *et al.* [HZHL20], Dryło, Kijko, and Wroński [DKW20]	
Twisted Jacobi intersections	Hu, Wang, and Zhou [HWZ21]	

post-quantum cryptography 3rd round competition [oST16]. An advantage of isogeny-based cryptography is that their key sizes are smaller than those of other NIST 3rd round candidates of post-quantum cryptography. In contrast, isogeny-based cryptography requires more computational costs for execution than other candidates because, to compute isogenies, we use modular polynomials or Vélu's formulas, which are costly calculations.

In 2006, Rostovtsev and Stolbunov [RS06,Sto10] and Couveignes [Cou06] proposed the first cryptosystem based on the hardness of computing isogenies using a class group action on ordinary curves. However, this scheme is infeasible because of the difficulty in constructing suitable curves for efficient isogeny computation. Charles, Lauter, and Goren proposed the first isogeny-based hash function called the CGL hash function [CLG09]. This is the first practical isogeny-based scheme that uses supersingular elliptic curves. In 2011, Jao and De Feo proposed a Diffie-Hellman style key exchange scheme from supersingular isogenies, SIDH [JDF11]. Castryck *et al.* proposed another isogeny-based key exchange scheme called CSIDH based on a commutative group action on supersingular curves [CLM$^+$18]. Castryck and Decru proposed an efficient variant of CSIDH using 2-isogenies called CSURF [CD20]. Due to its algebraic structure, some digital signatures and public key encryptions are constructed based on CSIDH (*e.g.,* SeaSign [DFG19], CSI-FiSh [BKV19], SiGamal [MOT20b], and SimS [FP21]). Recently, in 2020, De Feo *et al.* proposed a novel isogeny-based digital signature called SQISign [DFKL$^+$20].

The main part of algorithms in isogeny-based cryptosystems consists of scalar multiplications on elliptic curves and isogeny computations. One typically uses Vélu's formulas [Vél71] to compute isogenies. In pursuit of efficiency of the formulas, many one-coordinate Vélu-type formulas have been constructed. For example, formulas based on the x-coordinates of Montgomery curves, on the w-coordinates of Edwards curves, on the w-coordinates of Huff's curves, and on the ω-coordinates of twisted Jacobi intersections curves are known. These constructions have been performed individually. Table 1 summarizes such studies. In addition to these, there exist formulas for twisted Hessian curves in [FJ10,BCKL15,BDFM21]. Because these formulas use two coordinates, these are out of scope of this study.

For each of the coordinates, there are studies constructing efficient formulas. Meyer and Reith constructed efficient formulas for isogeny computations on the

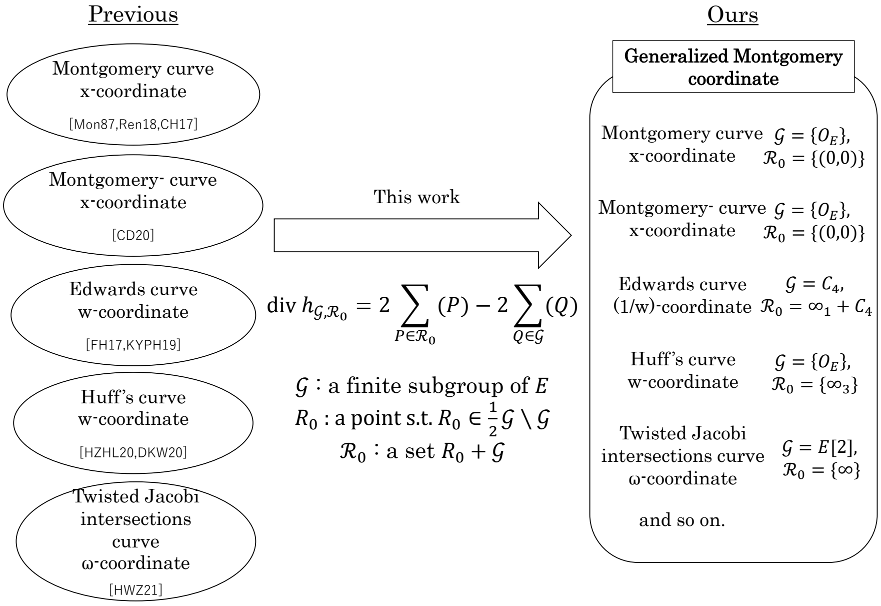
Previous
Montgomery curve x-coordinate
[Mon87,Ren18,CH17]
Montgomery- curve x-coordinate
[CD20]
Edwards curve w-coordinate
[FH17,KYPH19]
Huff's curve w-coordinate
[HZHL20,DKW20]
Twisted Jacobi intersections curve ω-coordinate
[HWZ21]
This work
$\operatorname{div} h_{\mathcal{G},\mathcal{R}_0} = 2\sum_{P\in\mathcal{R}_0}(P) - 2\sum_{Q\in\mathcal{G}}(Q)$
$\mathcal{G}$: a finite subgroup of E
R_0 : a point s.t. $R_0 \in \frac{1}{2}\mathcal{G} \setminus \mathcal{G}$
$\mathcal{R}_0$: a set $R_0 + \mathcal{G}$
Ours
Generalized Montgomery coordinate
Montgomery curve x-coordinate $\mathcal{G} = \{O_E\}$, $\mathcal{R}_0 = \{(0,0)\}$
Montgomery- curve x-coordinate $\mathcal{G} = \{O_E\}$, $\mathcal{R}_0 = \{(0,0)\}$
Edwards curve (1/w)-coordinate $\mathcal{G} = C_4$, $\mathcal{R}_0 = \infty_1 + C_4$
Huff's curve w-coordinate $\mathcal{G} = \{O_E\}$, $\mathcal{R}_0 = \{\infty_3\}$
Twisted Jacobi intersections curve ω-coordinate $\mathcal{G} = E[2]$, $\mathcal{R}_0 = \{\infty\}$
and so on.

Fig. 1. Our unified one-coordinate formulas

x-coordinate of Montgomery curves [MR18], and Bernstein *et al.* developed a method to compute this formula in $\tilde{O}(\sqrt{\ell})$ times [BDFLS20], while the original Vélu's formulas are computed in $O(\ell)$ times. They described this method on the x-coordinates of Montgomery curves. This method is extended to the w-coordinate of Edwards curves [MOT20a] and the w-coordinate of Huff's curves [Wro21,Kim21].

As described above, miscellaneous studies have been conducted regarding different coordinates of elliptic curves of various models. However, one can observe that these formulas are very similar. Therefore, we propose the following question:

Can we construct one-coordinate formulas of scalar multiplication and isogeny computation of elliptic curves in a unified way?

By considering the generalization of the x-coordinates of Montgomery curves, we can define a generalized coordinate of elliptic curves, and construct a generalized formula to compute scalar multiplications and isogeny computations.

1.1 Contribution

In this work, we give an affirmative answer to the above research question. We contribute to the literature by improving the visibility of the isogeny computation of different forms of elliptic curves (see Figure 1).

The core of our work is that we introduce a novel function on elliptic curves, which we call a generalized Montgomery coordinate (Definition 1). This is a generalization of coordinates which can be used in isogeny-based cryptography, *i.e.*, the x-coordinates of Montgomery curves, the x-coordinates of Montgomery$^-$ curves, the w-coordinates of Edwards curves, and the w-coordinates of Huff's curves. One can see that these coordinates have similar divisors, and thus, we can obtain a generalization of these coordinates by considering divisors with the appropriate form. In particular, the set of poles and zero points of these coordinates can be seen as a finite subgroup $\mathcal{G}$ of elliptic curve E and the shifted set of $\mathcal{G}$ by one point in E, respectively. More precisely, a generalized Montgomery coordinate for an elliptic curve E can be defined by specifying a finite subgroup $\mathcal{G} \subset E$ as poles and a set $\mathcal{R}_0 = R_0 + \mathcal{G}$ as zero points, where R_0 is a point such that $2R_0 \in \mathcal{G}$ and $R_0 \notin \mathcal{G}$. Indeed, we can show that a generalized Montgomery coordinate is essentially the same as the composition of an isogeny and the x-coordinate of a (standard) Montgomery curve (Theorem 12).

Moreover, we construct explicit formulas for scalar multiplications and isogeny computations, which are required for any scheme of isogeny-based cryptography, via a generalized Montgomery coordinate. There are two formulas to construct a formula for scalar multiplication: one is the formula of pseudo addition, and the other is that of pseudo doubling. We construct both formulas by considering the divisors of the functions of the computational results of each formula. For example, the pseudo doubling formula is constructed from the divisor of the function $h \circ [2]$, where h is a generalized Montgomery coordinate. This method of construction has a high affinity with the definition of a generalized Montgomery coordinate. Furthermore, two formulas exist to construct the formula of isogeny computation: one is the formula of computing an image point under an isogeny, and the other is that of computing a coefficient of a codomain curve under an isogeny. We construct the first formula in the same way as the formula of scalar multiplication. In contrast, the second formula is constructed from information of a generalized Montgomery coordinate of the codomain curve. Because this formula is not constructed by its divisor, this formula has several representations. In fact, it is known that the formula proposed in [Ren18] and that proposed in [MR18] are different. We prove that this difference is due to the division polynomial of the generalized Montgomery coordinates (Theorem 27).

We believe there are many applications of the theory of a generalized Montgomery coordinate. In this paper, we consider two applications as an initial trial. First, we construct a new efficient formula to compute isogenies on Montgomery curves. This formula is obtained by transplanting the formula of Edwards curves to Montgomery curves and is more efficient than the previous formula for high degree isogenies in our implementation. This method of the construction is easier than considering the isomorphism between Montgomery curves and Edwards curves. Next, we propose a new generalized Montgomery coordinate of Montgomery$^-$ curves called the w-coordinate. We can construct a new algorithm of CSURF via the w-coordinate. Some accelerating techniques exist in previous algorithms of CSURF, and we need to consider a proper isogeny from a Montgomery$^-$ curve to a Montgomery curve to use these techniques. However, our proposed algorithm can use these techniques through the w-coordinate without considering any isogenies. Thus, our new algorithm gives a simple implementation of CSURF.

Organization. In Section 2, we introduce some mathematical concepts as preliminaries. In Section 3.1, we define the generalized Montgomery coordinate and basic notations related to it, and in Section 3.2, we prove some important properties of a generalized Montgomery coordinate. Section 3.3 provides some examples of a generalized Montgomery coordinate. We prove theorems of formulas of pseudo addition and pseudo doubling in Section 4.1, and we define division polynomials of the generalized Montgomery coordinates in Section 4.2. In Section 5, we construct formulas to compute isogenies via a generalized Montgomery coordinate. Section 6 shows some applications of the theory of a generalized Montgomery coordinate. Finally, we conclude this paper in Section 7.

2 Preliminaries

In this section, we introduce some important mathematical concepts for our study. The details of the following facts are provided in [Sil09,Gal12].

Let K be a field. An *elliptic curve defined over* K is a pair (E, O_E) of a smooth algebraic curve E defined over K with genus 1 and a point O_E in $E(K)$. It is known that $E(L)$ has a group structure whose identity element is O_E, where L is an algebraic extension field of K. In this paper, we omit the identity point O_E, we fix K, and if not mentioned, we always fix E over $\overline{K}$ (*i.e.,* it is defined over the algebraic closure of K).

Let n be an integer. We denote the multiplication-by-n map between elliptic curves by $[n]$, and denote a point $[n](P)$ by nP. We define the *n-torsion subgroup of* $E(\overline{K})$ as

$$E[n] = \{P \in E(\overline{K}) \mid nP = O_E\}.$$

If $\mathrm{ch}(K) = 0$ or $\mathrm{ch}(K) \nmid n$, then it holds that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Here, $\mathrm{ch}(K)$ is the characteristic of K. For a subset $S \subset E$, we define a set $\frac{1}{2}S$ as follows:

$$\frac{1}{2}S := \{P \in E \mid 2P \in S\}.$$

Let E and E' be elliptic curves defined over K. An *isogeny* $\phi\colon E \to E'$ *defined over* K is a nontrivial morphism defined over K of algebraic curves such that $\phi(O_E) = O_{E'}$. It is known that ϕ is a group morphism of elliptic curves. From an isogeny ϕ, we obtain an injective map $\phi^*\colon \overline{K}(E') \to \overline{K}(E)$, where $\overline{K}(E)$ and $\overline{K}(E')$ are the function fields of E and E' respectively. The *degree of* ϕ denoted by $\deg\phi$ is the degree of the finite extension $\overline{K}(E)/\phi^*(\overline{K}(E'))$. If this extension is separable, then an isogeny ϕ is called a *separable isogeny.* If an isogeny ϕ is separable, it holds that $\deg\phi = \#\ker\phi$. An *ℓ-isogeny* is a separable isogeny whose kernel is a cyclic subgroup of order ℓ. For any isogeny $\phi : E \to E'$, there is an isogeny $\hat{\phi} : E' \to E$ such that $\phi \circ \hat{\phi} = [\deg\phi]\colon E' \to E'$ and $\hat{\phi} \circ \phi = [\deg\phi]\colon E \to E$. This isogeny is called the *dual isogeny of* ϕ. Let G be a finite subgroup of E. There is a unique elliptic curve E/G up to isomorphism and a separable isogeny $\phi\colon E \to E/G$ such that $\ker\phi = G$. Vélu proposed formulas to compute this isogeny in [Vél71]. We call these *Vélu's formulas.*

Let $P \in E$. Let ord_P be the normalized valuation on the local ring of E at P. The *divisor group of an elliptic curve* E is the free commutative group generated by points of E, and a *divisor* is an element of the divisor group of E. Let f be a function in $\overline{K}(E)^\times$. The *divisor of* f, denoted by $\mathrm{div}\, f$, is defined as follows:

$$\mathrm{div}\, f = \sum_{P \in E} \mathrm{ord}_P\,(f)(P).$$

Let $D = \sum n_P(P)$ be a divisor. There is a function $f \in \overline{K}(E)$ such that $D = \mathrm{div}\, f$ if and only if $\sum n_P = 0$ and $\sum n_P P = O_E$ in E. Let g be a function in $\overline{K}(E)^\times$. It holds that $\mathrm{div}\, f = \mathrm{div}\, g$ if and only if there is a constant value $c \in \overline{K}^\times$ such that $f = c \cdot g$.

3 Generalized Montgomery coordinates and their basic properties

In this section, we define a new function on elliptic curves called the generalized Montgomery coordinate. This function gives formulas to compute isogenies, which are independent of the forms of elliptic curves.

For the sake of defining generalized Montgomery coefficients, we need to fix the characteristic of K to other than 2. Hence, in this paper, we always let K be a field whose characteristic is not 2. It is not a problem for isogeny-based cryptography, because fields with large characteristic are always used in it so far.

3.1 Definition of a generalized Montgomery coordinate

In this subsection, we define a generalized Montgomery coordinate.

Before defining a generalized Montgomery coordinate, we consider properties common to the x-coordinate of Montgomery curves, the x-coordinate of Montgomery$^-$ curves, the w-coordinate of Edwards curves, and the w-coordinate of Huff's curves. These curves have several common properties. Particularly, we think that the following four properties are important as coordinates used in computations. Here, we denote a coordinate on an elliptic curve E as h.

i). It holds that $h \in \overline{K}(E)$.

ii). There is a finite subgroup $\mathcal{G} \subset E$ such that

$$h(P) = h(Q) \Longleftrightarrow P + Q \in \mathcal{G} \text{ or } P - Q \in \mathcal{G}.$$

iii). It holds that $h(O_E) = \infty$.

iv). There is a point R_0 satisfying $2R_0 \in \mathcal{G}$ and $h(R_0) = 0$.

Properties iii) and iv) do not hold for the w-coordinates of Edwards curves, but do hold for w^{-1}. The property i) indicates that h is a morphism between E and the projective line $\mathbb{P}^1$. The property ii) claims that $h(P) = h(Q)$ if and only if the addition of P and Q or their subtraction belongs to a finite subgroup $\mathcal{G}$. This property comes from the intuition that coordinates with good symmetry may be related to a subgroup of elliptic curves. This intuition is also found in other papers. For example, Kohel constructed an efficient model of elliptic curves in characteristic 2 based on this intuition [Koh11]. The property iii) means O_E is a pole of h, and the property iv) means there is a zero point of h whose doubling belongs to $\mathcal{G}$.

From the properties ii-iv), we obtain zero points and poles of h. Therefore, we can write down the condition of the divisor of h. By considering the simplest condition of $\operatorname{div} h$, we can construct the following definition of a generalized Montgomery coordinate.

Definition 1 (Generalized Montgomery coordinate). *Let E be an elliptic curve defined over $\overline{K}$. Let $\mathcal{G}$ be a finite subgroup of E, and let R_0 be a point satisfying $R_0 \notin \mathcal{G}$ and $2R_0 \in \mathcal{G}$. We denote a set $R_0 + \mathcal{G} = \{R_0 + P \mid P \in \mathcal{G}\}$ by $\mathcal{R}_0$. If a function $h_{\mathcal{G},\mathcal{R}_0} \in \overline{K}(E)$ satisfies the following equality, we call $h_{\mathcal{G},\mathcal{R}_0}$ a generalized Montgomery coordinate of E with respect to $\mathcal{G}$ and $\mathcal{R}_0$:*

$$\operatorname{div} h_{\mathcal{G},\mathcal{R}_0} = 2\sum_{P\in\mathcal{G}}(P + R_0) - 2\sum_{P\in\mathcal{G}}(P).$$

Remark 2. When we fix $\mathcal{G}$ and $\mathcal{R}_0$, a generalized Montgomery coordinate with respect to $\mathcal{G}$ and $\mathcal{R}_0$ always exists, because it holds that

$$2\sum_{P\in\mathcal{G}} P + (2\#\mathcal{G})R_0 - 2\sum_{P\in\mathcal{G}} P = O_E.$$

Remark 3. The name "generalized Montgomery coordinate" comes from Theorem 12.

Let E be a Montgomery curve, let $\mathcal{G} = \{O_E\}$, and let $\mathcal{R}_0 = \{(0, 0)\}$; then, the x-coordinate of E is a normalized generalized Montgomery coordinate with respect to $\mathcal{G}$ and $\mathcal{R}_0$. As shown in Table 2, other coordinates are also obtained by determining $\mathcal{G}$ and $\mathcal{R}_0$ properly. The definition of a normalized generalized Montgomery coordinate is given in Definition 10. In Subsection 3.3, we show that these coordinates are generalized Montgomery coordinates.

Next, we introduce an important notation regarding a generalized Montgomery coordinate which plays a role as a standard Montgomery coefficient. Before defining this notation, we prove the following lemma.

Lemma 4. *Let E be an elliptic curve, and let $\mathcal{G}$ be a finite subgroup of E. Then, the set $\frac{1}{2}\mathcal{G}$ is a subgroup of E including $\mathcal{G}$ and is decomposed as follows:*

$$\frac{1}{2}\mathcal{G} = \mathcal{G} \sqcup (R_0 + \mathcal{G}) \sqcup (R_1 + \mathcal{G}) \sqcup (R_0 + R_1 + \mathcal{G}),$$

Table 2. Examples of normalized generalized Montgomery coordinates (Definition 1)

Forms	Coordinate	$h_{\mathcal{G},\mathcal{R}_0}$ (normalized)	$\mathcal{G}$	$\mathcal{R}_0$
Montgomery	x	x	$\{O_E\}$	$\{(0,0)\}$
Montgomery$^-$	x	$\sqrt{-1}x$	$\{O_E\}$	$\{(0,0)\}$
Edwards	$w = dx^2y^2$	w^{-1}	C_4	$\infty_1 + C_4$
Huff	$w = 1/(xy)$	w	$\{O_E\}$	$\{\infty_3\}$
Twisted Jacobi intersections	$\omega = \sqrt{ab}x^2$	ω^{-1}	$E[2]$	{points at infinity}

where, $\sqcup$ is a symbol for a disjoint union, R_0 is a point in $\frac{1}{2}\mathcal{G} \setminus \mathcal{G}$, and R_1 is a point in $\frac{1}{2}\mathcal{G} \setminus (\mathcal{G} \sqcup (R_0 + \mathcal{G}))$.

We denote $R_1 + \mathcal{G}$ by $\mathcal{R}_1$.

Proof. Let [2] be a doubling map. Since $[2]^{-1}(\mathcal{G}) = \frac{1}{2}\mathcal{G}$, $\frac{1}{2}\mathcal{G}$ is a subgroup of E. Note that $[2]|_{\frac{1}{2}\mathcal{G}} \colon \frac{1}{2}\mathcal{G} \to \mathcal{G}$ is surjective. As the kernel of $[2]|_{\frac{1}{2}\mathcal{G}}$ is $E[2]$, the index of $\mathcal{G}$ in $\frac{1}{2}\mathcal{G}$ is 4. Since $[2](\frac{1}{2}\mathcal{G}) \subset \mathcal{G}$, it holds that

$$\left(\frac{1}{2}\mathcal{G}\right)/\mathcal{G} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

This completes the proof of Lemma 4. □

Now, we define a generalized Montgomery coefficient.

Definition 5 (Generalized Montgomery coefficient). *Let $(E, h_{\mathcal{G}_E,\mathcal{R}_0})$ be a pair of an elliptic curve defined over K and its generalized Montgomery coordinate. Let $\mathcal{R}_1$ be a set defined in Lemma 4, and let R_1 be a point in $\mathcal{R}_1$. We call a value $\alpha_{h_{\mathcal{G},\mathcal{R}_0}} \in \overline{K}$ defined by*

$$\alpha_{h_{\mathcal{G},\mathcal{R}_0}} = -h_{\mathcal{G},\mathcal{R}_0}(R_1) - \frac{1}{h_{\mathcal{G},\mathcal{R}_0}(R_1)}$$

the generalized Montgomery coefficient of $h_{\mathcal{G},\mathcal{R}_0}$.

Remark 6. We can easily show that $\alpha_{h_{\mathcal{G},\mathcal{R}_0}}$ is uniquely determined regardless of the way to decide $\mathcal{R}_1$ and R_1 from Theorem 11 and Lemma 9.

Remark 7. If $h_{\mathcal{G}_E,\mathcal{R}_0}$ is the x-coordinate of a Montgomery curve, then the generalized Montgomery coefficient is the standard Montgomery coefficient.

Remark 8. Let E be an elliptic curve, and let h be a generalized Montgomery coordinate with respect to a finite subgroup $\mathcal{G} \subset E$. Though a Montgomery curve can be determined from its standard Montgomery coefficient, it is not always possible to determine E from the generalized Montgomery coefficient of h and the group structure of $\mathcal{G}$.

As shown in the following lemma, there is a constant ambiguity in a generalized Montgomery coordinate. For the sake of brevity in future discussions, we define a "normalized" generalized Montgomery coordinate.

Lemma 9. *For a generalized Montgomery coordinate $h_{\mathcal{G},\mathcal{R}_0}$, there exists a constant value c in $\overline{K}^{\times}$ such that*

$$h_{\mathcal{G},\mathcal{R}_0}(P+R_0) = \frac{c}{h_{\mathcal{G},\mathcal{R}_0}(P)}$$

for any P in E and R_0 in $\mathcal{R}_0$.

Proof. We define the two maps ϕ_1 and ϕ_2 mapping from E to $\mathbb{P}^1$ as

$$\phi_1(z) = h_{\mathcal{G},\mathcal{R}_0}(z+R_0), \quad \phi_2(z) = \frac{1}{h_{\mathcal{G},\mathcal{R}_0}(z)}.$$

By considering zero points and poles of ϕ_1 and ϕ_2, we have $\operatorname{div}\phi_1 = \operatorname{div}\phi_2$. Therefore, there is a constant value $c \neq 0$ such that $\phi_1 = c \cdot \phi_2$. □

Definition 10 (Normalized generalized Montgomery coordinate). *If $c = 1$ in Lemma 9, we call $h_{\mathcal{G},\mathcal{R}_0}$ a normalized generalized Montgomery coordinate.*

By replacing $h_{\mathcal{G},\mathcal{R}_0}$ with $\frac{1}{\sqrt{c}}h_{\mathcal{G},\mathcal{R}_0}$, we can always take $h_{\mathcal{G},\mathcal{R}_0}$ as normalized.

3.2 Basic properties of a generalized Montgomery coordinate

In this subsection, we see some basic properties of a generalized Montgomery coordinate. Theorem 11 shows that a generalized Montgomery coordinate satisfies property ii) in Section 3.1, and Theorem 12 tells us that a normalized generalized Montgomery coordinate is a composition of the x-coordinate of a Montgomery curve and an isogeny.

Theorem 11. *Let $\mathcal{G}$ be a finite subgroup of E, let R_0 be a point such that $2R_0 \in \mathcal{G}$ and $R_0 \notin \mathcal{G}$, and let $\mathcal{R}_0$ be a set $R_0 + \mathcal{G}$. Let $h_{\mathcal{G},\mathcal{R}_0}$ be a generalized Montgomery coordinate with respect to $\mathcal{G}$ and $\mathcal{R}_0$. Then, for $P, Q \in E$, it holds that*

$$h_{\mathcal{G},\mathcal{R}_0}(P) = h_{\mathcal{G},\mathcal{R}_0}(Q) \iff P+Q \in \mathcal{G} \text{ or } P-Q \in \mathcal{G}.$$

Proof. First, we prove that the left-hand side follows from the right-hand side. We show

$$h_{\mathcal{G},\mathcal{R}_0}(P) = h_{\mathcal{G},\mathcal{R}_0}(-P+S),$$

for all $S \in \mathcal{G}$ and $P \in E$. We prove this by comparing divisors of both sides and substituting a proper point in E. For $S \in \mathcal{G}$, we define a map $\phi_S \in \overline{K}(E)$ as follows:

$$\phi_S(z) = h_{\mathcal{G},\mathcal{R}_0}(-z+S).$$

It is clear that $\operatorname{div} h_{\mathcal{G},\mathcal{R}_0} = \operatorname{div}\phi_S$. We now prove that the constant function $h_{\mathcal{G},\mathcal{R}_0}/\phi_S$ is 1 in two cases. If there is a point $\tilde{S}$ such that $2\tilde{S} = S$, $\tilde{S} \notin \mathcal{G}$, and $\tilde{S} \notin \mathcal{R}_0$, we have $h_{\mathcal{G},\mathcal{R}_0}(\tilde{S}) = \phi_S(\tilde{S})$. Because $h_{\mathcal{G},\mathcal{R}_0}(\tilde{S})$ is neither 0 nor ∞, it holds that $h_{\mathcal{G},\mathcal{R}_0} = \phi_S$. Suppose that there is no point satisfying the above property. Take a point $\tilde{S}$ as a point satisfying $2\tilde{S} = S$. Note that $\tilde{S} \in \mathcal{G}$ or $\tilde{S} \in \mathcal{R}_0$. Let R be a point of order 2, and define a function $f \in \overline{K}(E)$ satisfying

$$\operatorname{div} f = \begin{cases} 2(\tilde{S}+R) - 2(\tilde{S}) & (\text{if } \tilde{S} \in \mathcal{G}), \\ 2(\tilde{S}) - 2(\tilde{S}+R) & (\text{if } \tilde{S} \in \mathcal{R}_0). \end{cases}$$

Let R' be a point in $E[2] \setminus \{O_E, R\}$. Because we have

$$f(\tilde{S}+R') = f(-(\tilde{S}+R')+S) \neq 0, \infty,$$

it holds that $f(z) = f(-z+S)$ from considering their divisors. It holds that $(h_{\mathcal{G},\mathcal{R}_0}/f)(z) = c \cdot (h_{\mathcal{G},\mathcal{R}_0}/f)(-z+S)$, where c is a constant value. Since

$$(h_{\mathcal{G},\mathcal{R}_0}/f)(\tilde{S}) = (h_{\mathcal{G},\mathcal{R}_0}/f)(-\tilde{S}+S) \neq 0, \infty,$$

it holds that $c = 1$. Therefore, $h_{\mathcal{G},\mathcal{R}_0}(z) = h_{\mathcal{G},\mathcal{R}_0}(-z+S)$. Note that $h_{\mathcal{G},\mathcal{R}_0}(z) = h_{\mathcal{G},\mathcal{R}_0}(-z)$ by substituting $S = O_E$. We have

$$h_{\mathcal{G},\mathcal{R}_0}(P) = h_{\mathcal{G},\mathcal{R}_0}(Q) \Longleftarrow P+Q \in \mathcal{G} \text{ or } P-Q \in \mathcal{G}.$$

Next, we prove the converse. This is showed by considering the property of the degree of $h_{\mathcal{G},\mathcal{R}_0}$ and seeing there are no points that satisfy $h_{\mathcal{G},\mathcal{R}_0}(P) = h_{\mathcal{G},\mathcal{R}_0}(Q)$ other than points in $\pm P + \mathcal{G}$. If $P \in \mathcal{G}$ or $P \in \mathcal{R}_0$, the converse is true. Suppose that $P \notin \frac{1}{2}\mathcal{G}$. Then, we have

$$\#\{Q \in E \mid P+Q \in \mathcal{G} \text{ or } P-Q \in \mathcal{G}\} = 2\#\mathcal{G}.$$

Because $\deg h_{\mathcal{G},\mathcal{R}_0} = 2\#\mathcal{G}$, the converse holds. Suppose that $P \in \mathcal{R}_1 \cup (\mathcal{R}_0 + \mathcal{R}_1)$, where $\mathcal{R}_1$ is a set defined in Lemma 4. From Lemma 4 and the above discussion, if $Q \notin \mathcal{R}_1 \cup (\mathcal{R}_0 + \mathcal{R}_1)$, then it holds that $h_{\mathcal{G},\mathcal{R}_0}(P) \neq h_{\mathcal{G},\mathcal{R}_0}(Q)$. Therefore, it suffices to show that $h_{\mathcal{G},\mathcal{R}_0}(P) \neq h_{\mathcal{G},\mathcal{R}_0}(P+R_0)$. We define a map $\psi \in \overline{K}(E)$ as $\psi(z) = h_{\mathcal{G},\mathcal{R}_0}(z) - h_{\mathcal{G},\mathcal{R}_0}(z+R_0)$. Let $\tilde{R}_0$ be a point such that $2\tilde{R}_0 = R_0$. By considering poles of ψ, we have $\deg \psi = 4\#\mathcal{G}$. Note that points belonging to $\tilde{R}_0 + \mathcal{G}$, $-\tilde{R}_0 + \mathcal{G}$, $P + \tilde{R}_0 + \mathcal{G}$, or $P - \tilde{R}_0 + \mathcal{G}$ are zero points of ψ. From Lemma 4, these sets are disjoint. Therefore, there are no zero points other than those belonging to these sets. Because $\pm\tilde{R}_0, P \pm \tilde{R}_0 \notin \mathcal{G}$, we have P does not belong to the set of zero points of ψ. Hence, it holds that $\psi(P) \neq 0$. This completes the proof of Theorem 11. □

Next, we state the important theorem (Theorem 12). This theorem shows that a generalized Montgomery coordinate can be seen as a natural generalization of x-coordinates of Montgomery curves.

Theorem 12. *Let $\mathcal{G}$ be a finite subgroup of E, let R_0 be a point satisfying $R_0 \in \frac{1}{2}\mathcal{G} \setminus \mathcal{G}$, let $\mathcal{R}_0$ be a set $R_0 + \mathcal{G}$, and let $h_{\mathcal{G},\mathcal{R}_0}$ be a normalized generalized Montgomery coordinate with respect to $\mathcal{G}$ and $\mathcal{R}_0$. Then, there is a Montgomery curve E' and a separable isogeny $\phi\colon E \to E'$ with $\ker\phi = \mathcal{G}$ such that $h_{\mathcal{G},\mathcal{R}_0} = x \circ \phi$, where x is an x-coordinate of E'. Moreover, the Montgomery coefficient of E' is the generalized Montgomery coefficient of $h_{\mathcal{G},\mathcal{R}_0}$.*

Before proving this theorem, we prove the following lemma.

Lemma 13. *If a point $\tilde{R}$ satisfies $h_{\mathcal{G},\mathcal{R}_0}(2\tilde{R}) = 0$,*

$$h_{\mathcal{G},\mathcal{R}_0}(\tilde{R})^2 = 1.$$

Proof. Because $h_{\mathcal{G},\mathcal{R}_0}(2\tilde{R}) = 0$, we have $2\tilde{R} \in \mathcal{R}_0$. Thus, $4\tilde{R}$ belongs to $\mathcal{G}$. From Lemma 9,

$$h_{\mathcal{G},\mathcal{R}_0}(\tilde{R} + R_0) = \frac{1}{h_{\mathcal{G},\mathcal{R}_0}(\tilde{R})},$$

where $R_0 \in \mathcal{R}_0$. Therefore, by Theorem 11,

$$\frac{1}{h_{\mathcal{G},\mathcal{R}_0}(\tilde{R})} = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R} + R_0) = h_{\mathcal{G},\mathcal{R}_0}(3\tilde{R}) = h_{\mathcal{G},\mathcal{R}_0}(-\tilde{R}) = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}).$$

This completes the proof of Lemma 13. □

Now, we prove Theorem 12.

Proof (Theorem 12). Let ϕ be a separable isogeny $\phi\colon E \to E/\mathcal{G}$ with $\ker\phi = \mathcal{G}$. Let $\tilde{R}_0$ be a point in E such that $h_{\mathcal{G},\mathcal{R}_0}(2\tilde{R}_0) = 0$. It is easy to see that there is an isomorphism between $E/\mathcal{G}$ and a Montgomery curve E' mapping $2\phi(\tilde{R}_0)$ to $(0, 0)$. If necessary, we compose this isomorphism and the map $E' \to E''$; $(x, y) \mapsto (-x, \sqrt{-1}y)$, and we denote E'' by E'. Then, the x-coordinate of $\phi(\tilde{R}_0)$ in E' is $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0)$, because $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0) = \pm 1$ from Lemma 13. It is easy to check that

$$\operatorname{div} h_{\mathcal{G},\mathcal{R}_0} = \operatorname{div}(x \circ \phi).$$

Therefore, $h_{\mathcal{G},\mathcal{R}_0} = x \circ \phi$.

Let R_1 be a point of E defined in Lemma 4. Then, the generalized Montgomery coefficient of $h_{\mathcal{G},\mathcal{R}_0}$ is $-h_{\mathcal{G},\mathcal{R}_0}(R_1) - \frac{1}{h_{\mathcal{G},\mathcal{R}_0}(R_1)}$. In contrast, $\phi(R_1)$ is a point of order 2 in E' other than $(0, 0)$. Therefore, the Montgomery coefficient of E' can be represented by $-x(\phi(R_1)) - \frac{1}{x(\phi(R_1))}$. From $h_{\mathcal{G},\mathcal{R}_0} = x \circ \phi$, this completes the proof of Theorem 12. □

Remark 14. It is trivial that the formula of scalar multiplication and the formula of isogeny computation via a generalized Montgomery coordinate immediately hold from Theorem 12 and the formulas on the x-coordinate of Montgomery curves; however, in Section 4 and 5, we prove these formulas without using formulas on Montgomery curves. These proofs of formulas are those for several coordinates, including the x-coordinate of Montgomery curves, and can be considered as more essential.

3.3 Examples of generalized Montgomery coordinates

In this subsection, we show some examples of generalized Montgomery coordinates already used for computations of isogenies. Table 2 is the summary of this subsection.

Montgomery curves. Montgomery curves are elliptic curves named after Montgomery [Mon87] defined by the equation $y^2 = x^3 + \alpha x^2 + x$, where $\alpha \neq \pm 2$. It is known that some computations of Montgomery curves are realized using x-coordinates [BL17,CH17]. One can see that the x-coordinate of Montgomery curves is a generalized Montgomery coordinate with respect to $\{O_E\}$ and $\mathcal{R}_0 = \{(0,0)\}$. In fact, it holds that

$$\operatorname{div} x = 2((0,0)) - 2(O_E).$$

Moreover, direct calculations lead to the fact that $x(P+(0,0)) = 1/x(P)$. Therefore, x-coordinates are normalized.

Montgomery$^-$ curves. Montgomery$^-$ curves are defined by the equation $y^2 = x^3 + \alpha x^2 - x$, where $\alpha \neq \pm 2\sqrt{-1}$. From [CD20], it holds that some computations of Montgomery$^-$ curves are computed only using x-coordinates. Since it holds that

$$\operatorname{div} x = 2((0,0)) - 2(O_E),$$

we have that the x-coordinate of Montgomery$^-$ curves is a generalized Montgomery coordinate with respect to $\{O_E\}$ and $\mathcal{R}_0 = \{(0,0)\}$. Moreover, direct calculations lead to the fact that $x(P + (0,0)) = -1/x(P)$. Therefore, $\sqrt{-1}x$ is a normalized generalized Montgomery coordinate.

Remark 15. Formulas of Montgomery$^-$ curves shown in [CD20] are obtained by applying formulas of a normalized generalized Montgomery coordinate, which we will prove in Section 4, to $\sqrt{-1}x$.

Edwards curves. Edwards curves are elliptic curves defined by the equation $x^2+y^2 = 1+dx^2y^2$, where $d \neq 0, 1$ [Edw07,BL07]. The w-coordinates of Edwards curves are defined as $w = dx^2y^2$. It is known that there are some formulas on the w-coordinate of Edwards curves [FH17,KYPH19]. For an Edwards curve E, we denote a cyclic group $\{(0, \pm 1), (\pm 1, 0)\}$ in $E(\overline{K})$ by C_4. Because

$$\begin{aligned}\operatorname{div} x &= ((0,1)) + ((0,-1)) - (\infty_1) - (\infty_2),\\ \operatorname{div} y &= ((1,0)) + ((-1,0)) - (\infty_3) - (\infty_4),\end{aligned}$$

it holds that

$$\operatorname{div} w = 2\sum_{P \in C_4}(P) - 2\sum_{P \in C_4}(P + \infty_1),$$

where ∞_1 and ∞_2 are points at infinity of order 2, and ∞_3 and ∞_4 are points at infinity of order 4. Therefore, w^{-1} is a generalized Montgomery coordinate with respect to C_4 and $\mathcal{R}_0 = \infty_1 + C_4$. From direct calculations, we have $w(P+\infty_1) = 1/w(P)$. Hence, w^{-1} is a normalized generalized Montgomery coordinate.

Huff's curves. Huff's curves are defined by the equation $cx(y^2-1) = y(x^2-1)$, where $c \neq \pm 1$ [Huf48,JTV10]. It is known that some formulas of Huff curves can be computed using w-coordinates defined as $w = 1/(xy)$ [DKW20,HZHL20]. Since

$$\begin{aligned} \operatorname{div} x &= (O_E) + (\infty_1) - (\infty_2) - (\infty_3), \\ \operatorname{div} y &= (O_E) + (\infty_2) - (\infty_1) - (\infty_3), \end{aligned}$$

it holds that

$$\operatorname{div} w = 2(\infty_3) - 2(O_E),$$

where ∞_1, ∞_2, and ∞_3 are points at infinity of order 2. Therefore, w is a generalized Montgomery coordinate with respect to $\{O_E\}$ and $\mathcal{R}_0 = \{\infty_3\}$. From direct calculations, we have $w(P + \infty_3) = 1/w(P)$. Therefore, w is a normalized generalized Montgomery coordinate.

Twisted Jacobi intersections curves. Twisted Jacobi intersections curves are defined by the equation

$$J_{a,b} \colon \begin{cases} ax^2 + y^2 = 1, \\ bx^2 + z^2 = 1, \end{cases}$$

where $ab(a-b) \neq 0$ [FNW10]. It is known that some formulas of twisted Jacobi intersections curves can be computed using ω-coordinates defined as $\omega(x, y, z) = \sqrt{ab}x^2$ [HWZ21]. By the direct computation, we have

$$\operatorname{div} x = (O_{J_{a,b}}) + ((0,-1,1)) + ((0,1,-1)) + ((0,-1,-1)) - (\infty_1) - (\infty_2) - (\infty_3) - (\infty_4),$$

where $\infty_1, \dots, \infty_4$ are points at infinity of $J_{a,b}$. We now show that $(\sqrt{ab}x^2)^{-1}$ is a normalized generalized Montgomery coordinate. From [FNW10, Theorem 1] and some computations, there is an isomorphism

$$\begin{array}{ccc} E_M \colon v^2 = u^3 - \frac{a+b}{\sqrt{ab}}u^2 + u & \longrightarrow & J_{a,b} \\ (u, v) & \longmapsto & \left(-\frac{2v}{\sqrt[4]{ab}(u^2-1)}, \frac{u^2-2\sqrt{\frac{a}{b}}u+1}{u^2-1}, \frac{u^2-2\sqrt{\frac{b}{a}}u+1}{u^2-1} \right). \end{array}$$

Therefore, ω-coordinate is the same as the function $\frac{4v^2}{(u^2-1)^2} = \frac{1}{(u \circ [2])(u,v)}$ on E_M. Since u is a normalized generalized Montgomery coordinate, ω^{-1} is also a normalized generalized Montgomery coordinate.

4 Scalar multiplication

In this section, we construct the formula of scalar multiplication via a generalized Montgomery coordinate and define the division polynomial of the generalized Montgomery coordinates. Basic pseudo-operations of a generalized Montgomery coordinate are given in Theorem 16 and Theorem 17. These theorems lead to the scalar multiplication algorithm on an elliptic curve using a generalized Montgomery coordinate using the same method as the Montgomery ladder [BL17,CS18].

4.1 Formulas for scalar multiplication

In this subsection, we fix a field K with characteristic other than 2, an elliptic curve E defined over $\overline{K}$, its subgroup $\mathcal{G}$, a point R_0 such that $R_0 \in \frac{1}{2}\mathcal{G} \setminus \mathcal{G}$, and a set $\mathcal{R}_0 = R_0 + \mathcal{G}$, and we let $h_{\mathcal{G},\mathcal{R}_0}$ be a normalized generalized Montgomery coordinate with respect to $\mathcal{G}$ and $\mathcal{R}_0$.

We get the following theorems.

Theorem 16 (pseudo addition). *Let P, Q be points of E such that $P \pm Q \notin \mathcal{G}$. Then, it holds that*

$$h_{\mathcal{G},\mathcal{R}_0}(P+Q)h_{\mathcal{G},\mathcal{R}_0}(P-Q) = \frac{(h_{\mathcal{G},\mathcal{R}_0}(Q)h_{\mathcal{G},\mathcal{R}_0}(P)-1)^2}{(h_{\mathcal{G},\mathcal{R}_0}(P)-h_{\mathcal{G},\mathcal{R}_0}(Q))^2}.$$

Theorem 17 (pseudo doubling). *Let P be a point in E such that $2P \notin \mathcal{G}$. Then, it holds that*

$$h_{\mathcal{G},\mathcal{R}_0}(2P) = \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)-1)^2(h_{\mathcal{G},\mathcal{R}_0}(P)+1)^2}{4h_{\mathcal{G},\mathcal{R}_0}(P)\left(h_{\mathcal{G},\mathcal{R}_0}(P)^2+\alpha_{h_{\mathcal{G},\mathcal{R}_0}}h_{\mathcal{G},\mathcal{R}_0}(P)+1\right)},$$

where $\alpha_{h_{\mathcal{G},\mathcal{R}_0}}$ is the generalized Montgomery coefficient of $h_{\mathcal{G},\mathcal{R}_0}$ (Definition 5).

Before proving these theorems, we prove some lemmas.

Lemma 18. *It holds that*

$$h_{\mathcal{G},\mathcal{R}_0}(P+Q)h_{\mathcal{G},\mathcal{R}_0}(P-Q) = \frac{h_{\mathcal{G},\mathcal{R}_0}(Q)^2(h_{\mathcal{G},\mathcal{R}_0}(P)-h_{\mathcal{G},\mathcal{R}_0}(R_0+Q))^2}{(h_{\mathcal{G},\mathcal{R}_0}(P)-h_{\mathcal{G},\mathcal{R}_0}(Q))^2}.$$

Proof. We define the two maps ϕ_1 and ϕ_2 mapping from $E \times E$ to $\mathbb{P}^1$ as

$$\phi_1(P,Q) = h_{\mathcal{G},\mathcal{R}_0}(P+Q)h_{\mathcal{G},\mathcal{R}_0}(P-Q),$$
$$\phi_2(P,Q) = \frac{h_{\mathcal{G},\mathcal{R}_0}(Q)^2(h_{\mathcal{G},\mathcal{R}_0}(P)-h_{\mathcal{G},\mathcal{R}_0}(R_0+Q))^2}{(h_{\mathcal{G},\mathcal{R}_0}(P)-h_{\mathcal{G},\mathcal{R}_0}(Q))^2}.$$

Suppose $Q \notin \mathcal{R}_0 \cup \mathcal{G}$. Let $\phi_{1,Q}(z) = \phi_1(z,Q)$ and $\phi_{2,Q}(z) = \phi_2(z,Q)$. By considering zero points and poles of $\phi_{1,Q}$ and $\phi_{2,Q}$, we have $\operatorname{div}\phi_{1,Q} = \operatorname{div}\phi_{2,Q}$. Therefore, there is a constant value c such that $\phi_{1,Q} = c \cdot \phi_{2,Q}$. We have $c = 1$ because

$$\phi_{1,Q}(R_0) = h_{\mathcal{G},\mathcal{R}_0}(R_0+Q)h_{\mathcal{G},\mathcal{R}_0}(R_0-Q) = h_{\mathcal{G},\mathcal{R}_0}(R_0+Q)^2,$$
$$\phi_{2,Q}(R_0) = h_{\mathcal{G},\mathcal{R}_0}(R_0+Q)^2.$$

As $\mathcal{R}_0 \cup \mathcal{G}$ is a finite set, it holds that $\phi_1(P,z) = \phi_2(P,z)$ for a fixed point P. Therefore, we have $\phi_1 = \phi_2$. □

Lemma 19. *The set $\frac{1}{2}\mathcal{R}_0$ can be decomposed as follows:*

$$(\tilde{R}_0 + \mathcal{G}) \sqcup (\tilde{R}_0 + \mathcal{R}_0) \sqcup (\tilde{R}_0 + \mathcal{R}_1) \sqcup (\tilde{R}_0 + \mathcal{R}_0 + \mathcal{R}_1),$$

where $\tilde{R}_0$ is a point satisfying $2\tilde{R}_0 \in \mathcal{R}_0$, and $\mathcal{R}_1$ is a set defined in Lemma 4.

Moreover, one of the following holds:

- $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+\mathcal{G}) = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+\mathcal{R}_0) = \{1\}$ *and* $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+\mathcal{R}_1) = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+\mathcal{R}_0+\mathcal{R}_1) = \{-1\}$*;*
- $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+\mathcal{G}) = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+\mathcal{R}_0) = \{-1\}$ *and* $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+\mathcal{R}_1) = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+\mathcal{R}_0+\mathcal{R}_1) = \{1\}$*.*

Proof. Because $E[2] \subset \frac{1}{2}\mathcal{G}$, we have $\frac{1}{2}\mathcal{R}_0 = \tilde{R}_0 + \frac{1}{2}\mathcal{G}$. From Lemma 4, the first part of Lemma 19 holds.

Let R_1 be a point in $\mathcal{R}_1$. By Lemma 13, we have

$$h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0)^2 = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+R_0)^2 = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+R_1)^2 = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+R_0+R_1)^2 = 1.$$

Therefore, from Lemma 9,

$$h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0) = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+R_0) \text{ and } h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+R_1) = h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+R_0+R_1).$$

Since the number of points in $h_{\mathcal{G},\mathcal{R}_0}^{-1}(z)$ for some $z \in \mathbb{P}^1$ is at most $2\#\mathcal{G}$, it holds that $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+R_0) \neq h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0+R_1)$. From Theorem 11, this completes the proof of Lemma 19. □

Now, we prove Theorem 16 and Theorem 17.

Proof (Theorem 16). It follows from Lemma 18 and Lemma 9. □

Proof (Theorem 17). We define the two maps $\phi_1, \phi_2 \colon E \to \mathbb{P}^1$ as follows:

$$\begin{aligned}
\phi_1(z) &= h_{\mathcal{G},\mathcal{R}_0}(2z),\\
\phi_2(z) &= \frac{(h_{\mathcal{G},\mathcal{R}_0}(z)-1)^2(h_{\mathcal{G},\mathcal{R}_0}(z)+1)^2}{h_{\mathcal{G},\mathcal{R}_0}(z)(h_{\mathcal{G},\mathcal{R}_0}(z)-h_{\mathcal{G},\mathcal{R}_0}(R_1))(h_{\mathcal{G},\mathcal{R}_0}(z)-h_{\mathcal{G},\mathcal{R}_0}(R_0+R_1))},
\end{aligned}$$

where R_1 is a point in $\mathcal{R}_1$. Note that the set of zero point of ϕ_1 is $\frac{1}{2}\mathcal{R}_0$, and the set of poles of ϕ_1 is $\frac{1}{2}\mathcal{G}$. Therefore, from Lemma 4 and Lemma 19, we have $\operatorname{div}\phi_1 = \operatorname{div}\phi_2$. Hence, it holds that $\phi_1 = c \cdot \phi_2$, where c is a constant value.

From Theorem 16, it holds that

$$h_{\mathcal{G},\mathcal{R}_0}(4z)h_{\mathcal{G},\mathcal{R}_0}(2z) = \frac{(h_{\mathcal{G},\mathcal{R}_0}(3z)h_{\mathcal{G},\mathcal{R}_0}(z)-1)^2}{(h_{\mathcal{G},\mathcal{R}_0}(3z)-h_{\mathcal{G},\mathcal{R}_0}(z))^2}.$$

Note that $\alpha_{h_{\mathcal{G},\mathcal{R}_0}} = -(h_{\mathcal{G},\mathcal{R}_0}(R_1) + h_{\mathcal{G},\mathcal{R}_0}(R_0+R_1))$. We also have

$$h_{\mathcal{G},\mathcal{R}_0}(4z)h_{\mathcal{G},\mathcal{R}_0}(2z) = c \cdot \frac{(h_{\mathcal{G},\mathcal{R}_0}(2z)^2-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(2z)^2 + \alpha_{h_{\mathcal{G},\mathcal{R}_0}} h_{\mathcal{G},\mathcal{R}_0}(2z) + 1}.$$

Using Theorem 16 again, we get

$$h_{\mathcal{G},\mathcal{R}_0}(3z)h_{\mathcal{G},\mathcal{R}_0}(z) = \frac{(h_{\mathcal{G},\mathcal{R}_0}(2z)h_{\mathcal{G},\mathcal{R}_0}(z)-1)^2}{(h_{\mathcal{G},\mathcal{R}_0}(2z)-h_{\mathcal{G},\mathcal{R}_0}(z))^2}.$$

Therefore, it holds that

$$c \cdot \frac{(h_{\mathcal{G},\mathcal{R}_0}(2z)^2-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(2z)^2+\alpha_{h_{\mathcal{G},\mathcal{R}_0}} h_{\mathcal{G},\mathcal{R}_0}(2z)+1} = \frac{\left(\frac{(h_{\mathcal{G},\mathcal{R}_0}(2z)h_{\mathcal{G},\mathcal{R}_0}(z)-1)^2}{(h_{\mathcal{G},\mathcal{R}_0}(2z)-h_{\mathcal{G},\mathcal{R}_0}(z))^2}-1\right)^2 h_{\mathcal{G},\mathcal{R}_0}(z)^2}{\left(\frac{(h_{\mathcal{G},\mathcal{R}_0}(2z)h_{\mathcal{G},\mathcal{R}_0}(z)-1)^2}{(h_{\mathcal{G},\mathcal{R}_0}(2z)-h_{\mathcal{G},\mathcal{R}_0}(z))^2}-h_{\mathcal{G},\mathcal{R}_0}(z)^2\right)^2}.$$

The right-hand side of this identity can be transformed as follows:

$$\frac{(h_{\mathcal{G},\mathcal{R}_0}(2z)^2-1)^2(h_{\mathcal{G},\mathcal{R}_0}(z)^2-1)^2 h_{\mathcal{G},\mathcal{R}_0}(z)^2}{(2h_{\mathcal{G},\mathcal{R}_0}(2z)h_{\mathcal{G},\mathcal{R}_0}(z)-h_{\mathcal{G},\mathcal{R}_0}(z)^2-1)^2(h_{\mathcal{G},\mathcal{R}_0}(z)^2-1)^2}.$$

Hence, we have

$$c \cdot \frac{1}{h_{\mathcal{G},\mathcal{R}_0}(2z)^2+\alpha_{h_{\mathcal{G},\mathcal{R}_0}} h_{\mathcal{G},\mathcal{R}_0}(2z)+1} = \frac{h_{\mathcal{G},\mathcal{R}_0}(z)^2}{(2h_{\mathcal{G},\mathcal{R}_0}(2z)h_{\mathcal{G},\mathcal{R}_0}(z)-h_{\mathcal{G},\mathcal{R}_0}(z)^2-1)^2}.$$

Let $\tilde{R}_0$ be a point satisfying $2\tilde{R}_0 \in \mathcal{R}_0$. Note that $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0) = \pm 1$, and $h_{\mathcal{G},\mathcal{R}_0}(2\tilde{R}_0) = 0$. By substituting $\tilde{R}_0$ for z, we get $c = \frac{1}{4}$. □

4.2 Division polynomials of the generalized Montgomery coordinates

In this subsection, we define the division polynomials of the generalized Montgomery coordinates. Although this definition is not the same as that of standard division polynomials, they are essentially the same.

Before defining the division polynomials, we prove the following proposition.

Proposition 20. *Let $\Psi = 4(h^2+\alpha h+1)$. For any $m \in \mathbb{Z}_{\geq 1}$, there exist polynomials $\Phi_m, \Psi_m \in \mathbb{Z}[\alpha, h]$ such that, for any elliptic curve E and any normalized generalized Montgomery coordinate $h_{\mathcal{G},\mathcal{R}_0}$, the following three properties hold: If m is odd,*

- *It holds that*

$$h_{\mathcal{G},\mathcal{R}_0}(mP) = \frac{h_{\mathcal{G},\mathcal{R}_0}(P)\Phi_m^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(P))}{\Psi_m^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(P))};$$

- *The highest term of $\Phi_m(\alpha, h)$ in the variable h is $h^{\frac{m^2-1}{2}}$;*
- *The highest term of $\Psi_m(\alpha, h)$ in the variable h is $m \cdot h^{\frac{m^2-1}{2}}$.*

If m is even,

- *It holds that*

$$h_{\mathcal{G},\mathcal{R}_0}(mP) = \frac{\Phi_m^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(P))}{h_{\mathcal{G},\mathcal{R}_0}(P)\Psi_m^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(P)) \cdot \Psi(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(P))};$$

- *The highest term of $\Phi_m(\alpha, h)$ in the variable h is $h^{\frac{m^2}{2}}$;*
- *The highest term of $\Psi_m(\alpha, h)$ in the variable h is $\frac{m}{2} \cdot h^{\frac{m^2-4}{2}}$.*

Here, $\alpha_{h_{\mathcal{G},\mathcal{R}_0}}$ is the generalized Montgomery coefficient of $h_{\mathcal{G},\mathcal{R}_0}$.

Proof. We prove this proposition by mathematical induction. In the case of $m = 1$, we have $\Phi_1(\alpha, h) = 1$, and $\Psi_1(\alpha, h) = 1$. In the case of $m = 2$, from Theorem 17, we have $\Phi_2(\alpha, h) = h^2 - 1$, and $\Psi_2(\alpha, h) = 1$. Let s be an odd integer greater than or equal to one. Suppose that Proposition 20 holds for $m = s$ and $m = s + 1$. From Theorem 16, it holds that

$$\begin{aligned} h_{\mathcal{G},\mathcal{R}_0}((2s+1)P) &= \frac{(h_{\mathcal{G},\mathcal{R}_0}(sP)h_{\mathcal{G},\mathcal{R}_0}((s+1)P) - 1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)(h_{\mathcal{G},\mathcal{R}_0}(sP) - h_{\mathcal{G},\mathcal{R}_0}((s+1)P))^2} \\ &= \frac{h_{\mathcal{G},\mathcal{R}_0}(P)(\Phi_s^2\Phi_{s+1}^2 - \Psi_s^2\Psi_{s+1}^2\Psi)^2}{(h_{\mathcal{G},\mathcal{R}_0}(P)^2\Phi_s^2\Psi_{s+1}^2\Psi - \Phi_{s+1}^2\Psi_s^2)^2}. \end{aligned}$$

In this proof, as in the equation above, we often omit $(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(P))$. We define

$$\begin{aligned} \Phi_{2s+1}(\alpha, h) &= \Phi_s(\alpha, h)^2\Phi_{s+1}(\alpha, h)^2 - \Psi_s(\alpha, h)^2\Psi_{s+1}(\alpha, h)^2\Psi(\alpha, h), \\ \Psi_{2s+1}(\alpha, h) &= h^2\Phi_s(\alpha, h)^2\Psi_{s+1}(\alpha, h)^2\Psi(\alpha, h) - \Phi_{s+1}(\alpha, h)^2\Psi_s(\alpha, h)^2. \end{aligned}$$

It is easy to show that the highest term of $\Phi_{2s+1}(\alpha, h)$ in the variable h is $h^{\frac{(2s+1)^2-1}{2}}$, and that of $\Psi_{2s+1}(\alpha, h)$ in the variable h is $(2s+1) \cdot h^{\frac{(2s+1)^2-1}{2}}$. Therefore, Proposition 20 holds for $m = 2s + 1$. From Theorem 17, it holds that

$$\begin{aligned} h_{\mathcal{G},\mathcal{R}_0}(2sP) &= \frac{h_{\mathcal{G},\mathcal{R}_0}(2P)\Phi_s^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(2P))}{\Psi_s^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(2P))} \\ &= \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)^2 - 1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)\Psi} \frac{\Phi_s^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)^2-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)\Psi}) \cdot (h_{\mathcal{G},\mathcal{R}_0}(P)\Psi)^{s^2-1}}{\Psi_s^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)^2-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)\Psi}) \cdot (h_{\mathcal{G},\mathcal{R}_0}(P)\Psi)^{s^2-1}}. \end{aligned}$$

We define

$$\begin{aligned} \Phi_{2s}(\alpha, h) &= (h^2 - 1)(\Phi_s(\alpha, (h^2-1)^2/(h\Psi(\alpha, h))) \cdot (h\Psi(\alpha, h))^{\frac{s^2-1}{2}}), \\ \Psi_{2s}(\alpha, h) &= \Psi_s(\alpha, (h^2-1)^2/(h\Psi(\alpha, h))) \cdot (h\Psi(\alpha, h))^{\frac{s^2-1}{2}}. \end{aligned}$$

It is easy to show that the highest term of $\Phi_{2s}(\alpha, h)$ in the variable h is $h^{\frac{(2s)^2}{2}}$, and that of $\Psi_{2s}(\alpha, h)$ in the variable h is $s \cdot h^{\frac{(2s)^2-4}{2}}$. Therefore, Proposition 20 holds for $m = 2s$.

Next, we consider the case that s is even. Suppose that Proposition 20 holds for $m = s$ and $m = s + 1$. From Theorem 16, it holds that

$$h_{\mathcal{G},\mathcal{R}_0}((2s+1)P) = \frac{h_{\mathcal{G},\mathcal{R}_0}(P)(\Phi_s^2\Phi_{s+1}^2 - \Psi_s^2\Psi_{s+1}^2\Psi)^2}{(h_{\mathcal{G},\mathcal{R}_0}(P)^2\Phi_{s+1}^2\Psi_s^2\Psi - \Phi_s^2\Psi_{s+1}^2)^2}.$$

We define

$$\begin{aligned}\varPhi_{2s+1}(\alpha,h) &= \varPhi_s(\alpha,h)^2\varPhi_{s+1}(\alpha,h)^2 - \varPsi_s(\alpha,h)^2\varPsi_{s+1}(\alpha,h)^2\varPsi(\alpha,h),\\ \varPsi_{2s+1}(\alpha,h) &= \varPhi_s(\alpha,h)^2\varPsi_{s+1}(\alpha,h)^2 - h^2\varPhi_{s+1}(\alpha,h)^2\varPsi_s(\alpha,h)^2\varPsi(\alpha,h).\end{aligned}$$

It is easy to show that the highest term of $\varPhi_{2s+1}$ in the variable h is $h^{\frac{(2s+1)^2-1}{2}}$, and that of $\varPsi_{2s+1}$ in the variable h is $(2s+1)\cdot h^{\frac{(2s+1)^2-1}{2}}$. Therefore, Proposition 20 holds for $m = 2s+1$. From Theorem 17, it holds that

$$\begin{aligned} h_{\mathcal{G},\mathcal{R}_0}(2sP) &= \frac{\varPhi_s^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(2P))}{h_{\mathcal{G},\mathcal{R}_0}(2P)\varPsi_s^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(2P))\varPsi(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(2P))}\\ &= \frac{1}{h_{\mathcal{G},\mathcal{R}_0}(P)\varPsi}\frac{\varPhi_s^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)^2-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)\varPsi})\cdot(h_{\mathcal{G},\mathcal{R}_0}(P)\varPsi)^{s^2}}{(h_{\mathcal{G},\mathcal{R}_0}(P)^2-1)^2\varPsi_s^2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)^2-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)\varPsi})\cdot\tilde{\varPsi}^2\cdot(h_{\mathcal{G},\mathcal{R}_0}(P)\varPsi)^{s^2-4}},\end{aligned}$$

where $\tilde{\varPsi}(\alpha,h)$ is a polynomial

$$\tilde{\varPsi}(\alpha,h) = 2(h^4+2\alpha h^3+6h^2+2\alpha h+1).$$

We define

$$\begin{aligned}\varPhi_{2s}(\alpha,h) &= \varPhi_s(\alpha,(h^2-1)^2/(h\varPsi(\alpha,h)))\cdot(h\varPsi(\alpha,h))^{\frac{s^2}{2}},\\ \varPsi_{2s}(\alpha,h) &= (h^2-1)\cdot\varPsi_s(\alpha,(h^2-1)^2/(h\varPsi(\alpha,h)))\cdot\tilde{\varPsi}(\alpha,h)\cdot(h\varPsi(\alpha,h))^{\frac{s^2-4}{2}}.\end{aligned}$$

It is easy to show that the highest term of $\varPhi_{2s}(\alpha,h)$ in the variable h is $h^{\frac{(2s)^2}{2}}$, and that of $\varPsi_{2s}(\alpha,h)$ in the variable h is $s\cdot h^{\frac{(2s)^2-4}{2}}$. Therefore, Proposition 20 holds for $m = 2s$. This completes the proof of Proposition 20. □

Now, we define the division polynomials of the generalized Montgomery coordinates.

Definition 21 (Division polynomials of the generalized Montgomery coordinates). *Let $m \in \mathbb{Z}_{\geq 1}$, and let $\varPsi_m$ and $\varPsi$ be polynomials defined in the proof of Proposition 20. We define a polynomial $\psi'_m \in \mathbb{Z}[\alpha,h]$ as*

$$\psi'_m(\alpha,h) = \begin{cases}\varPsi_m(\alpha,h) & (m\ \textit{is odd}),\\ h\cdot\varPsi_m(\alpha,h)\cdot\varPsi(\alpha,h) & (m\ \textit{is even}).\end{cases}$$

We define a polynomial $\psi_m \in \mathbb{Z}[\alpha,h]$ as $\psi_m = \psi'_m/d$, where d is the maximal integer such that ψ'_m/d is in $\mathbb{Z}[\alpha,h]$. That is, ψ_m is primitive. We call the polynomial ψ_m the m-th division polynomial of the generalized Montgomery coordinates.

The following theorem claims an important property of division polynomials of the generalized Montgomery coordinates. This property provides the condition for the equality of the computational results of different formulas (Theorem 27).

Theorem 22. *Let p be the characteristic of $\overline{K}$, and let $m \in \mathbb{Z}_{\geq 1}$ satisfy $p \nmid m$ if $p \neq 0$. We define an ideal I_m in a polynomial ring $\mathbb{Z}[\alpha, h]$ as follows:*

$$I_m = \{\psi \mid \psi(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(P)) = 0 \in \overline{K} \text{ for all } (E, h_{\mathcal{G},\mathcal{R}_0}) \text{ and } P \in E[m] \setminus \mathcal{G}\}.$$

Then, it holds that $I_m = (p, \psi_m)$, where ψ_m is the m-th division polynomial of the generalized Montgomery coordinates.

Proof. First, we consider the case of $p > 0$. It is clear that $p \in I_m$. Therefore, we prove that $\overline{\psi_m}\mathbb{F}_p[\alpha, h] = \overline{I_m}$, where $\overline{\psi_m}$ is an image of ψ_m under the canonical map $\mathbb{Z}[\alpha, h] \to \mathbb{F}_p[\alpha, h]$, and $\overline{I_m}$ is the ideal generated by an image of I_m under the canonical map $\mathbb{Z}[\alpha, h] \to \mathbb{F}_p[\alpha, h]$. Because $p \nmid m$, we have $\overline{\psi_m} \neq 0$ from Proposition 20. We define the ideal J_m of $\mathbb{F}_p(\alpha)[h]$ as

$$\left\{ \psi \in \mathbb{F}_p(\alpha)[h] \;\middle|\; \begin{array}{l} \exists f \in \mathbb{F}_p[\alpha] \setminus \{0\} \text{ s.t. } (f \cdot \psi)(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(P)) = 0 \\ \text{for all } (E, h_{\mathcal{G},\mathcal{R}_0}) \text{ and } P \in E[m] \setminus \mathcal{G} \end{array} \right\}.$$

Since $\mathbb{F}_p(\alpha)$ is a field, J_m is a principal ideal. We now prove that $J_m = \overline{\psi_m}\mathbb{F}_p(\alpha)[h]$. From the construction of ψ_m, it is clear that $\overline{\psi_m} \in J_m$. Suppose that $\overline{\psi_m}$ is not a generator of J_m. Then, there is a polynomial ψ_0 such that $\deg_h \psi_0 < \deg_h \overline{\psi_m}$ and $J_m = \psi_0 \mathbb{F}_p(\alpha)[h]$. Let $h_{\mathcal{G},\mathcal{R}_0}$ be a normalized generalized Montgomery coordinate with respect to $\{O_E\}$ (*e.g.,* x-coordinates of Montgomery curves). By the definition of J_m, elements in $h_{\mathcal{G},\mathcal{R}_0}(E[m] \setminus \{O_E\})$ are the roots of $(f \cdot \psi_0)(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h)$ for some $f \in \mathbb{F}_p[\alpha] \setminus \{0\}$. We redefine ψ_0 as $f \cdot \psi'$. Note that all elements in $\overline{K} \setminus \{\pm 2\}$ can be a Montgomery coefficient of some elliptic curve. Changing E if necessary, we may assume that $\psi_0(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h) \neq 0$. Therefore, $\deg_h \psi_0(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h)$ is larger than $\#h_{\mathcal{G},\mathcal{R}_0}(E[m] \setminus \{O_E\})$. Note that $\#h_{\mathcal{G},\mathcal{R}_0}(E[m] \setminus \{O_E\})$ is $\frac{m^2-1}{2}$ if m is odd, and it is $\frac{m^2+2}{2}$ if m is even. Therefore, from Proposition 20, $\deg_h \overline{\psi_m}$ is the number of elements in $h_{\mathcal{G},\mathcal{R}_0}(E[m] \setminus \{O_E\})$. However, we have $\deg_h \psi_0(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h) \leq \deg_h \psi_0 < \deg_h \overline{\psi_m}$. This is a contradiction. Hence, it holds that $J_m = \overline{\psi_m}\mathbb{F}_p(\alpha)[h]$.

Let ψ be a polynomial in $\overline{I_m}$. It is easy to see that $\psi \in J_m = \overline{\psi_m}\mathbb{F}_p(\alpha)[h]$. Therefore, $\psi/\overline{\psi_m}$ is in $\mathbb{F}_p(\alpha)[h]$. We denote $\psi/\overline{\psi_m}$ by $F(\alpha, h)$. From Proposition 20, we get that the coefficient of the highest term in the variable h of $\overline{\psi_m}$ is in $\mathbb{F}_p \setminus \{0\}$. Therefore, $\overline{\psi_m}$ is primitive as a polynomial in $(\mathbb{F}_p[\alpha])[h]$. Note that $\psi \in \mathbb{F}_p[\alpha, h]$. From Gauss's Lemma, we have $F(\alpha, h) \in \mathbb{F}_p[\alpha, h]$. Therefore, $\psi \in \overline{\psi_m}\mathbb{F}_p[\alpha, h]$. In other words, it holds that $\overline{I_m} \subset \overline{\psi_m}\mathbb{F}_p[\alpha, h]$. Because it is clear that $\overline{\psi_m} \in \overline{I_m}$, we have $\overline{I_m} = \overline{\psi_m}\mathbb{F}_p[\alpha, h]$. This completes the proof of the case of $p > 0$.

We now consider the case of $p = 0$. We can prove the most part by changing $\mathbb{F}_p[\alpha, h]$ to $\mathbb{Q}[\alpha, h]$ and having a similar discussion. The rest is the part that proves $F(\alpha, h) \in \mathbb{Z}[\alpha, h]$, where $F(\alpha, h)$ is a polynomial in $\mathbb{Q}(\alpha)[h]$ such that $F(\alpha, h) = \psi/\psi_m$ for some $\psi \in I_m$. Remember that ψ_m is primitive by its definition. From Gauss's Lemma, $F(\alpha, h) \in \mathbb{Z}[\alpha, h]$. □

5 Isogeny computation

In this section, we construct formulas to compute isogenies via a generalized Montgomery coordinate. Throughout this section, we fix a field K with characteristic other than 2, an elliptic curve E defined over $\overline{K}$, its subgroup $\mathcal{G}$, a point R_0 such that $R_0 \notin \mathcal{G}$ and $2R_0 \in \mathcal{G}$, and a set $\mathcal{R}_0 = R_0 + \mathcal{G}$, and we let $h_{\mathcal{G},\mathcal{R}_0}$ be a normalized generalized Montgomery coordinate with respect to $\mathcal{G}$ and $\mathcal{R}_0$.

To compute isogenies, we need two formulas: the formula to compute an image point under the isogeny and the formula to compute the coefficient of the codomain elliptic curve. In the subsection 5.1, we construct the first formula, and in the subsection 5.2, we construct one of the second formulas. The second formulas are known to be of various types. In Subsection 5.3, we explain that this difference comes from the division polynomial of the generalized Montgomery coordinates.

5.1 Formula for image points

In this subsection, we explain formulas for computing image points under isogenies using a generalized Montgomery coordinate.

Theorem 23 (odd degree isogeny). *Let G be a finite subgroup of E satisfying*

$$G \cap (\mathcal{G} \cup \mathcal{R}_0) = \{O_E\}.$$

Let ϕ be a separable isogeny $\phi\colon E \to E/G$ with $\ker\phi = G$. Then, there is a normalized generalized Montgomery coordinate of E/G with respect to $\phi(\mathcal{G})$ and $\phi(\mathcal{R}_0)$ satisfying

$$h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}(\phi(P)) = h_{\mathcal{G},\mathcal{R}_0}(P) \prod_{Q \in G\setminus\{O_E\}} \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)h_{\mathcal{G},\mathcal{R}_0}(Q) - 1)}{(h_{\mathcal{G},\mathcal{R}_0}(P) - h_{\mathcal{G},\mathcal{R}_0}(Q))}.$$

Proof. We define a map $h_{\phi(\mathcal{G}),\phi(R_0)} \in \overline{K}(E/G)$ satisfying

$$\operatorname{div} h_{\phi(\mathcal{G}),\phi(R_0)} = 2\sum_{P \in \phi(\mathcal{G})} (\phi(R_0) + P) - 2\sum_{P \in \phi(\mathcal{G})} (P).$$

It is clear that $h_{\phi(\mathcal{G}),\phi(R_0)}$ is a generalized Montgomery coordinate of E/G with respect to $\phi(\mathcal{G})$ and $\phi(\mathcal{R}_0)$. By multiplying by a constant value, we can assume that $h_{\phi(\mathcal{G}),\phi(R_0)}$ is normalized. Let $\tilde{R}_0$ be a point of E satisfying $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0) = 1$. From Theorem 11 and Lemma 19, we have

$$h_{\phi(\mathcal{G}),\phi(R_0)}(2\phi(\tilde{R}_0)) = h_{\phi(\mathcal{G}),\phi(R_0)}(\phi(R_0)) = 0.$$

Therefore, by Lemma 19, it holds that $h_{\phi(\mathcal{G}),\phi(R_0)}(\phi(\tilde{R}_0)) = \pm 1$. If this value is -1, we multiply $h_{\phi(\mathcal{G}),\phi(R_0)}$ by -1. We define two maps $\phi_1, \phi_2 \in \overline{K}(E)$ as

$$\begin{aligned}
\phi_1(z) &= h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}(\phi(z)),\\
\phi_2(z) &= h_{\mathcal{G},\mathcal{R}_0}(z) \prod_{Q \in G\setminus\{O_E\}} \frac{(h_{\mathcal{G},\mathcal{R}_0}(z)h_{\mathcal{G},\mathcal{R}_0}(Q) - 1)}{(h_{\mathcal{G},\mathcal{R}_0}(z) - h_{\mathcal{G},\mathcal{R}_0}(Q))}.
\end{aligned}$$

It is easy to check that $\operatorname{div}\phi_1 = \operatorname{div}\phi_2$. Since $\phi_1(\tilde{R}_0) = \phi_2(\tilde{R}_0) = 1$, it holds that $\phi_1 = \phi_2$. This completes the proof of Theorem 23. □

Theorem 23 gives us the formula for computing an isogeny whose kernel is G, which satisfies $G \cap (\mathcal{G} \cup \mathcal{R}_0) = \{O_E\}$. If $E[2] \not\subset \mathcal{G}$, and R_0 is a point of order 2, then we can construct the natural formula of a 2-isogeny whose kernel is $\langle R_0 \rangle$.

Theorem 24 (2-isogeny). *We assume that $E[2] \not\subset \mathcal{G}$, and R_0 is a point of order 2. Let $G = \langle R_0 \rangle$, and let $\phi\colon E \to E/G$ be a separable isogeny with $\ker\phi = G$. Then, there are six normalized generalized Montgomery coordinates of E/G with respect to $\phi(\mathcal{G})$ satisfying the following equalities:*

$$\begin{aligned}
h_{1,\pm}(\phi(P)) &= \pm\frac{1}{2\sqrt{\alpha_{h_{\mathcal{G},\mathcal{R}_0}}+2}} \cdot \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)},\\
h_{2,\pm}(\phi(P)) &= \pm\frac{1}{2\sqrt{-\alpha_{h_{\mathcal{G},\mathcal{R}_0}}+2}} \cdot \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)+1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)},\\
h_{3,\pm}(\phi(P)) &= \pm\frac{1}{\sqrt{\alpha_{h_{\mathcal{G},\mathcal{R}_0}}^2-4}} \cdot \frac{h_{\mathcal{G},\mathcal{R}_0}(P)^2+\alpha_{h_{\mathcal{G},\mathcal{R}_0}}h_{\mathcal{G},\mathcal{R}_0}(P)+1}{h_{\mathcal{G},\mathcal{R}_0}(P)},
\end{aligned}$$

where $\alpha_{h_{\mathcal{G},\mathcal{R}_0}}$ is the generalized Montgomery coefficient of $h_{\mathcal{G},\mathcal{R}_0}$.

Proof. Let $\mathcal{R}_1$ be a set defined in Lemma 4, let R_1 be a point in $\mathcal{R}_1$, and let $\tilde{R}_0$ be a point satisfying $2\tilde{R}_0 = R_0$. One can check that $2\phi(\tilde{R}_0) \in \phi(\mathcal{G})$ and $\phi(\tilde{R}_0) \notin \phi(\mathcal{G}) \cup \phi(\mathcal{R}_1)$. Therefore, from Lemma 4, we have

$$\frac{1}{2}\phi(\mathcal{G}) = \phi(\mathcal{G}) \sqcup \phi(\mathcal{R}_1) \sqcup (\phi(\tilde{R}_0) + \phi(\mathcal{G})) \sqcup (\phi(\tilde{R}_0) + \phi(\mathcal{R}_1)).$$

Hence, we get the following normalized generalized Montgomery coordinates:

- $h_{1,+}$ and $h_{1,-}$ with respect to $\phi(\mathcal{G})$ and $\phi(\tilde{R}_0) + \phi(\mathcal{G})$,
- $h_{2,+}$ and $h_{2,-}$ with respect to $\phi(\mathcal{G})$ and $\phi(\tilde{R}_0) + \phi(R_1) + \phi(\mathcal{G})$,
- $h_{3,+}$ and $h_{3,-}$ with respect to $\phi(\mathcal{G})$ and $\phi(R_1) + \phi(\mathcal{G})$,

where $h_{i,-} = -h_{i,+}$ for $i = 1, 2, 3$. Note that $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0 + R_1) = -1$ from Lemma 19. By considering zero points and poles, we have

$$\begin{aligned}
h_{1,\pm}(\phi(P)) &= \pm c_1 \cdot \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)},\\
h_{2,\pm}(\phi(P)) &= \pm c_2 \cdot \frac{(h_{\mathcal{G},\mathcal{R}_0}(P)+1)^2}{h_{\mathcal{G},\mathcal{R}_0}(P)},\\
h_{3,\pm}(\phi(P)) &= \pm c_3 \cdot \frac{h_{\mathcal{G},\mathcal{R}_0}(P)^2+\alpha_{h_{\mathcal{G},\mathcal{R}_0}}h_{\mathcal{G},\mathcal{R}_0}(P)+1}{h_{\mathcal{G},\mathcal{R}_0}(P)},
\end{aligned}$$

where c_1, c_2, and c_3 are constant values of $\overline{K}$.

Next, we find these constant values. From Lemma 9, it holds that

$$h_1(\phi(\tilde{R}_0)+\phi(R_1))\cdot h_1(\phi(R_1))=1.$$

Therefore, it holds that

$$c_1^2\cdot(-4)\cdot\frac{(h_{\mathcal{G},\mathcal{R}_0}(R_1)-1)^2}{h_{\mathcal{G},\mathcal{R}_0}(R_1)}=1.$$

Thus, we have $c_1=\frac{1}{2\sqrt{\alpha_{h_{\mathcal{G},\mathcal{R}_0}}+2}}$. It also holds that

$$h_2(\phi(\tilde{R}_0))\cdot h_2(\phi(R_1))=1.$$

Therefore, by a similar calculation, we also have $c_2=\frac{1}{2\sqrt{-\alpha_{h_{\mathcal{G},\mathcal{R}_0}}+2}}$. It also holds that

$$h_3(\phi(\tilde{R}_0)+\phi(R_1))\cdot h_3(\phi(\tilde{R}_0))=1.$$

Hence, we also have $c_3=\frac{1}{\sqrt{\alpha^2_{h_{\mathcal{G},\mathcal{R}_0}}-4}}$. This completes the proof of Theorem 24. □

5.2 Formula for generalized Montgomery coefficients

In this subsection, we construct formulas to compute generalized Montgomery coefficients of target curves of isogenies by Theorem 23, 24. The following theorems give these formulas.

Theorem 25 (odd degree isogeny). *Let $\mathcal{R}_1$ be a subset of E defined in Lemma 4, let R_1 be a point in $\mathcal{R}_1$, and let G be a subgroup of E satisfying*

$$G\cap(\mathcal{G}\cup\mathcal{R}_0\cup\mathcal{R}_1)=\{O_E\}.$$

Let ϕ be a separable isogeny $\phi\colon E\to E/G$ with $\ker\phi=G$, and let $h_{\phi(\mathcal{G}),\phi(R_0)}$ be a normalized generalized Montgomery coordinate of E/G which is defined in Theorem 23. Then, the generalized Montgomery coefficient of $h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}$ is

$$\begin{aligned}\alpha_{h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}}=&-h_{\mathcal{G},\mathcal{R}_0}(R_1)\prod_{Q\in G\setminus\{O_E\}}\frac{(h_{\mathcal{G},\mathcal{R}_0}(R_1)h_{\mathcal{G},\mathcal{R}_0}(Q)-1)}{(h_{\mathcal{G},\mathcal{R}_0}(R_1)-h_{\mathcal{G},\mathcal{R}_0}(Q))}\\&-\frac{1}{h_{\mathcal{G},\mathcal{R}_0}(R_1)}\prod_{Q\in G\setminus\{O_E\}}\frac{(h_{\mathcal{G},\mathcal{R}_0}(R_1)-h_{\mathcal{G},\mathcal{R}_0}(Q))}{(h_{\mathcal{G},\mathcal{R}_0}(R_1)h_{\mathcal{G},\mathcal{R}_0}(Q)-1)}.\end{aligned}$$

Proof. Because $2\phi(R_1)=\phi(2R_1)\in\phi(\mathcal{G})$ and $R_1\notin G$, the generalized Montgomery coefficient of $h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}$ is

$$-h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}(\phi(R_1))-\frac{1}{h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}(\phi(R_1))}.$$

Theorem 23 completes the proof. □

Theorem 26 (2-isogeny). *Assume that $E[2] \not\subset \mathcal{G}$, and R_0 is a point of order 2. Let $G = \langle R_0 \rangle$, and let $\phi\colon E \to E/G$ be a separable isogeny with $\ker \phi = G$. Let $h_{1,\pm}$, $h_{2,\pm}$, and $h_{3,\pm}$ be normalized generalized Montgomery coordinates in Theorem 24. Then, the generalized Montgomery coefficients of these generalized Montgomery coordinates are as follows:*

$$\alpha_{h_{1,\pm}} = \pm \frac{\alpha_{h_{\mathcal{G},\mathcal{R}_0}} + 6}{2\sqrt{\alpha_{h_{\mathcal{G},\mathcal{R}_0}} + 2}}, \ \alpha_{h_{2,\pm}} = \pm \frac{\alpha_{h_{\mathcal{G},\mathcal{R}_0}} - 6}{2\sqrt{-\alpha_{h_{\mathcal{G},\mathcal{R}_0}} + 2}}, \ \alpha_{h_{3,\pm}} = \mp \frac{2\alpha_{h_{\mathcal{G},\mathcal{R}_0}}}{\sqrt{\alpha^2_{h_{\mathcal{G},\mathcal{R}_0}} - 4}},$$

where $\alpha_{h_{\mathcal{G},\mathcal{R}_0}}$ is the generalized Montgomery coefficient of $h_{\mathcal{G},\mathcal{R}_0}$.

Proof. Most parts of the proof can be shown in the same way as the proof of Theorem 25. The rest part is that of $\alpha_{h_{3,\pm}}$. Since $h_{3,\pm}(\phi(R_1)) = 0$, we cannot use the same discussion as the previous proofs. It is easy to see that a point $\phi(\tilde{R}_0)$ represents the generalized Montgomery coefficients of $h_{3,\pm}$, where $\tilde{R}_0$ is a point such that $2\tilde{R}_0 = R_0$. From the fact that $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0) = 1$ or $h_{\mathcal{G},\mathcal{R}_0}(\tilde{R}_0) = -1$, we get the formulas to compute the generalized Montgomery coefficients of $h_{3,\pm}$. This completes the proof of Theorem 26. □

5.3 Difference of some formulas for generalized Montgomery coefficients

Now, we focus on the formulas for odd-degree isogenies. By considering the symmetry of the equality and formulas of scalar multiplications, we show that formulas in Theorem 25 can be represented by the ratio of two polynomials in $\mathbb{Z}[\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q)]$. These formulas are correct; however, one may know that there are some different formulas to compute generalized Montgomery coefficients on Montgomery curves (*e.g.,* those proposed in [CH17], and those proposed in [MR18]). Thus, a question arises: Are these formulas generalized by formulas via a generalized Montgomery coordinate? The answer is yes. The following theorem claims that we can construct these formulas by considering division polynomials of the generalized Montgomery coordinates (Definition 21).

Theorem 27. *Let ℓ be an odd prime, and K be a field whose characteristic is neither 2 nor ℓ. Suppose that $\phi_1, \phi_2, \phi_3, \phi_4$ are polynomials in $\mathbb{Z}[\alpha, h]$ always satisfying $\phi_2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q)) \neq 0$, $\phi_4(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q)) \neq 0$, and*

$$\alpha_{h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}} = \frac{\phi_1(\alpha_{h_{\mathcal{G}_E,\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q))}{\phi_2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q))} = \frac{\phi_3(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q))}{\phi_4(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q))}.$$

Here, E is an arbitrary elliptic curve defined over $\overline{K}$, $h_{\mathcal{G},\mathcal{R}_0}$ is its arbitrary normalized generalized Montgomery coordinate, Q is an arbitrary point of order ℓ in E, ϕ is a separable isogeny with $\ker \phi = \langle Q \rangle$, and $h_{\phi(\mathcal{G}),\phi(\mathcal{R}_0)}$ is a normalized generalized Montgomery coordinate of $E/\langle Q \rangle$ defined in Theorem 23. Then, it holds that if the characteristic of K is $p > 0$,

$$\frac{\phi_1(\alpha, h)}{\phi_2(\alpha, h)} - \frac{\phi_3(\alpha, h)}{\phi_4(\alpha, h)} \equiv \psi_\ell(\alpha, h) \cdot \frac{\varphi_1(\alpha, h)}{\varphi_2(\alpha, h)} \pmod{p},$$

and if the characteristic of K *is* 0*,*

$$\frac{\phi_1(\alpha,h)}{\phi_2(\alpha,h)} - \frac{\phi_3(\alpha,h)}{\phi_4(\alpha,h)} = \psi_\ell(\alpha,h)\cdot\frac{\varphi_1(\alpha,h)}{\varphi_2(\alpha,h)},$$

where ψ_ℓ *is the* ℓ*-th division polynomial of the generalized Montgomery coordinates, and* φ_1 *and* φ_2 *are polynomials in* $\mathbb{Z}[\alpha,h]$ *such that* $\varphi_2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q)) \neq 0$ *for all* $(E, h_{\mathcal{G},\mathcal{R}_0})$ *and* Q*.*

Proof. Suppose that the characteristic of K is $p > 0$. We define $\phi(\alpha,h) \in \mathbb{Z}[\alpha,h]$ as

$$\phi(\alpha,h) = \phi_1(\alpha,h)\phi_4(\alpha,h) - \phi_2(\alpha,h)\phi_3(\alpha,h).$$

Then, it holds that $\phi(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q)) = 0$ for all $(E, h_{\mathcal{G},\mathcal{R}_0})$ and $Q \in E[\ell] \setminus \{O_E\}$ because ℓ is a prime number. Therefore, from Theorem 22, there is a polynomial φ_1 in $\mathbb{Z}[\alpha,h]$ such that $\phi(\alpha,h) \equiv \psi_\ell(\alpha,h)\cdot\varphi_1(\alpha,h) \pmod{p}$. We define $\varphi_2 \in \mathbb{Z}[\alpha,h]$ as $\varphi_2(\alpha,h) = \phi_2(\alpha,h)\phi_4(\alpha,h)$. It is clear that $\varphi_2(\alpha_{h_{\mathcal{G},\mathcal{R}_0}}, h_{\mathcal{G},\mathcal{R}_0}(Q)) \neq 0$ for all $(E, h_{\mathcal{G},\mathcal{R}_0})$ and $Q \in E[\ell] \setminus \{O_E\}$. This completes the proof in the case that the characteristic of K is $p > 0$.

The case that the characteristic of K is 0 can be proved similarly. □

Remark 28. In Theorem 27, we fix that ℓ is a prime number. However, if ℓ is not prime, similar theorems also hold. In these theorems, the parts of division polynomials of their equalities get slightly complicated.

From Theorem 27, the problem of constructing an efficient formula is reduced to the problem of finding a proper element in an ideal I_m defined in Theorem 22. We believe that we can use this consideration to estimate the lower bound of the cost of formulas of isogeny computation. This will be done in our future works.

6 Applications of a generalized Montgomery coordinate

In this section, we explain two applications of a generalized Montgomery coordinate. The first one is the construction of a new efficient formula to compute isogenies on Montgomery curves. The second one is the construction of a new generalized Montgomery coordinate on Montgomery$^-$ curves which can construct the new algorithm of CSURF.

6.1 New formulas to compute isogenies on Montgomery curves

As was seen in Subsection 3.3, the inverse of the w-coordinate on an Edwards curve is a normalized generalized Montgomery coordinate. Therefore, we know that the formula on Montgomery curves and that on Edwards curves are essentially same. This sight leads to a formula of w-coordinates to those of x-coordinates. Kim *et al.* proposed in [KYPH19] formulas to compute odd degree isogenies. Let ℓ be an odd integer, and let P be a point of order ℓ. Let ϕ be an isogeny $E \to E/\langle P\rangle$ with $\ker\phi = \langle P\rangle$. Then, we can compute an Edwards coefficient of $E/\langle P\rangle$ denoted by d' as follows [KYPH19]:

$$d' = d^{\ell} \prod_{k=1}^{s} \frac{(w(kP)+1)^8}{2^8},$$

where d is the Edwards coefficient of E, and s is an integer such that $\ell = 2s+1$. From the doubling formula of w-coordinates of Edwards curves in [FH17], we have the generalized Montgomery coefficient of w^{-1} is $2 - 4/d$. Hence, from Theorem 12, there is an isogeny $\phi\colon E \to F$ of degree 4 such that $x \circ \phi = w^{-1}$, where F is a Montgomery curve whose coefficient is $2 - 4/d$. Now, we can construct a new formula on Montgomery curves. Let ϕ' be an isogeny $F \to F/\langle Q\rangle$ with $\ker\phi' = \langle Q\rangle$, where Q is a point in F of order ℓ. Since ℓ is odd, it is easy to see that the Montgomery coefficient of $F/\langle Q\rangle$ is $2 - 4/d'$. Note that for any $\alpha \in K \setminus \{\pm 2\}$, the curve

$$x^2 + y^2 = 1 + \frac{4}{2-\alpha}x^2y^2$$

is an Edwards curve, and its w-coordinate corresponds to the x-coordinate of the Montgomery curve $y^2 = x^3 + \alpha x^2 + x$. Thus, we can compute the Montgomery coefficient of $F/\langle Q\rangle$ denoted by α' as follows:

$$\frac{2-\alpha'}{4} = \left(\frac{2-\alpha}{4}\right)^{\ell} \prod_{k=1}^{s} \frac{(2x(kQ))^8}{(1+x(kQ))^8},$$

where α is the Montgomery coefficient of F. Moreover, by considering the quadratic twist, we can also construct the following formula:

$$\frac{\alpha'+2}{4} = \left(\frac{\alpha+2}{4}\right)^{\ell} \prod_{k=1}^{s} \frac{(2x(kQ))^8}{(1-x(kQ))^8}.$$

One may transplant the formula on Edwards curves to Montgomery curves by using an isomorphism between these curves. However, this process is more complicated than the construction using a generalized Montgomery coordinate. That is, by considering a generalized Montgomery coordinate, we can transplant formulas naturally.

This formula is as efficient as that proposed by Meyer and Reith [MR18] for basic calculations. In addition, as the √élu's formula, this formula is more efficient than that proposed in [BDFLS20]. The √élu's formula is a method for making computations of large prime degree isogenies more efficient. In [BDFLS20], Bernstein *et al.,* first proposed the √élu's formula on Montgomery curves. In [MOT20a], Moriya, Onuki, and Takagi suggested that the √élu's formula on Edwards curves is more efficient than the original √élu's formula for large degree isogenies. Because we can adapt the method of [MOT20a] to our new formula, this is more efficient than that proposed in [BDFLS20] for large degree isogenies.

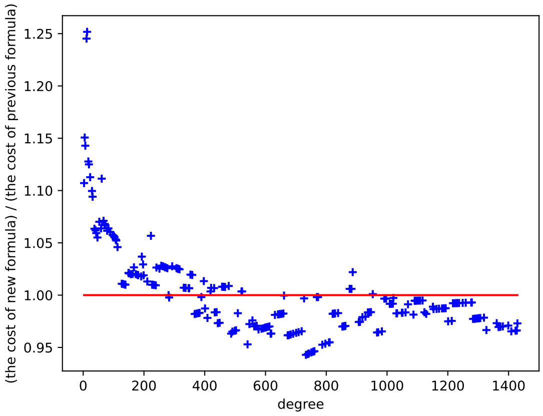

Fig. 2. Ratio of the cost of our new formula to that of the previous formula

We implemented our new formula based on the SIBC Python library [ACDRH21] in [ACDRH20], and compared its cost to that obtained by the previous formula implemented by [ACDRH21] at various prime degrees. The implementation results are in Figure 2. Here, we use the 4096-bits prime defined in [ACDRH21] as p, and measured the number of multiplications and squarings in $\mathbb{F}_p$ as the cost. The vertical line shows the ratio of the cost of our new formula to that of the previous formula, and the horizontal line shows the degree of isogenies. That is, at the points below the line of 1.00, our new formula is more efficient than the previous one. Therefore, for large degree isogenies, our proposed formula is faster in terms of the number of multiplications and squarings in $\mathbb{F}_p$ in our implementation. It is one of our future works to confirm this formula is faster than previous one when implemented in low-level programming languages (*e.g.*, C) in practical. Our source code is available from `http://tomoriya.work/code.html`.

6.2 New generalized Montgomery coordinate to compute isogenies on Montgomery$^-$ curves

In this subsection, we construct a new normalized generalized Montgomery coordinate on a Montgomery$^-$ curve. Montgomery$^-$ curves are mainly used for CSURF [CD20]. This coordinate allows us to compute isogenies on Montgomery$^-$ curves by the same formulas on Montgomery curves.

Let E be a Montgomery$^-$ curve $y^2 = x^3 + \alpha x^2 - x$, and let $(a, 0)$ and $(-1/a, 0)$ be points of order 2 other than $(0, 0)$. We have

$$\operatorname{div} x = 2((0,0)) - 2(O_E),$$
$$\operatorname{div} y = ((a,0)) + ((-1/a,0)) + ((0,0)) - 3(O_E).$$

Therefore, it holds that

$$\operatorname{div}(y^2/x^2) = 2((a,0)) + 2((-1/a,0)) - 2((0,0)) - 2(O_E).$$

Direct calculation leads to

$$\frac{y(P)^2}{x(P)^2} \cdot \frac{y(P+(a,0))^2}{x(P+(a,0))^2} = \frac{(a^2+1)^2}{a^2} = \alpha^2 + 4.$$

Therefore, $\frac{1}{\sqrt{\alpha^2+4}} y^2/x^2$ is a normalized generalized Montgomery coordinate on E with respect to $\langle(0,0)\rangle$ and $(a,0)$. Here, we take p satisfying $p \equiv 3 \pmod 4$, and fix $\sqrt{\cdot} \colon \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ such that $\sqrt{\cdot}|_{(\mathbb{F}_p)^2} \colon (\mathbb{F}_p)^2 \to \mathbb{F}_p$ to $\sqrt{A} = A^{\frac{p+1}{4}}$. We denote $\frac{1}{\sqrt{\alpha^2+4}} y^2/x^2$ by w. Because the double of $(\sqrt{-1}, \sqrt{-\alpha - 2\sqrt{-1}})$ is $(0,0)$, the generalized Montgomery coefficient of w is

$$\alpha_w = -w(\sqrt{-1}, \sqrt{-\alpha - 2\sqrt{-1}}) - \frac{1}{w(\sqrt{-1}, \sqrt{-\alpha - 2\sqrt{-1}})} = -\frac{2\alpha}{\sqrt{\alpha^2+4}}.$$

Remark 29. If a supersingular elliptic curve E defined over $\mathbb{F}_p$ has the $\mathbb{F}_p$-endomorphism ring isomorphic to $\mathbb{Z}[\frac{\sqrt{-p}+1}{2}]$, we say E is on the surface, and if a supersingular elliptic curve E defined over $\mathbb{F}_p$ has the $\mathbb{F}_p$-endomorphism ring isomorphic to $\mathbb{Z}[\sqrt{-p}]$, we say E is on the floor.

From Theorem 12, the w-coordinate of the Montgomery$^-$ curve can be represented by $w = x \circ \phi$, where ϕ is an isogeny with $\ker\phi = \langle(0,0)\rangle$. This isogeny is the 2-isogeny which maps an elliptic curve on the surface to that on the floor [CD20, Lemma 2].

Since $\#\langle(0,0)\rangle = 2$, we can compute isogenies of odd degree of Montgomery$^-$ curves by the same formulas on Montgomery curves via the w-coordinates. In [CDV20], the authors mentioned that by considering an isogeny from Montgomery$^-$ curves to curves on the floor, the CSURF algorithm becomes more efficient because formulas on Montgomery curves are used. From Remark 29, this technique is the same as considering the w-coordinate of Montgomery$^-$ curves.

However, the calculation of 2-isogenies dose not work via the w-coordinates. Let $\phi \colon E \to E'$ be a 2-isogeny between Montgomery$^-$ curves with $\ker\phi = \langle(a,0)\rangle$. We denote the w-coordinates on E and E' by w_E and $w_{E'}$, respectively. Suppose that there is a map $f \colon \mathbb{P}^1 \to \mathbb{P}^1$ such that $w_{E'}(\phi(P)) = f(w_E(P))$. As $w_E(P + (0,0)) = w_E(P)$, it holds that $f(w_E(P + (0,0))) = f(w_E(P))$. In contrast, because $\phi(0,0)$ is the back track point of ϕ (*i.e.,* $\ker\hat{\phi} = \langle\phi(0,0)\rangle$), it holds that $w_{E'}(\phi(P + (0,0))) = 1/w_{E'}(\phi(P))$. This is a contradiction. Therefore, we cannot compute $w_{E'}(P)$ from $w_E(P)$. However, we can compute the generalized Montgomery coefficient of $w_{E'}$ from that of w_E by the following theorems.

Theorem 30 (2-isogeny). *Let $p \equiv 7 \pmod 8$ and let $\phi \colon E \to E'$ be a 2-isogeny defined over $\mathbb{F}_p$ with $\ker\phi = \langle P\rangle$. We denote the w-coordinates on E and E' by w_E and $w_{E'}$, respectively. We denote the generalized Montgomery* *coefficients of these coordinates by α_{w_E} and $\alpha_{w_{E'}}$, respectively. Then, if the halves of P are defined over $\mathbb{F}_p$, it holds that*

$$\alpha_{w_{E'}} = -2\frac{\alpha_{w_E}+6-12\sqrt{\alpha_{w_E}+2}}{\alpha_{w_E}+6+4\sqrt{\alpha_{w_E}+2}} = -2+\frac{32\sqrt{\alpha_{w_E}+2}}{(\sqrt{\alpha_{w_E}+2}+2)^2}, \tag{1}$$

and if the halves of P are in $\ker(\pi_p+1)$, the formula is obtained by replacing $\alpha_{w_{E'}}$ and α_{w_E} in the equation (1) with $-\alpha_{w_{E'}}$ and $-\alpha_{w_E}$, respectively, where π_p is the p-Frobenius map on E.

Theorem 31 (4-isogeny). *Let $p \equiv 7 \pmod 8$, and let $\phi\colon E \to E'$ be a 4-isogeny defined over $\mathbb{F}_p$ with $\ker\phi = \langle P\rangle$ defined over $\mathbb{F}_p$. We denote the w-coordinates on E and E' by w_E and $w_{E'}$, respectively. We denote the generalized Montgomery coefficients of these coordinates by α_{w_E} and $\alpha_{w_{E'}}$, respectively. Then, if P is defined over $\mathbb{F}_p$, it holds that*

$$\frac{\alpha_{w_{E'}}+2}{4} = \frac{8\varepsilon\sqrt[4]{\frac{\alpha_{w_E}+2}{4}}\left(\sqrt{\frac{\alpha_{w_E}+2}{4}}+1\right)}{\left(2\sqrt[4]{\frac{\alpha_{w_E}+2}{4}}+\varepsilon\left(\sqrt{\frac{\alpha_{w_E}+2}{4}}+1\right)\right)^2}, \tag{2}$$

where $\varepsilon = (-1)^{\frac{p+1}{8}}$, and if P is in $\ker(\pi_p+1)$, the formula is obtained by replacing $\alpha_{w_{E'}}$ and α_{w_E} in the equation (2) with $-\alpha_{w_{E'}}$ and $-\alpha_{w_E}$, respectively.

To prove these theorems, we first prove the following lemmas.

Lemma 32. *Let $p \equiv 7 \pmod 8$, and let α be a generalized Montgomery coefficient of the w-coordinate of a supersingular Montgomery$^-$ curve defined over $\mathbb{F}_p$. Then, it holds that $\alpha+2 \in (\mathbb{F}_p)^2$ and $2-\alpha \in (\mathbb{F}_p)^2$.*

Proof. Let E be a Montgomery curve $y^2 = x^3+\alpha x^2+x$. From Remark 28,it holds that $\mathrm{End}_p(E) \cong \mathbb{Z}[\pi_p]$. Therefore, we have $E[8]\cap\ker(\pi_p-1) \cong \mathbb{Z}/8\mathbb{Z}$ and $E[8]\cap\ker(\pi_p+1) \cong \mathbb{Z}/8\mathbb{Z}$. Since $(1,\sqrt{\alpha+2}) \in E[4]$, $(1,\sqrt{\alpha+2})$ belongs to $2(\ker(\pi_p-1))$ or $2(\ker(\pi_p+1))$. From [MOT20b, Proposition 1], we have $(1,\sqrt{\alpha+2}) \in \ker(\pi_p-1)$. Therefore, $\alpha+2 \in (\mathbb{F}_p)^2$. Note that E has only one point of order 2 defined over $\mathbb{F}_p$. Hence, it holds that $\alpha^2-4 \notin (\mathbb{F}_p)^2$. Since $\alpha+2 \in (\mathbb{F}_p)^2$, it holds that $2-\alpha \in (\mathbb{F}_p)^2$. □

Lemma 33. *Let $p \equiv 7 \pmod 8$, and let α be a generalized Montgomery coefficient of the w-coordinate of a supersingular Montgomery$^-$ curve defined over $\mathbb{F}_p$. If $p \equiv 15 \pmod{16}$, then $\sqrt{\alpha+2}+2 \in (\mathbb{F}_p)^2$ and $\sqrt{2-\alpha}+2 \in (\mathbb{F}_p)^2$, and if $p \equiv 7 \pmod{16}$, then $\sqrt{\alpha+2}+2 \notin (\mathbb{F}_p)^2$ and $\sqrt{2-\alpha}+2 \notin (\mathbb{F}_p)^2$.*

Proof. Since $-\alpha$ is also a generalized Montgomery coefficient of the w-coordinate of some supersingular Montgomery$^-$ curve, it is suffice to consider whether $\sqrt{\alpha+2}+2$ is square or not. Let E be a Montgomery curve $y^2 = x^3+\alpha x^2+x$. Since E is on the floor, it holds that $E(\mathbb{F}_p)[8] \cong \mathbb{Z}/8\mathbb{Z}$. From Lemma 32, we have $(1,\sqrt{\alpha+2}) \in E(\mathbb{F}_p)[4]$. Therefore, the following equation has the roots in $\mathbb{F}_p$:

$$4(x^3+\alpha x^2+x) = (x^2-1)^2.$$

It is easy to see that the roots of this equation are $-\frac{1}{2}(\sqrt[4]{\alpha+2} \pm \sqrt{\sqrt{\alpha+2}-2})^2$ and $\frac{1}{2}(\sqrt[4]{\alpha+2} \pm \sqrt{\sqrt{\alpha+2}+2})^2$. From Lemma 32, it holds that $\sqrt[4]{\alpha+2} \in \mathbb{F}_p$ and

$$(\sqrt{\alpha+2}-2)(\sqrt{\alpha+2}+2) = \alpha - 2 \notin (\mathbb{F}_p)^2.$$

Therefore, if $\sqrt{\alpha+2}+2$ is square in $\mathbb{F}_p$, then $\frac{1}{2}(\sqrt[4]{\alpha+2} \pm \sqrt{\sqrt{\alpha+2}+2})^2$ is a x-coordinate of a point of order 8 defined over $\mathbb{F}_p$, and if $\sqrt{\alpha+2}+2$ is not square in $\mathbb{F}_p$, then $-\frac{1}{2}(\sqrt[4]{\alpha+2} \pm \sqrt{\sqrt{\alpha+2}-2})^2$ is a x-coordinate of a point of order 8 defined over $\mathbb{F}_p$. We let P be a point of order 8 defined over $\mathbb{F}_p$. From [MOT20b, Proposition 1], if $\sqrt{\alpha+2}+2$ is square in $\mathbb{F}_p$, then $P \in 2E(\mathbb{F}_p)$. Hence, it holds that $16 \mid \#E(\mathbb{F}_p)$ and $p \equiv 15 \pmod{16}$. If $\sqrt{\alpha+2}+2$ is not square in $\mathbb{F}_p$, then $P \notin 2E(\mathbb{F}_p)$. Hence, it holds that $16 \nmid \#E(\mathbb{F}_p)$ and $p \equiv 7 \pmod{16}$. This completes the proof of Lemma 33. □

Now, we prove Theorem 30 and Theorem 31.

Proof (Theorem 30). From [CD20, Lemma 2 and Lemma 5], the halves of P are in $\ker(\pi_p - 1)$, or they are in $\ker(\pi_p + 1)$. We first consider a 4-isogeny from $F\colon y^2 = x^3 + \alpha_{w_E}x^2 + x$. From [JDF11, equation (20)] and Lemma 32, it holds that

$$F_1 := F/\langle(1, \sqrt{\alpha_{w_E}+2})\rangle \colon y^2 = x^3 - 2\frac{\alpha_{w_E}+6}{2-\alpha_{w_E}}x^2 + x,$$
$$F_2 := F/\langle(-1, \sqrt{(-1)(2-\alpha_{w_E})})\rangle \colon y^2 = x^3 - 2\frac{\alpha_{w_E}-6}{\alpha_{w_E}+2}x^2 + x.$$

Denote one of the halves of P by Q. Let $\psi\colon E \to F$ be a 2-isogeny satisfying $w_E = x \circ \psi$. It is clear that if $Q \in \ker(\pi_p - 1)$ (*resp.* $Q \in \ker(\pi_p + 1)$), then $\psi(Q) \in \ker(\pi_p - 1)$ (*resp.* $\psi(Q) \in \ker(\pi_p + 1)$). Therefore, if $Q \in \ker(\pi_p - 1)$, then $Q = (1, \sqrt{\alpha_{w_E}+2})$, and if $Q \in \ker(\pi_p + 1)$, then $Q = (-1, \sqrt{\alpha_{w_E}-2})$. Hence, if $Q \in \ker(\pi_p - 1)$, then $E' \cong F_1$, and if $Q \in \ker(\pi_p + 1)$, then $E' \cong F_2$.

We now fix $Q \in \ker(\pi_p - 1)$. From Remark 28,it is suffice to consider a 2-isogeny from F_1 to an elliptic curve on the floor. The points of order 2 are $(0,0)$ and

$$\left(\frac{\alpha_{w_E}+6 \pm 4\sqrt{\alpha_{w_E}+2}}{2-\alpha_{w_E}}, 0\right).$$

Since $(0,0)$ is the backtrack point of the isogeny $F \to F_1$, the codomain of the isogeny whose kernel is $\langle(0,0)\rangle$ is on the surface. From [CD20, Lemma 2 and Lemma 5], the generator of the kernel of the isogeny mapping from F to an elliptic curve on the floor satisfies the x-coordinates of its halves are not in $\mathbb{F}_p$. Let

$$\tilde{\alpha}_\pm := \frac{\alpha_{w_E}+6 \pm 4\sqrt{\alpha_{w_E}+2}}{2-\alpha_{w_E}},$$

respectively. The x-coordinates of the halves of $(\tilde{\alpha}_\pm, 0)$ are the roots of the equation

$$\tilde{\alpha}_\pm = \frac{(x^2-1)^2}{4(x^3 - (\tilde{\alpha}_\pm + 1/\tilde{\alpha}_\pm)x^2 + x)}.$$

The roots of this equation is $x = \tilde{\alpha}_\pm \pm \sqrt{\tilde{\alpha}_\pm^2 - 1}$. Therefore, if $\tilde{\alpha}_\pm^2 - 1 \notin (\mathbb{F}_p)^2$, then $(\tilde{\alpha}_\pm, 0)$ is the generator of the kernel of the isogeny mapping from F to an elliptic curve on the floor. We have

$$\begin{aligned}\tilde{\alpha}_+^2 - 1 &= \frac{8\sqrt{\alpha_{w_E}+2}}{(2-\alpha_{w_E})^2}(\sqrt{\alpha_{w_E}+2}+2)^2,\\ \tilde{\alpha}_-^2 - 1 &= -\frac{8\sqrt{\alpha_{w_E}+2}}{(2-\alpha_{w_E})^2}(\sqrt{\alpha_{w_E}+2}-2)^2.\end{aligned}$$

From Lemma 32, it holds that $\sqrt{\alpha_{w_E}+2}^{\frac{p-1}{2}} = (\alpha_{w_E}+2)^{\frac{p-1}{2}\frac{p+1}{4}} = 1$. Therefore, $\sqrt{\alpha_{w_E}+2} \in (\mathbb{F}_p)^2$. Since $p \equiv 7 \pmod 8$, we have $8 \in (\mathbb{F}_p)^2$. Therefore, $\tilde{\alpha}_+^2 - 1 \in (\mathbb{F}_p)^2$ and $\tilde{\alpha}_-^2 - 1 \notin (\mathbb{F}_p)^2$. So, the generator of the kernel of the target isogeny is $(\tilde{\alpha}_-, 0)$. Note that $\tilde{\alpha}_- = (\sqrt{\alpha_{w_E}+2}-2)^2/(2-\alpha_{w_E}) \in (\mathbb{F}_p)^2$. From [Ren18, Proposition 2], we have $F_1/\langle(\tilde{\alpha}_-, 0)\rangle$ is

$$y^2 = x^3 - 2\frac{\alpha_{w_E}+6-12\sqrt{\alpha_{w_E}+2}}{\alpha_{w_E}+6+4\sqrt{\alpha_{w_E}+2}}x^2 + x.$$

Since $\alpha_{w_{E'}}$ is the Montgomery coefficient of this curve, we complete the half of the proof.

In the case that $Q \in \ker(\pi_p + 1)$, we have the following equation by the same discussion as above:

$$\alpha_{w_{E'}} = 2\frac{\alpha_{w_E}-6+12\sqrt{2-\alpha_{w_E}}}{\alpha_{w_E}-6-4\sqrt{2-\alpha_{w_E}}}.$$

This completes the proof of Theorem 30. □

Proof (Theorem 31). Since Montgomery$^-$ curves defined over $\mathbb{F}_p$ are on surface [CD20, Figure 1 and Figure 2], the given 4-isogeny is the composition of 2-isogenies in Theorem 30. Lemma 33 gives us the proof of Theorem 31. □

From [CD20, Figure 2] and Theorem 12, the generalized Montgomery coefficient of the w-coordinate is unique for an $\mathbb{F}_p$-isomorphism class. Then, from above theorems, we can construct a new CSURF algorithm via the w-coordinate of Montgomery$^-$ curves. In the previous CSURF algorithm, we had to move from the elliptic curves on the surface to those on the floor because of some speed-up techniques (*e.g.*, Radical isogenies [CDV20,OM21]). In contrast, since our proposed algorithm consists only of the arithmetic of curves on the floor, we can use these speed-up techniques without moving from one curve to another. Thus, this algorithm realizes a simple implementation using only one coordinate.

7 Conclusion

In this paper, we proposed a novel function on elliptic curves called the generalized Montgomery coordinate. This is a generalization of some standard coordinates in isogeny-based cryptography which have been studied separately, *i.e.*, the

x-coordinate of Montgomery curves, the x-coordinate of Montgomery$^-$ curves, the w-coordinate of Edwards curves, and the w-coordinate of Huff's curves.

Next, we constructed explicit formulas of scalar multiplication including the division polynomial and isogeny computation via a generalized Montgomery coordinate. We obtained these formulas by considering the divisors of the functions related to scalar multiplication and isogeny computation. Note that our new formulas are independently constructed from the forms of elliptic curves that decide the above conventional coordinates. Moreover, there are two formulas for isogeny computation: a formula for an image point and a formula for a target elliptic curve. The formula for an image point is unique for any generalized Montgomery coordinate; however, that for a target elliptic curve has some different forms. We proved that this difference is due to the division polynomial of the generalized Montgomery coordinates.

We believe the theory of a generalized Montgomery coordinate has many applications. In this paper, we considered two applications as an initial trial. First, we constructed a new formula for isogeny computation of Montgomery curves. This formula is based on that of w-coordinates on Edwards curves and is more efficient for large degree isogenies than previous formulas of Montgomery curves in our implementation. Furthermore, we proposed a new generalized Montgomery coordinate of Montgomery$^-$ curves. This coordinate allows us to construct the new algorithm of CSURF that gives a simple implementation. It is an open problem to construct further applications of a generalized Montgomery coordinate.

Acknowledgment. This work was supported by JSPS KAKENHI Grant Number JP21J10711, JSPS KAKENHI Grant Number JP21K17739, JST ACT-X Grant Number JPMJAX2001, and JST CREST Grant Number JPMJCR2113.

References

ACC$^+$17. Reza Azarderakhsh, Matthew Campagna, Craig Costello, LD Feo, Basil Hess, A Jalali, D Jao, B Koziel, B LaMacchia, P Longa, et al. Supersingular isogeny key encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 2017.

ACDRH20. Gora Adj, Jesús-Javier Chi-Domínguez, and Francisco Rodríguez-Henríquez. Karatsuba-based square-root Vélu's formulas applied to two isogeny-based protocols. *IACR Cryptology ePrint Archive*, 2020:1109, 2020. `https://ia.cr/2020/1109`.

ACDRH21. Gora Adj, Jesús-Javier Chi-Domínguez, and Francisco Rodríguez-Henríquez. SIBC python library. `https://github.com/JJChiDguez/sibc/`, 2021.

BCKL15. Daniel J Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted Hessian curves. In *International Conference on Cryptology and Information Security in Latin America–LATINCRYPT 2015*, pages 269–294. Springer, 2015.

BDFLS20. Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In *Proceedings* *of the Fourteenth Algorithmic Number Theory Symposium–ANTS 2020*, volume 4, pages 39–55. Mathematical Sciences Publishers, 2020.

BDFM21. Fouazou Lontouo Perez Broon, Thinh Dang, Emmanuel Fouotsa, and Dustin Moody. Isogenies on twisted Hessian curves. *Journal of Mathematical Cryptology*, 15(1):345–358, 2021.

BKV19. Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2019*, pages 227–247. Springer, 2019.

BL07. Daniel J Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2007*, pages 29–50. Springer, 2007.

BL17. Daniel J. Bernstein and Tanja Lange. Montgomery curves and the Montgomery ladder. In *Topics in Computational Number Theory Inspired by Peter L. Montgomery*, page 82–115, 2017.

CD20. Wouter Castryck and Thomas Decru. CSIDH on the surface. In *International Conference on Post-Quantum Cryptography–PQCrypto 2020*, page 1404. Springer, 2020.

CDV20. Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2020*, pages 493–519. Springer, 2020.

CH17. Craig Costello and Huseyin 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–ASIACRYPT 2017*, pages 303–329. Springer, 2017.

CLG09. Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *Journal of CRYPTOLOGY*, 22(1):93–113, 2009.

CLM$^+$18. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2018*, pages 395–427. Springer, 2018.

Cou06. Jean Marc Couveignes. Hard homogeneous spaces. *IACR Cryptology ePrint Archive*, 2006:291, 2006. `https://ia.cr/2006/291`.

CS18. Craig Costello and Benjamin Smith. Montgomery curves and their arithmetic: The case of large characteristic fields. *Journal of Cryptographic Engineering*, 8(3):227–240, 2018.

DFG19. Luca De Feo and Steven D Galbraith. SeaSign: Compact isogeny signatures from class group actions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques–EUROCRYPT 2019*, pages 759–789. Springer, 2019.

DFKL$^+$20. Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2020*, pages 64–93. Springer, 2020.

DKW20. Robert Dryło, Tomasz Kijko, and Michał Wroński. Efficient Montgomery-like formulas for general Huff's and Huff's elliptic curves and their applications to the isogeny-based cryptography. *IACR Cryptology ePrint Archive*, 2020:526, 2020. `https://ia.cr/2020/526`.

Edw07. Harold Edwards. A normal form for elliptic curves. *Bulletin of the American mathematical society*, 44(3):393–422, 2007.

FH17. Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini. Differential addition on Twisted Edwards curves. In *Australasian Conference on Information Security and Privacy–ACISP 2017*, pages 366–378. Springer, 2017.

FJ10. Reza R Farashahi and Marc Joye. Efficient arithmetic on Hessian curves. In *International Workshop on Public Key Cryptography–PKC 2010*, pages 243–260. Springer, 2010.

FNW10. Rongquan Feng, Menglong Nie, and Hongfeng Wu. Twisted Jacobi intersections curves. In *International Conference on Theory and Applications of Models of Computation–TAMC 2010*, pages 199–210. Springer, 2010.

FP21. Tako Boris Fouotsa and Christophe Petit. SimS: A simplification of SiGamal. In *International Conference on Post-Quantum Cryptography–PQCrypto 2021*, pages 277–295. Springer, 2021.

Gal12. Steven D Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2012.

Huf48. Gerald B Huff. Diophantine problems in geometry and elliptic ternary forms. *Duke mathematical journal*, 15(2):443–453, 1948.

HWZ21. Zhi Hu, Lin Wang, and Zijian Zhou. Isogeny computation on Twisted Jacobi intersections. In *International Conference on Information Security Practice and Experience–ISPEC 2021*, pages 46–56. Springer, 2021.

HZHL20. Yan Huang, Fangguo Zhang, Zhi Hu, and Zhijie Liu. Optimized arithmetic operations for isogeny-based cryptography on Huff curves. In *Australasian Conference on Information Security and Privacy–ACISP 2020*, pages 23–40. Springer, 2020.

JDF11. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography–PQCrypto 2011*, pages 19–34. Springer, 2011.

JTV10. Marc Joye, Mehdi Tibouchi, and Damien Vergnaud. Huff's model for elliptic curves. In *International Algorithmic Number Theory Symposium–ANTS 2010*, pages 234–250. Springer, 2010.

Kim21. Suhri Kim. Complete analysis of implementing isogeny-based cryptography using Huff form of elliptic curves. *IEEE Access*, 9:154500–154512, 2021.

Koh11. David Kohel. Addition law structure of elliptic curves. *Journal of Number Theory*, 131(5):894–919, 2011.

KYPH19. 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.

Mon87. Peter L Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987.

MOT20a. 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. The extended version is in IACR Cryptology ePrint Archive, 2019:843, 2019. `https://ia.cr/2019/843`.

MOT20b. Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. SiGamal: A supersingular isogeny-based pke and its application to a prf. In *International Conference on the Theory and Application of Cryptology and Information Security–ASIACRYPT 2020*, pages 551–580. Springer, 2020.

MR18. Michael Meyer and Steffen Reith. A faster way to the CSIDH. In *International Conference on Cryptology in India–INDOCRYPT 2018*, pages 137–152. Springer, 2018.

OM21. Hiroshi Onuki and Tomoki Moriya. Radical isogenies on Montgomery curves. *IACR Cryptology ePrint Archive*, 2021:699, 2021. `https://ia.cr/2021/699`.

oST16. National Institute of Standards and Technology. Post–quantum cryptography standardization, December 2016. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`.

Ren18. Joost Renes. Computing isogenies between Montgomery curves using the action of (0, 0). In *International Conference on Post-Quantum Cryptography–PQCrypto 2018*, pages 229–247. Springer, 2018.

RS06. Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006:145, 2006. `https://ia.cr/2006/145`.

Sho94. Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

Sil09. Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

Sto10. Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications*, 4(2):215–235, 2010.

Vél71. Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris Sér. A*, 273(5):238–241, 1971.

Wro21. Michał Wroński. Application of Velusqrt algorithm to Huff's and general Huff's curves. *IACR Cryptol. ePrint Arch.*, 2021:73, 2021. `https://ia.cr/2021/73`.