IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2024, No. 4, pp. 737–762. DOI:10.46586/tches.v2024.i4.737-762

Faster Complete Addition Laws for Montgomery Curves

Reza Rezaeian Farashahi[1,3,*], Mojtaba Fadavi[2] and Soheila Sabbaghian[1]

[1] Department of Mathematical Sciences, Isfahan University of Technology, 84156-83111, Isfahan, Iran, farashahi@iut.ac.ir, s.sabbaghian@math.iut.ac.ir

[2] Department of Computer Science, University of Calgary, 2500 University Drive, NW Calgary T2N 1N4, Canada, mojtaba.fadavi@ucalgary.ca

[3] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P.O. Box 19395-5746, Tehran, Iran.

Abstract. An addition law for an elliptic curve is *complete* if it is defined for all possible pairs of input points on the elliptic curve. In Elliptic Curve Cryptography (ECC), a complete addition law provides a natural protection against side-channel attacks which are based on Simple Power Analysis (SPA). Montgomery curves are a specific family of elliptic curves that play a crucial role in ECC because of its well-known Montgomery ladder, particularly in the Elliptic Curve Diffie-Hellman Key Exchange (ECDHKE) protocol and the Elliptic Curve factorization Method (ECM). However, the complete addition law for Montgomery curves, as stated in the literature, has a computational cost of $14\mathbf{M}+2\mathbf{D}$, where $\mathbf{M},\mathbf{D}$ denote the costs of a field multiplication and a field multiplication by a constant, respectively. The lack of a competitive complete addition law has led implementers towards twisted Edwards curves, which offer a complete addition law at a lower cost of $8\mathbf{M}+1\mathbf{D}$ for appropriately chosen curve constants.

In this paper, we introduce extended Montgomery coordinates as a novel representation for points on Montgomery curves. This coordinate system enables us to define birational multiplication-free maps between the extended twisted Edwards coordinates and extended Montgomery coordinates. Using this map, we can transfer the complete addition laws from twisted Edwards curves to Montgomery curves without incurring additional multiplications or squarings. In addition, we employ a technique known as *scaling* to refine the addition laws for twisted Edwards curves, which results in having i) Complete addition laws with the costs varying between $8\mathbf{M}+1\mathbf{D}$ and $9\mathbf{M}+1\mathbf{D}$ for a broader range of twisted Edwards curves, ii) Incomplete addition laws for twisted Edwards curves with the cost of $8\mathbf{M}$. Consequently, by leveraging our birational multiplication-free maps, we present complete addition laws for Montgomery curves with the cost of $8\mathbf{M}+1\mathbf{D}$. This shows a significant improvement for complete addition law for Montgomery curves by reducing the computational cost by $6\mathbf{M}+1\mathbf{D}$. This improvement makes Montgomery curves a more attractive option for applications where an efficient complete addition law is essential.

Keywords: Elliptic Curve Cryptography · Montgomery curve · Complete addition law

1 Introduction

In the mid-1980s, Koblitz [Kob87] and Miller [Mil85] independently introduced Elliptic Curve Cryptography (ECC) by proposing the use of elliptic curves in designing cryptographic schemes. ECC stands out as an attractive asymmetric key cryptosystem, achieving

[*] Corresponding author

Received: 2024-04-15 Accepted: 2024-06-15 Published: 2024-09-05

the same level of security with significantly smaller key sizes than its counterparts. This efficiency reduces storage and transmission requirements and makes ECC particularly well-suited for environments with constrained resources. Beyond its foundational capabilities, ECC is equipped with unique mathematical constructions, such as bilinear pairings, which allow for the development of many novel cryptographic protocols. Notably, pairing-based cryptography has facilitated the creation of an identity-based encryption scheme [BF03], a short signature scheme [BLS04], and an efficient one-round protocol for tripartite Diffie-Hellman key exchange [Jou04]. However, in the presence of large-scale quantum computers, quantum algorithms break the security of the cryptographic schemes that rely on the Discrete Logarithm Problem [DH76, Gam85]. To avoid this fundamental problem, ECC has shifted towards the development of cryptographic schemes whose security is based on the difficulty of computing isogenies between elliptic curves as an intractable problem for large-scale quantum computers [Cou06, RS06, FJP14, CLM$^+$18, BKV19, FKL$^+$20]. Such an approach ensures that ECC continues to play a vital role in the advancement of secure post-quantum cryptography.

An elliptic curve E over a field $\mathbb{F}$ is a nonsingular absolutely irreducible projective curve of genus 1 defined over a field $\mathbb{F}$ with at least one $\mathbb{F}$-rational point. Every elliptic curve E over $\mathbb{F}$ can be represented by the projective Weierstrass equation

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \ a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}. \tag{1}$$

Let $E(\mathbb{F})$ be the set of $\mathbb{F}$-rational points of the Weierstrass curves E given in (1). The chord-tangent process turns $E(\mathbb{F})$ into an abelian additive group with identity element $\mathcal{O} = (0 : 1 : 0)$. Since efficiency in computing point addition and doubling is crucial for ECC, extensive research has focused on elliptic curves over finite fields to improve their arithmetic performance. In particular, alternative equations, such as the Legendre, Hessian, Montgomery, and Edwards, are used in ECC which have more efficient arithmetic. Representing an elliptic curve by these equations all depends on its group structure over the field $\mathbb{F}$. Furthermore, adopting different coordinate systems, including standard, weighted, and extended, serves as another strategy to enhance arithmetic operations on elliptic curves [Sil86, CFA$^+$05, Gal12].

In [Mon87], Montgomery introduced the family of Montgomery curves and the Montgomery ladder, initially to enhance Lenstra's Elliptic Curve factorization Method [Len87]. While they continue to be a vital part of contemporary factoring software, Montgomery curves are an appropriate choice for ECC due to their efficient arithmetic, most notably Bernstein's *Curve25519 software* [Ber06]. In [Edw07], Edwards introduced the family of Edwards curves, whose symmetric addition law quickly drew the attention of Bernstein and Lange so that they proposed using the Edwards curves in ECC [BL07a]. Inspired by the family of Edwards curves, they later introduced the family of twisted Edwards curves in [BBJ$^+$08], which covers a larger proportion of elliptic curves by containing both Edwards curves and their non-trivial quadratic twists. In the same work, they proved that the family of Montgomery curves and twisted Edwards curves are the same. To enhance arithmetic efficiency on twisted Edwards curves, they also introduced inverted coordinates in [BL07b]. Hisil et al. in [HWCD08] proposed extended twisted Edwards coordinates whose arithmetic is even more efficient compared to the arithmetic of inverted twisted Edwards coordinates.

Complete addition law. For an elliptic curve E defined over a field $\mathbb{F}$, an addition law is called $\mathbb{F}$-*complete* if for any two arbitrary points $P_1, P_2 \in E(\mathbb{F})$ the addition law outputs a point $P_1+P_2 \in E(\mathbb{F})$ without requiring separate considerations for different cases, i.e. $P_1 = P_2$, or $P_1 = -P_2$, or $P_1 = \mathcal{O}$, or $P_2 = \mathcal{O}$ or otherwise. Branching during addition operations in ECC implementations can expose vulnerabilities to side-channel attacks, enabling adversaries to extract secret information. One notable example is Simple Power

Analysis (SPA), where an attacker observes variations in power consumption during scalar multiplication. By analyzing these power traces, the attacker can deduce the secret scalar used in the computation without directly breaking the underlying cryptographic algorithm. To counteract SPA, ECC often uses constant-time algorithms, such as only x-coordinate operations and complete addition laws, to ensure consistent power consumption. For more details on only x-coordinate operations of Montgomery curves and the complete addition law of twisted Edwards curves, see [Mon87, BBJ$^+$08, HWCD08]. Furthermore, the complete addition law facilitates the efficient implementation of the addition law.

In [BL95], Bosma and Lenstra proved that every addition law on E has at least one exceptional pair of inputs when considered over $\overline{\mathbb{F}}$, the algebraic closure of $\mathbb{F}$. Thus, a $\mathbb{F}$-complete addition law on the elliptic curve E defined over $\mathbb{F}$ does not necessarily retain its completeness when applied to the same elliptic curve E defined over an arbitrary extension of $\mathbb{F}$. In their work, they demonstrated that the minimum number of addition laws for a system of complete addition laws for E equals two, i.e. for any pair of points $P_1, P_2 \in E(\overline{\mathbb{F}})$ at least one of the two addition laws in the collection outputs a point $P_3 = P_1 + P_2 \in E(\overline{\mathbb{F}})$.

Related works. Numerous studies have significantly contributed to the development of complete addition laws for different forms of elliptic curves defined over the finite field $\mathbb{F}_q$ [BL07a, FJ10, RCB16, FH17, KPKK19]. From now on, we shall focus exclusively on elliptic curves defined over $\mathbb{F}_q$, unless specified otherwise. Consequently, we will refer to the addition law as “complete" instead of “$\mathbb{F}_q$-complete".

In [BL07a], Bernstein and Lange highlighted that the addition law of Edwards curves is complete under a certain condition, with a computational cost of $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$, where $\mathbf{M}, \mathbf{S}$, and $\mathbf{D}$ denote the costs of a multiplication, a squaring, and a multiplication by a constant in $\mathbb{F}_q$, respectively. Then, Bernstein et al. introduced the family of twisted Edwards curves in [BBJ$^+$08] and proved that this family also has a complete addition law under a certain condition, albeit at a slightly higher cost of $10\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$. In [HWCD08], Hisil et al. introduced extended twisted Edwards coordinates and showed that this representation enables a more efficient complete addition law for twisted Edwards curves, requiring $9\mathbf{M} + 2\mathbf{D}$ and $8\mathbf{M} + 1\mathbf{D}$ in general and specific cases, respectively. Progressing in this field, Rezaeian and Joy [FJ10] presented a complete addition law for Hessian curves with the cost of $12\mathbf{M} + 1\mathbf{D}$, contributing to the diversification of curve families with efficient arithmetic properties. Renes et al. applied the methodologies devised by Bosma and Lenstra to provide an optimized complete addition law with the cost of $12\mathbf{M} + 5\mathbf{D}$ for the elliptic curves without a point of order two [BL95, RCB16]. Their work is significant for achieving secure and exception-free implementations on all prime order elliptic curves in the NIST and many other standards [fSN23, BHH$^+$14]. In [KPKK19], Kim et al. investigated two approaches to establish a complete addition law for Montgomery curves. Their first approach was leveraging the complete addition law of twisted Edwards curves to find a complete addition law for Montgomery curves using the birational map between them. However, this approach not only fails to yield a complete addition law but also has a computational cost of $19\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$, which is significantly higher compared to those for twisted Edwards curves[1]. Their second approach adopted Bosma and Lenstra's techniques to find a complete addition law for Montgomery curves under specific conditions, and it has a computational cost of $14\mathbf{M} + 2\mathbf{D}$.

Our contribution. Montgomery curves offer advantages in terms of both speed and security for cryptographic protocols, making them a popular choice in practical implementations. However, the complete addition law on Montgomery curves requires $14\mathbf{M} + 2\mathbf{D}$ computations, indicating a substantial gap from optimal efficiency and highlighting the need for further optimization. The main objective of this work is to develop a highly

[1] In [KPKK19], the cost is incorrectly represented as $16\mathbf{M}$, and the authors overlooked that the addition law is not complete.

efficient and complete addition law for Montgomery curves. Toward the end of this paper, we will propose novel complete addition laws for Montgomery curves that require only $9\mathbf{M} + 2\mathbf{D}$ and $8\mathbf{M} + 1\mathbf{D}$ computations in general and specific cases, respectively. Thereby reducing the computational cost by $6\mathbf{M} + 1\mathbf{D}$ compared to the most efficient algorithm currently known. The contributions of this paper are threefold.

1. We introduce extended Montgomery coordinates as a new representation of points on Montgomery curves. Employing this coordinate system enables us to define birational multiplication-free maps between extended twisted Edwards coordinates and extended Montgomery coordinates. Being multiplication-free is a notable property that significantly enhances the computational efficiency of transformations between Montgomery curves and twisted Edwards curves.
2. We employ a technique known as *scaling* to introduce a new coordinate system, enhancing the efficiency of addition laws for twisted Edwards curves. This approach reduces computational costs to between $8\mathbf{M}$ and $9\mathbf{M} + 1\mathbf{D}$.
3. Using the scaling technique and the multiplication-free maps between extended Montgomery coordinates and extended twisted Edwards coordinates, we present complete addition laws for Montgomery curves with computational costs of $9\mathbf{M}+2\mathbf{D}$ and $8\mathbf{M} + 1\mathbf{D}$ in general and specific cases, respectively.

Organization. The rest of the paper is organized as follows. In Section 2, we explore Bosma and Lenstra's fundamental idea for complete addition laws for elliptic curves, along with a review of twisted Edwards curves and Montgomery curves. In Section 3, we explain how the scaling technique will allow us to present addition laws for twisted Edwards curves at a computational cost of $8\mathbf{M}+1\mathbf{D}$ and without resorting to $\mathbb{F}_q$-isomorphic curves. In Section 4, we introduce extended Montgomery coordinates and prove that every extended Montgomery coordinates is birationally equivalent to an extended twisted Edwards coordinates, and vice versa. In Section 5, we present our complete addition laws for Montgomery curves.

Notation. Throughout the paper, the letter p always denotes an odd prime number and q denotes a prime power of p. For any field $\mathbb{F}$, we denote an arbitrary extension of $\mathbb{F}$ by $\mathbb{K}$, its algebraic closure by $\overline{\mathbb{F}}$, and its multiplicative group with $\mathbb{F}^*$. Let χ denote the quadratic character in $\mathbb{F}_q$, where $p \geq 3$. Then, for any q where $p \geq 3$, we have $u = w^2$ for some $w \in \mathbb{F}_q^*$ if and only if $\chi(u) = 1$.

2 Preliminaries

For a positive integer n and a field $\mathbb{F}$, the projective space $\mathbb{P}^n(\mathbb{F})$ is the set of points $\{(X_0 : X_1 : \cdots : X_n) \mid X_0, X_1, \cdots, X_n \in \mathbb{F}\}$, where for any $\lambda \in \mathbb{F}_q^*$ we have $(X_0 : X_1 : \cdots : X_n) = (\lambda X_0 : \lambda X_1 : \cdots : \lambda X_n)$. Elliptic curve E given in (1) is defined in $\mathbb{P}^2(\mathbb{F})$, therefore the set of $\mathbb{F}$-rational points of E, denoted by $E(\mathbb{F})$, are triples $(x : y : z) \in \mathbb{P}^2(\mathbb{F})$ which lie on (1). The chord-tangent process turns the set $E(\mathbb{F})$ into an abelian additive group with identity element $\mathcal{O} = (0 : 1 : 0)$ and the inverse of any point $P = (x : y : z) \in E(\mathbb{F})$ is the point $-P = (x : -y - a_1x - a_3z : z) \in E(\mathbb{F})$. Given the significant computational overhead associated with inversions in finite fields as compared to multiplications, ECC utilizes projective coordinates. This approach allows the implementation of addition laws in projective space, removing the need for inversions.

2.1 Complete Addition Laws

In this subsection, we briefly review Bosma and Lenstra's results on a complete set of addition laws for the elliptic curves E given in equation (1) [BL95].

Following the notation of Bosma and Lenstra [BL95], let

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 \in \mathbb{F}[x, y, z].$$

For any two positive integers μ and ν, an addition law of bidegree (μ, ν) on E is defined by a set of three polynomials

$$\mathcal{X}, \mathcal{Y}, \mathcal{Z} \in \frac{\mathbb{F}[x_1, y_1, z_1, x_2, y_2, z_2]}{\langle F(x_1, y_1, z_1), F(x_2, y_2, z_2)\rangle}$$

satisfying the following properties. i) $\mathcal{X}, \mathcal{Y}$, and $\mathcal{Z}$ are bihomogeneous of bidegree (μ, ν), that is homogeneous of degree μ in the variables x_1, y_1, z_1, and homogeneous of degree ν in the variables x_2, y_2, z_2. ii) If $\mathbb{K}$ is an extension field of $\mathbb{F}$, $P_1 = (X_1 : Y_1 : Z_1) \in E(\mathbb{K})$, $P_2 = (X_2 : Y_2 : Z_2) \in E(\mathbb{K})$, and

$$\begin{aligned} X_3 &= \mathcal{X}(X_1, Y_1, Z_1, X_2, Y_2, Z_2), \\ Y_3 &= \mathcal{Y}(X_1, Y_1, Z_1, X_2, Y_2, Z_2), \\ Z_3 &= \mathcal{Z}(X_1, Y_1, Z_1, X_2, Y_2, Z_2), \end{aligned}$$

then either $X_3 = Y_3 = Z_3 = 0$ or the point $P_3 = (X_3 : Y_3 : Z_3) \in E(\mathbb{K})$ and P_3 equals to $P_1 + P_2$. A pair P_1, P_2 is called *exceptional* for the addition law if the first case holds, and if no such exceptional pairs exist for the addition law, then it is called $\mathbb{K}$-complete. Also, two addition laws are called *equivalent* if there exists an element $d \in \mathbb{F}^*$ such that $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ in the first addition law are d times of their counterparts in the second.

A *complete system of addition laws* on E is a collection of addition laws on E with the property that for any pair of points $P_1, P_2 \in E(\overline{\mathbb{F}})$, at least one of the addition laws in the collection outputs a point $P_3 = P_1 + P_2 \in E(\overline{\mathbb{F}})$. In [LR87], Lange and Ruppert presented a complete system of addition laws, consisting of three separate laws, each defined by bihomogeneous polynomials of bidegree $(2, 2)$. In [BL95], Bosma and Lenstra ([BL95]) established a foundational result regarding addition laws on elliptic curves, E: specifically, that each addition law must have at least one exceptional pair of inputs within the algebraic closure. They characterized all addition laws of bidegree $(2, 2)$ through a one-to-one correspondence between points $(a : b : c) \in \mathbb{P}^2(\mathbb{F})$ and equivalence classes of nonzero addition laws of the same bidegree on E. They proved that the pair $P_1, P_2 \in E(\mathbb{K})$ is exceptional for the addition law corresponding to $(a : b : c)$ if $P_1 - P_2$ lies on the intersection of $E(\mathbb{K})$ and the line $aX + bY + cZ = 0$ in $\mathbb{P}^2(\mathbb{K})$. This relationship implies that any two distinct lines in $\mathbb{P}^2(\mathbb{F})$ intersecting outside $E(\mathbb{F})$ can define a complete system comprising two addition laws on E. For instance, the addition law corresponding to two lines $Y = 0$ and $Z = 0$, or equivalently corresponding to the points $(0 : 1 : 0)$ and $(0 : 0 : 1)$ in $\mathbb{P}^2$, form one such system. Furthermore, if $a_6 \neq 0$ the addition laws corresponding to two lines $Y = 0$ and $X = 0$ constitute a complete system; similarly if $bc' - b'c \neq 0$ the addition laws corresponding to two lines $bY + cZ = 0$ and $b'Y + c'Z = 0$ represent another complete system. Thus, Bosma and Lenstra conclusively demonstrated that the minimal number of addition laws required to form a complete system on E is two.

In their work, they present three addition laws

$$\mathcal{A}_1 = (\mathcal{X}_1 : \mathcal{Y}_1 : \mathcal{Z}_1), \quad \mathcal{A}_2 = (\mathcal{X}_2 : \mathcal{Y}_2 : \mathcal{Z}_2), \quad \mathcal{A}_3 = (\mathcal{X}_3 : \mathcal{Y}_3 : \mathcal{Z}_3)$$

corresponding to the points

$$(0 : 0 : 1), \quad (0 : 1 : 0), \quad (1 : 0 : 0),$$

and show that the addition law corresponding to the point $(a : b : c) \in \mathbb{P}^2(\mathbb{F})$ is

$$a\mathcal{A}_3 + b\mathcal{A}_2 + c\mathcal{A}_1 = (a\mathcal{X}_3 + b\mathcal{X}_2 + c\mathcal{X}_1 : a\mathcal{Y}_3 + b\mathcal{Y}_2 + c\mathcal{Y}_1 : a\mathcal{Z}_3 + b\mathcal{Z}_2 + c\mathcal{Z}_1).$$

Since there is no point of order two on an elliptic curve E over $\mathbb{F}$, there is no point on the intersection of the line $Y = 0$ and $E(\mathbb{F})$. Therefore, the addition law $\mathcal{A}_2$, which corresponds to the point $(0 : 1 : 0) \in \mathbb{P}^2$, is a $\mathbb{F}$-complete addition law on E. Employing this insight, Renes et al. in [RCB16] introduced an optimized $\mathbb{F}_q$-complete addition law with the cost of $12\mathbf{M} + 5\mathbf{D}$ for odd-order elliptic curves defined over $\mathbb{F}_q$.

2.2 Montgomery Curve

A Montgomery curve over $\mathbb{F}_q$ is defined by the affine equation

$$E_{M,A,B} : Bv^2 = u^3 + Au^2 + u, \qquad A, B \in \mathbb{F}_q, \quad B(A^2 - 4) \neq 0. \tag{2}$$

Let $E_{M,A,B}(\mathbb{F}_q)$ be the set of all affine $\mathbb{F}_q$-rational points of points on $E_{M,A,B}$. Using the substitution $(u, v) = (U/W, V/W)$, the projective form of the Montgomery curve (2) is as follows:

$$\mathbf{E}_{M,A,B} : BV^2W = U^3 + AU^2W + UW^2, \qquad B(A^2 - 4) \neq 0.$$

Let $\mathbf{E}_{M,A,B}(\mathbb{F}_q)$ be the set of all $\mathbb{F}_q$-rational points of $\mathbf{E}_{M,A,B}$. In such a case, each affine point $(u, v) \in E_{M,A,B}(\mathbb{F}_q)$ is represented as $(u : v : 1) \in \mathbf{E}_{M,A,B}(\mathbb{F}_q)$. Also, $(U : V : W) \in \mathbf{E}_{M,A,B}(\mathbb{F}_q)$ with $W \neq 0$ represents the affine point $(U/W, V/W) \in E_{M,A,B}(\mathbb{F}_q)$. There is only one point at infinity $\mathcal{O} = (0 : 1 : 0)$ on $\mathbf{E}_{M,A,B}$ and the negative of every point $(U : V : W) \in \mathbf{E}_{M,A,B}(\mathbb{F}_q)$ is $(U : -V : W) \in \mathbf{E}_{M,A,B}(\mathbb{F}_q)$. For two given projective points $P_1 = (U_1 : V_1 : W_1)$, and $P_2 = (U_2 : V_2 : W_2)$ in $\mathbf{E}_{M,A,B}(\mathbb{F}_q)$, $P_3 = P_1 + P_2$ is computed as follows. If either of the points is the point at infinity, then P_3 equals to the other point, and if $P_1 = -P_2$, then $P_1 + P_2 = \mathcal{O}$. Otherwise $P_3 = (U_3 : V_3 : W_3)$, where

$$\begin{aligned}
U_3 &= BI_1^2H_1W_1W_2 - (AW_1W_2 + U_1W_2 + U_2W_1)H_1^3,\\
V_3 &= -BI_1^3W_1W_2 + (AW_1W_2 + 2U_1W_2 + U_2W_1)I_1H_1^2 - V_1W_2H_1^3,\\
W_3 &= H_1^3W_1W_2.
\end{aligned}$$

and

$$(I_1, H_1) = \begin{cases} (V_2W_1 - V_1W_2,\ U_2W_1 - U_1W_2), & \text{if } P_1 \neq P_2,\\ (3U_1^2 + 2AU_1W_1 + W_1^2,\ 2BV_1W_1), & \text{if } P_1 = P_2. \end{cases}$$

The computation of $P_3 = P_1 + P_2$ using this addition law necessitates a case-by-case analysis of the inputs, indicating that the law is not complete. Also, the cost of addition and doubling is $13\mathbf{M} + 2\mathbf{S} + 2\mathbf{D}$ and $11\mathbf{M} + 3\mathbf{S} + 4\mathbf{D}$, respectively [KPKK19][2].

2.3 Twisted Edwards Curve

In [Edw07], Edwards proved that, if $\mathbb{F}$ is algebraically closed, every elliptic curve over a non-binary field $\mathbb{F}$ can be represented as a normal form $x^2 + y^2 = c^2(1 + x^2y^2)$ with $c^5 \neq c$. However, over a finite field $\mathbb{F}_q$, only a small fraction of elliptic curves can be expressed in this form [FS10, FMW12]. Covering a larger fraction of elliptic curves over $\mathbb{F}_q$ prompted Bernstein and Lange to introduce the family of *Edwards curves* given by the equation $x^2 + y^2 = 1 + dx^2y^2$, with $d \in \mathbb{F}_q$ and $d(d - 1) \neq 0$ [BL07a]. Their first algorithms for computing the group operations on projective coordinates indicated efficiency for Edwards curves, which is an essential parameter in ECC. In [BBJ+08], Bernstein et al. generalized the family of Edwards curves to a bigger family called twisted Edwards, which contains both Edwards curves and their twists.

[2] In [KPKK19], the cost of addition and doubling are given $13\mathbf{M} + 2\mathbf{S} + 1\mathbf{D}$ and $11\mathbf{M} + 3\mathbf{S} + 2\mathbf{D}$, respectively, based on the condition $B = 1$.

Twisted Edwards Curves. A twisted Edwards curve over $\mathbb{F}_q$ is defined by the affine equation

$$E_{TE,a,d} : ax^2 + y^2 = 1 + dx^2y^2, \qquad a, d \in \mathbb{F}_q, \quad ad(a-d) \neq 0. \tag{3}$$

Let $E_{TE,a,d}(\mathbb{F}_q)$ be the set of affine $\mathbb{F}_q$-rational points of $E_{TE,a,d}$ and $(x_1, y_1), (x_2, y_2) \in E_{TE,a,d}(\mathbb{F}_q)$. The affine addition law for twisted Edwards curves is defined as

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right) = (x_3, y_3). \tag{4}$$

The point $(0, 1)$ is the identity element and the negative of every point (x, y) is $(-x, y)$. This addition law is unified, i.e. supports both addition and doubling, and is proven to be complete if $\chi(d) = \chi(ad) = -1$ [BBJ+08].

Hisil et al. in [HWCD08] presented another addition law for twisted Edwards curves as

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 + ax_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - y_1x_2} \right) = (x_3, y_3). \tag{5}$$

Both addition laws (4) and (5) yield identical outputs, however, the later cannot compute the point doubling and the exceptional cases arise even when $\chi(d) = \chi(ad) = -1$.

Using the substitution $(x, y) = (X/Z, Y/Z)$, the projective form of the twisted Edwards curve (3) in the projective space $\mathbb{P}^2$ is the following equation

$$\mathbf{E}_{TE,a,d} : (aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2, \qquad ad(a-d) \neq 0.$$

Let $\mathbf{E}_{TE,a,d}(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-rational points of the twisted Edwards curve $\mathbf{E}_{TE,a,d}$. Each point $(x, y) \in E_{TE,a,d}(\mathbb{F}_q)$ is represented as $(x : y : 1) \in \mathbf{E}_{TE,a,d}(\mathbb{F}_q)$. Also, the projective point $(X : Y : Z) \in \mathbf{E}_{TE,a,d}(\mathbb{F}_q)$ with $Z \neq 0$ represents the affine point $(X/Z, Y/Z) \in E_{TE,a,d}(\mathbb{F}_q)$. Moreover, $\mathbf{E}_{TE,a,d}(\mathbb{F}_q)$ has two points at infinity $\mathcal{O}_1 = (1 : 0 : 0)$ and $\mathcal{O}_2 = (0 : 1 : 0)$, which are both singular even if $ad(a-d) \neq 0$. In the nonsingular model of $\mathbf{E}_{TE,a,d}$, the point $\mathcal{O}_1$ splits into two distinct $\mathbb{F}_q$-rational points if $\chi(ad) = 1$ and is removed if $\chi(ad) = -1$. Similarly, above the point $\mathcal{O}_2$, there exist exactly two distinct points if $\chi(d) = 1$ and no point if $\chi(d) = -1$. So, if $\chi(d) = \chi(ad) = -1$, then $\mathbf{E}_{TE,a,d}(\mathbb{F}_q) = E_{TE,a,d}(\mathbb{F}_q)$ [FH17]. For two given points $(X_1 : Y_1 : Z_1), (X_2 : Y_2 : Z_2) \in \mathbf{E}_{TE,a,d}(\mathbb{F}_q)$, the projective addition law outputs $(X_3 : Y_3 : Z_3)$, where

$$\begin{aligned}
X_3 &= Z_1Z_2(X_1Y_2 + Y_1X_2)((Z_1Z_2)^2 - dX_1X_2Y_1Y_2),\\
Y_3 &= Z_1Z_2(Y_1Y_2 - aX_1X_2)((Z_1Z_2)^2 + dX_1X_2Y_1Y_2),\\
Z_3 &= ((Z_1Z_2)^2 - dX_1X_2Y_1Y_2)((Z_1Z_2)^2 + dX_1X_2Y_1Y_2).
\end{aligned}$$

The identity element of this addition law is $(0 : 1 : 1)$ and the negative of every point $(X : Y : Z)$ is $(-X : Y : Z)$. Also, the computational costs for addition and doubling are $10\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ and $3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$, respectively [BBJ+08].

Inverted Twisted Edwards Coordinates. In [BL07a], Bernstein and Lange introduced inverted Edwards coordinates to enhance the efficiency of arithmetic on twisted Edwards curves. Subsequently, in [BBJ+08], they introduced inverted twisted Edwards coordinates, where $(X : Y : Z)$ with $XYZ \neq 0$ that satisfies equation

$$X^2Z^2 + aY^2Z^2 = X^2Y^2 + dZ^4, \qquad ad(a-d) \neq 0$$

represents the affine point $(Z/X, Z/Y) \in E_{TE,a,d}(\mathbb{F}_q)$. This coordinate system reduces the cost of addition and doubling laws to $9\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$ and $3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$, respectively.

Extended Twisted Edwards Coordinates. To enhance the efficiency of point multiplication and remove the singularity of the points at infinity $\mathcal{O}_1, \mathcal{O}_2 \in \mathbf{E}_{TE,a,d}(\mathbb{F}_q)$, Hisil et al. considered twisted Edwards curves in $\mathbb{P}^3$ [HWCD08]. Later, Bernstein and Lange examined twisted Edwards curves in $\mathbb{P} \times \mathbb{P}$, introducing a complete set of addition laws for twisted Edwards curves [BL09]. Our new complete addition law for Montgomery curves has a significant correlation with the twisted Edwards curves represented in $\mathbb{P}^3$.

Twisted Edwards curve $E_{TE,a,d}$ over $\mathbb{F}_q$ in extended coordinates is represented as

$$\mathcal{E}_{TE,a,d} : aX^2 + Y^2 = Z^2 + dT^2, \qquad XY = ZT. \tag{6}$$

Let $\mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-rational points of $\mathcal{E}_{TE,a,d}$. In this coordinate, if $\chi(ad) = 1$ the $\mathbb{F}_q$-rational points $(1 : 0 : \pm\sqrt{a/d} : 0) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ are above the singular point $\mathcal{O}_1 \in \mathbf{E}_{TE,a,d}$, and if $\chi(d) = 1$ the the $\mathbb{F}_q$-rational points $(0 : \pm\sqrt{d} : 1 : 0) \in \mathcal{E}_{TE,a,d}$ are above the singular point $\mathcal{O}_2 \in \mathbf{E}_{TE,a,d}$ [HWCD08, FH17].

The addition law (4) for $\mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ takes two points $P_1 = (X_1 : Y_1 : T_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : T_2 : Z_2)$ in $\mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ and outputs $P_3 = (X_3 : Y_3 : T_3 : Z_3)$, where

$$\begin{aligned} X_3 &= (X_1Y_2 + Y_1X_2)(Z_1Z_2 - dT_1T_2), & Y_3 &= (Y_1Y_2 - aX_1X_2)(Z_1Z_2 + dT_1T_2), \\ T_3 &= (Y_1Y_2 - aX_1X_2)(X_1Y_2 + Y_1X_2), & Z_3 &= (Z_1Z_2 - dT_1T_2)(Z_1Z_2 + dT_1T_2). \end{aligned} \tag{7}$$

The identity element of this addition law is $(0 : 1 : 0 : 1)$, and the negative of a point $(X : Y : T : Z)$ is $(-X : Y : -T : Z)$. The point $(0 : -1 : 0 : 1)$ is a point of order 2, and the points $(1 : 0 : \pm\sqrt{a/d} : 1)$ are the points of order 2 if $\chi(ad) = 1$.

As shown in [HWCD08], this addition law requires $9\mathbf{M} + 2\mathbf{D}$ computation. The mixed addition formula involves adding a point $(X_1 : Y_1 : T_1 : Z_1)$ to an extended affine point (x_2, y_2, x_2y_2), or equivalently $(x_2 : y_2 : x_2y_2 : 1)$ and incurs a cost of $8\mathbf{M}+2\mathbf{D}$. Furthermore, if $\chi(-a) = 1$ then $\mathcal{E}_{TE,a,d}$ is $\mathbb{F}_q$-isomorphic to the twisted Edwards curve $\mathcal{E}_{TE,-1,-d/a}$ via the map $(X, Y, T, Z) \to (X', Y', T', Z') = (\sqrt{-a}X, Y, \sqrt{-a}T, Z)$. As shown in [HWCD08], for the twisted Edwards curve $\mathcal{E}_{TE,-1,-d/a}$, the addition law (7) and its mixed addition law require $8\mathbf{M} + 1\mathbf{D}$ and $7\mathbf{M} + 1\mathbf{D}$ computations, respectively.

The addition law corresponding to (5) takes two points $P_1 = (X_1 : Y_1 : T_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : T_2 : Z_2)$ in $\mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ and outputs $P_3 = (X_3 : Y_3 : T_3 : Z_3) \in \mathcal{E}_{TE,a,d}$ as

$$\begin{aligned} X_3 &= (T_1Z_2 + Z_1T_2)(X_1Y_2 - Y_1X_2), & Y_3 &= (T_1Z_2 - Z_1T_2)(Y_1Y_2 + aX_1X_2), \\ T_3 &= (T_1Z_2 + Z_1T_2)(T_1Z_2 - Z_1T_2), & Z_3 &= (Y_1Y_2 + aX_1X_2)(X_1Y_2 - Y_1X_2). \end{aligned} \tag{8}$$

The addition law (8) is neither unified nor complete and requires $9\mathbf{M}+1\mathbf{D}$, while its mixed addition needs $8\mathbf{M}+1\mathbf{D}$. The given addition laws in (7) and (8) produce the same outputs. However, the addition law (8) has exceptional cases even if $\chi(d) = \chi(ad) = -1$. Using these two addition laws, two other addition laws with the computational costs $9\mathbf{M} + 2\mathbf{D}$ and $9\mathbf{M} + 1\mathbf{D}$ were presented in [HWCD08] as follows

$$\begin{aligned} X_3 &= (T_1Z_2 + Z_1T_2)(Z_1Z_2 - dT_1T_2), & Y_3 &= (Y_1Y_2 - aX_1X_2)(Y_1Y_2 + aX_1X_2), \\ T_3 &= (T_1Z_2 + Z_1T_2)(Y_1Y_2 - aX_1X_2), & Z_3 &= (Y_1Y_2 + aX_1X_2)(Z_1Z_2 - dT_1T_2), \end{aligned} \tag{9}$$

and

$$\begin{aligned} X_3 &= (X_1Y_2 + Y_1X_2)(X_1Y_2 - Y_1X_2), & Y_3 &= (T_1Z_2 - Z_1T_2)(Z_1Z_2 + dT_1T_2), \\ T_3 &= (X_1Y_2 + Y_1X_2)(T_1Z_2 - Z_1T_2), & Z_3 &= (Z_1Z_2 + dT_1T_2)(X_1Y_2 - Y_1X_2). \end{aligned} \tag{10}$$

As mentioned before, the addition law (7) for $\mathcal{E}_{TE,a,d}$ is complete if $\chi(d) = \chi(ad) = -1$. In [FH17], Rezaeian et al. proved that $\mathcal{E}_{TE,a,d}$ and $\mathcal{E}_{TE,d,a}$ are connected through the map

$$\begin{aligned} &\mathcal{E}_{TE,a,d}(\mathbb{F}_q) \to \mathcal{E}_{TE,d,a}(\mathbb{F}_q), \\ &(X : Y : T : Z) \to (T : Z : X : Y). \end{aligned} \tag{11}$$

Using this map, they proved that the addition law (9) is complete for $\mathcal{E}_{TE,a,d}$ if $\chi(a) = \chi(ad) = -1$. Therefore, if $\chi(ad) = -1$, a complete addition law exists for the twisted Edwards curve $\mathcal{E}_{TE,a,d}$.

The following proposition uses the map (11) to relate the addition laws of $\mathcal{E}_{TE,a,d}$ with those of $\mathcal{E}_{TE,d,a}$. This correspondence explains the completeness of the addition law (9) for $\mathcal{E}_{TE,a,d}$ when $\chi(a) = \chi(ad) = -1$.

Proposition 1. *Let $a, d \in \mathbb{F}_q$ such that $ad(a-d) \neq 0$. The addition laws given in (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$ correspond to the addition laws (9), (10), (7), and (8) for $\mathcal{E}_{TE,d,a}$, respectively.*

Proof. First, we reformulate the addition laws (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$ using the following components. Let

$$\mathcal{X} = (X_1Y_2 + Y_1X_2), \qquad \mathcal{Z} = (Z_1Z_2 + dT_1T_2), \tag{12}$$

$$\mathcal{Y} = (Y_1Y_2 - aX_1X_2), \qquad \mathcal{T} = (Z_1Z_2 - dT_1T_2), \tag{13}$$

$$\mathcal{X}' = (T_1Z_2 + Z_1T_2), \qquad \mathcal{Z}' = (Y_1Y_2 + aX_1X_2), \tag{14}$$

$$\mathcal{Y}' = (T_1Z_2 - Z_1T_2), \qquad \mathcal{T}' = (X_1Y_2 - Y_1X_2). \tag{15}$$

Then, for $\mathcal{E}_{TE,a,d}$

- The addition law (7) outputs $(X_3 : Y_3 : T_3 : Z_3) = (\mathcal{X}\mathcal{T} : \mathcal{Y}\mathcal{Z} : \mathcal{X}\mathcal{Y} : \mathcal{Z}\mathcal{T})$,
- The addition law (8) outputs $(X_3 : Y_3 : T_3 : Z_3) = (\mathcal{X}'\mathcal{T}' : \mathcal{Y}'\mathcal{Z}' : \mathcal{X}'\mathcal{Y}' : \mathcal{Z}'\mathcal{T}')$,
- The addition law (9) outputs $(X_3 : Y_3 : T_3 : Z_3) = (\mathcal{X}'\mathcal{T} : \mathcal{Y}\mathcal{Z}' : \mathcal{X}'\mathcal{Y} : \mathcal{Z}'\mathcal{T})$,
- The addition law (10) outputs $(X_3 : Y_3 : T_3 : Z_3) = (\mathcal{X}\mathcal{T}' : \mathcal{Y}'\mathcal{Z} : \mathcal{X}\mathcal{Y}' : \mathcal{Z}\mathcal{T}')$.

Clearly, $\mathcal{E}_{TE,a,d}$ and $\mathcal{E}_{TE,d,a}$ have swapped coefficients, and the map (11) swaps X with T and Y with Z. Therefore, using the map (11) tuple $(\mathcal{X}, \mathcal{Y}, \mathcal{T}, \mathcal{Z}, \mathcal{X}', \mathcal{Y}', \mathcal{T}', \mathcal{Z}')$ for $\mathcal{E}_{TE,a,d}$ will be transferred to the tuple $(\mathcal{X}', \mathcal{T}, \mathcal{Y}, \mathcal{Z}', \mathcal{X}, \mathcal{T}', \mathcal{Y}', \mathcal{Z})$ for $\mathcal{E}_{TE,d,a}$. Consequently, for $\mathcal{E}_{TE,d,a}$

- The addition law (7) outputs $(X_3 : Y_3 : T_3 : Z_3) = (\mathcal{X}'\mathcal{T} : \mathcal{Y}\mathcal{Z}' : \mathcal{X}'\mathcal{Y} : \mathcal{Z}'\mathcal{T})$,
- The addition law (8) outputs $(X_3 : Y_3 : T_3 : Z_3) = (\mathcal{X}\mathcal{T}' : \mathcal{Y}'\mathcal{Z} : \mathcal{X}\mathcal{Y}' : \mathcal{Z}\mathcal{T}')$,
- The addition law (9) outputs $(X_3 : Y_3 : T_3 : Z_3) = (\mathcal{X}\mathcal{T} : \mathcal{Y}\mathcal{Z} : \mathcal{X}\mathcal{Y} : \mathcal{Z}\mathcal{T})$,
- The addition law (10) outputs $(X_3 : Y_3 : T_3 : Z_3) = (\mathcal{X}'\mathcal{T}' : \mathcal{Y}'\mathcal{Z}' : \mathcal{X}'\mathcal{Y}' : \mathcal{Z}'\mathcal{T}')$.

A simple comparison shows that the addition laws (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$ is the same as the addition laws (9), and (10), (7), and (8) for $\mathcal{E}_{TE,d,a}$, respectively. □

In [BL09], Bernstein and Lange introduced alternative coordinates to represent the twisted Edwards curve $E_{TE,a,d}$ in which it provides a $\bar{\mathbb{F}}$-complete set of addition laws. In this coordinate system, a point $(x, y) \in E_{TE,a,d}(\mathbb{F}_q)$ is mapped to $((x : 1), (y : 1)) \in \mathbb{P}(\mathbb{F}_q) \times \mathbb{P}(\mathbb{F}_q)$. Thus, the twisted Edwards curve (3) in the projective space $\mathbb{P} \times \mathbb{P}$, is obtained through the substitution $(x, y) = (X/Z, Y/T)$, leading to the equation

$$\bar{\mathbf{E}}_{TE,a,d} : aX^2T^2 + Y^2Z^2 = Z^2T^2 + dX^2Y^2. \tag{16}$$

Let $\bar{\mathbf{E}}_{TE,a,d}(\mathbb{F}_q)$ be the set of all $((X : Z), (Y : T)) \in \mathbb{P}(\mathbb{F}_q) \times \mathbb{P}(\mathbb{F}_q)$ that satisfies (16). For two points $P_1 = ((X_1 : Z_1), (Y_1 : T_1)))$ and $P_2 = ((X_2 : Z_2), (Y_2 : T_2))$ in $\bar{\mathbf{E}}_{TE,a,d}(\mathbb{F}_q)$, their

$\bar{\mathbb{F}}$-complete set of addition laws outputs either $((X_3 : Z_3), (Y_3 : T_3))$ or $((X_3' : Z_3'), (Y_3' : T_3'))$ as $P_3 = P_1 + P_2 \in \bar{\mathbf{E}}_{TE,a,d}(\mathbb{F}_q)$, where

$$X_3 = X_1Y_2Z_2T_1 + X_2Y_1Z_1T_2, \qquad Z_3 = Z_1Z_2T_1T_2 + dX_1X_2Y_1Y_2$$
$$Y_3 = Y_1Y_2Z_1Z_2 - aX_1X_2T_1T_2, \qquad T_3 = Z_1Z_2T_1T_2 - dX_1X_2Y_1Y_2.$$

and

$$X_3' = X_1Y_1Z_2T_2 + X_2Y_2Z_1T_1, \qquad Z_3' = aX_1X_2T_1T_2 + Y_1Y_2Z_1Z_2,$$
$$Y_3' = X_1Y_1Z_2T_2 - X_2Y_2Z_1T_1, \qquad T_3' = X_1Y_2Z_2T_1 - X_2Y_1Z_1T_2.$$

Remark 1. Similar to Bernstein and Lange's result, we can show that the addition laws (7) and (8) as well as the addition laws (9) and (10), each form distinct $\bar{\mathbb{F}}$-complete sets of addition laws.

Table 1: Cost of addition laws for twisted Edwards curves in different coordinates. (Ext. and Inv. stand for Extended and Inverted, respectively.)

Curve	Addition	Doubling	Completeness (Addition)	Unified
Edwards (Ed.) [BL07a]	$10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$	$3\mathbf{M} + 4\mathbf{S}$	$\chi(d) = -1$	Yes
Inverted Ed. [BL07b]	$9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$	$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	No	Yes
Twisted Ed. [BBJ+08]	$10\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$	$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$\chi(a) = 1,\ \chi(d) = -1$	Yes
Inv. Twisted Ed. [BBJ+08]	$9\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$	$3\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	No	Yes
Ext. Twisted Ed. [HWCD08]	$9\mathbf{M} + 2\mathbf{D}$	$4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$\chi(a) = 1,\ \chi(d) = -1$	Yes
Ext. Twisted Ed. [HWCD08]	$9\mathbf{M} + 1\mathbf{D}$	$4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	No	No
Ext. Twisted Ed. [HWCD08]	$8\mathbf{M} + 1\mathbf{D}$	$4\mathbf{M} + 4\mathbf{S}$	$a = -1,\ \chi(-1) = 1,\ \chi(d) = -1$	Yes
Ext. Twisted Ed. [HWCD08]	$8\mathbf{M}$	–	No	No
Ext. Twisted Ed. [FH17]	$9\mathbf{M} + 2\mathbf{D}$	–	$\chi(a) = -1,\ \chi(d) = 1$	Yes
Inv. Twisted Ed. [LY22]	$9\mathbf{M} + 2\mathbf{D}$	$4\mathbf{M} + 4\mathbf{S} + 2\mathbf{D}$	$\chi(a) = 1,\ \chi(d) = -1$	Yes
Inv. Twisted Ed. [LY22]	$8\mathbf{M} + 1\mathbf{D}$	$4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$	$a = -1,\ \chi(-1) = 1,\ \chi(d) = -1$	Yes

2.4 Complete Addition Law for Montgomery Curves

In this subsection, we will review two approaches that were investigated in [KPKK19] for establishing a complete addition law for Montgomery curves. The first method leverages the mutual relationship between Montgomery curves and twisted Edwards curves in projective space $\mathbb{P}^2(\mathbb{F}_q)$, whereas the second employs the Bosma-Lenstra technique to establish a complete addition law for Montgomery curves. It must be emphasized that the first approach does not result in a complete addition law, which was not stated in [KPKK19]. The computational cost of the addition law of the second approach is $14\mathbf{M} + 2\mathbf{D}$. In Section 5, we present a significantly more efficient complete addition law for Montgomery curves, which requires only $9\mathbf{M} + 2\mathbf{D}$ and $8\mathbf{M} + 1\mathbf{D}$ computations in general and specific cases, respectively.

First approach. In their seminal work on the Edwards curves, Bernstein and Lange established a fundamental equivalence between the family of Montgomery curves and the family of twisted Edwards curves [BBJ+08]. Beyond this equivalence, they explicitly provided the birational maps that correspond Montgomery curves to twisted Edwards curves and vice versa. Specifically, if $a, d, A, B \in \mathbb{F}_q$, where $ad(a - d) \neq 0$, $A = 2(a + d)/(a - d)$ and $B = 4/(a - d)$, the explicit rational maps between the twisted Edwards curve $\mathbf{E}_{TE,a,d}$

and the Montgomery curve $\mathbf{E}_{M,A,B}$ are defined as

$$\psi : \mathbf{E}_{TE,a,d} \to \mathbf{E}_{M,A,B} \tag{17}$$

$$\psi(X:Y:Z) = \begin{cases} (0:0:1), & \text{if } (X:Y:Z) = (0:-1:1), \\ (X(Z+Y):Z(Z+Y):X(Z-Y)), & \text{otherwise, where } Z \neq 0. \end{cases}$$

and

$$\psi^{-1} : \mathbf{E}_{M,A,B} \to \mathbf{E}_{TE,a,d}, \tag{18}$$

$$\psi^{-1}(U:V:W) = \begin{cases} (0:1:1), & \text{if } (U:V:W) = (0:1:0), \\ (0:-1:1), & \text{if } (U:V:W) = (0:0:1), \\ (U(U+W):V(U-W):V(U+W)), & \text{otherwise.} \end{cases}$$

In [KPKK19], Kim et al. claimed that the following calculation yields a complete addition law for Montgomery curves over $\mathbb{F}_q$ if $\chi(d) = \chi(ad) = -1$. However, this is incorrect due to the exceptional points of the maps ψ and ψ^{-1}. Their main idea is as follows. To compute $P_1 + P_2$ for points $P_1, P_2 \in \mathbf{E}_{M,A,B}$, one initially computes $\psi^{-1}(P_1)$ and $\psi^{-1}(P_2)$ to obtain the corresponding points on $\mathbf{E}_{TE,a,d}(\mathbb{F}_q)$, necessitating $6\mathbf{M}$ computations. Then, $\psi^{-1}(P_1) + \psi^{-1}(P_2)$ is computed with a cost of $10\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$. Finally, the map ψ is applied to the result to obtain $P_1 + P_2 = \psi(\psi^{-1}(P_1) + \psi^{-1}(P_2))$, requiring an additional $3\mathbf{M}$ computations, resulting in a total computational cost of $19\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$.

Second approach. Every Montgomery curve $\mathbf{E}_{M,A,1} : V^2W = U^3 + AU^2W + UW^2$ can be considered as a Weierstrass curve given in (1) with $(a_1, a_2, a_3, a_4, a_6) = (0, A, 0, 1, 0)$. Using this coincidence, Kim et al. introduced a complete addition law for the Montgomery curves $\mathbf{E}_{M,A,1}$ by the Bosma-Lenstra method [KPKK19]. More precisely, having an irreducible polynomial $X^3 + AX^2 + X - s^2 \in \mathbb{F}_q[X]$ implies that there is no point in $\mathbf{E}_{M,A,1}(\mathbb{F}_q)$ with a y-coordinate of s. Consequently, the line defined by $Y - sZ = 0$ does not intersect $\mathbf{E}_{M,A,1}$ in $\mathbb{P}^2(\mathbb{F}_q)$. Employing the Bosma-Lenstra method, as outlined in subsection 2.1, the addition law $\mathcal{A}_2 - s\mathcal{A}_1$, corresponding to the point $(0:1:-s)$, serves as a complete addition law for these Montgomery curves as follows. Let $(X_1 : Y_1 : Z_1), (X_2 : Y_2 : Z_2) \in \mathbf{E}_{M,A,1}(\mathbb{F}_q)$, their addition law outputs $(X_3 : Y_3 : Z_3)$ where

$$X_3 = C + D, \quad Y_3 = E + F, \quad Z_3 = 2(U-W)(R+V) + C - D + E - F$$

and

$$\begin{aligned} R &= Y_1Z_2 + Y_2Z_1, & W &= s(Y_1Z_2 - Y_2Z_1) + (X_1Z_2 + X_2Z_1) + AX_1X_2 + Y_1Y_2, \\ S &= s(X_1Y_2 - X_2Y_1) + X_1X_2 - Z_1Z_2, & U &= s(X_1Z_2 - X_2Z_1) - (X_1Y_2 + X_2Y_1), \\ V &= A(X_1Z_2 + X_2Z_1) + 3X_1X_2 + Z_1Z_2, & T &= (X_1Z_2 + X_2Z_1) + AX_1X_2 - Y_1Y_2, \end{aligned}$$
$$C = (R+T)(S-U), D = (R-T)(S+U), E = (T+V)(W-S), F = (T-V)(W+S).$$

The computational cost of this complete addition law is $14\mathbf{M} + 2\mathbf{D}$. It also requires $3s + 31$ additions in $\mathbb{F}_q$, thus the existence of a small s for a Montgomery curve enhances the efficiency of its point additions. In Table 1 of [KPKK19], Kim et al. provide a list of known Montgomery curves with small s, but they did not prove that such a small s exists for every Montgomery curve $\mathbf{E}_{M,A,1}$. In Section 4, we present an innovative multiplication-free birational map between twisted Edwards curves and Montgomery curves, which enables us to develop a complete addition law for the family of Montgomery curves at a reduced cost of $8\mathbf{M} + 1\mathbf{D}$, representing a significant decrease of $6\mathbf{M} + 1\mathbf{D}$.

Remark 2. The family of Montgomery curves can be divided into two subfamilies: those with $\chi(B) = 1$ and those with $\chi(B) = -1$. Clearly, the later subfamily is the non-trivial quadratic twist of the first subfamily. Using the map $(U, V, W) \to (U', V', W') =$

$(U, \sqrt{B}V, W)$, every Montgomery curve $\mathbf{E}_{M,A,B}$ in the first subfamily is $\mathbb{F}_q$-isomorphic with a Montgomery curve $\mathbf{E}_{M,A,1}$. Thus, the second approach can be generalized for the family of Montgomery curves with $\chi(B) = 1$.

3 Revisited Addition Law for Extended Twisted Edwards Coordinates

Hisil et al. in [HWCD08] explained that if $\chi(-a) = 1$, then $\mathcal{E}_{TE,a,d}$ is $\mathbb{F}_q$-isomorphic to $\mathcal{E}_{TE,-1,-d/a}$, whose addition law (7) has a computational cost of $8\mathbf{M} + 1\mathbf{D}$, compared to $9\mathbf{M} + 2\mathbf{D}$ for the same addition law on $\mathcal{E}_{TE,a,d}$. This indicates a preference for using $\mathcal{E}_{TE,-1,-d/a}$. In this section, we introduce a new coordinate system and demonstrate how to compute the addition law on $\mathcal{E}_{TE,a,d}$ with the same cost as the addition law on $\mathcal{E}_{TE,-1,-d/a}$ when $\chi(-a) = 1$ or $\chi(-d) = 1$. This is achieved using a technique called scaling, without resorting to $\mathbb{F}_q$-isomorphic curves of $\mathcal{E}_{TE,a,d}$.

Our new coordinate system is defined as follows:

$$(\bar{X} : \bar{Y} : \bar{T} : \bar{Z}) = \begin{cases} (\sqrt{-a}X : Y : \sqrt{-a}T : Z), & \text{if } \chi(-a) = 1, \\ (\sqrt{-d}X : Y : \sqrt{-d}T : Z), & \text{if } \chi(-d) = 1. \end{cases} \tag{19}$$

As highlighted in Subsection 2.3, the addition laws (7), (8), (9), and (10) have computational costs of $9\mathbf{M}+2\mathbf{D}$, and $9\mathbf{M}+1\mathbf{D}$, $9\mathbf{M}+2\mathbf{D}$, and $9\mathbf{M}+1\mathbf{D}$. The following theorem demonstrates that by using the coordinate system (19), we can scale these addition laws for $\mathcal{E}_{TE,a,d}$ to reduce their computational costs. Specifically, the costs are reduced to $8\mathbf{M}+1\mathbf{D}$, $8\mathbf{M}$, $9\mathbf{M}+1\mathbf{D}$, and $9\mathbf{M}+1\mathbf{D}$ respectively if $\chi(-a) = 1$ (to $9\mathbf{M}+1\mathbf{D}$, $9\mathbf{M}+1\mathbf{D}$, $8\mathbf{M} + 1\mathbf{D}$, and $8\mathbf{M}$ respectively if $\chi(-d) = 1$).

Given two points $P_1 = (X_1 : Y_1 : T_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : T_2 : Z_2)$ in $\mathcal{E}_{TE,a,d}(\mathbb{F}_q)$, to compute $P_1 + P_2$, we must transform P_1 and P_2 into the new coordinate by multiplying their first and third coordinates by $\sqrt{-a}$ (by $\sqrt{-d}$ for the second case) to reach the points $(\bar{X}_1, \bar{Y}_1, \bar{T}_1, \bar{Z}_1)$ and $(\bar{X}_2, \bar{Y}_2, \bar{T}_2, \bar{Z}_2)$. The sum $P_1 + P_2$ is given by $(\bar{X}_3/\sqrt{-a} : \bar{Y}_3 : \bar{T}_3/\sqrt{-a} : \bar{Z}_3) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ (by $(\bar{X}_3/\sqrt{-d} : \bar{Y}_3 : \bar{T}_3/\sqrt{-d} : \bar{Z}_3) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ for the second case). For computation, we handle $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3) \notin \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ and retrieve $P_1 + P_2$ by multiplying the first and third components by $\frac{1}{\sqrt{-a}}$ (by $\frac{1}{\sqrt{-d}}$ for the second case). The multiplications by $\sqrt{-a}$ and $\frac{1}{\sqrt{-a}}$ (or $\sqrt{-d}$ and $\frac{1}{\sqrt{-d}}$) are not included in the computational cost because, during the scalar multiplication kP, where $k \in \mathbb{Z}$ and $P = (X : Y : T : Z) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$, these multiplications are computed only at the beginning and the end of the algorithm. In fact, unlike standard scalar multiplication algorithms that take $k \in \mathbb{Z}$ and $P = (X : Y : T : Z) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ and output $kP \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$, the scalar multiplication based on the following technique takes $k \in \mathbb{Z}$ and $(\sqrt{-a}X : Y : \sqrt{-a}T : Z)$ (or $(\sqrt{-d}X : Y : \sqrt{-d}T : Z)$ for the second case) as input, and retrieves kP in the final step by multiplying the first and third coordinates by $\frac{1}{\sqrt{-a}}$ (or $\frac{1}{\sqrt{-d}}$ for the second case). Therefore, these multiplications are excluded from the computational costs.

Theorem 1. *Let $a, d \in \mathbb{F}_q$ such that $ad(a - d) \neq 0$.*

1. *If $\chi(-a) = 1$, then the addition laws given in (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$ can be optimized, reducing computational costs to $8\mathbf{M} + 1\mathbf{D}$, $8\mathbf{M}$, $9\mathbf{M} + 1\mathbf{D}$, and $9\mathbf{M} + 1\mathbf{D}$, respectively.*

2. *If $\chi(-d) = 1$, then the addition laws given in (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$ can be optimized, reducing computational costs to $9\mathbf{M} + 1\mathbf{D}$, $9\mathbf{M} + 1\mathbf{D}$, $8\mathbf{M} + 1\mathbf{D}$, and $8\mathbf{M}$, respectively.*

Proof. In both cases, we use the scaling method to define new coordinates, allowing us to reformulate the equations (12), (13), (14), and (15). This adjustment optimizes the computational cost associated with $P_1 + P_2$.

1. If $\chi(-a) = 1$, then coordinates $(\bar{X} : \bar{Y} : \bar{T} : \bar{Z}) = (\sqrt{-a}X : Y : \sqrt{-a}T : Z)$ are well-defined. In this coordinate system, $(\bar{X}_1 : \bar{Y}_1 : \bar{T}_1 : \bar{Z}_1) = (\sqrt{-a}X_1 : Y_1 : \sqrt{-a}T_1 : Z_1)$ and $(\bar{X}_2 : \bar{Y}_2 : \bar{T}_2 : \bar{Z}_2) = (\sqrt{-a}X_2 : Y_2 : \sqrt{-a}T_2 : Z_2)$. Defining new variables

$$\bar{\mathcal{X}} = (\bar{X}_1\bar{Y}_2 + \bar{Y}_1\bar{X}_2), \qquad \bar{\mathcal{Z}} = (\bar{Z}_1\bar{Z}_2 - \frac{d}{a}\bar{T}_1\bar{T}_2), \tag{20}$$

$$\bar{\mathcal{Y}} = (\bar{Y}_1\bar{Y}_2 + \bar{X}_1\bar{X}_2), \qquad \bar{\mathcal{T}} = (\bar{Z}_1\bar{Z}_2 + \frac{d}{a}\bar{T}_1\bar{T}_2), \tag{21}$$

$$\bar{\mathcal{X}}' = (\bar{T}_1\bar{Z}_2 + \bar{Z}_1\bar{T}_2), \qquad \bar{\mathcal{Z}}' = (\bar{Y}_1\bar{Y}_2 - \bar{X}_1\bar{X}_2), \tag{22}$$

$$\bar{\mathcal{Y}}' = (\bar{T}_1\bar{Z}_2 - \bar{Z}_1\bar{T}_2), \qquad \bar{\mathcal{T}}' = (\bar{X}_1\bar{Y}_2 - \bar{Y}_1\bar{X}_2), \tag{23}$$

shows that the variables $\mathcal{X}, \mathcal{Y}, \mathcal{T}, \mathcal{Z}, \mathcal{X}', \mathcal{Y}', \mathcal{T}'$, and $\mathcal{Z}'$ given in (12), (13), (14), and (15) are in relation with variables $\bar{\mathcal{X}}, \bar{\mathcal{Y}}, \bar{\mathcal{T}}, \bar{\mathcal{Z}}, \bar{\mathcal{X}}', \bar{\mathcal{Y}}', \bar{\mathcal{T}}'$, and $\bar{\mathcal{Z}}'$ as follows

$$\begin{aligned} \mathcal{X} &= \frac{1}{\sqrt{-a}}\bar{\mathcal{X}}, \quad \mathcal{Z} = \bar{\mathcal{Z}}, \quad \mathcal{Y} = \bar{\mathcal{Y}}, \quad \mathcal{T} = \bar{\mathcal{T}}, \\ \mathcal{X}' &= \frac{1}{\sqrt{-a}}\bar{\mathcal{X}}', \quad \mathcal{Z}' = \bar{\mathcal{Z}}', \quad \mathcal{Y}' = \frac{1}{\sqrt{-a}}\bar{\mathcal{Y}}', \quad \mathcal{T}' = \frac{1}{\sqrt{-a}}\bar{\mathcal{T}}'. \end{aligned} \tag{24}$$

The addition laws presented in Proposition 1 are expressed in terms of $\mathcal{X}, \mathcal{Y}, \mathcal{T}, \mathcal{Z}, \mathcal{X}'$, $\mathcal{Y}', \mathcal{T}'$, and $\mathcal{Z}'$. Using the relations given in (24) and the fact that the first and third coordinates need to be multiplied by $\sqrt{-a}$, we can express $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3)$ in terms of $\bar{\mathcal{X}}, \bar{\mathcal{Y}}, \bar{\mathcal{T}}, \bar{\mathcal{Z}}, \bar{\mathcal{X}}', \bar{\mathcal{Y}}', \bar{\mathcal{T}}'$, and $\bar{\mathcal{Z}}'$, as

- For the addition law (7), $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3) = (\sqrt{-a}\mathcal{X}\mathcal{T} : \mathcal{Y}\mathcal{Z} : \sqrt{-a}\mathcal{X}\mathcal{Y} : \mathcal{Z}\mathcal{T}) = (\bar{\mathcal{X}}\bar{\mathcal{T}} : \bar{\mathcal{Y}}\bar{\mathcal{Z}} : \bar{\mathcal{X}}\bar{\mathcal{Y}} : \bar{\mathcal{Z}}\bar{\mathcal{T}})$.
- For the addition law (8), $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3) = (\sqrt{-a}\mathcal{X}'\mathcal{T}' : \mathcal{Y}'\mathcal{Z}' : \sqrt{-a}\mathcal{X}'\mathcal{Y}' : \mathcal{Z}'\mathcal{T}') = (\bar{\mathcal{X}}'\bar{\mathcal{T}}' : \bar{\mathcal{Y}}'\bar{\mathcal{Z}}' : \bar{\mathcal{X}}'\bar{\mathcal{Y}}' : \bar{\mathcal{Z}}'\bar{\mathcal{T}}')$.
- For the addition law (9), $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3) = (\sqrt{-a}\mathcal{X}'\mathcal{T} : \mathcal{Y}\mathcal{Z}' : \sqrt{-a}\mathcal{X}'\mathcal{Y} : \mathcal{Z}'\mathcal{T}) = (\bar{\mathcal{X}}'\bar{\mathcal{T}} : \bar{\mathcal{Y}}\bar{\mathcal{Z}}' : \bar{\mathcal{X}}'\bar{\mathcal{Y}} : \bar{\mathcal{Z}}'\bar{\mathcal{T}})$.
- For the addition law (10), $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3) = (\sqrt{-a}\mathcal{X}\mathcal{T}' : \mathcal{Y}'\mathcal{Z} : \sqrt{-a}\mathcal{X}\mathcal{Y}' : \mathcal{Z}\mathcal{T}') = (\bar{\mathcal{X}}\bar{\mathcal{T}}' : \bar{\mathcal{Y}}'\bar{\mathcal{Z}} : \bar{\mathcal{X}}\bar{\mathcal{Y}}' : \bar{\mathcal{Z}}\bar{\mathcal{T}}')$.

The following arithmetic demonstrate the procedure of computing the addition laws (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$, where their computational costs are $8\mathbf{M} + 1\mathbf{D}$, $8\mathbf{M}$, $9\mathbf{M} + 1\mathbf{D}$, and $9\mathbf{M} + 1\mathbf{D}$, respectively.

Addition (7)

$$\begin{gathered} A \leftarrow (\bar{X}_1 + \bar{Y}_1)(\bar{X}_2 + \bar{Y}_2), \quad B \leftarrow (\bar{X}_1 - \bar{Y}_1)(\bar{X}_2 - \bar{Y}_2), \quad C \leftarrow \bar{Z}_1\bar{Z}_2, \quad D \leftarrow \frac{d}{a}\bar{T}_1\bar{T}_2, \\ \bar{\mathcal{X}} \leftarrow A - B, \quad \bar{\mathcal{Y}} \leftarrow A + B, \quad \bar{\mathcal{Z}} \leftarrow 2(C - D), \quad \bar{\mathcal{T}} \leftarrow 2(C + D), \\ \bar{X}_3 \leftarrow \bar{\mathcal{X}}\bar{\mathcal{T}}, \quad \bar{Y}_3 \leftarrow \bar{\mathcal{Y}}\bar{\mathcal{Z}} \quad \bar{T}_3 \leftarrow \bar{\mathcal{X}}\bar{\mathcal{Y}}, \quad \bar{Z}_3 \leftarrow \bar{\mathcal{Z}}\bar{\mathcal{T}} \end{gathered} \tag{25}$$

Addition (8)

$$\begin{gathered} E \leftarrow \bar{T}_1\bar{Z}_2, \quad F \leftarrow \bar{Z}_1\bar{T}_2, \quad G \leftarrow (\bar{Y}_1 + \bar{X}_1)(\bar{Y}_2 - \bar{X}_2), \quad H \leftarrow (\bar{Y}_1 - \bar{X}_1)(\bar{Y}_2 + \bar{X}_2), \\ \bar{\mathcal{X}}' \leftarrow 2(E + F), \quad \bar{\mathcal{Y}}' \leftarrow 2(E - F), \quad \bar{\mathcal{Z}}' \leftarrow G + H, \quad \bar{\mathcal{T}}' \leftarrow G - H, \\ \bar{X}_3 \leftarrow \bar{\mathcal{X}}'\bar{\mathcal{T}}', \quad \bar{Y}_3 \leftarrow \bar{\mathcal{Y}}'\bar{\mathcal{Z}}' \quad \bar{T}_3 \leftarrow \bar{\mathcal{X}}'\bar{\mathcal{Y}}', \quad \bar{Z}_3 \leftarrow \bar{\mathcal{Z}}'\bar{\mathcal{T}}' \end{gathered} \tag{26}$$

Addition (9)

$$
\begin{gathered}
A \leftarrow \bar{X}_1\bar{X}_2, \quad B \leftarrow \bar{Y}_1\bar{Y}_2, \quad C \leftarrow \bar{Z}_1\bar{Z}_2, \quad D \leftarrow \bar{T}_1\bar{T}_2, \\
\bar{\mathcal{X}}' \leftarrow (\bar{T}_1 + \bar{Z}_1)(\bar{T}_2 + \bar{Z}_2) - C - D, \quad \bar{\mathcal{Y}} \leftarrow B + A, \quad \bar{\mathcal{Z}}' \leftarrow B - A, \quad \bar{\mathcal{T}} \leftarrow C + \frac{d}{a}D, \\
\bar{X}_3 \leftarrow \bar{\mathcal{X}}'\bar{\mathcal{T}}, \quad \bar{Y}_3 \leftarrow \bar{\mathcal{Y}}\bar{\mathcal{Z}}' \quad \bar{T}_3 \leftarrow \bar{\mathcal{X}}'\bar{\mathcal{Y}}, \quad \bar{Z}_3 \leftarrow \bar{\mathcal{Z}}'\bar{\mathcal{T}}
\end{gathered}
\tag{27}
$$

Addition (10)

$$
\begin{gathered}
E \leftarrow \bar{Y}_1\bar{X}_2, \quad F \leftarrow \bar{X}_1\bar{Y}_2, \quad G \leftarrow \bar{Z}_1\bar{Z}_2, \quad H \leftarrow \bar{T}_1\bar{T}_2, \\
\bar{\mathcal{X}} \leftarrow F + E, \quad \bar{\mathcal{Y}}' \leftarrow (\bar{T}_1 - \bar{Z}_1).(\bar{T}_2 + \bar{Z}_2) - H + G, \quad \bar{\mathcal{Z}} \leftarrow G - \frac{d}{a}H, \quad \bar{\mathcal{T}}' \leftarrow F - E, \\
\bar{X}_3 \leftarrow \bar{\mathcal{X}}\bar{\mathcal{T}}', \quad \bar{Y}_3 \leftarrow \bar{\mathcal{Y}}'\bar{\mathcal{Z}} \quad \bar{T}_3 \leftarrow \bar{\mathcal{X}}\bar{\mathcal{Y}}', \quad \bar{Z}_3 \leftarrow \bar{\mathcal{Z}}\bar{\mathcal{T}}'
\end{gathered}
\tag{28}
$$

2. If $\chi(-d) = 1$, then new coordinates $(\bar{X} : \bar{Y} : \bar{T} : \bar{Z}) = (\sqrt{-d}X : Y : \sqrt{-d}T : Z)$ are well-defined. Consequently, $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3)$ can be computed in the addition laws (7), (8), (9), and (10) for $\mathcal{E}_{TE,d,a}$. According to Proposition 1, these addition laws correspond to the addition laws (9), (10), (7), and (8) for $\mathcal{E}_{TE,a,d}$, which completes the proof.

□

Corollary 1. *Let $a, d \in \mathbb{F}_q$ such that $ad(a-d) \neq 0$.*

1. *Let $\chi(-a) = 1$. If $q \equiv 1 \pmod 4$ and $\chi(d) = -1$, then the addition law (7) is complete for $\mathcal{E}_{TE,a,d}$. If $q \equiv 3 \pmod 4$ and $\chi(d) = 1$, then the addition law (9) is complete for $\mathcal{E}_{TE,a,d}$.*
2. *Let $\chi(-d) = 1$. If $q \equiv 3 \pmod 4$ and $\chi(a) = 1$, then the addition law (7) is complete for $\mathcal{E}_{TE,a,d}$. If $q \equiv 1 \pmod 4$ and $\chi(a) = -1$, then the addition law (9) is complete for $\mathcal{E}_{TE,a,d}$.*

Proof. The addition laws (7) and (9) are complete if $\chi(d) = \chi(ad) = -1$ and $\chi(a) = \chi(ad) = -1$, respectively. Thus, if $\chi(-a) = 1$, then the addition law (7) is complete if $q \equiv 1 \pmod 4$ and $\chi(d) = -1$, and the addition law (9) is complete if $q \equiv 3 \pmod 4$ and $\chi(d) = 1$. If $\chi(-d) = 1$, then the addition law (7) is complete if $q \equiv 3 \pmod 4$ and $\chi(a) = 1$, and the addition law (9) is complete if $q \equiv 1 \pmod 4$ and $\chi(a) = -1$. □

Table 2: Revisited Addition for Extended Twisted Edwards Coordinates

Addition	Condition	Map	Cost	Condition for completeness
(25)	$\chi(-a) = 1$	$(\bar{X} : \bar{Y} : \bar{T} : \bar{Z}) = (\sqrt{-a}X, Y, \sqrt{-a}T, Z)$	$8\mathbf{M} + 1\mathbf{D}$	$q \equiv 1 \pmod 4, \quad \chi(d) = -1$
(26)			$8\mathbf{M}$	Incomplete
(27)			$9\mathbf{M} + 1\mathbf{D}$	$q \equiv 3 \pmod 4, \quad \chi(d) = 1$
(28)			$9\mathbf{M} + 1\mathbf{D}$	Incomplete
Analogous to (25)	$\chi(-d) = 1$	$(\bar{X} : \bar{Y} : \bar{T} : \bar{Z}) = (\sqrt{-d}X, Y, \sqrt{-d}T, Z)$	$8\mathbf{M} + 1\mathbf{D}$	$q \equiv 1 \pmod 4, \quad \chi(a) = -1$
Analogous to (26)			$8\mathbf{M}$	Incomplete
Analogous to (27)			$9\mathbf{M} + 1\mathbf{D}$	$q \equiv 3 \pmod 4, \quad \chi(a) = 1$
Analogous to (28)			$9\mathbf{M} + 1\mathbf{D}$	Incomplete

Table 2 summarizes Theorem 1 and Corollary 1 regarding the computational costs and the completeness of the addition laws (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$. The table indicates that, when $q \equiv 1 \pmod 4$ then $\mathcal{E}_{TE,a,d}$ has complete addition laws with costs $8\mathbf{M} + 1\mathbf{D}$ if $\chi(ad) = \chi(d) = -1$ or $\chi(ad) = \chi(a) = -1$. Conversely, for $q \equiv 3 \pmod 4$, $\mathcal{E}_{TE,a,d}$ has complete addition laws with costs $9\mathbf{M} + 1\mathbf{D}$ under the same conditions. Moreover, if $\chi(-a) = 1$ or $\chi(-d) = 1$, we have incomplete addition laws for $\mathcal{E}_{TE,a,d}$ with computational costs of $8\mathbf{M}$.

4 Extended Montgomery Coordinates

As highlighted in Subsection 2.4, two maps, $\psi : \mathbf{E}_{TE,a,d} \to \mathbf{E}_{M,A,B}$ and $\psi^{-1} : \mathbf{E}_{M,A,B} \to \mathbf{E}_{TE,a,d}$, were used in [KPKK19] to establish an addition law for the Montgomery curves. However, this addition law is not complete due to the exceptional points of the maps ψ and ψ^{-1}. Additionally, its computational cost is $19\mathbf{M} + 1\mathbf{S} + 2\mathbf{D}$. We propose replacing ψ and ψ^{-1} with two more efficient maps, π and π^{-1}, which present an addition law for Montgomery curves $\mathbf{E}_{M,A,B}$ with a computational cost of $15\mathbf{M} + 2\mathbf{S} + 2\mathbf{D}$. Nevertheless, this addition law remains incomplete because of the exceptional points of the maps π and π^{-1}, we can employ these maps to introduce two multiplication-free maps, ϕ and ϕ^{-1}, between Montgomery and twisted Edwards curves in extended coordinates. The maps ϕ and ϕ^{-1} are multiplication-free and have no exceptional points; thus, they not only induce the complete addition laws of twisted Edwards curves to Montgomery curves but also reduce the computational costs to $9\mathbf{M} + 2\mathbf{D}$ and $8\mathbf{M} + 1\mathbf{D}$, respectively, matching the computational costs of the complete addition laws for twisted Edwards curves. Let

$$\begin{gathered}\pi : \mathcal{E}_{TE,a,d}(\mathbb{F}_q) \to \mathbf{E}_{M,A,B}(\mathbb{F}_q), \\ (X : Y : T : Z) \to \begin{cases} (0 : 0 : 1), & \text{if } (X : Y : T : Z) = (0 : -1 : 0 : 1), \\ (X + T : Z + Y : X - T), & \text{otherwise.} \end{cases}\end{gathered} \tag{29}$$

and

$$\begin{gathered}\pi^{-1} : \mathbf{E}_{M,A,B}(\mathbb{F}_q) \to \mathcal{E}_{TE,a,d}(\mathbb{F}_q), \\ (U : V : W) \to \begin{cases} (0 : 1 : 0 : 1), & \text{if } (U : V : W) = (0 : 1 : 0), \\ (0 : -1 : 0 : 1), & \text{if } (U : V : W) = (0 : 0 : 1), \\ (U(U + W) : V(U - W) : U(U - W) : V(U + W)), & \text{otherwise.} \end{cases}\end{gathered} \tag{30}$$

These two maps are computed using the following diagram

$$\begin{tikzcd} \mathbf{E}_{TE,a,d} \arrow[r, "\psi"] & \mathbf{E}_{M,A,B} \\ \mathcal{E}_{TE,a,d} \arrow[u, "\rho"] \arrow[ur, "\pi"'] & \end{tikzcd} \qquad \begin{tikzcd} \mathbf{E}_{TE,a,d} \arrow[d, "\rho^{-1}"'] & \mathbf{E}_{M,A,B} \arrow[l, "\psi^{-1}"'] \arrow[dl, "\pi^{-1}"] \\ \mathcal{E}_{TE,a,d} & \end{tikzcd}$$

where $\rho : \mathcal{E}_{TE,a,d} \to \mathbf{E}_{TE,a,d}$ is defined by $\rho(X : Y : T : Z) = (X : Y : Z)$, and $\rho^{-1} : \mathbf{E}_{TE,a,d} \to \mathcal{E}_{TE,a,d}$ is given by $\rho^{-1}(X : Y : Z) = (XZ : YZ : XY : Z^2)$ if $Z \neq 0$. For twisted curves over $\mathbb{F}_q$, we note that $\rho(1 : 0 : \pm\sqrt{a/d} : 0) = (1 : 0 : 0)$ if $\chi(ad) = 1$ and $\rho(0 : \pm\sqrt{d} : 1 : 0) = (0 : 1 : 0)$ if $\chi(d) = 1$.

In contrast to ψ, which requires $3\mathbf{M}$ computations, π avoids this cost. This is because we can simplify the map $\pi = \psi \circ \rho$ using the equality $XY = TZ$, eliminating the $3\mathbf{M}$ computation needed to transport points on $\mathcal{E}_{TE,a,d}$ to $\mathbf{E}_{M,A,B}$ as follows

$$\begin{aligned} \pi(X : Y : T : Z) = \psi(\rho(X : Y : T : Z)) &= \psi(X : Y : Z) \\ &= (XZ + XY : Z^2 + ZY : XZ - XY) \\ &= (XZ + TZ : Z^2 + ZY : XZ - TZ) \end{aligned}$$

$$= \quad (X+T : Z+Y : X-T).$$

Moreover, using this extended coordinate system allows us to reduce the computational cost of $10\mathbf{M}+1\mathbf{S}+2\mathbf{D}$ to $9\mathbf{M}+2\mathbf{D}$. Therefore, employing π and π^{-1}, rather than ψ and ψ^{-1}, results in an addition law with computational cost of $15\mathbf{M}+2\mathbf{S}+2\mathbf{D}$ in the general case. More concretely, to compute P_1+P_2 for points $P_1, P_2 \in \mathbf{E}_{M,A,B}$, one initially computes the corresponding points $\pi^{-1}(P_1), \pi^{-1}(P_2) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$, necessitating $6\mathbf{M}+2\mathbf{S}$ computations, then computes $\pi^{-1}(P_1)+\pi^{-1}(P_2) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ with the computational cost of $9\mathbf{M}+2\mathbf{D}$. Finally, applies the multiplication-free map π to the output to obtain $P_1+P_2 = \pi(\pi^{-1}(P_1)+\pi^{-1}(P_2))$, resulting in a total computational cost of $15\mathbf{M}+2\mathbf{S}+2\mathbf{D}$. In addition, when $q \equiv 1 \pmod 4$ if $\chi(ad) = \chi(d) = -1$ or $\chi(ad) = \chi(a) = -1$, this computational cost can be reduced to $14\mathbf{M}+2\mathbf{S}+1\mathbf{D}$ as the computational cost of $\mathcal{E}_{TE,a,d}$ can be reduced to $8\mathbf{M}+1\mathbf{D}$.

In the rest of this Section, we investigate how to present maps between twisted Edwards curves and Montgomery curves such that they i) have no exceptional points as ψ, ψ^{-1}, π, and π^{-1}, and ii) are multiplication-free in both directions, from twisted Edwards curves to Montgomery curves and vice versa. These properties not only allow the complete addition laws from twisted Edwards curves to be applied to Montgomery curves, but they also reduce the computational costs to $9\mathbf{M}+2\mathbf{D}$ and $8\mathbf{M}+1\mathbf{D}$ in general and specific cases, respectively. To achieve this goal, we introduce a new representation system for points on the Montgomery curves, called extended Montgomery coordinates.

In Subsection 2.3, we discussed how Hisil et al. used an auxiliary coordinate $t = xy$ to enhance the arithmetic efficiency on twisted Edwards curves [HWCD08]. In this coordinate system, each point (x, y) on the curve $E_{TE,a,d}$ defined over $\mathbb{F}_q$ corresponds to the point (x, y, t), which satisfies the equation $ax^2 + y^2 = 1 + dt^2$. This extended affine point (x, y, t) is mapped to extended projective point $(x : y : t : 1)$ on the curve $\mathcal{E}_{TE,a,d}$, as detailed in (6). Conversely, each point $(X : Y : T : Z) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$, where $Z \neq 0$, directly corresponds to an extended affine point $(X/Z, Y/Z, T/Z)$.

By employing the same technique, we introduce extended Montgomery coordinates, denoted by $\mathcal{E}_{M,A,B}$. This novel point representation results in a multiplication-free map between $\mathcal{E}_{M,A,B}$ and $\mathcal{E}_{TE,a,d}$ without any exceptional points. Therefore, we can employ the complete addition law $\mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ to develop a complete addition law for $\mathcal{E}_{M,A,B}$, maintaining the same computational cost of $9\mathbf{M}+2\mathbf{D}$ and $8\mathbf{M}+1\mathbf{D}$ in general and specific cases, respectively. This approach provides a faster complete addition law for Montgomery curves compared to the most efficient known complete addition law for them, which demands $14\mathbf{M}+2\mathbf{D}$ computations.

As we stated in Subsection 2.2, an affine Montgomery curve $E_{M,A,B}$ is defined by the equation $Bv^2 = u^3 + Au^2 + u$, where $B(A^2-4) \neq 0$. Using the auxiliary coordinate $s = v/u$, we can correspond each point $(u, v) \in E_{M,A,B}(\mathbb{F}_q)$ to a point (u, v, s) satisfying the equation

$$Bsv = u^2 + Au + 1, \qquad B(A^2-4) \neq 0.$$

The extended projective closure of the given curve in $\mathbb{P}^3$, is obtained through the substitution $(u, v, s) = (U/W, V/W, S/W)$, leading to the equations

$$\mathcal{E}_{M,A,B} : BSV = U^2 + AUW + W^2, \qquad SU = VW. \tag{31}$$

Given $A, B \in \mathbb{F}_q$ with $B(A^2-4) \neq 0$, we fix $a = (A+2)/B$ and $d = (A-2)/B$, so we have $ad(a-d) \neq 0$. Using the diagram

$$\begin{tikzcd}
 & \mathbf{E}_{M,A,B}(\mathbb{F}_q) \arrow[d, "\sigma"] \\
\mathcal{E}_{TE,a,d}(\mathbb{F}_q) \arrow[ur, "\pi"] \arrow[r, "\phi"'] & \mathcal{E}_{M,A,B}(\mathbb{F}_q)
\end{tikzcd}$$

where π is the map (29) and

$$\begin{aligned} \sigma : \mathbf{E}_{M,A,B}(\mathbb{F}_q) &\to \mathcal{E}_{M,A,B}(\mathbb{F}_q), \\ (U:V:W) &\to \begin{cases} (0:1:0:0), & \text{if } (U:V:W)=(0:1:0), \\ (0:0:1:0), & \text{if } (U:V:W)=(0:0:1), \\ (U^2:UV:VW:UW), & \text{otherwise,} \end{cases} \end{aligned} \tag{32}$$

we can define the birational map $\phi : \mathcal{E}_{TE,a,d}(\mathbb{F}_q) \longrightarrow \mathcal{E}_{M,A,B}(\mathbb{F}_q)$. Let $P = (X:Y:T:Z)$ be a point of $\mathcal{E}_{TE,a,d}(\mathbb{F}_q)$, and let $Q = \pi(P)$ given by the map (29). We see that $P = (0:1:0:1)$ if and only if $Q = (0:1:0)$ and $P = (0:-1:0:1)$ if and only if $Q = (0:0:1)$. We compute $\phi(P)$ as follows.

- If $P = (0:1:0:1)$, then $Q = \pi(P) = (0:1:0)$. And, if $Q = (0:1:0)$, then $X+T = X-T = 0$ and $Y+Z \neq 0$. Thus, $X = T = 0$ and $Y = Z \neq 0$. So, $P = (0:1:0:1)$. In this case, we have $\phi(P) = \sigma(\pi(P)) = \sigma(Q) = (0:1:0:0)$.
- If $P = (0:-1:0:1)$, then $Q = \pi(P) = (0:0:1)$. And, if $Q = (0:0:1)$ and if $P \neq (0:-1:0:1)$, then $X+T = 0$, $X-T = 1$, and $Z+Y = 0$. From the curve equation $aX^2 - dT^2 = Z^2 - Y^2$, we obtain $a = d$, which is a contradiction. So, if $Q = (0:0:1)$, then $P = (0:-1:0:1)$. In this case, we have $\phi(P) = \sigma(\pi(P)) = \sigma(Q) = (0:0:1:0)$.
- If $P \neq (0:\pm1:0:1)$, then $Q = (X+T:Z+Y:X-T) \neq (0:1:0), (0:0:1)$. Since $XY = TZ$, we have $(X+T)(Z-Y) = (Z+Y)(X-T)$ and $X+T \neq 0$. Thus,

$$\begin{aligned} \phi(P) &= \sigma(\pi(P)) = \sigma(Q) \\ &= \sigma(X+T:Z+Y:X-T) \\ &= ((X+T)^2:(X+T)(Z+Y):(Z+Y)(X-T):(X+T)(X-T)) \\ &= ((X+T)^2:(X+T)(Z+Y):(X+T)(Z-Y):(X+T)(X-T)) \\ &= (X+T:Z+Y:Z-Y:X-T). \end{aligned}$$

Therefore, the birational map ϕ is defined as

$$\begin{aligned} \phi : \mathcal{E}_{TE,a,d}(\mathbb{F}_q) &\longrightarrow \mathcal{E}_{M,A,B}(\mathbb{F}_q) \\ (X:Y:T:Z) &\longrightarrow (U:V:S:W) = (X+T:Z+Y:Z-Y:X-T). \end{aligned} \tag{33}$$

Using the linear map ϕ, the birational map ϕ^{-1} is defined as

$$\begin{aligned} \phi : \mathcal{E}_{M,A,B}(\mathbb{F}_q) &\longrightarrow \mathcal{E}_{TE,a,d}(\mathbb{F}_q) \\ (U:V:S:W) &\longrightarrow (X:Y:T:Z) = (U+W:V-S:U-W:V+S). \end{aligned} \tag{34}$$

Obviously, the maps ϕ and ϕ^{-1}, presented in (33) and (34), are the multiplication-free maps without exceptional points between Montgomery curves and twisted Edwards curves in extended coordinates, and we proved the following theorem.

Theorem 2. *Let $a, d, A, B \in \mathbb{F}_q$ such that $ad(a-d) \neq 0$, $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$. There are birational multiplication-free maps $\phi : \mathcal{E}_{TE,a,d}(\mathbb{F}_q) \longrightarrow \mathcal{E}_{M,A,B}(\mathbb{F}_q)$ and $\phi^{-1} : \mathcal{E}_{M,A,B}(\mathbb{F}_q) \longrightarrow \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ as given in (33) and (34).*

An alternative approach to find the birational maps ϕ and ϕ^{-1} is as follows. Consider the following curves, each of which is an intersection of two quadratic surfaces, and they present the twisted Edwards curve and the Montgomery curve, respectively, in extended coordinates.

- $aX^2 + Y^2 = Z^2 + dT^2, \qquad XY = ZT.$
- $BSV = U^2 + AUW + W^2, \qquad SU = VW.$

According to the equation $aX^2 + Y^2 = Z^2 + dT^2$ we have

$$(Z - Y)(Z + Y) = aX^2 - dT^2. \tag{35}$$

By comparing the equation (35) with

$$BSV = U^2 + AUW + W^2,$$

we let $S = Z - Y$ and $V = Z + Y$. In addition, having $\frac{X}{T} = \frac{Z}{Y}$ implies $\frac{X+T}{X-T} = \frac{Z+Y}{Z-Y}$ and having the equality $\frac{U}{W} = \frac{V}{S} = \frac{Z+Y}{Z-Y}$ implies $U = X + T$ and $W = X - T$. Therefore,

$$\begin{aligned} U^2 + AUW + W^2 &= (X + T)^2 + A(X + T)(X - T) + (X - T)^2 \\ &= (A + 2)X^2 - (A - 2)T^2. \end{aligned} \tag{36}$$

On the other hand,

$$BSV = B(Z^2 - Y^2) = BaX^2 - BdT^2. \tag{37}$$

Since $BSV = U^2 + AUW + W^2$, the left-hand side of the equations (36) and (37) are the same and we conclude that $Ba = (A + 2)$ and $Bd = (A - 2)$, or equivalently $a = \frac{A+2}{B}$ and $d = \frac{A-2}{B}$. Therefore, the map ϕ, given in (34), transforms the extended twisted Edwards curve

$$aX^2 + Y^2 = Z^2 + dT^2, \qquad XY = ZT$$

to

$$BSV = U^2 + AUW + W^2, \qquad SU = VW.$$

We can also extract the map ϕ^{-1} from the map ϕ.

Remark 3. With the same discussion, we can show if we consider the equation $(Y - Z)(Y + Z) = \bar{d}T^2 - \bar{a}X^2$, rather than the equation (35), then $S = Y - Z$ and $V = Y + Z$. Consequently, we have $U = T + X$ and $W = T - X$. Therefore, $U^2 + AUW + W^2 = (2 + A)T^2 + (2 - A)X^2$ and $BSV = B\bar{d}T^2 - B\bar{a}X^2$, so $\bar{d} = \frac{A+2}{B}$ and $\bar{a} = \frac{A-2}{B}$. This shows that the map $(X : Y : T : Z) \to (U : V : S : W) = (T + X : Y + Z : Y - Z : T - X)$ transfers $\mathcal{E}_{TE,\bar{a},\bar{d}} = \mathcal{E}_{TE,d,a}$ to $\mathcal{E}_{M,A,B}$. Here, $a = \frac{A+2}{B}$ and $d = \frac{A-2}{B}$. In other word, above map transfers $\mathcal{E}_{TE,a,d}$ to $\mathcal{E}_{M,-A,-B}$. The inverse of above map $(U : V : S : W) \to (X : Y : T : Z) = (U - W : V + S : U + W : V - S)$ transfers $\mathcal{E}_{M,A,B}$ to $\mathcal{E}_{TE,d,a}$.

The following theorem leverages Theorem 2 to extend the concept of completeness from twisted Edwards curves to Montgomery curves.

Theorem 3. *Every complete addition law for extended twisted Edwards coordinates can be translated into a complete addition law for extended Montgomery coordinates.*

Proof. Suppose that $\tau : \mathcal{E}_{TE,a,d} \times \mathcal{E}_{TE,a,d} \to \mathcal{E}_{TE,a,d}$ be a complete addition law for $\mathcal{E}_{TE,a,d}$. So, for any pair $P_1, P_2 \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$, $\tau(P_1, P_2)$ is defined. We can define an addition law for $\mathcal{E}_{M,A,B}$ as

$$\begin{aligned} &\tau' : \mathcal{E}_{M,A,B} \times \mathcal{E}_{M,A,B} \to \mathcal{E}_{M,A,B} \\ &\tau'(Q_1, Q_2) = \phi(\tau(\phi^{-1}(Q_1), \phi^{-1}(Q_2))), \end{aligned} \tag{38}$$

where $Q_1, Q_2 \in \mathcal{E}_{M,A,B}(\mathbb{F}_q)$, and ϕ and ϕ^{-1} are the maps (33) and (34). Clearly, since τ is well-defined, this addition law τ' is well-defined too, outputting $Q_1 + Q_2 \in \mathcal{E}_{M,A,B}$. □

Since τ is a complete addition law for $\mathcal{E}_{TE,a,d}$ and the maps ϕ^{-1} and ϕ are both multiplication-free maps between $\mathcal{E}_{M,A,B}$ and $\mathcal{E}_{TE,a,d}$, the addition law τ' not only is complete but also its computational costs is the same as τ (up to the number of additions). In the following section, we present the complete addition laws for Montgomery curves, derived from those established for twisted Edwards curves.

5 Arithmetic in $\mathcal{E}_{M,A,B}$

In this section, we use the Theorem 3 to derive the addition laws (40), (41), (42), and (43) for the Montgomery curve $\mathcal{E}_{M,A,B}$ using the addition laws (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$. Then, in Subsection 5.1, we introduce a coordinate system for Montgomery curves, similar to the one defined in Section 3 for twisted Edwards curves, to derive more efficient complete addition laws (44) and (45) for the Montgomery curve $\mathcal{E}_{M,A,B}$ with the same computational cost as the complete addition laws (25) and (27) for $\mathcal{E}_{TE,a,d}$.

Let $i = 1, 2$ and $P_i = (U_i : V_i : S_i : W_i) \in \mathcal{E}_{M,A,B}(\mathbb{F}_q)$. Using the map ϕ^{-1} we first compute $Q_i = \phi^{-1}(P_i) = (X_i : Y_i : T_i : Z_i) \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$, where

$$\begin{aligned} X_1 &= U_1 + W_1, \quad Y_1 = V_1 - S_1, \quad T_1 = U_1 - W_1, \quad Z_1 = V_1 + S_1, \\ X_2 &= U_2 + W_2, \quad Y_2 = V_2 - S_2, \quad T_2 = U_2 - W_2, \quad Z_2 = V_2 + S_2. \end{aligned} \tag{39}$$

Following to the addition law (7) for $\mathcal{E}_{TE,a,d}$, $P_1 + P_2 = (U_3 : V_3 : S_3 : W_3) \in \mathcal{E}_{M,A,B}$ can be computed with the cost of $9\mathbf{M} + 2\mathbf{D}$ as follows:

$$\begin{aligned} &A' \leftarrow X_1X_2, \quad B' \leftarrow Y_1Y_2, \quad C' \leftarrow \frac{A-2}{B}T_1T_2, \quad D' \leftarrow Z_1Z_2, \\ &E' \leftarrow (X_1 + Y_1)(X_2 + Y_2) - A' - B', \quad F' \leftarrow D' - C', \quad G' \leftarrow D' + C', \\ &H' \leftarrow B' - \frac{A+2}{B}A', \quad X_3 \leftarrow E'F', \quad Y_3 \leftarrow G'H', \quad T_3 \leftarrow E'H', \quad Z_3 \leftarrow F'G' \\ &U_3 \leftarrow X_3 + T_3, \quad V_3 \leftarrow Z_3 + Y_3, \quad S_3 \leftarrow Z_3 - Y_3, \quad W_3 \leftarrow X_3 - T_3. \end{aligned} \tag{40}$$

In the final step, we applied the map ϕ, as defined in (33) to convert the point $Q_3 = (X_3 : Y_3 : T_3 : Z_3) = Q_1 + Q_2 \in \mathcal{E}_{TE,a,d}(\mathbb{F}_q)$ to the point $P_3 = (U_3 : V_3 : S_3 : W_3) = P_1 + P_2 \in \mathcal{E}_{M,A,B}(\mathbb{F}_q)$. This conversion is similarly applied in the addition laws (41), (42), and (43).

Following the addition law (8) for $\mathcal{E}_{TE,a,d}$, we compute $P_1 + P_2 = (U_3 : V_3 : S_3 : W_3) \in \mathcal{E}_{M,A,B}$ with the cost of $9\mathbf{M} + 1\mathbf{D}$ as follows:

$$\begin{aligned} &A' \leftarrow X_1X_2, \quad B' \leftarrow Y_1Y_2, \quad C' \leftarrow T_1Z_2, \quad D' \leftarrow Z_1T_2, \quad E' \leftarrow \frac{A+2}{B}A', \\ &F' \leftarrow (X_1 - Y_1)(X_2 + Y_2) - A' + B', \quad G' \leftarrow C' - D', \quad H' \leftarrow C' + D', \\ &I' \leftarrow B' + E', \quad X_3 \leftarrow H'F', \quad Y_3 \leftarrow I'G', \quad T_3 \leftarrow H'G', \quad Z_3 \leftarrow I'F' \\ &U_3 \leftarrow X_3 + T_3, \quad V_3 \leftarrow Z_3 + Y_3, \quad S_3 \leftarrow Z_3 - Y_3, \quad W_3 \leftarrow X_3 - T_3 \end{aligned} \tag{41}$$

Following to the addition law (9) for $\mathcal{E}_{TE,a,d}$, we compute $P_1 + P_2 = (U_3 : V_3 : S_3 : W_3) \in \mathcal{E}_{M,A,B}$ with the cost of $9\mathbf{M} + 2\mathbf{D}$ as follows:

$$\begin{aligned} &A' \leftarrow X_1X_2, \ B' \leftarrow Y_1Y_2, \ C' \leftarrow T_1T_2, \ D' \leftarrow Z_1Z_2, \ E' \leftarrow \frac{A+2}{B}A', \\ &F' \leftarrow \frac{A-2}{B}C', \ G' \leftarrow (T_1 + Z_1)(T_2 + Z_2) - C' - D', \quad H' \leftarrow D' - F', \ I' \leftarrow B' - E', \\ &J' \leftarrow B' + E', \ X_3 \leftarrow G'H', \ Y_3 \leftarrow I'J', \ T_3 \leftarrow G'I', \ Z_3 \leftarrow J'H' \\ &U_3 \leftarrow X_3 + T_3, \quad V_3 \leftarrow Z_3 + Y_3, \quad S_3 \leftarrow Z_3 - Y_3, \quad W_3 \leftarrow X_3 - T_3 \end{aligned} \tag{42}$$

Following the addition law (10) for $\mathcal{E}_{TE,a,d}$, we compute $P_1 + P_2 = (U_3 : V_3 : S_3 : W_3) \in \mathcal{E}_{M,A,B}$ with the cost of $9\mathbf{M} + 1\mathbf{D}$ as follows:

$$\begin{aligned} &A' \leftarrow X_1Y_2, \ B' \leftarrow Y_1X_2, \ C' \leftarrow T_1T_2, \ D' \leftarrow Z_1Z_2, \ E' \leftarrow \frac{A-2}{B}C', \\ &F' \leftarrow (T_1 - Z_1)(T_2 + Z_2) - C' + D', \quad G' \leftarrow A' + B', \quad H' \leftarrow A' - B', \quad I' \leftarrow D' + E', \\ &X_3 \leftarrow G'H', \quad Y_3 \leftarrow F'I', \quad T_3 \leftarrow G'F', \quad Z_3 \leftarrow I'H' \end{aligned} \tag{43}$$

$$U_3 \leftarrow X_3 + T_3, \quad V_3 \leftarrow Z_3 + Y_3, \quad S_3 \leftarrow Z_3 - Y_3, \quad W_3 \leftarrow X_3 - T_3$$

The conditions $\chi(d) = \chi(ad) = -1$ and $\chi(a) = \chi(ad) = -1$ are equivalent to $\chi\left(\frac{A-2}{B}\right) = \chi(A^2-4) = -1$ and $\chi\left(\frac{A+2}{B}\right) = \chi(A^2-4) = -1$, respectively. Therefore, since the addition laws (7) and (9) for $\mathcal{E}_{TE,a,d}$ are complete with a computational cost of $9\mathbf{M} + 2\mathbf{D}$ if $\chi(d) = \chi(ad) = -1$ and $\chi(a) = \chi(ad) = -1$, respectively, the addition laws (40) and (42) are complete with the same computational cost if $\chi\left(\frac{A-2}{B}\right) = \chi(A^2-4) = -1$ and $\chi\left(\frac{A+2}{B}\right) = \chi(A^2-4) = -1$, respectively.

5.1 More Efficient Arithmetic in $\mathcal{E}_{M,A,B}$

In Section 3, we demonstrated that the new coordinate system (19) reduces the computational costs of the addition laws (7), (8), (9), and (10) for $\mathcal{E}_{TE,a,d}$. Similarly, we can introduce a coordinate system for Montgomery curves as follows:

$$(\bar{U} : \bar{V} : \bar{S} : \bar{W}) = \begin{cases} \left(\sqrt{-\frac{A+2}{B}}U : V : S : \sqrt{-\frac{A+2}{B}}W\right), & \text{if } \chi(-\frac{A+2}{B}) = 1, \\ \left(\sqrt{-\frac{A-2}{B}}U : V : S : \sqrt{-\frac{A-2}{B}}W\right), & \text{if } \chi(-\frac{A-2}{B}) = 1. \end{cases}$$

Using this coordinate system we can reduce the computational costs of the addition laws (40), (41), (42), and (43) on $\mathcal{E}_{M,A,B}$ to $8\mathbf{M} + 1\mathbf{D}$, $8\mathbf{M}$, $9\mathbf{M} + 1\mathbf{D}$, and $9\mathbf{M} + 1\mathbf{D}$, respectively, if $\chi\left(-\frac{A+2}{B}\right) = 1$, and to $9\mathbf{M}+1\mathbf{D}$, $9\mathbf{M}+1\mathbf{D}$, $8\mathbf{M}+1\mathbf{D}$, and $8\mathbf{M}$, respectively, if $\chi\left(-\frac{A-2}{B}\right) = 1$.

Let $\chi(-\frac{A+2}{B}) = 1$. To compute $P_1 + P_2$ in this coordinate system, for two given points $P_1 = (U_1 : V_1 : S_1 : W_1)$ and $P_2 = (U_2 : V_2 : S_2 : W_2)$ in $\mathcal{E}_{M,A,B}(\mathbb{F}_q)$, we use the following arithmetic that corresponds to the addition law (40). The inputs of this coordinate system are the points

$$(\bar{U}_i : \bar{V}_i : \bar{S}_i : \bar{W}_i) = \left(\sqrt{-\frac{A+2}{B}}U_i : V_i : S_i : \sqrt{-\frac{A+2}{B}}W_i\right),$$

where $i = 1, 2$.

$$\begin{aligned}
&\bar{X}_1 = \bar{U}_1 + \bar{W}_1, \quad \bar{Y}_1 = \bar{V}_1 - \bar{S}_1, \quad \bar{T}_1 = \bar{U}_1 - \bar{W}_1, \quad \bar{Z}_1 = \bar{V}_1 + \bar{S}_1, \\
&\bar{X}_2 = \bar{U}_2 + \bar{W}_2, \quad \bar{Y}_2 = \bar{V}_2 - \bar{S}_2, \quad \bar{T}_2 = \bar{U}_2 - \bar{W}_2, \quad \bar{Z}_2 = \bar{V}_2 + \bar{S}_2, \\
&A' \leftarrow (\bar{X}_1 + \bar{Y}_1)(\bar{X}_2 + \bar{Y}_2), \quad B' \leftarrow (\bar{X}_1 - \bar{Y}_1)(\bar{X}_2 - \bar{Y}_2), \quad C' \leftarrow \bar{Z}_1\bar{Z}_2, \quad D' \leftarrow \frac{A-2}{A+2}\bar{T}_1\bar{T}_2, \\
&\mathcal{X} \leftarrow A' - B', \quad \mathcal{Y} \leftarrow A' + B', \quad \mathcal{Z} \leftarrow 2(C' - D'), \quad \mathcal{T} \leftarrow 2(C' + D'), \\
&\bar{X}_3 \leftarrow \mathcal{X}\mathcal{T}, \quad \bar{Y}_3 \leftarrow \mathcal{Y}\mathcal{Z}, \quad \bar{T}_3 \leftarrow \mathcal{X}\mathcal{Y}, \quad \bar{Z}_3 \leftarrow \mathcal{Z}\mathcal{T}, \\
&\bar{U}_3 \leftarrow \bar{X}_3 + \bar{T}_3, \quad \bar{Y}_3 \leftarrow \bar{Z}_3 + \bar{Y}_3, \quad \bar{S}_3 \leftarrow \bar{Z}_3 - \bar{Y}_3, \quad \bar{W}_3 \leftarrow \bar{X}_3 - \bar{T}_3.
\end{aligned} \tag{44}$$

Since $\bar{U}_i$ and $\bar{W}_i$ have the same coefficient $\sqrt{-\frac{A+2}{B}}$, $\bar{X}_i$ and $\bar{T}_i$ have the same coefficient $\sqrt{-a}$. Similarly, $\bar{Y}_i$ and $\bar{Z}_i$ have the same coefficient. Therefore, $(\bar{X}_1 : \bar{Y}_1 : \bar{T}_1 : \bar{W}_1)$ and $(\bar{X}_2 : \bar{Y}_2 : \bar{T}_2 : \bar{W}_2)$ are aligned with the defined coordinates in (19) for the case $\chi(-a) = 1$. The arithmetic given in (25) compute $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3)$. Finally, $(\bar{U}_3 : \bar{V}_3 : \bar{S}_3 : \bar{W}_3)$ is derived from $(\bar{X}_3 : \bar{Y}_3 : \bar{T}_3 : \bar{Z}_3)$. This addition law corresponds to the addition law (25), so has computational cost of $8\mathbf{M} + 1\mathbf{D}$ and is complete if $\chi\left(\frac{A-2}{B}\right) = \chi(A^2-4) = -1$. Specifically, satisfying $\chi(-\frac{A+2}{B}) = 1$ implies $\chi(-1) = 1$, or equivalently $q \equiv 1 \pmod 4$. Similar to the Section 3, we note that $(\bar{U}_3 : \bar{V}_3 : \bar{S}_3 : \bar{W}_3) \notin \mathcal{E}_{M,A,B}$, and $P_1 + P_2 = \left(\bar{U}_3/\sqrt{-\frac{A+2}{B}} : \bar{V}_3 : \bar{S}_3 : \bar{W}_3/\sqrt{-\frac{A+2}{B}}\right)$.

We can even consider Montgomery curves with small $\frac{A-2}{A+2}$ to reduce the computational cost of the addition law to 8**M**.

Example 1. Let $p = 2^{255} - 19$,

$$\begin{aligned} A = {} & 228773935936828030342021151168887095595 \\ & 48329372953616433827097594226971366740 7, \end{aligned}$$

and $B = 1$. Having small $\frac{A-2}{A+2} = 13763$ allows us to consider the addition law (44) with the computational cost of 8**M** for the Montgomery curve $\mathbf{E}_{M,A,B}$. This curve has the order 16ℓ, for the prime

$$\begin{aligned} \ell = {} & 3618502788666131106986593281521497120 4 \\ & 0970104703127466559953260900896225571 7, \end{aligned}$$

Also, The twisted of this curve has the order $4\ell'$, for the prime

$$\begin{aligned} \ell' = {} & 14474011154664524427946373126085988 48 \\ & 167869197828504234746626556594243338710 7, \end{aligned}$$

Similarly, we can derive the addition laws corresponding to (26), (27), and (28) with computational costs of 8**M**, 9**M**+1**D**, and 9**M**+1**D**, respectively. For example, the following addition law corresponds to (27) and is therefore complete if $\chi\left(\frac{A+2}{B}\right) = \chi(A^2-4) = -1$. Satisfying $\chi(-\frac{A+2}{B}) = 1$ implies $\chi(-1) = -1$, or equivalently $q \equiv 3 \pmod 4$.

$$\begin{aligned}
&\bar{X}_1 = \bar{U}_1 + \bar{W}_1, \quad \bar{Y}_1 = \bar{V}_1 - \bar{S}_1, \quad \bar{T}_1 = \bar{U}_1 - \bar{W}_1, \quad \bar{Z}_1 = \bar{V}_1 + \bar{S}_1, \\
&\bar{X}_2 = \bar{U}_2 + \bar{W}_2, \quad \bar{Y}_2 = \bar{V}_2 - \bar{S}_2, \quad \bar{T}_2 = \bar{U}_2 - \bar{W}_2, \quad \bar{Z}_2 = \bar{V}_2 + \bar{S}_2, \\
&A' \leftarrow \bar{X}_1\bar{X}_2, \quad B' \leftarrow \bar{Y}_1\bar{Y}_2, \quad C' \leftarrow \bar{Z}_1\bar{Z}_2, \quad D' \leftarrow \bar{T}_1\bar{T}_2, \\
&\bar{\mathcal{X}}' \leftarrow (\bar{T}_1 + \bar{Z}_1)(\bar{T}_2 + \bar{Z}_2) - C' - D', \ \bar{\mathcal{Y}} \leftarrow B' + A', \ \bar{\mathcal{Z}}' \leftarrow B' - A', \ \bar{\mathcal{T}} \leftarrow C' + \frac{A-2}{A+2}D', \\
&\bar{X}_3 \leftarrow \bar{\mathcal{X}}'\bar{\mathcal{T}}, \quad \bar{Y}_3 \leftarrow \bar{\mathcal{Y}}\bar{\mathcal{Z}}', \quad \bar{T}_3 \leftarrow \bar{\mathcal{X}}'\bar{\mathcal{Y}}, \quad \bar{Z}_3 \leftarrow \bar{\mathcal{Z}}'\bar{\mathcal{T}}, \\
&\bar{U}_3 \leftarrow \bar{X}_3 + \bar{T}_3, \quad \bar{Y}_3 \leftarrow \bar{Z}_3 + \bar{Y}_3, \quad \bar{S}_3 \leftarrow \bar{Z}_3 - \bar{Y}_3, \quad \bar{W}_3 \leftarrow \bar{X}_3 - \bar{T}_3.
\end{aligned} \tag{45}$$

Analogous to the complete addition laws (44) and (45) for the case $\chi\left(-\frac{A+2}{B}\right) = 1$, we can formulate complete addition laws for $\mathcal{E}_{M,A,B}$ under the condition $\chi\left(-\frac{A-2}{B}\right) = 1$ with the same cost.

It is worth mentioning that if $\chi(-a) = 1$ or $\chi(-d) = 1$, $\mathcal{E}_{TE,a,d}$ has incomplete addition laws with computational costs of 8**M**. Similarly, if $\chi(-\frac{A+2}{B}) = 1$ or $\chi(-\frac{A-2}{B}) = 1$, $\mathcal{E}_{M,A,B}$ has incomplete addition laws with computational costs of 8**M**.

Remark 4. Similar to [HWCD08], we can use $\mathbb{F}_q$-isomorphic curves instead of these coordinates to compute $P_1 + P_2$. Specifically, if $\chi\left(-\frac{A+2}{B}\right) = 1$, the Montgomery curve $\mathcal{E}_{M,A,B}$ is $\mathbb{F}_q$-isomorphic to the Montgomery curve $\mathcal{E}_{M,A,-(A+2)}$ via the map $(U,V,S,W) \to \left(\sqrt{-\frac{A+2}{B}}U, V, S, \sqrt{-\frac{A+2}{B}}W\right)$. Furthermore, $\mathcal{E}_{M,A,-(A+2)}$ is $\mathbb{F}_q$-isomorphic to the twisted Edwards curve $\mathcal{E}_{TE,-1,-\frac{A-2}{A+2}}$. Consequently, the computational costs of the addition laws for $\mathcal{E}_{M,A,B}$ match those for $\mathcal{E}_{TE,-1,-\frac{A-2}{A+2}}$. Additionally, if $\chi\left(-\frac{A-2}{B}\right) = 1$, then $\mathcal{E}_{M,A,B}$ is $\mathbb{F}_q$-isomorphic to $\mathcal{E}_{M,A,-(A-2)}$ via the map $(U,V,S,W) \to \left(\sqrt{-\frac{A-2}{B}}U, V, S, \sqrt{-\frac{A-2}{B}}W\right)$, and $\mathcal{E}_{M,A,-(A-2)}$ is $\mathbb{F}_q$-isomorphic to $\mathcal{E}_{TE,-\frac{A+2}{A-2},-1}$. Therefore, the computational costs of the addition laws for $\mathcal{E}_{M,A,B}$ are equivalent to those for $\mathcal{E}_{TE,-\frac{A+2}{A-2},-1}$.

Table 4 in Appendix A presents some well-known Montgomery curves, along with the conditions ensuring they have complete addition laws with computational costs of 8**M** + 1**D** and 9**M** + 1**D**.

Table 3: Cost of complete addition laws for families of elliptic curves

Curve	Addition	Mixed Addition	Condition for completeness
Edwards (Ed.) [BL07a]	$10\mathbf{M}+1\mathbf{S}+1\mathbf{D}$	$9\mathbf{M}+1\mathbf{S}+1\mathbf{D}$	$\chi(d)=-1$
Twisted Ed. [BBJ+08]	$10\mathbf{M}+1\mathbf{S}+2\mathbf{D}$	$9\mathbf{M}+1\mathbf{S}+2\mathbf{D}$	$\chi(a)=1,\ \chi(d)=-1$
Extended Twisted Ed. [HWCD08]	$9\mathbf{M}+2\mathbf{D}$	$8\mathbf{M}+2\mathbf{D}$	$\chi(a)=1,\ \chi(d)=-1$
Extended Twisted Ed. [HWCD08]	$8\mathbf{M}+1\mathbf{D}$	$7\mathbf{M}+1\mathbf{D}$	$q\equiv 1 \pmod 4,\ a=-1,\ \chi(d)=-1$
Extended Twisted Ed. [FH17]	$9\mathbf{M}+2\mathbf{D}$	$8\mathbf{M}+2\mathbf{D}$	$\chi(a)=-1,\ \chi(d)=1$
Jacobi quartic [HWCD09]	$10\mathbf{M}+3\mathbf{S}+3\mathbf{D}$	$8\mathbf{M}+3\mathbf{S}+3\mathbf{D}$	$\chi(d)=-1$
Hessian [FJ10]	$12\mathbf{M}+1\mathbf{D}$	$10\mathbf{M}+1\mathbf{D}$	c is not a cubic element
Short Weierstrass [RCB16]	$12\mathbf{M}+5\mathbf{D}$	$11\mathbf{M}+5\mathbf{D}$	The curve has no $\mathbb{F}_q$-rational point of order 2
Montgomery with $B=1$ [KPKK19]	$14\mathbf{M}+2\mathbf{D}$	$11\mathbf{M}+2\mathbf{D}$	$X^3+AX^2+X-s^2\in\mathbb{F}_q[X]$ is irreducible
Montgomery [This work (44)]	$8\mathbf{M}+1\mathbf{D}$	$7\mathbf{M}+1\mathbf{D}$	$q\equiv 1 \pmod 4,\ \chi(\frac{A+2}{B})=1,\ \chi(\frac{A-2}{B})=-1$
Montgomery [This work (Analogous to (44))]	$8\mathbf{M}+1\mathbf{D}$	$7\mathbf{M}+1\mathbf{D}$	$q\equiv 1 \pmod 4,\ \chi(\frac{A+2}{B})=-1,\ \chi(\frac{A-2}{B})=1$
Montgomery [This work (45)]	$9\mathbf{M}+1\mathbf{D}$	$8\mathbf{M}+1\mathbf{D}$	$q\equiv 3 \pmod 4,\ \chi(\frac{A+2}{B})=-1,\ \chi(\frac{A-2}{B})=1$
Montgomery [This work (Analogous to (45))]	$9\mathbf{M}+1\mathbf{D}$	$8\mathbf{M}+1\mathbf{D}$	$q\equiv 3 \pmod 4,\ \chi(\frac{A+2}{B})=1,\ \chi(\frac{A-2}{B})=-1$

6 Concluding Remarks

In this study, we introduced extended Montgomery coordinates $\mathcal{E}_{M,A,B}$, as a novel representation for points on Montgomery curves. These coordinate system enabled us to define birational multiplication-free maps between the extended twisted Edwards coordinates $\mathcal{E}_{TE,a,d}$ and $\mathcal{E}_{M,A,B}$. These maps have no exceptional points; thus, by employing them, we transferred the complete addition laws from $\mathcal{E}_{TE,a,d}$ to $\mathcal{E}_{M,A,B}$ with the same computational costs (up to 12 additions). Furthermore, by applying the scaling technique on the addition laws for $\mathcal{E}_{TE,a,d}$ we noticed that if $q \equiv 1 \pmod 4$ then $\mathcal{E}_{TE,a,d}$ has complete addition laws with costs $8\mathbf{M}+1\mathbf{D}$ if $\chi(ad)=\chi(d)=-1$ or $\chi(ad)=\chi(a)=-1$. Conversely, if $q\equiv 3 \pmod 4$, $\mathcal{E}_{TE,a,d}$ has complete addition laws with costs $9\mathbf{M}+1\mathbf{D}$ under the same conditions. Moreover, for $\chi(-a)=1$ or $\chi(-d)=1$, $\mathcal{E}_{TE,a,d}$ has incomplete addition laws with costs of $8\mathbf{M}$. Leveraging our birational multiplication-free maps between $\mathcal{E}_{TE,a,d}$ and $\mathcal{E}_{M,A,B}$ and using these results, we conclude that if $q\equiv 1 \pmod 4$ then $\mathcal{E}_{M,A,B}$ has complete addition laws with costs $8\mathbf{M}+1\mathbf{D}$ if $\chi(\frac{A-2}{B})=\chi(A^2-4)=-1$ or $\chi(\frac{A+2}{B})=\chi(A^2-4)=-1$. Also, if $q\equiv 3 \pmod 4$, $\mathcal{E}_{M,A,B}$ has complete addition laws with cost $9\mathbf{M}+1\mathbf{D}$ under the same conditions.

Table 3 compares our complete addition laws with the known complete addition laws for other families of elliptic curves. Our complete addition laws for Montgomery curves significantly improve efficiency, reducing the computational cost by $6\mathbf{M}+1\mathbf{D}$ compared to that reported in [KPKK19]. Additionally, having the same computational costs compared to the complete addition laws for twisted Edwards curves makes Montgomery curves a more attractive choice for applications.

In future work, we will apply the same technique to explore the relationships between other families of elliptic curves, such as Jacobi intersection and Huff, with twisted Edwards curves to introduce complete addition laws for these curves with the same computational cost as those for twisted Edwards curves.

Acknowledgments

The authors would like to thank anonymous reviewers for their useful comments. This research was in part supported by a grant from IPM (No. 1403110419).

References

[ABGR13] Diego F. Aranha, Paulo S. L. M. Barreto, C. C. F. Pereira Geovandro, and Jefferson E. Ricardini. A note on high-security general-purpose elliptic curves. *IACR Cryptol. ePrint Arch.*, page 647, 2013.

[BBJ+08] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In Serge Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer, 2008.

[BCLN16] Joppe W. Bos, Craig Costello, Patrick Longa, and Michael Naehrig. Selecting elliptic curves for cryptography: an efficiency and security analysis. *J. Cryptogr. Eng.*, 6(4):259–286, 2016.

[Ber06] Daniel J. Bernstein. Curve25519: New diffie-hellman speed records. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings*, volume 3958 of *Lecture Notes in Computer Science*, pages 207–228. Springer, 2006.

[BF03] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3):586–615, 2003.

[BHH+14] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow. Elliptic curve cryptography in practice. In Nicolas Christin and Reihaneh Safavi-Naini, editors, *Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, volume 8437 of *Lecture Notes in Computer Science*, pages 157–175. Springer, 2014.

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. Csi-fish: Efficient isogeny based signatures through class group computations. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 227–247. Springer, 2019.

[BL95] Wieb Bosma and Hendrik W. Lenstra. Complete systems of two addition laws for elliptic curves. *Journal of Number Theory*, 53(2):229–240, 1995.

[BL07a] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In Kaoru Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer, 2007.

[BL07b] Daniel J. Bernstein and Tanja Lange. Inverted edwards coordinates. In Serdar Boztas and Hsiao-feng Lu, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium, AAECC-17, Bangalore, India, December 16-20, 2007, Proceedings*, volume 4851 of *Lecture Notes in Computer Science*, pages 20–27. Springer, 2007.

[BL09] Daniel J. Bernstein and Tanja Lange. A complete set of addition laws for incomplete edwards curves. *IACR Cryptol. ePrint Arch.*, page 580, 2009.

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. *J. Cryptol.*, 17(4):297–319, 2004.

[CFA$^+$05] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Chapman and Hall/CRC, 2005.

[CLM$^+$18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[Cou06] Jean Marc Couveignes. Hard homogeneous spaces. *IACR Cryptol. ePrint Arch.*, page 291, 2006.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976.

[Edw07] Harold M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007.

[FH17] Reza Rezaeian Farashahi and Seyed Gholamhossein Hosseini. Differential addition on twisted edwards curves. In Josef Pieprzyk and Suriadi Suriadi, editors, *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*, volume 10343 of *Lecture Notes in Computer Science*, pages 366–378. Springer, 2017.

[FJ10] Reza Rezaeian Farashahi and Marc Joye. Efficient arithmetic on hessian curves. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*, volume 6056 of *Lecture Notes in Computer Science*, pages 243–260. Springer, 2010.

[FJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.

[FKL$^+$20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. Sqisign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 64–93. Springer, 2020.

[FMW12] Reza Rezaeian Farashahi, Dustin Moody, and Hongfeng Wu. Isomorphism classes of edwards curves over finite fields. *Finite Fields Their Appl.*, 18(3):597–612, 2012.

[FS10] Reza Rezaeian Farashahi and Igor E. Shparlinski. On the number of distinct elliptic curves in some families. *Des. Codes Cryptogr.*, 54(1):83–99, 2010.

[fSN23] National Institute for Standards and Technology (NIST). *Digital Signature Standard (DSS).* Federal Information Processing Standard Publication 186-5, 2023.

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

[Gam85] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory*, 31(4):469–472, 1985.

[Ham15] Mike Hamburg. Ed448-goldilocks, a new elliptic curve. *IACR Cryptol. ePrint Arch.*, page 625, 2015.

[HWCD08] Hüseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted edwards curves revisited. In Josef Pieprzyk, editor, *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, volume 5350 of *Lecture Notes in Computer Science*, pages 326–343. Springer, 2008.

[HWCD09] Hüseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Jacobi quartic curves revisited. In Colin Boyd and Juan Manuel González Nieto, editors, *Information Security and Privacy, 14th Australasian Conference, ACISP 2009, Brisbane, Australia, July 1-3, 2009, Proceedings*, volume 5594 of *Lecture Notes in Computer Science*, pages 452–468. Springer, 2009.

[Jou04] Antoine Joux. A one round protocol for tripartite diffie-hellman. *J. Cryptol.*, 17(4):263–276, 2004.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.

[KPKK19] Jae Heon Kim, Je Hong Park, Dong-Chan Kim, and Woo-Hwan Kim. Complete addition law for montgomery curves. In Jae Hong Seo, editor, *Information Security and Cryptology - ICISC 2019 - 22nd International Conference, Seoul, South Korea, December 4-6, 2019, Revised Selected Papers*, volume 11975 of *Lecture Notes in Computer Science*, pages 260–277. Springer, 2019.

[Len87] Hendrik W. Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.

[LR87] Herbert Lange and Wolfgang A. F. Ruppert. Addition laws on elliptic curves in arbitrary characteristics. *Journal of Algebra*, 107:106–116, 1987.

[LY22] Luying Li and Wei Yu. A note on inverted twisted edwards curve. In Yi Deng and Moti Yung, editors, *Information Security and Cryptology - 18th International Conference, Inscrypt 2022, Beijing, China, December 11-13, 2022, Revised Selected Papers*, volume 13837 of *Lecture Notes in Computer Science*, pages 295–304. Springer, 2022.

[Mil85] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985.

[Mon87] Peter L. Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48:243–264, 1987.

[RCB16] Joost Renes, Craig Costello, and Lejla Batina. Complete addition formulas for prime order elliptic curves. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 403–428. Springer, 2016.

[RS06] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptol. ePrint Arch.*, page 145, 2006.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate texts in mathematics*. Springer, 1986.

Appendix. The table below lists well-known Montgomery curves and the conditions under which they achieve complete addition laws with computational costs of $8\mathbf{M}+1\mathbf{D}$ and $9\mathbf{M}+1\mathbf{D}$.

Table 4: Montgomery curves ($B = 1$)

Curve	A	p	Reference	Completeness condition	Cost
Curve25519	$486,662$	$2^{255}-19$	[Ber06]	$p \equiv 1 \pmod 4$ $\chi(A+2)=1$ $\chi(A-2)=-1$	$8\mathbf{M}+1\mathbf{D}$ [This work (44)]
Curve383187	$229,969$	$2^{383}-187$	[ABGR13]		
M-221	$117,050$	$2^{221}-3$	[ABGR13]		
M-383	$2,065,150$	$2^{383}-187$	[ABGR13]		
M-511	$530,438$	$2^{511}-187$	[ABGR13]		
Curve448	$156,326$	$2^{448}-2^{224}-1$	[Ham15]	$p \equiv 3 \pmod 4$ $\chi(A+2)=-1$ $\chi(A-2)=1$	$9\mathbf{M}+1\mathbf{D}$ [This work (45)]
ed-256-mont	$-54,314$	$2^{240}(2^{16}-88)-1$	[BCLN16]		
ed-254-mont	$-55,790$	$2^{240}(2^{14}-127)-1$	[BCLN16]		
ed-256-mers	$-61,370$	$2^{256}-189$	[BCLN16]		
ed-255-mers	$-240,222$	$2^{255}-765$	[BCLN16]		
ed-384-mont	$-113,758$	$2^{376}(2^{8}-79)-1$	[BCLN16]		
ed-382-mont	$-2,870,790$	$2^{368}(2^{14}-5)-1$	[BCLN16]		
ed-384-mers	$-1,332,778$	$2^{384}-317$	[BCLN16]		
ed-383-mers	$-2,095,962$	$2^{383}-421$	[BCLN16]		
ed-512-mont	$-305,778$	$2^{496}(2^{16}-491)-1$	[BCLN16]		
ed-510-mont	$-2,320,506$	$2^{496}(2^{14}-290)-1$	[BCLN16]		
ed-512-mers	$-2,550,434$	$2^{512}-569$	[BCLN16]		
ed-512-mers	$-4,390,390$	$2^{511}-481$	[BCLN16]		