Efficient Pairing Computations via Biextensions on Montgomery Curves

Jianming Lin[1,2], Kaizhan Lin[3], Damien Robert[4], Chang-An Zhao[1,5], and Yuhao Zheng[1]

[1] School of Mathematics, Sun Yat-sen University,
Guangzhou, 510275, China.
linjm76@mail.sysu.edu.cn
zhaochan3@mail.sysu.edu.cn
zhengyh57@mail2.sysu.edu.cn

[2] School of Mathematics, Jiaying University,
Meizhou, 514015, China.

[3] College of Computer Science and Artificial Intelligence,
Shanghai, 200438, China.
linkzh@fudan.edu.cn

[4] Inria Bordeaux, Institut de Math´ematiques de Bordeaux, France.
damien.robert@inria.fr

[5] Guangdong Key Laboratory of Information Security,
Guangzhou 510006, P.R. China.

Abstract. Pairing is a fundamental tool in public key cryptography and has been studied for several decades. It plays a crucial role in various cryptographic applications, including identity-based encryption (IBE), Joux's one round protocol for tripartite Diffie–Hellman, and zero-knowledge proofs. Recently, Damien Robert proposed novel cubical arithmetic to compute pairings via biextensions, which significantly improves pairing computation efficiency in isogeny-based schemes such as SQIsign and CSIDH. However, when applied to classical pairing-based cryptography, the biextension technique has not yet achieved satisfactory performance. Especially, the biextension technique outperforms Miller's algorithm only for specific families with the lack of twists.

This paper aims to enhance the practicality of the biextension technique combined with cubical arithmetic. Since Montgomery curves allow for efficient cubical arithmetic, we establish the connections between the pairing-friendly curves in the literature and Montgomery model. For curves with the lack of twists, we propose an effective approach to determine whether they can be translated to Montgomery forms. As for the curves admitting degree-d twists, it is suffices to require their twists to be converted to Montgomery model. To this end, we also provide new decision theorems for this circumstance.

Building on these theoretical results, we can identify which pairing-friendly curves—or their twists—from the literature admit such a conversion. By selecting suitable parameters, we optimize pairing computations on these curves using cubical arithmetic on the Montgomery model. The cost analysis demonstrates that the biextension technique integrated with Montgomery model outperforms Miller's algorithm by bit on curves admitting degree-d twists ($d \leq 3$). Specifically, our optimized method approximately reduces 50.3%, 45.3%, 10.9%, 6.3% and 6.4% multiplications over finite fields $\mathbb{F}_p$ in terms of Miller loops on pairing-friendly curves CP5-663, CP7-512, BW14-382, BLS15-383 and BLS21-511, respectively.

Keywords: Pairing · Montgomery curves · Biextension · Cubical arithmetic

1 Introduction

Bilinear pairings play a significant role in pulic key cryptography, enabling applications such as identity-based encryption (IBE) [5], one-round tripartite Diffie–Hellman key agreement [27], and zero-knowledge proofs [17,18]. Currently, the predominant and most efficient method for computing pairings in pairing-based cryptography is Miller's algorithm [30]. Alternative approaches have also been explored, such as the elliptic net algorithm (ENA) [35] and its variants [10,7]. However, ENA and its variants have seen limited adoption in practice due to their comparatively lower computational efficiency.

Biextensions as an algorithmic tool to compute the Weil and Tate pairings was first investigated by Stange in her PhD thesis [35], where she proved that elliptic nets compute the Poincaré biextension cocycle. In 2024, the third author [33] pioneered the use of cubical arithmetic to improve the biextension arithmetic compared to elliptic nets. The core idea involves utilizing level 2 cubical arithmetic, which employs fast cubical x-only operations on Montgomery curves. These improvements benefit pairing computations in isogeny-based schemes [32], including the compact digital signature scheme SQIsign [16] and the non-interactive key exchange protocol CSIDH [9]. The biextension technique has also been extended to the ate pairing, optimal ate pairing, and super-optimal pairing [29]. However, its performance in general settings remains unsatisfactory. As shown in [29, Table 4], the biextension technique outperforms Miller's algorithm only for specific curves that lack twists. The main bottleneck is that most pairing-friendly curves in the literature are defined in short Weierstrass form, which admits inefficient cubical arithmetic. Specifically, the cubical ladder algorithm requires only 15 field multiplications per bit on Montgomery models [33], compared to 29 on short Weierstrass curves [33, Section 5.4].

Motivated by this gap, we aim to broaden the applicability of the biextension approach in pairing-based cryptography by leveraging the Montgomery model. Although several works [31,12] have investigated the conversion between short Weierstrass and Montgomery forms, there remains a lack of research that systematically establishes the relationships between pairing-friendly curves in the literature and Montgomery models to make them more compatible with the biextension method. Comprehensively determining which pairing-friendly curves admit such a transformation is non-trivial. Directly applying the results from [31,12] is not effective, as they are general and not tailored to the specific properties of most pairing-friendly curves. This paper proposes more compact and effective theorems for determining whether a pairing-friendly curve can be converted to a Montgomery model. Specifically, for curves E that lack twists, we ensure that they can be transformed into Montgomery form over the ground field $\mathbb{F}_p$ to maximize the efficiency of the biextension approach. To this end, we propose a new approach (see Theorem 4 in Section 3) for effective determination that relies only on the trace t of the p-power Frobenius endomorphism π, avoiding the need to find rational 2-torsion points or compute quadratic residue symbols, unlike the propositions in [12]. For curves admitting degree-d twists E', the cubical arithmetic can be carried out entirely on E' defined over the finite field $\mathbb{F}_{p^{k/d}}$ by leveraging morphism properties of bilinear pairings to accelerate the biextension approach, where k denotes the embedding degree. Hence, it suffices to require that E' is $\mathbb{F}_{p^{k/d}}$-isomorphic to the Montgomery model, making it more suitable for the biextension technique. Based on the former case, we also derive corresponding effective decision approaches by utilizing the algebraic properties of twists, which are summarized in Lemma 1 and Theorem 5.

1.1 Contributions

This paper explores how to adapt the biextension technique proposed in [33] to exploit the Montgomery model for pairing computations on a wider range of pairing-friendly curves. The main contributions are as follows:

1. We investigate the intrinsic connections between Weierstrass and Montgomery curves, establishing necessary and sufficient conditions for converting an ordinary short Weierstrass curve E over a finite field $\mathbb{F}_q$ of characteristic p into a Montgomery curve $E_{A,B}$ when E has CM-discriminant 1 or 3. In particular, for curves that do not admit twists, we ensure that they are $\mathbb{F}_p$-isomorphic to Montgomery curves. For curves admitting degree-d twists E', it suffices to require that E' is $\mathbb{F}_{p^{k/d}}$-isomorphic to the Montgomery model. We also generalize the aforementioned conditions and propose effective decision theorems for the latter situation.
2. We revisit pairing-friendly curves in the literature and apply our proposed theorems to identify those that can be transformed into Montgomery models. To the best of our knowledge, this is the first systematic work to investigate the relationships between pairing-friendly curves and Montgomery curves. For curves that can be converted to Montgomery form, we present explicit formulas derived via level 2 biextensions to compute pairings efficiently. Furthermore, we provide concrete parameters for selected curves admitting such transformations at the 128- or 192-bit security level.
3. We employ efficient cubical arithmetic on Montgomery curves and provide a concrete cost analysis. The results demonstrate that:
   - For curves admitting degree-d twists ($d \leq 3$), the biextension technique implemented on the Montgomery model outperforms Miller's algorithm in doubling iterations, especially for curves that lack twists. This shows that our method significantly enhances the competitiveness of the biextension technique in pairing-based cryptography.

- For Miller loops on the exTNFS-resistant Cocks-Pinch curves CP5-663 and CP7-512 with small target finite fields [25], our approach reduces the number of $\mathbb{F}_p$-multiplications by 50.3% and 45.3%, respectively, compared to Miller's algorithm.
- For the curve BW14-382, which admits a quadratic twist [13], we propose a mixed and shared ladder to accelerate the super-optimal pairing via biextension, achieving an approximate 10.9% reduction in $\mathbb{F}_p$-multiplications within the Miller loop.
- For the curves BLS15-383 and BLS21-511, which admit cubic twists [1,24], we save approximately 6.3% and 6.4% of $\mathbb{F}_p$-multiplications in the Miller loops, respectively.

1.2 Organization of This Paper

The mathematical preliminaries and definitions are presented in Section 2, which recalls the concepts of Montgomery curves and biextensions. Section 3 presents the main theorems and lemmas for the conversion between short Weierstrass and Montgomery forms. The pairing-friendly curves and the corresponding formulas via biextensions compatible with our optimized approach are provided in Section 4. We illustrate the cost analysis and comparison in Section 5. Finally, our conclusions and future work are discussed in Section 6.

2 Preliminaries

This section introduces the mathematical preliminaries required for this paper, including twists of elliptic curves, Montgomery curves, and biextensions.

Let E be a short Weierstrass curve defined over a finite field $\mathbb{F}_q$ of characteristic p, with equation:

$$E/\mathbb{F}_q : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{F}_q$. Let $\mathcal{O}_E$ denote the point at infinity. The order of the additive abelian group $E(\mathbb{F}_q)$ is given by $\#E(\mathbb{F}_q) = q + 1 - t$ [36, Theorem 4.12], where t is the trace of the q-power Frobenius endomorphism $\pi : (x, y) \mapsto (x^q, y^q)$.

The curve E is called supersingular if $t \equiv 0 \bmod p$, and ordinary otherwise. Let r be a prime divisor of $\#E(\mathbb{F}_q)$. The embedding degree k of E with respect to r is the smallest positive integer such that $r \mid q^k - 1$. The n-torsion subgroup is defined as:

$$E[n] = \{P \in E \mid [n]P = \mathcal{O}_E\}.$$

For efficient pairing computation, the following two r-torsion groups are typically used as inputs:

$$\begin{aligned}\mathbb{G}_1 &= E(\mathbb{F}_q)[r] = E[r] \cap \{P \in E \mid \pi(P) = P\},\\ \mathbb{G}_2 &= E[r] \cap \{P \in E \mid \pi(P) = [q]P\}.\end{aligned}$$

The j-invariant of E is defined as $j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2}$. Additionally, the curves with $j(E) = 0$ (resp. $j(E) = 1728$) possess efficiently computable automorphisms σ, described as follows:

$$\begin{array}{llll} E : y^2 = x^3 + b, & \text{with } j(E) = 0 & \text{and} & \sigma : (x, y) \mapsto (wx, y), \\ E : y^2 = x^3 + ax, & \text{with } j(E) = 1728 & \text{and} & \sigma : (x, y) \mapsto (-x, iy), \end{array}$$

where w and i are primitive cubic and quartic roots of unity in $\mathbb{F}_q^*$, respectively.

2.1 Twists of Elliptic Curves

Let E and E' be elliptic curves over a finite field $\mathbb{F}_q$ of characteristic p. Then E' is a degree-d twist ($d > 1$) of E if there exists an isomorphism ϕ between E and E' defined over $\mathbb{F}_{q^d}$, with d minimal. The map ϕ is called the degree-d twisting isomorphism.

The following proposition characterizes all possible twists. We refer to appendix B for a much more detailed overview.

Proposition 1. *[26, Proposition 1] Let $p \geq 5$ be a prime. The set of twists of E is canonically isomorphic to $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$, where $d = 2$ if $j(E) \neq 0, 1728$; $d = 4$ if $j(E) = 1728$; and $d = 3, 6$ if $j(E) = 0$. Specifically, twists corresponding to $\zeta \in \mathbb{F}_{q^e}^*/(\mathbb{F}_{q^e}^*)^d$ are given by:*

$$\begin{array}{lll} d = 2 : & y^2 = x^3 + a/\zeta^2 x + b/\zeta^3, & \phi : E' \to E : (x, y) \mapsto (\zeta x, \zeta^{3/2} y), \\ d = 4 : & y^2 = x^3 + a/\zeta x, & \phi : E' \to E : (x, y) \mapsto (\zeta^{1/2} x, \zeta^{3/4} y), \\ d = 3, 6 : & y^2 = x^3 + b/\zeta, & \phi : E' \to E : (x, y) \mapsto (\zeta^{1/3} x, \zeta^{1/2} y). \end{array}$$

Quadratic twists can also be represented as:

$$d = 2 : \zeta y^2 = x^3 + ax + b, \quad \phi : E' \to E : (x, y) \mapsto (x, \zeta^{1/2} y).$$

For ordinary curves, the group order of $E'(\mathbb{F}_q)$ can be determined as follows.

Proposition 2. *[26, Proposition 2] Let E be an ordinary curve over $\mathbb{F}_q$ admitting a degree-d twist E', with $\#E(\mathbb{F}_q) = q + 1 - t$. Then the orders of $E'(\mathbb{F}_q)$ are:*

$$\begin{array}{ll} d = 2 : \#E'(\mathbb{F}_q) = q + 1 + t, & \\ d = 3 : \#E'(\mathbb{F}_q) = q + 1 - (\pm 3f - t)/2 & \textit{with } t^2 - 4q = -3f^2, \\ d = 4 : \#E'(\mathbb{F}_q) = q + 1 \pm f & \textit{with } t^2 - 4q = -f^2, \\ d = 6 : \#E'(\mathbb{F}_q) = q + 1 - (\pm 3f + t)/2 & \textit{with } t^2 - 4q = -3f^2. \end{array}$$

In pairing-based cryptography, we often consider a curve E over $\mathbb{F}_p$ with small embedding degree k, admitting a degree-d twist E' over $\mathbb{F}_{p^{k/d}}$. In this case, $d = \gcd(\#\mathrm{Aut}(E), k)$, and the pairing subgroup $\mathbb{G}_2$ can be efficiently represented as $\mathbb{G}_2 = E'(\mathbb{F}_{p^{k/d}})[r]$.

2.2 Montgomery Curves

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

$$E_{A,B}/\mathbb{F}_q : By^2 = x^3 + Ax^2 + x,$$

where $A, B \in \mathbb{F}_q$ satisfy $B \neq 0$ and $A^2 - 4 \neq 0$.

A Montgomery curve $E_{A,B}$ can be transformed into short Weierstrass form. The converse transformation is possible under the following conditions.

Proposition 3. *[31, Proposition 1] A short Weierstrass curve $E : y^2 = x^3 + ax + b$ can be transformed into a Montgomery curve $E_{A,B} : By^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_q$ if and only if:*

1. *E has an $\mathbb{F}_q$-rational 2-torsion point $(\alpha, 0)$, and*
2. *$\left(\frac{3\alpha^2+a}{q}\right)_2 = 1$,*

where $\left(\frac{\cdot}{\cdot}\right)_2$ denotes the quadratic residue symbol modulo q.

The isomorphism between these curves is defined by:

$$\begin{aligned} \psi : E &\to E_{A,B}, \\ (x, y) &\mapsto \left(\frac{x-\alpha}{\beta}, \frac{y}{\beta}\right), \end{aligned}$$

where $A = 3\alpha/\beta$, $B = 1/\beta$, and β is a square root of $3\alpha^2 + a$ over $\mathbb{F}_q$.

In appendix B we investigate when an elliptic curve has a twist that can be put in a Montgomery form.

2.3 Biextensions and Bilinear Pairings

Biextensions [33] provide a framework for computing bilinear pairings on abelian varieties. This subsection introduces biextensions and their connection to pairings; see [29,32] for further details.

Let $D = (\mathcal{O}_E)$ be the polar divisor on an elliptic curve E. The biextension X_D associated with D is defined as follows.

Definition 1 ([33]). *Let D_P denote the divisor $(-P) - (\mathcal{O}_E)$. A biextension element is a tuple $(P, Q, g_{P,Q}) \in X_D$, where $P, Q \in E$ and $g_{P,Q}$ is a rational function with divisor:*

$$div(g_{P,Q}) = (-P - Q) + (\mathcal{O}_E) - (-P) - (-Q).$$

From this definition, we can derive the connection between $g_{P,Q}$ and the Miller function $f_{r,P}$ [30], which satisfies $\mathrm{div}(f_{r,P}) = r(P) - ([r]P) - (r-1)(\mathcal{O}_E)$:

$$f_{r,-P}((\cdot) - (\cdot + Q)) = \frac{g_{[r]P,Q}(\cdot)}{g_{P,Q}(\cdot)^r}. \tag{1}$$

It is preferable to work at level 2 for efficiency. Let X and Z be two sections of $2D = 2(\mathcal{O}_E)$ such that $x = X/Z$. A level 2 cubical point $\widetilde{P}$ is given by $\widetilde{P} = (X(\widetilde{P}), Z(\widetilde{P}))$. For simplicity, we drop the tilde and denote $P = (X_P, Z_P)$. Note that the sections X, Z at level 2 correspond to the projective coordinates of the Kummer line $E/\langle \pm 1 \rangle$.

When $R = \mathcal{O}_E$, an extended value is required to evaluate $g_{P,Q}$ at R [33, Remark 2.8]. The level 2 biextension function evaluated at $\mathcal{O}_E$ [29, Equation (11)] is given by

$$g_{2D,P,Q}(\mathcal{O}_E) = g_{P,Q}(\mathcal{O}_E)^2 = \frac{Z_{P+Q} \cdot X_{\mathcal{O}_E}}{Z_P \cdot Z_Q}.$$

If P is an r-torsion point, then Z evaluated at $[r]P$ yields $X_{[r]P}$. Thus

$$g_{2D,[r]P,Q}() = g_{[r]P,Q}(\mathcal{O}_E)^2 = \frac{Z_{[r]P+Q} \cdot X_{\mathcal{O}_E}}{X_{[r]P} \cdot Z_Q}. \tag{2}$$

In the following, we use $g_{P,Q}$ to represent the level 2 biextension element. Based on Equations (1) and (2), the formula for the Tate pairing via cubical arithmetic [32, Appendix A.10, Theorem 5] can be derived. If $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_q)$, then the square of the non-reduced Tate pairing is

$$e_r(P,Q)^2 = \frac{Z_{[r]P+Q} \cdot X_{\mathcal{O}_E}}{Z_Q \cdot X_{[r]P}}.$$

Pairing-based cryptography often uses $\mathbb{G}_2 \times \mathbb{G}_1$ as input subgroups, leading to variants of the Tate pairing with shorter Miller loops, such as ate pairings, optimal ate pairings, and super-optimal ate pairings. These can also be computed via biextensions [29, Section 3], as cubical arithmetic behaves well with isomorphisms on elliptic curves. Explicit formulas for these pairings via biextensions are summarized in [29, Table 1].

The coordinates $Z_{[n]Q+P}$ and $Z_{[n]Q}$ (for $n \in \mathbb{Z}$) can be computed using cubical or double-and-add ladder algorithms. Cubical arithmetic for pairing-friendly curves with j-invariants 0 or 1728, and for supersingular Montgomery curves with embedding degree 2, are detailed in [29, Section 4] and [32, Section 4], respectively.

3 Characterization of Weierstrass-Montgomery Curve Conversion

As mentioned in Section 1, Montgomery curves admit fast cubical arithmetic, which is highly compatible with pairing computations via biextensions. Thus, we aim to transform existing pairing-friendly curves into Montgomery form, and try to broaden the applications of biextensions for pairing computations. In this section, we introduce the framework of our method and propose propositions to effectively determine whether short Weierstrass curves or their degree-d twists can be converted to Montgomery form.

Let E denote a pairing-friendly curve admitting short Weierstrass form over $\mathbb{F}_p$ with embedding degree k, where p is an odd prime. According to [14], pairing-friendly curves can be divided into two classes: curves admitting degree-d twists and curves without twists.

In general, the pairing computation on E is executed over the input subgroups $\mathbb{G}_2 \times \mathbb{G}_1$ (e.g., in the ate pairing, optimal pairing, and super-optimal ate pairing) to achieve a short Miller loop. For curves without twists, the subgroup $\mathbb{G}_2$ should be expressed by $\mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap \ker(\pi - [p])$ since no twists are available. For those that can be translated into Montgomery model, the pairing computations are performed as follows:

$$e(\psi(P), \psi(Q)) = e(P, Q)^{\deg(\psi)} = e(P, Q), \quad P \in \mathbb{G}_1, Q \in \mathbb{G}_2,$$

where ψ represents the isomorphism between E and $E_{A,B}$. To maximize the efficiency, we expect that E is $\mathbb{F}_p$-isomorphic to Montgomery model.

We provide an effective way to handle this circumstance. For ordinary short Weierstrass curves with CM-discriminant 1 or 3 over a finite field $\mathbb{F}_q$, Proposition 4 presents the condition under which these curves are $\mathbb{F}_q$-isomorphic to the Montgomery form.

Proposition 4. *Let $\mathbb{F}_q$ be a finite field with characteristic $p \geq 5$. Let E denote an ordinary short Weierstrass curve with CM−discriminant $D = 1$ or 3 over $\mathbb{F}_q$. Define t to be the trace of the q-power Frobenius endomorphism. Then E is $\mathbb{F}_q$-isomorphic to a Montgomery curve $E_{A,B}$ if and only if $t \equiv 2 \pmod 4$.*

Proof. We prove this proposition for the two cases $D = 1$ and $D = 3$.
(1) The short Weierstrass curve with CM-discriminant 1 has $j(E) = 1728$, and the curve is of the form

$$E/\mathbb{F}_q : y^2 = x^3 + ax.$$

Since E is ordinary, from the proof of [34, Chapter V.4, Theorem 4.1] we have $p \equiv 1 \pmod 4$, and thus -1 is a quadratic residue modulo p. It follows that

$$q \equiv p^m \equiv 1 \pmod 4, \qquad \left(\frac{-1}{q}\right)_2 = \left(\frac{-1}{p}\right)_2^m = 1,$$

where $\left(\frac{\cdot}{\cdot}\right)_2$ denotes the Legendre or Jacobi residue symbol.

We first prove the sufficiency. Obviously, $(0, 0) \in E[2]$. By Proposition 3, we need to show

$$\left(\frac{3 \cdot 0^2 + a}{q}\right)_2 = \left(\frac{a}{q}\right)_2 = \left(\frac{-1}{q}\right)_2 \cdot \left(\frac{-a}{q}\right)_2 = 1,$$

i.e., $-a$ is a quadratic residue modulo q. From $t \equiv 2 \pmod 4$, we obtain

$$\#E(\mathbb{F}_q) = q + 1 - t \equiv 0 \pmod 4.$$

Since $j(E) = 1728$, by [15, Corollary 1] we deduce that $E[2] \subseteq E(\mathbb{F}_q)$. Consequently, $E(\mathbb{F}_q)[2] = \{(0, 0), (\pm\alpha, 0), \mathcal{O}_E\}$ for some $\alpha \in \mathbb{F}_q$. This implies that

$-a$ is a square in $\mathbb{F}_q^*$. Therefore, the curve with $D = 1$ can be converted to the Montgomery form.

We now consider the necessity. Since E is $\mathbb{F}_q$-isomorphic to a Montgomery curve $E_{A,B}$, by [22, Lemma 9.12.9] we have

$$q + 1 - t \equiv 0 \pmod 4.$$

It follows from $q \equiv 1 \pmod 4$ that $t \equiv 2 \pmod 4$, which completes the proof of necessity.

(2) If E has CM-discriminant 3, then it satisfies the equation

$$E/\mathbb{F}_q : y^2 = x^3 + b,$$

and $j(E) = 0$. From the assumption that E is ordinary and [34, Chapter V.4, Theorem 4.1] we have $p \equiv 1 \pmod 3$, which implies that

$$q \equiv p^m \equiv 1 \pmod 3, \quad \left(\frac{q}{3}\right)_2 = \left(\frac{p}{3}\right)_2^m = 1.$$

We now prove the sufficiency. From $t \equiv 2 \pmod 4$, it follows that

$$q + 1 - t \equiv 0 \pmod 2.$$

Thus, there exists an $\mathbb{F}_q$-rational 2-torsion point $(\alpha, 0)$ on E. Note that

$$\left(\frac{3\alpha^2 + a}{q}\right)_2 = \left(\frac{3\alpha^2}{q}\right)_2 = \left(\frac{3}{q}\right)_2,$$

since $a = 0$ for this curve. By Proposition 3, it remains to prove that 3 is a quadratic residue modulo q. Since $q \equiv 1 \pmod 3$, there exists a primitive cube root of unity $\omega \in \mathbb{F}_q$ such that $\alpha\omega$ and $\alpha\omega^2$ are also roots of

$$x^3 + b \equiv 0 \pmod q,$$

i.e., $(\alpha\omega, 0), (\alpha\omega^2, 0) \in E(\mathbb{F}_q)$. This implies that $E[2] \subseteq E(\mathbb{F}_q)$, and hence

$$q + 1 - t \equiv 0 \pmod 4.$$

Given $t \equiv 2 \pmod 4$, we have $q \equiv 1 \pmod 4$. By the quadratic reciprocity law,

$$\left(\frac{3}{q}\right)_2 \cdot \left(\frac{q}{3}\right)_2 = (-1)^{\frac{q-1}{2}} = 1,$$

which implies that

$$\left(\frac{3}{q}\right)_2 = 1 = \left(\frac{q}{3}\right)_2.$$

Therefore, the curve E with $D = 3$ is $\mathbb{F}_q$-isomorphic to a Montgomery curve by Proposition 3.

The following proves the necessity. From Proposition 3, we deduce that

$$\left(\frac{3\alpha^2 + a}{q}\right)_2 = \left(\frac{3}{q}\right)_2 = 1,$$

where $(\alpha, 0)$ is a rational 2-torsion point in $E(\mathbb{F}_q)$. This implies that

$$\left(\frac{3}{q}\right)_2 \cdot \left(\frac{q}{3}\right)_2 = 1 = (-1)^{\frac{q-1}{2}}.$$

Then $q \equiv 1 \pmod 4$, which implies that $t \equiv 2 \pmod 4$. This completes the proof. □

Once we have Proposition 4, it is sufficient to verify the condition $t \equiv 2 \pmod 4$, where t is the trace of p-power Frobenius endomorphism to determine whether E can be switched to Montgomery model over $\mathbb{F}_p$.

For curves admitting twists, the subgroup $\mathbb{G}_2 \cong E'(\mathbb{F}_{p^{k/d}})[r]$, where E' is the degree-d twist of E and $\phi : E'/\mathbb{F}_{p^{k/d}} \to E/\mathbb{F}_p$ the twisting isomorphism over $\mathbb{F}_{p^k}$. Moreover, it follows from [26, Section 5] that

$$\hat{e}(P, Q) = e(P, \phi(Q)) = e(\phi^{-1}(P), Q),\ P \in \mathbb{G}_1 = E(\mathbb{F}_p)[r],\ Q \in E'(\mathbb{F}_{p^{k/d}})[r]$$

also defines a bilinear pairing. Hence, some computations can be operated over the subfield $\mathbb{F}_{p^{k/d}}$ to enhance efficiency. By [4, Theorem IX.10],

$$e(\psi \circ \phi^{-1}(P), \psi(Q)) = e(\phi^{-1}(P), Q)^{\deg(\psi)} = e(P, \phi(Q)),$$

where ψ denotes the isomorphism between E' and a Montgomery curve $E'_{A,B}$. By imposing this requirement, we can leverage the twist technique on Montgomery curves to optimize pairing computation.

Remark 1. Note that for curves E admitting degree-d twists E', we do not require that E itself is isomorphic to a Montgomery model, as the entire computation can be executed on the Montgomery curve $E'_{A,B}$ derived from E'.

In this context, we require that E' is $\mathbb{F}_{p^{k/d}}$-isomorphic to $E'_{A,B}$, and investigate to obtain propositions to effectively determine whether a degree-d twist of a pairing-friendly curve can be translated to Montgomery model over the subfield $\mathbb{F}_{p^{k/d}}$. Proposition 4 can be extended to determine whether a degree-d twist E' of E with $j(E) = 0$ or 1728 is $\mathbb{F}_q$-isomorphic to a Montgomery curve, as stated in Corollary 1.

Corollary 1. *With the notation as in Theorem 4, let E' denote a degree-d twist of E over $\mathbb{F}_q$. Define t' as the trace of $\sigma' \circ \pi'_q$ such that $\#E'(\mathbb{F}_q) = q + 1 - t'$, where σ' and π'_q are the automorphism and the q-power Frobenius endomorphism on E', respectively. Then E' is $\mathbb{F}_q$-isomorphic to a Montgomery curve $E'_{A,B}$ if and only if $t' \equiv 2 \pmod 4$.*

Proof. The proof follows directly by applying the same reasoning as in Proposition 4, replacing t with t'. □

In the following, we focus on the curve E with embedding degree k over $\mathbb{F}_q$, admitting a quadratic twist E' over $\mathbb{F}_{q^{k/2}}$. The following lemma illustrates the relationship between E' and the quadratic twist $E'_{A,B}$ of a Montgomery curve $E_{A,B}$.

Lemma 1. *Let E denote a short Weierstrass curve $E: y^2 = x^3 + ax + b$ over $\mathbb{F}_q$ of embedding degree k with respect to r. Assume that E admits a quadratic twist E' over $\mathbb{F}_{q^{k/2}}$. Then E is $\mathbb{F}_q$-isomorphic to a Montgomery curve $E_{A,B}$ if and only if E' is $\mathbb{F}_{q^{k/2}}$-isomorphic to a Montgomery curve $E'_{A,B}$.*

Proof. We first prove the necessity. Let φ denote the $\mathbb{F}_q$-isomorphism from E to $E_{A,B}$. We need to prove that there exists an isomorphism between E' and $E'_{A,B}$ defined over $\mathbb{F}_{q^{k/2}}$.

From [22, Lemma 9.12.12], $E_{A,B}$ has a unique quadratic twist $E'_{A,B}$. Assume that ζ is a non-square in $\mathbb{F}^*_{q^{k/2}}$. Then by Proposition 1,

$$\phi : E' \to E,\ (x, y) \mapsto (\zeta x, \zeta^{3/2} y)$$

and

$$\phi' : E'_{A,B} \to E_{A,B},\ (x, y) \mapsto (x, \zeta^{1/2} y)$$

are the corresponding twisting isomorphisms.

Additionally, from Proposition 3, the isomorphism ψ is of the form

$$\psi : E \to E_{A,B},\ (x, y) \mapsto \left(\frac{x-\alpha}{\beta}, \frac{y}{\beta}\right).$$

where $\alpha, \beta \in \mathbb{F}_q$. Define $\psi' = \phi'^{-1} \circ \psi \circ \phi$. It is clear that

$$\psi' : E' \to E'_{A,B},\ (x, y) \mapsto \left(\frac{\zeta x-\alpha}{\beta}, \frac{\zeta y}{\beta}\right).$$

is an isomorphism over $\mathbb{F}_{q^{k/2}}$. This completes the proof of the necessity.

We now consider the sufficiency. Since $E' : y^2 = x^3 + a/\zeta^2 x + b/\zeta^3$ is $\mathbb{F}_{p^{k/2}}$-isomorphic to Montgomery model, we have

$$\left(\frac{3(\alpha/\zeta)^2 + a/\zeta^2}{q^{k/2}}\right)_2 = \left(\frac{3\alpha^2 + a}{q}\right)_2^{k/2} = 1,$$

where α is an $\mathbb{F}_p$-rational 2-torsion point on E. One can show that $k/2$ is odd since the degree $d = \gcd(k, \#\mathrm{Aut}(E))$ is 2, yielding $\left(\frac{3\alpha^2+a}{q}\right)_2 = 1$. This ends the proof of sufficiency. □

Lemma 1 provides an effective criterion for determining whether a quadratic twist of an ordinary short Weierstrass curve E is $\mathbb{F}_{q^{k/2}}$-isomorphic to a Montgomery curve. For curves admitting degree-d twists ($d \geq 3$), we present Proposition 5.

Proposition 5. *Let E be an ordinary short Weierstrass curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$ of embedding degree k with respect to r. Suppose E admits a degree-d twist E' over $\mathbb{F}_{q^{k/d}}$ for $d \geq 3$. Let t denote the trace of the q-power Frobenius endomorphism, and let t_n denote the trace of the q^n-power Frobenius endomorphism.*

(1) *If $d = 4$, then E' is $\mathbb{F}_{q^{k/d}}$-isomorphic to a Montgomery curve if and only if*

$$t \equiv 0 \pmod 4 \quad \text{and} \quad \frac{k}{d} \equiv 1 \pmod 2.$$

(2) *If $d = 3$ or 6, then E' is $\mathbb{F}_{q^{k/d}}$-isomorphic to a Montgomery curve if and only if*

$$d = 3, t \equiv 1 \text{ (mod 2)}, \frac{k}{d} \not\equiv 0 \text{ (mod 3)}, t_{k/d} \equiv \pm f \text{ (mod } r\text{)}, \text{and} \;\; t_{k/d} \equiv \mp f \text{ (mod 8)},$$

or

$$d = 6, t \equiv 1 \text{ (mod 2)}, \frac{k}{d} \not\equiv 0 \text{ (mod 3)}, t_{k/d} \equiv \pm 3f \text{ (mod } r\text{)}, \text{and} \;\; t_{k/d} \equiv \pm f \text{ (mod 8)},$$

where f is a positive integer such that $3f^2 = 4q^{k/d} - t_{k/d}^2$.

To prove this proposition, we use the following lemma characterizing the relationship between t and t_n.

Lemma 2. *Using the above notation, the following holds:*

(1) *t_n is odd if and only if t is odd and $n \not\equiv 0 \pmod 3$.*
(2) *If $t \not\equiv 2 \pmod 4$ and $q \equiv 1 \pmod 4$, then $t_n \equiv 0 \pmod 4$ if and only if $t \equiv 0 \pmod 4$ and n is odd.*

Proof. It follows from [36, Lemma 4.13] that

$$t_{n+1} = t \cdot t_n - q \cdot t_{n-1}, \quad \text{with} \quad t_0 = 2, \; t_1 = t.$$

(1) We first prove the sufficiency and claim that

$$t_n \equiv 0 \pmod 2, \quad t_{n+1} \equiv t_{n+2} \equiv 1 \pmod 2, \quad \text{for } n = 3l, \; l \in \mathbb{N}. \tag{3}$$

For $l = 0$, we have

$$t_0 \equiv 0 \pmod 2, \quad t_1 = t \equiv 1 \pmod 2, \quad t_2 = t^2 - 2q \equiv 1 \pmod 2.$$

Assume that Equation (3) holds for $l \leq m$. Then

$$t_{3m} \equiv 0 \pmod 2, \quad t_{3m+1} \equiv t_{3m+2} \equiv 1 \pmod 2.$$

For $l = m + 1$, we compute:

$$\begin{aligned} t_{3m+3} &= t \cdot t_{3m+2} - q \cdot t_{3m+1} \equiv 1 - 1 \equiv 0 \pmod 2, \\ t_{3m+4} &= t \cdot t_{3m+3} - q \cdot t_{3m+2} \equiv 0 - 1 \equiv 1 \pmod 2, \\ t_{3m+5} &= t \cdot t_{3m+4} - q \cdot t_{3m+3} \equiv 1 - 0 \equiv 1 \pmod 2. \end{aligned}$$

By induction, the sufficiency is proved.

We now prove the necessity. From the sufficiency proof, it remains to show that t is odd. Suppose, for contradiction, that t is even, and let m be the minimal positive integer such that t_m is odd. Since $t_2 = t^2 - 2q \equiv 0 \pmod 2$, we have $m > 2$ and

$$t_m = t \cdot t_{m-1} - q \cdot t_{m-2}.$$

By the minimality of m, we have $t_{m-1} \equiv t_{m-2} \equiv 0 \pmod 2$, which implies

$$t_m \equiv 0 \pmod 2,$$

a contradiction.

(2) We first prove the sufficiency. Since $t \equiv 0 \pmod 4$ and $q \equiv 1 \pmod 4$, we have

$$t_{n+1} \equiv -t_{n-1} \equiv 3t_{n-1} \pmod 4.$$

Note that $t_1 = t \equiv 0 \pmod 4$. Assume $t_n \equiv 0 \pmod 4$ for all odd integers $n \leq m$. Then

$$t_{m+2} \equiv 3t_m \equiv 0 \pmod 4.$$

By induction, the sufficiency is proved.

To prove the necessity, first note that t cannot be odd. Assume $t \equiv 1 \pmod 4$, and let m be the minimal positive integer such that $t_m \equiv 0 \pmod 4$. Since

$$t_0 \equiv 2 \pmod 4, \quad t_1 \equiv 1 \pmod 4, \quad t_2 \equiv 3 \pmod 4, \quad t_3 \equiv 2 \pmod 4,$$

we have $m > 3$ and

$$t_m \equiv t \cdot t_{m-1} - q \cdot t_{m-2} \equiv t_{m-1} - t_{m-2} \equiv (t_{m-2} - t_{m-3}) - t_{m-2} \equiv -t_{m-3} \pmod 4.$$

This implies $t_{m-3} \equiv 0 \pmod 4$, contradicting the minimality of m. A similar contradiction arises for $t \equiv 3 \pmod 4$. Hence, $t \equiv 0 \pmod 4$.

It remains to prove that n is odd. Suppose n is even. Then

$$t_n \equiv t \cdot t_{n-1} - q \cdot t_{n-2} \equiv 3t_{n-2} \equiv 0 \pmod 4.$$

By induction, this would imply $t_n \equiv 0 \pmod 4$ for all even n, contradicting $t_0 \equiv 2 \pmod 4$.

The following is the proof of Proposition 5.

Proof of Proposition 5. (1) Since $d = 4$, Proposition 1 implies $j(E) = j(E') = 1728$. Since E is ordinary, we have $q \equiv 1 \pmod 4$, and

$$4q^{k/d} \equiv 4 \pmod{16}.$$

We first prove the necessity. From the proof of Lemma 1, if E' is $\mathbb{F}_{q^{k/d}}$-isomorphic to a Montgomery curve $E'_{A,B}$, then E cannot be $\mathbb{F}_q$-isomorphic to a Montgomery curve $E_{A,B}$. Otherwise, one could construct a degree-4 twisting isomorphism between $E'_{A,B}$ and $E_{A,B}$, contradicting [22, Lemma 9.12.12]. Consequently, by Theorem 4 and Corollary 1, we have

$$t'_{k/d} \equiv 2 \pmod 4, \quad t_{k/d} \not\equiv 2 \pmod 4, \quad \text{and} \quad t \not\equiv 2 \pmod 4.$$

Then, by Proposition 2,

$$t_{k/d}^2 \equiv 4q^{k/d} - t'^2_{k/d} \equiv 0 \pmod{16},$$

implying $t_{k/d} \equiv 0 \pmod 4$. By Lemma 2(2), the necessity follows.

For sufficiency, Lemma 2(2) implies $t_{k/d} \equiv 0 \pmod 4$. Then

$$t'^2_{k/d} \equiv 4q^{k/d} - t_{k/d}^2 \equiv 4 \pmod{16},$$

so $t'_{k/d} \equiv 2 \pmod 4$. By Corollary 1, E' is $\mathbb{F}_{q^{k/d}}$-isomorphic to a Montgomery curve.

(2) By Proposition 1, curves admitting degree-3 or 6 twists have $j(E) = j(E') = 0$. By Proposition 2,

$$t'_{k/d} = \begin{cases} \dfrac{\pm 3f - t_{k/d}}{2}, & \text{if } d = 3, \\ \dfrac{\pm 3f + t_{k/d}}{2}, & \text{if } d = 6, \end{cases} \tag{4}$$

where $3f^2 = 4q^{k/d} - t_{k/d}^2$. Note that $t_{k/d}$ and f have the same parity. For brevity, we only consider the case $d = 3$; the case $d = 6$ is similar.

We first prove the necessity. Assume $t'_{k/d} = (3f - t_{k/d})/2$. Since $q^{k/d} + 1 - t_{k/d} \equiv 0 \pmod r$, we derive

$$\frac{3f - t_{k/d}}{2} \equiv t_{k/d} \pmod r,$$

equivalent to $t_{k/d} \equiv f \pmod r$. As before, E cannot be $\mathbb{F}_q$-isomorphic to a Montgomery curve. By Theorem 4 and Corollary 1,

$$t'_{k/d} \equiv 2 \pmod 4, \quad t_{k/d} \not\equiv 2 \pmod 4, \quad \text{and} \quad t \not\equiv 2 \pmod 4.$$

Thus,

$$3f - t_{k/d} \equiv 2t'_{k/d} \equiv 4 \pmod 8.$$

If $t_{k/d}$ were even, then f would also be even. Write $t_{k/d} = 2a$, $f = 2b$ for $a, b \in \mathbb{Z}$. Then

$$a - 3b \equiv 2 \pmod 4.$$

Since $t_{k/d} \not\equiv 2 \pmod 4$, we have $t_{k/d} \equiv 0 \pmod 4$, so a is even. Then b must be even. However, from $3f^2 = 4q^{k/d} - t_{k/d}^2$,

$$12b^2 \equiv 4b^2 \equiv 4q^{k/d} - 4a^2 \equiv 4q^{k/d} \pmod 8,$$

implying $b^2 \equiv q^{k/d} \pmod 2$, a contradiction. Hence, $t_{k/d}$ is odd. By Lemma 2(1), $t \equiv 1 \pmod 2$ and $k/d \not\equiv 0 \pmod 3$. Moreover, f is odd, and $t_{k/d}^2 \equiv f^2 \equiv 1 \pmod 8$. From $3f - t_{k/d} \equiv 4 \pmod 8$, we deduce

$$t_{k/d} \equiv -f \pmod 8.$$

The case $t'_{k/d} = (-3f - t_{k/d})/2$ is similar, yielding

$$t \equiv 1 \text{ (mod 2)}, \frac{k}{d} \not\equiv 0 \text{ (mod 3)}, t_{k/d} \equiv -f \text{ (mod } r\text{)}, \text{and } \ t_{k/d} \equiv f \text{ (mod 8)}.$$

We now prove sufficiency. Suppose

$$t \equiv 1 \text{ (mod 2)}, \frac{k}{d} \not\equiv 0 \text{ (mod 3)}, t_{k/d} \equiv f \text{ (mod } r\text{)}, \text{and } \ t_{k/d} \equiv -f \text{ (mod 8)}.$$

By Lemma 2(1), $t_{k/d}$ is odd, so f is odd. From $t_{k/d} \equiv f \pmod r$ and the twist order, we have

$$t'_{k/d} = \frac{3f - t_{k/d}}{2}.$$

Since $t_{k/d} \equiv -f \pmod 8$,

$$3f - t_{k/d} \equiv 4 \pmod 8,$$

so $t'_{k/d} \equiv (3f - t_{k/d})/2 \equiv 2 \pmod 4$. By Corollary 1, E' is $\mathbb{F}_{q^{k/d}}$-isomorphic to a Montgomery curve. □

4 Pairing-friendly Curves Admitting Conversions to Montgomery Model

In this section, we utilize the results in Section 3 to determine the pairing-friendly curves or their twists that can be converted to the Montgomery model, as found in the literature, and provide appropriate parameters at the 128-bit or 192-bit security level. Note that all the curves considered in the remaining part of this paper are ordinary.

According to the construction method, the prevalent pairing-friendly curves can be roughly classified as follows.

- Cocks-Pinch curves [11,25].
- Cyclotomic families, including Barreto-Lynn-Scott (BLS) [3], Brezing-Weng (BW) [6], Freeman-Scott-Teske (FST) [21] and Fotiadis-Martindale (FM) [20].
- Subfield families, including Kachisa-Schaefer-Scott (KSS) [28] and Gasnier-Guillevic (GG) [23].

In the following, we review these three types of pairing-friendly curves mentioned above and select those curves or their twists that can be converted into the Montgomery model.

4.1 Cocks-Pinch curves

In [25], Guillevic, Masson and Thomé generated four Cocks-Pinch [11] curves with embedding degrees 5 to 8 at the 128-bit security level, see [25, Section 6.1] for more details. To distinguish them by embedding degrees, we name these four short Weierstrass curves as CP5 to CP8, respectively.

For CP8 admitting a quartic twist over $\mathbb{F}_{p^2}$, it holds that $k/d = 2 \equiv 0 \bmod 2$, where d denotes the degree of twist. Then, by Proposition 5, this twist cannot be translated to Montgomery form over $\mathbb{F}_{p^2}$. While CP6 has a sextic twist over $\mathbb{F}_p$. It can be verified through the parameters of CP6 in [25, Section 6.1] that the trace of p-power Frobenius endomorphism $t \equiv 0 \bmod 2$. Thus, it follows from Proposition 5 that this sextic twist cannot be $\mathbb{F}_p$-isomorphic to Montgomery model. Consequently, our acceleration approach in Section 3 is not applicable to CP6 and CP8.

It remains to determine whether CP5 and CP7, which do not have suitable twists, can be converted to the Montgomery model over $\mathbb{F}_p$. According to the parameters in [25, Section 6.1], there exists an $\mathbb{F}_p$-rational 2-torsion point $(\alpha, 0)$ on CP5 (resp. CP7) such that $\left(\frac{3\alpha^2+a}{p}\right)_2 = 1$. By Proposition 3, these two curves can be converted to Montgomery form over $\mathbb{F}_p$. Consequently, CP5 and CP7 are preferred for pairing optimization.

4.2 Cyclotomic families

Cyclotomic families are constructed using the BLS [3] and BW [6] methods along with their variants [21,1,20]. For efficiency reasons, this paper only considers families with embedding degrees ranging from 9 to 28 and CM-discriminants of 1 or 3.

Before proceeding with the selection, we first exclude some families. For families with $k = 9, 18, 27$ and CM-discriminant 3 that admit cubic or sextic twists, we have $k/d \equiv 0 \bmod 3$. Furthermore, for families with $k = 16$ and CM-discriminant 1 that admit quartic twists, we have $k/d \equiv 0 \bmod 2$. Then, by Proposition 5, the twists of these families cannot be converted to Montgomery form over $\mathbb{F}_{p^{k/d}}$. Consequently, they are not compatible with the optimization approach described in Section 3. Moreover, we are not interested in families with $k = 17, 19, 22, 23, 25$, and 26 because they simultaneously exhibit relatively high embedding degrees and small-degree twists (or lack twists), resulting in inefficient pairing computations. This is the reason why such families are not discussed in this paper.

Most of the well-known complete cyclotomic families with embedding degrees 10-15, 20, 21, 24, and 28 found in the literature are summarized in [24, Table 5], [21, Section 6], and [20, Appendix C]. By applying the propositions in Section 3, we can identify which curves (or their degree-d twists) from these cyclotomic families can be converted to Montgomery form over $\mathbb{F}_p$ (or $\mathbb{F}_{p^{k/d}}$, respectively). Additionally, we provide the results for our selection. Assume that the polynomials $p(x)$, $t(x)$, and $r(x)$ parameterize the characteristic p, the trace t of p-power

Frobenius map π, and the large prime factor r of $\#E(\mathbb{F}_p)$, respectively. Denote by $\mathbf{Cyclo}_{\boldsymbol{k,D,e}}$ a cyclotomic family with embedding degree k, CM-discriminant D, and an integer e such that $t(x) \equiv x^{me} + 1 \mod r(x)$, where $m = 4/\gcd(4,k)$ (resp. $m = 3/\gcd(3,k)$) for $D = 1$ (resp. $D = 3$).

Curves without twists. The families without twists mentioned above have embedding degrees $k = 11$ and 13. By Proposition 4, the curves in $\mathrm{Cyclo}_{11,1,1}$ and $\mathrm{Cyclo}_{13,1,1}$ (see [24, Table 5] for more details) are $\mathbb{F}_p$-isomorphic to the Montgomery model for the families with CM-discriminant 1. As for those with CM discriminant 3, we deduce that the curves in $\mathrm{Cyclo}_{11,3,1}$ and $\mathrm{Cyclo}_{13,3,1}$ can be converted to the Montgomery model over $\mathbb{F}_p$ if the parameter seed $x \equiv 1 \bmod 12$.

Curves admitting quadratic twists. We now consider the families that admit quadratic twists with embedding degrees $k = 10$ and 14, as shown in [24, Table 5] and [13, Table 4]. Under this circumstance, Lemma 1 demonstrates that the twists of curves in $\mathrm{Cyclo}_{10,1,1}$, $\mathrm{Cyclo}_{10,1,9}$, and $\mathrm{Cyclo}_{14,1,1}$ are $\mathbb{F}_{p^{k/2}}$-isomorphic to Montgomery curves. Besides, if the parameter seed $x \equiv 1 \bmod 12$, then the twists of the curves in $\mathrm{Cyclo}_{10,3,1}$ can be converted to the Montgomery model over $\mathbb{F}_{p^{k/2}}$.

Curves admitting quartic twists. For the families admitting quartic twists with embedding degrees $k = 20$ and 28 illustrated in [24, Table 5], it follows from Proposition 5 that the quartic twists of these two families can be translated to the Montgomery model over $\mathbb{F}_{p^{k/4}}$ if $x \equiv 3 \bmod 4$.

Curves admitting cubic and sextic twists. Finally, we focus on the families admitting cubic or sextic twists with embedding degrees $k = 12$, 15, 21, and 24 in [24, Table 5]. Proposition 5 shows that if $x \equiv 4 \bmod 6$, then the sextic (resp. cubic) twists of the curves in $\mathrm{Cyclo}_{24,3,1}$ (resp. $\mathrm{Cyclo}_{21,3,1}$) can be transformed to Montgomery model over $\mathbb{F}_{p^{k/6}}$ (resp. $\mathbb{F}_{p^{k/3}}$). While the cubic twists of the curves in $\mathrm{Cyclo}_{15,3,11}$ can be converted to Montgomery form over $\mathbb{F}_{p^{k/3}}$ if $x \equiv 5 \bmod 6$.

4.3 Subfield families

The subfield families are primarily divided into two categories: KSS [28] and GG [23]. By utilizing Proposition 5, the quartic (resp. sextic) twists of the curves with embedding degree 16 (resp. 18) and CM-discriminant 1 (resp. 3) cannot be transformed into Montgomery form over $\mathbb{F}_{p^4}$ (resp. $\mathbb{F}_{p^3}$). Therefore, families KSS16 and KSS18 are incompatible with our optimization techniques. On the other hand, we explore that families GG20b and GG28 (see [23, Examples 5.2 and 5.3] for more details) admitting quartic twists are suitable for the acceleration approach proposed in Section 3.

5 Cost Analysis and Comparison

In this section, we describe the cubical arithmetic for pairing computations via biextensions on curves that admit a Montgomery model, including those with twists and those without twists. Additionally, we provide concrete computational costs for an iteration of the cubical or double-and-add ladder on Montgomery curves, as well as for a basic Miller iteration on short Weierstrass curves. Finally, we present a cost comparison for the Miller loops on selected curves from Table 2. The notations for computational costs used in the remainder of this paper are introduced as follows.

Notations. Let $\mathbf{m}$, $\mathbf{s}$, and $\mathbf{i}$ denote the computational costs of multiplication, squaring, and inversion in $\mathbb{F}_p$, respectively, where p is an odd prime. Let $\mathbf{m}_k$, $\mathbf{s}_k$, $\mathbf{i}_k$, and $\mathbf{f}_k$ represent the costs of multiplication, squaring, inversion, and Frobenius endomorphism in $\mathbb{F}_{p^k}$, respectively. Denote by $\mathbf{m}_0$ the cost of multiplication by a constant.

According to Section 2.3, pairing computations via biextension require updating the coordinates $Z_{[n]Q+P}$ and $Z_{[n]Q}$, where $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. For this purpose, we employ the cubical and double-and-add ladders, shown in Algorithms 5 and 6, respectively. Further details can be found in Appendix A.

5.1 Cubical arithmetic on Montgomery model

The computational procedures for cubical point doubling, differential addition, and compatible addition on a Montgomery curve $E_{A,B}$ are summarized in Algorithms 1, 2, and 3, respectively.

Algorithm 1 Cubical point doubling [32, Algorithm 1].

```
Input: A cubical point $P = (X_P, Z_P)$ over $\mathbb{F}_{p^k}$, The parameter $A_{24} = (A+2)/4$,
    where $A$ is the coefficient of a Montgomery curve $E_{A,B}$.
Output: The cubical point $[2]P = (X_{[2]P}, Z_{[2]P})$.
$t_0 \leftarrow (X_P + Z_P)^2,\ t_1 \leftarrow (X_P - Z_P)^2$
$X_{[2]P} \leftarrow t_0 \cdot t_1$
$t_2 \leftarrow t_0 - t_1$
$t_0 \leftarrow A_{24} \cdot t_2$
$Z_{[2]P} \leftarrow t_2 \cdot (t_0 + t_1)$
return $X_{[2]P},\ Z_{[2]P}$
```

Algorithm 2 Cubical differential addition [32, Algorithm 2].

```
Input: The cubical points $P = (X_P, Z_P)$, $Q = (X_Q, Z_Q)$ over $\mathbb{F}_{p^k}$, and the inverse
    coordinates $(X_{P-Q}^{-1}, 1)$ of the normalized difference $P - Q$.
Output: The cubical point $(X_{P+Q}, Z_{P+Q})$.
$t_0 \leftarrow (X_P - Z_P) \cdot (X_Q + Z_Q),\ t_1 \leftarrow (X_P + Z_P) \cdot (X_Q - Z_Q)$
$X_{P+Q} \leftarrow X_{P-Q}^{-1} \cdot (t_0 + t_1)^2$
$Z_{P+Q} \leftarrow (t_0 - t_1)^2$
return $X_{P+Q},\ Z_{P+Q}$
```

In Algorithm 2, we assume that $Z_{P-Q} = 1$ since the point $P - Q$ involved in the cubical or double-and-add ladder for pairing computations is always normalized. Unlike [32, Algorithm 4], we omit the final division by 4 because curves with embedding degree one are outside the scope of this paper, and the cofactor 4 will be eliminated by the final exponentiation.

Algorithm 3 Cubical compatible addition.

```
Input: The cubical points $P_1 = (X_{P_1}, 1)$, $P_2 = (X_{P_2}, Z_{P_2})$, $P_1 - Q = (X_{P_1-Q}, 1)$
    and $P_2 + Q = (X_{P_2+Q}, Z_{P_2+Q})$ over $\mathbb{F}_{p^k}$. The coefficient $A$ of a Montgomery curve
    $E_{A,B}$.
Output: The cubical point $(X_{P_1+P_2}, Z_{P_1+P_2})$.
$t_1 \leftarrow X_{P_1} \cdot X_{P_2}$
$t_2 \leftarrow X_{P_1} \cdot Z_{P_2}$
$t_3 \leftarrow (t_1 - Z_{P_2})^2$
$t_4 \leftarrow 2(t_1 + Z_{P_2}) \cdot (t_2 + X_{P_2}) + 2A \cdot t_1 \cdot Z_{P_2}$
$t_5 \leftarrow X_{P_1-Q} \cdot X_{P_2+Q}$
$t_6 \leftarrow X_{P_1-Q} \cdot Z_{P_2+Q}$
$t_7 \leftarrow (t_5 - Z_{P_2+Q})^2$
$t_8 \leftarrow 2(t_5 + Z_{P_2+Q}) \cdot (t_6 + X_{P_2+Q}) + 2A \cdot t_5 \cdot Z_{P_2+Q}$
$X_{P_1+P_2} \leftarrow t_3 \cdot t_8 - t_4 \cdot t_7$
$t_9 \leftarrow (t_1 - Z_{P_2}) \cdot (t_5 - Z_{P_2+Q})$
$t_{10} \leftarrow (t_2 - X_{P_2}) \cdot (t_6 - X_{P_2+Q})$
$Z_{P_1+P_2} \leftarrow (t_9 + t_{10}) \cdot (t_9 - t_{10})$
return $X_{P_1+P_2}$, $Z_{P_1+P_2}$
```

In Algorithm 3, we set $Z_{P_1} = Z_{P_1-Q} = 1$ since both P_1 and $P_1 - Q$ are always normalized in practice. If $A = 0$, the cost of this algorithm reduces to $11\mathbf{m}_k + 2\mathbf{s}_k$.

5.2 Computational Cost Analysis and Comparison per Iteration

In this subsection, we analyze the computational cost per iteration of the cubical and double-and-add ladders on Montgomery curves converted from short Weierstrass curves or their twists.

For a short Weierstrass curve E without twists over $\mathbb{F}_p$, we convert it to a Montgomery curve $E_{A,B}$ over $\mathbb{F}_p$ as described in Section 3. Thus, the input points for the cubical or double-and-add ladder are $P \in E_{A,B}(\mathbb{F}_p)[r]$ and $Q \in E_{A,B}(\mathbb{F}_{p^k})[r] \cap \ker(\pi - [p])$. Since $E_{A,B}$ is defined over $\mathbb{F}_p$, we have $A_{24} = (A + 2)/4 \in \mathbb{F}_p$.

We first analyze the computational cost per bit for the cubical ladder. If the current bit is zero, the algorithm performs one cubical point doubling (Line 5 of Algorithm 5) along with two differential additions (Lines 3 and 5 of Algorithm 5) relative to point differences P and Q. Otherwise, it executes one cubical point doubling (Line 7 of Algorithm 5) together with two differential additions (Lines

3 and 7 of Algorithm 5) relative to Q and $Q-P$. The cost of multiplying two elements in $\mathbb{F}_p$ and $\mathbb{F}_{p^k}$ can be estimated as $k\mathbf{m}$.

Given that $A_{24}, X_P \in \mathbb{F}_p$, $X_Q, X_{Q-P} \in \mathbb{F}_{p^k}$, and following Algorithms 1 and 2, the cost per iteration of the cubical ladder is:

$$\begin{aligned}\mathrm{Cost}_{\mathrm{cub}_0} &= \mathrm{Cost}_{\mathrm{dbl}} + \mathrm{Cost}_{\mathrm{diff}_P} + \mathrm{Cost}_{\mathrm{diff}_Q} = 7\mathbf{m}_k + 6\mathbf{s}_k + 2k\mathbf{m},\\ \mathrm{Cost}_{\mathrm{cub}_1} &= \mathrm{Cost}_{\mathrm{dbl}} + \mathrm{Cost}_{\mathrm{diff}_Q} + \mathrm{Cost}_{\mathrm{diff}_{Q-P}} = 8\mathbf{m}_k + 6\mathbf{s}_k + k\mathbf{m}.\end{aligned} \tag{5}$$

Similarly, the cost per step of the double-and-add ladder can be derived as follows:

$$\begin{aligned}\mathrm{Cost}_{\mathrm{dadd}_0} &= \mathrm{Cost}_{\mathrm{dbl}} + \mathrm{Cost}_{\mathrm{diff}_P} = 4\mathbf{m}_k + 4\mathbf{s}_k + 2k\mathbf{m},\\ \mathrm{Cost}_{\mathrm{dadd}_1} &= \mathrm{Cost}_{\mathrm{diff}_Q} + \mathrm{Cost}_{\mathrm{diff}_{Q-P}} + \mathrm{Cost}_{\mathrm{add}} = 19\mathbf{m}_k + 6\mathbf{s}_k + 2k\mathbf{m}.\end{aligned} \tag{6}$$

The case of curves admitting twists is slightly more complex. According to Section 3, the Montgomery curve $E_{A,B}$ is obtained by converting a degree-d twist E' of a short Weierstrass curve E defined over $\mathbb{F}_{p^{k/d}}$. Therefore, the input points for the cubical arithmetic satisfy $P \in \psi \circ \phi^{-1}(E(\mathbb{F}_p)[r])$ and $Q \in E_{A,B}(\mathbb{F}_{p^{k/d}})[r]$, where $\psi : E' \to E_{A,B}$ and $\phi : E' \to E$ denote the $\mathbb{F}_{p^{k/d}}$-isomorphisms between E' and $E_{A,B}$, and the twisting isomorphism, respectively. More precisely, by selecting appropriate parameters and field constructions, we can simplify the forms of A and x_P, which is summarized in the following proposition. To ensure the applicability of our method, k/d should meet the conditions in Theorem 5 if $d \geq 3$.

Proposition 6. *With the notation as above, and let E be a short Weierstrass curve over $\mathbb{F}_p$ admitting a degree-d twist E' over $\mathbb{F}_{p^{k/d}}$. Define $E_{A,B}$ to be a Montgomery curve $\mathbb{F}_{p^{k/d}}$-isomorphic to E'. Let $P \in \psi \circ \phi^{-1}(P_0), P_0 \in E(\mathbb{F}_p)[r]$. Then there exist the following four cases.*

(1) *Case $d = 2$: if $j(E) = 1728$, then $A = 0$ and $x_P \in \mathbb{F}_p$. If $j(E) = 0$, then $A, x_P \in \mathbb{F}_p^*$ when $p \equiv 1 \bmod 4$.*

(2) *Case $d = 3$: if $k/d \equiv 1 \bmod 3$ (resp. $k/d \equiv 2 \bmod 3$), then we have $A \in \mathbb{F}_p^*$, $x_P = m_1\xi^{\frac{2k/d+1}{3}}v - m_2$ (resp. $x_P = m_1\xi^{\frac{2k/d+2}{3}} - m_2$) when $p \equiv 1 \bmod 4$, where m_i $(i = 1,2) \in \mathbb{F}_p^*$ and $\mathbb{F}_{p^{k/d}} = \mathbb{F}_p[\xi]/\left\langle \xi^{k/d} - n \right\rangle, \mathbb{F}_{p^k} = \mathbb{F}_{p^{k/d}}[v]/\left\langle v^3 - \xi \right\rangle$.*

(3) *Case $d = 4$: we have $A \in \mathbb{F}_p$, $x_P = m\xi^{\frac{k/d+1}{2}}v^2$, where $m \in \mathbb{F}_p$ and $\mathbb{F}_{p^{k/d}} = \mathbb{F}_p[\xi]/\left\langle \xi^{k/d} - n \right\rangle, \mathbb{F}_{p^{4k/d}} = \mathbb{F}_{p^k}[v]/\left\langle v^4 - \xi \right\rangle$.*

(4) *Case $d = 6$: if $k/d \equiv 1 \bmod 3$ (resp. $k/d \equiv 2 \bmod 3$), then we have $A \in \mathbb{F}_p^*$, $x_P = m_1\xi^{\frac{2k/d+1}{3}}v^2 - m_2$ (resp. $x_P = m_1\xi^{\frac{2k/d+2}{3}} - m_2$) when $p \equiv 1 \bmod 4$, where m_i $(i = 1,2) \in \mathbb{F}_p^*$ and $\mathbb{F}_{p^{k/d}} = \mathbb{F}_p[\xi]/\left\langle \xi^{k/d} - n \right\rangle, \mathbb{F}_{p^k} = \mathbb{F}_{p^{k/d}}[v]/\left\langle v^6 - \xi \right\rangle$.*

Proof. This can be proven by composing the degree-d twisting isomorphisms ϕ with the isomorphisms ψ between short Weierstrass and Montgomery curves, and applying the construction methods of extension fields.

From Proposition 6, we observe that multiplying x_P by an element in $\mathbb{F}_{p^k}$ can be estimated as $k\mathbf{m}$ for $d = 2, 4$ and $2k\mathbf{m}$ for $d = 3, 6$. This is because multiplying $\xi^i v^j$ by an element in $\mathbb{F}_{p^k}$ can be implemented using shift operations.

The computational process for the cubical or double-and-add ladder on a curve E admitting a degree-d twist is similar to the case without twists. The key difference is that some computations are performed in the subfield $\mathbb{F}_{p^{k/d}}$, such as Lines 4 and 8 of Algorithm 6. Additionally, some multiplications and squarings over $\mathbb{F}_{p^k}$ in the compatible addition (Line 7 of Algorithm 6) are sparse. Specifically, only the coefficients $a_0, b_0 \in \mathbb{F}_{p^{k/d}}$ of the final results $X_{[n+1]Q} = \sum_{i=1}^{d} a_i v^{i-1}$ and $Z_{[n+1]Q} = \sum_{i=1}^{d} b_i v^{i-1} \in \mathbb{F}_{p^k}$ are needed. This sparsity arises from employing an $\mathbb{F}_{p^{k/d}}$-linear form to ensure these cubical coordinates remain in $\mathbb{F}_{p^{k/d}}$ (see [29, Remark 2] for details).

Let $\mathbf{m}_s$ and $\mathbf{s}_s$ denote the costs of sparse multiplication and squaring over $\mathbb{F}_{p^k}$, respectively. Based on the cost analysis for the cubical ladder and Algorithms 1-3, the cost per iteration of the cubical or double-and-add ladder is

$$\begin{aligned}
\mathrm{Cost}_{\mathrm{cub}_0} &= \begin{cases} 2\mathbf{s}_k + (2d+5)\mathbf{m}_{k/d} + 4\mathbf{s}_{k/d} + \frac{k(d+1)}{d}\mathbf{m}, & d = 2, 4, \\ 2\mathbf{s}_k + (2d+5)\mathbf{m}_{k/d} + 4\mathbf{s}_{k/d} + \frac{k(2d+1)}{d}\mathbf{m}, & d = 3, 6, \end{cases} \\
\mathrm{Cost}_{\mathrm{cub}_1} &= \mathbf{m}_k + 2\mathbf{s}_k + (2d+5)\mathbf{m}_{k/d} + 4\mathbf{s}_{k/d} + \frac{k}{d}\mathbf{m}, \\
\mathrm{Cost}_{\mathrm{dadd}_0} &= \begin{cases} 2\mathbf{s}_k + (2d+2)\mathbf{m}_{k/d} + 2\mathbf{s}_{k/d} + \frac{k(d+1)}{d}\mathbf{m}, & d = 2, 4, \\ 2\mathbf{s}_k + (2d+2)\mathbf{m}_{k/d} + 2\mathbf{s}_{k/d} + \frac{k(2d+1)}{d}\mathbf{m}, & d = 3, 6, \end{cases} \\
\mathrm{Cost}_{\mathrm{dadd}_1} &= \begin{cases} 3\mathbf{m}_k + 2\mathbf{s}_k + 2\mathbf{m}_s + \mathbf{s}_s + (4d+6)\mathbf{m}_{k/d} + 3s_{k/d} + \frac{2k}{d}\mathbf{m}, & d = 2, 4, D = 1, \\ 3\mathbf{m}_k + 2\mathbf{s}_k + 3\mathbf{m}_s + \mathbf{s}_s + (4d+7)\mathbf{m}_{k/d} + 3s_{k/d} + \frac{4k}{d}\mathbf{m}, & d = 2, D = 3, \\ 3\mathbf{m}_k + 2\mathbf{s}_k + 3\mathbf{m}_s + \mathbf{s}_s + (4d+7)\mathbf{m}_{k/d} + 3s_{k/d} + \frac{6k}{d}\mathbf{m}, & d = 3, 6, \end{cases}
\end{aligned} \tag{7}$$

where $\mathbf{m}_s$ (resp. $\mathbf{s}_s$) in the compatible addition can be estimated as $2\mathbf{m}_{k/d}$ (resp. $2\mathbf{s}_{k/d}$), $3\mathbf{m}_{k/d}$ (resp. $\mathbf{m}_{k/d} + \mathbf{s}_{k/d}$), $4\mathbf{m}_{k/d}$ (resp. $\mathbf{m}_{k/d} + 2\mathbf{s}_{k/d}$) and $6\mathbf{m}_{k/d}$ $(2\mathbf{m}_{k/d} + 2\mathbf{s}_{k/d})$ when $d = 2, 3, 4$ and 6.

Remark 2. The double-and-add ladder can be combined with non-adjacent form (NAF) representation to further reduce computational costs. Additionally, the cubical and double-and-add ladders can be hybridized to maximize efficiency.

In pairing-based cryptography, the Miller loop typically has low Hamming weight. Consequently, the double-and-add ladder is generally more practical for implementation. Based on the above cost analysis, we compare the computational costs of the biextension approach (using cubical arithmetic) on Montgomery curves with Miller's algorithm. Table 1 presents the costs per basic iteration for the double-and-add ladder on Montgomery curves and for Miller's algorithm on short Weierstrass curves.

Table 1. Computational costs for a basic Miller iteration (including doubling and double-and-add steps) by employing biextension approach (double-and-add ladder) on Montgomery curves and Miller's algorithm on short Weierstrass curves. The cost calculations for Miller's algorithm are referred to [1, Table 7] and [24, Table 7].

Curve	This work Doubling step Double-and-add step	Miller's algorithm Doubling step Double-and-add step
$j = 0$ without twist	$4\mathbf{m}_k + 4\mathbf{s}_k + 2k\mathbf{m}$ $19\mathbf{m}_k + 6\mathbf{s}_k + 2k\mathbf{m}$	$9\mathbf{m}_k + 7\mathbf{s}_k + 3k\mathbf{m}$ $23\mathbf{m}_k + 10\mathbf{s}_k + 3k\mathbf{m}$
$j \neq 0$, 1728 without twist	$4\mathbf{m}_k + 4\mathbf{s}_k + 2k\mathbf{m}$ $19\mathbf{m}_k + 6\mathbf{s}_k + 2k\mathbf{m}$	$9\mathbf{m}_k + 8\mathbf{s}_k + 3k\mathbf{m}$ $23\mathbf{m}_k + 11\mathbf{s}_k + 3k\mathbf{m}$
$j = 0$ quadratic twist	$2\mathbf{s}_k + 6\mathbf{m}_{k/2} + 2\mathbf{s}_{k/2} + \frac{5k}{2}\mathbf{m}$ $3\mathbf{m}_k + 2\mathbf{s}_k + 21\mathbf{m}_{k/2} + 5\mathbf{s}_{k/2} + 2k\mathbf{m}$	$\mathbf{m}_k + \mathbf{s}_k + 2\mathbf{m}_{k/2} + 7\mathbf{s}_{k/2} + k\mathbf{m}$ $2\mathbf{m}_k + \mathbf{s}_k + 12\mathbf{m}_{k/2} + 9\mathbf{s}_{k/2} + 2k\mathbf{m}$
$j = 1728$ quadratic twist	$2\mathbf{s}_k + 6\mathbf{m}_{k/2} + 2\mathbf{s}_{k/2} + \frac{3k}{2}\mathbf{m}$ $3\mathbf{m}_k + 2\mathbf{s}_k + 18\mathbf{m}_{k/2} + 5\mathbf{s}_{k/2} + k\mathbf{m}$	$\mathbf{m}_k + \mathbf{s}_k + 2\mathbf{m}_{k/2} + 8\mathbf{s}_{k/2} + k\mathbf{m}$ $2\mathbf{m}_k + \mathbf{s}_k + 11\mathbf{m}_{k/2} + 13\mathbf{s}_{k/2} + 2k\mathbf{m}$
$j = 0$ cubic twist	$2\mathbf{s}_k + 8\mathbf{m}_{k/3} + 2\mathbf{s}_{k/3} + \frac{7k}{3}\mathbf{m}$ $3\mathbf{m}_k + 2\mathbf{s}_k + 29\mathbf{m}_{k/3} + 4\mathbf{s}_{k/3} + 2k\mathbf{m}$	$\mathbf{m}_k + \mathbf{s}_k + 6\mathbf{m}_{k/3} + 7\mathbf{s}_{k/3} + k\mathbf{m}$ $2\mathbf{m}_k + \mathbf{s}_k + 19\mathbf{m}_{k/3} + 12\mathbf{s}_{k/3} + 2k\mathbf{m}$
$j = 1728$ quartic twist	$2\mathbf{s}_k + 10\mathbf{m}_{k/4} + 2\mathbf{s}_{k/4} + \frac{5k}{4}\mathbf{m}$ $3\mathbf{m}_k + 2\mathbf{s}_k + 30\mathbf{m}_{k/4} + 5\mathbf{s}_{k/4} + \frac{k}{2}\mathbf{m}$	$\mathbf{m}_k + \mathbf{s}_k + 2\mathbf{m}_{k/4} + 8\mathbf{s}_{k/4} + \frac{k}{2}\mathbf{m}$ $2\mathbf{m}_k + \mathbf{s}_k + 11\mathbf{m}_{k/4} + 13\mathbf{m}_{k/4} + k\mathbf{m}$
$j = 0$ sextic twist	$2\mathbf{s}_k + 14\mathbf{m}_{k/6} + 2\mathbf{s}_{k/6} + \frac{13k}{6}\mathbf{m}$ $3\mathbf{m}_k + 2\mathbf{s}_k + 51\mathbf{m}_{k/6} + 5\mathbf{s}_{k/6} + k\mathbf{m}$	$\mathbf{m}_k + \mathbf{s}_k + 2\mathbf{m}_{k/6} + 7\mathbf{s}_{k/6} + \frac{k}{3}\mathbf{m}$ $2\mathbf{m}_k + \mathbf{s}_k + 12\mathbf{m}_{k/6} + 9\mathbf{s}_{k/6} + \frac{2k}{3}\mathbf{m}$

Table 1 shows that the biextension approach using the Montgomery model is more efficient than Miller's algorithm for the basic doubling step on curves admitting degree-d twists ($d \leq 3$), particularly for curves without twists. For curves with quartic twists, the cost per doubling step using our approach is comparable to Miller's algorithm. Compared to [29], adopting the Montgomery form allows the biextension technique to outperform Miller's algorithm on a wider range of curves; the approach in [29] only slightly outperforms Miller's algorithm for curves without twists.

5.3 Cost Analysis for Pairing Computations on Our Selected Curves

In this subsection, we select appropriate parameters for pairing-friendly curves equipped with degree-d ($d \leq 3$) twists admitting conversions to Montgomery model, and make concrete cost analysis for the corresponding pairing computations via biextensions.

To maximize efficiency, we aim to minimize the bit-lengths of the characteristic p, the parameterized seed x, as well as the Hamming weight of x. Based on the determinations in Section 4 and the security estimates in [1, Table 5] and [24, Table 5], the parameters for pairing-friendly curves compatible with our optimization framework (i.e. admitting conversions to Montgomery form) at the 128- or 192-bit security level are presented in Table 2.

We now derive pairing formulas via biextensions for the curves in Table 2, working directly with the Montgomery model obtained from these curves or their degree-d twists. According to [29, Table 1], we can derive the corresponding level-2 pairing formulas using cubical arithmetic, which are summarized in Table 3.

Table 2. The parameters for our selected pairing-friendly curves at the 128 or 192-bit security level. We distinguish them by the constructions, embedding degrees and characteristics. The notation $|x|$ represents the absolute value of the parametrized seed.

Curve	Construction	p bits	p^k bits	r bits	$\lvert x\rvert$ or $\lvert t-1\rvert$
CP5-663	Cocks-Pinch	663	3318	256	$2^{64}-2^{61}+2^{15}+1$
CP7-512	Cocks-Pinch	512	3584	256	$2^{43}-2^{41}-\texttt{0x47dfdb8}+1$
BW14-382	Cyclo$_{14,1,1}$	382	5338	256	$2^{21}+2^{19}-2^{16}+2^{13}+2^{10}+1$
BLS15-383	Cyclo$_{15,3,11}$	383	5737	257	$2^{32}+2^{16}+2^{12}+2^{2}+1$
BLS21-511	Cyclo$_{21,3,1}$	671	10715	384	$2^{32}-2^{25}-2^{6}-1$

Table 3. The level 2 pairing formulas via cubical arithmetic on Montgomery model translated from the curves (or their degree-d twists) in Table 2. Define $\pi' = \phi^{-1}\circ\pi\circ\phi$, $\sigma' = \phi^{-1}\circ\sigma\circ\phi$, and $\tau' = \sigma'\circ\pi'^{j}$ on E' to be the pullbacks of the q-power Frobenius endomorphism π, the efficiently computable endomorphism σ, and the composed map $\tau = \sigma\circ\pi^{j}$ ($j\in\mathbb{N}^*$), respectively, where ϕ is the degree-d twisting isomorphism. Let ψ denote an $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^{k/d}}$)-isomorphism between E (resp. E') and a Montgomery curve $E_{A,B}$ for a curve E without twists (resp. admitting a degree-d twist E'). To simplify the notation, for the curves E with the lack of twists we define $P\in\psi(\mathbb{G}_1) = E_{A,B}(\mathbb{F}_p)[r]$ and $Q\in\psi(\mathbb{G}_2) = E_{A,B}(\mathbb{F}_{p^k})[r]\cap\ker(\pi-[p])$. And we denote by P' and Q' the points in $\psi\circ\phi^{-1}(\mathbb{G}_1) = E_{A,B}(\mathbb{F}_{p^k})[r]$ and $\psi\circ\phi^{-1}(\mathbb{G}_2) = E_{A,B}(\mathbb{F}_{p^{k/d}})[r]$ for the curves admitting degree-d twists E'. Assume that the coordinates $Z_P,\ Z_Q,\ Z_{P+Q}$ or $Z_{P'},\ Z_{Q'},\ Z_{P'+Q'}$ are normalized.

curve	modular equality	pairing formula
CP5-663	$p+1-t\equiv 0 \bmod r$	$\left(\frac{Z_{[t-1]Q+P}}{Z_{[t-1]Q}}\right)^{\frac{p^5-1}{r}}$
CP7-512	$p+1-t\equiv 0 \bmod r$	$\left(\frac{Z_{[t-1]Q+P}}{Z_{[t-1]Q}}\right)^{\frac{p^7-1}{r}}$
BW14-382	$x^2+p^8\equiv 0 \bmod r$	$\left(Z_{[x]Q'+P'}^{xp^{10}}\cdot Z_{[x]Q'+\sigma'^{-1}(P')}\right)^{\frac{p^{14}-1}{r}}$
BLS15-383	$x+p^{11}\equiv 0 \bmod r$	$Z_{[x]Q'+P'}^{\frac{p^{15}-1}{r}}$
BLS21-511	$x-p\equiv 0 \bmod r$	$Z_{[x]Q'+P'}^{\frac{p^{21}-1}{r}}$

The computational costs for finite field arithmetic are derived from [19, Tables 3 and 11], [1, Table 9], and [13, Table 7]. For simplicity, we omit modular reductions and adopt the assumption from [13, Table 7] that $\mathbf{m}_u = \mathbf{m}$. The resulting costs of arithmetic operations in $\mathbb{F}_{p^k}$ for $k = 5, 7, 14, 15$ and 21 are presented in Table 4.

Table 4. The costs of multiplication, squaring in extension field $\mathbb{F}_{p^k}$ assuming $p \equiv 1 \bmod k$ for fast Frobenius endomorphism $\mathbf{f}_k$.

k	$\mathbf{m}_k$	$\mathbf{s}_k$	$\mathbf{f}_k$
5	$9\mathbf{m}$ [19, Tab. 3]	$9\mathbf{m}$ [19, Tab. 3]	$4\mathbf{m}$ [1, Tab. 9]
7	$13\mathbf{m}$ [19, Tab. 11]	$13\mathbf{m}$ [19, Tab. 11]	$6\mathbf{m}$ [1, Tab. 9]
14	$3\mathbf{m}_7$ [13, Tab. 8] $= 39\mathbf{m}$	$2\mathbf{m}_7$ [13, Tab. 8] $= 26\mathbf{m}$	$12\mathbf{m}$ [13, Tab. 8]
15	$6\mathbf{m}_5$ [1, Tab. 9] $= 54\mathbf{m}$	$2\mathbf{m}_5 + 3\mathbf{s}_5$ [1, Tab. 9] $= 45\mathbf{m}$	$14\mathbf{m}$ [1, Tab. 9]
21	$6\mathbf{m}_7$ [1, Tab. 9] $= 78\mathbf{m}$	$2\mathbf{m}_7 + 3\mathbf{s}_7$ [1, Tab. 9] $= 65\mathbf{m}$	$20\mathbf{m}$ [1, Tab. 9]

Following the formulas in Table 3, we provide a detailed cost analysis for Miller loops on Montgomery models $E_{A,B}$ converted from the pairing-friendly curves (or their degree-d twists) in Table 2. In more detail, we neglect the cost calculations for the building blocks with relatively low overhead, such as curve transformations, and primarily concentrate on the (cubical or double-and-add) ladder itself. Several techniques are also employed to make further optimizations.

We consider optimizing the last iterations for cubical or double-and-add ladders on Montgomery curves $E_{A,B}$. Let the notations be the same as Table 3. In the last iteration, it only requires to update Z-coordinates, and thus the operations to derive X-coordinates can be eliminated. It is worth noting that we do not need $Z_{[n]Q'} \in \mathbb{F}_{p^{k/d}}$ for curves admitting degree-d twists, since it can be killed by the final exponentiation. Furthermore, the computations for $[n+1]Q$ or $[n+1]Q'$ in cubical ladders can also be removed. We discuss two situations where the bits are 0 and 1, respectively.

We first consider the former case. Based on Algorithms 1, 2, 5 and 6 we can figure out the corresponding computational costs for the last steps of cubical and double-and-add ladders as

$$\mathrm{Cost}_{\mathrm{cub}_{\mathrm{last0}}}/\mathrm{Cost}_{\mathrm{dadd}_{\mathrm{last0}}} = \begin{cases} 3\mathbf{m}_k + 3\mathbf{s}_k, & \text{curves with the lack of twists, } A = 0, \\ 3\mathbf{m}_k + 3\mathbf{s}_k + k\mathbf{m}, & \text{curves with the lack of twists, } A \neq 0, \\ \mathbf{s}_k + 2d\mathbf{m}_{k/d}, & \text{curves admitting degree-}d\text{ twists.} \end{cases} \quad (8)$$

If the last bit is 1, then it follows from Algorithms 1, 2 and 5 that the cost for this iteration in a cubical ladder is

$$\mathrm{Cost}_{\mathrm{cub}_{\mathrm{last1}}} = \begin{cases} 4\mathbf{m}_k + 2\mathbf{s}_k, & \text{curves with the lack of twists,} \\ \mathbf{s}_k + 2d\mathbf{m}_{k/d}, & \text{curves admitting degree-}d\text{ twists.} \end{cases} \quad (9)$$

Nevertheless, we always need to employ double-and-add ladders since the Hamming-weights of Miller loops are relatively low. When the last bit is 1, it is unavoidable to perform a time-consuming compatible addition. Inspired by [37], we can utilize the trick of combining (level 2) cubical coordinates with (level 1) line functions to avoid performing this compatible addition and significantly improve the efficiency for curves admitting twists. We now present the computational process.

During this iteration, we aim to derive $Z_{[n]Q'+P'} = Z_{[2m+1]Q'+P'}$ from $[m]Q'+P'$ and $[m]Q'$. Since $P', Q', Q'+P'$ and $Q'-P'$ have been normalized, we have

$g_{P',Q'} = 1$, where $g_{P',Q'} \in X_{2(\mathcal{O}_{E_{A,B}})}$ is the level 2 biextension element. From [29, Eq. (8)] and since we are on level 2, it yields that

$$\begin{aligned}
g_{[n]Q',P'}^{\frac{p^k-1}{r}} &= Z_{[n]Q'+P'}^{\frac{p^k-1}{r}} \\
&= f_{n,Q'}(P')^{\frac{2(p^k-1)}{r}} \\
&= \left(f_{2m,Q'}(P') \cdot l_{[-n]Q',Q'}(P')\right)^{\frac{2(p^k-1)}{r}} \\
&= \left(g_{[2m]Q',P'} \cdot l_{[-n]Q',Q'}(P')^2\right)^{\frac{p^k-1}{r}} \\
&= \left(Z_{[2m]Q'+P'} \cdot l_{[-n]Q',Q'}(P')^2\right)^{\frac{p^k-1}{r}} .
\end{aligned}$$

Therefore, we can first execute a cubical differential addition to derive $Z_{[2m]Q'+P'}$, and then multiply it by $l_{[-n]Q',Q'}(P')^2$ to obtain $Z_{[n]Q'+P'}$. By the definition of line function and the formula for cubical differential addition, we deduce that

$$\begin{aligned}
Z_{[n]Q'+P'}^{\frac{p^k-1}{r}} &= \left(Z_{[2m]Q'+P'} \cdot (y_{P'} - y_{Q'} - \frac{y_{[-n]Q'} - y_{Q'}}{x_{[-n]Q'} - x_{Q'}}(x_{P'} - x_{Q'}))^2\right)^{\frac{p^k-1}{r}} . \\
&= \left(\left(X_{[m]Q'+P'} \cdot Z_{[m]Q'} - X_{[m]Q'} \cdot Z_{[m]Q'+P'}\right) \cdot M\right)^{\frac{2(p^k-1)}{r}} , \qquad (10)
\end{aligned}$$

where $M = (y_{P'} - y_{Q'})(x_{[n]Q'} - x_{Q'}) - (-y_{[n]Q'} - y_{Q'})(x_{P'} - x_{Q'})$. We drop the denominator $x_{P'} - x_{Q'} \in \mathbb{F}_{p^{k/d}}$ as it vanishes in the final exponentiation.

In practice, the level 1 curve coordinates $x_{[-n]Q'}$, $y_{[-n]Q'}$ can be efficiently computed. Recalled from Table 3, $[-n]Q'$ can be represented as $-\pi'(Q')$ for ate pairings, or $-\sigma' \circ \pi'^j(Q')$ for super-optimal ate pairings, whose cost can be neglected. On this basis, the computational costs for the last double-and-add step for curves admitting degree-d twists can be estimated as

$$\mathrm{Cost}_{\mathrm{dadd}_{\mathrm{last1}}} = \mathbf{s}_k + (3d+2)\mathbf{m}_{k/d}. \qquad (11)$$

Furthermore, we need to obtain values of form $\lambda^n \cdot Z_{[n]Q+P}$, $\lambda \in \mathbb{F}_q^*$ for Miller loops of super-optimal pairings. For instance, the value $Z_{[x]Q'+P'}^{xp^{10}} \cdot Z_{[x]Q'+\sigma'^{-1}(P')}$ should be computed for BW14-382 according to Table 3. A direct approach is to compute $Z_{[x]Q'+P'}$ and $Z_{[x]Q'+\sigma'^{-1}(P')}$ separately, and then execute an exponentiation x, a Frobenius endomorphism together with a multiplication to derive this value. However, since $Z_{[x]Q'+P'}$ lies in the full extension field $\mathbb{F}_{p^k}$, performing this exponentiation results in a huge number of multiplications over $\mathbb{F}_{p^k}$, which is relatively expensive. We provide a method simultaneously accomplishing this exponentiation and the computation of $Z_{[x]Q'+P'}$. Our approach relies on the following lemma in [32], showing that different choices scale the resulting cubical point by a projective factor $\lambda \in \mathbb{F}_q^*$.

Lemma 3. *[32, Lemma 2] Let* $\widetilde{P_i}'$, $\widetilde{P_i + P_j}'$ *be other choices of cubical points above* $\widetilde{P_i}$, $\widetilde{P_i + P_j}$. *Define* $Z_1(\widetilde{P})$ *to be the level 1 cubical coordinate of* $\widetilde{P}$, *where*

Z_1 is a section in biextension $X_{(\mathcal{O}_E)}$. If $\lambda_i,\ \lambda_{i,j} \in \mathbb{F}_q^*$ are such that $Z_1(\widetilde{P_i}') = \lambda_i \cdot Z_1(\widetilde{P_i})$ and $Z_1(\widetilde{P_i + P_j}') = \lambda_i\lambda_j\lambda_{i,j} \cdot Z_1(\widetilde{P_i + P_j})$, then

$$Z_1\left(\sum_{i=1}^{m}[n_i]\widetilde{P}_i'\right) = \lambda \cdot Z_1\left(\sum_{i=1}^{m}[n_i]\widetilde{P}_i\right),$$

where $\lambda := \prod_{i=1}^{m} \lambda_i^{n_i^2} \cdot \prod_{1\leq i\leq m} \lambda_{i,j}^{n_i n_j}$.

It follows from Lemma 3 that if we take $m = 2, n_1 = x, n_2 = 1, \lambda_1 = \lambda_2 = 1, \lambda_{12} = Z_1([x]\widetilde{Q' + P'})^{p^{10}}, \widetilde{P_1} = \widetilde{Q'}$ and $\widetilde{P_2} = \widetilde{\sigma'^{-1}(P')}$, then

$$Z_1([x]Q' \widetilde{+ \sigma'^{-1}(P')}') = Z_1([x]\widetilde{Q' + P'})^{xp^{10}} \cdot Z_1([x]Q' \widetilde{+ \sigma'^{-1}(P')}).$$

We now switch to level 2 with sections X and $Z = Z_1^2$. Since Lemma 3 works for every level, after scaling both $X_{Q'+\sigma'^{-1}(P')}$ and $Z_{Q'+\sigma'^{-1}(P')}$ by $Z_{[x]Q'+P'}^{p^{10}}$ we can derive $Z_{[x]Q'+P'}^{xp^{10}} \cdot Z_{[x]Q'+\sigma'^{-1}(P')}$. This gives an improvement insight. We can first compute $Z_{[x]Q'+P'}$ and store the shared cubical coordinates of $[m]Q'$ in each iteration which are also required for the computation of $Z_{[x]Q'+\sigma'^{-1}(P')}$. Then we multiply $X_{Q'+\sigma'^{-1}(P')}$, $Z_{Q'+\sigma'^{-1}(P')}$ by $Z_{[x]Q'+P'}^{p^{10}}$ and execute the second ladder utilizing the coordinates of $[m]Q'$ stored before to obtain the final result.

Recalled from Remark 2, we can mix the cubical and double-and-add ladder to speed up the iteration. According to the binary representation of the parametrized seed

$$x = [1, \underbrace{0,0,0,1,1,1,0,0,1,0,0,1}_{\text{cubical}}, \underbrace{0,0,0,0,0,0,0,0,0,1}_{\text{dadd}}]_2, \tag{12}$$

of BW14-382, we can exploit cubical ladder for the first 12 bits, and then switch to double-and-add ladder as the upcoming bits are successive 0s.

Combining the improvement for the last bit, we present Algorithm 4 to illustrate explicit computational procedure of super-optimal pairing on a Montgomery curve $E_{A,B}$ translated from the quadratic twist of BW14-382 as an example. We use tab_1 and tab_2 to store the X, Z-coordinates of cubical points $[m]Q'$ and $[m+1]Q'$ ($m \in \mathbb{N}^*$) in every iteration, respectively.

Remark 3. (1) Lines 13 and 14 of Algorithm 4 handle the last iteration before switching to double-and-add ladder. Since we do not keep track of the cubical point $[m+1]Q'$ during the double-and-add ladder, the cubical point doubling to obtain $[m+1]Q'$ need not be performed.

(2) Line 21 of Algorithm 4 corresponds to our key optimization idea in this subsection. In contrast to Lemma 3, it is further necessary for us to scale the cubical point $Q' \widetilde{- \sigma'^{-1}}(P')$, since the final result also relies on it. Consequently, compared with normal (cubical) differential addition, the differential addition with respect to $Q' \widetilde{- \sigma'^{-1}}(P')$ (Line 26 of Algorithm 4) involves one extra $\mathbf{m}_k$.

Algorithm 4 Mixed and shared ladder for super-optimal pairing for BW14-382

```
Input: The normalized cubical points $Q' = (x_{Q'}, 1)$, $P' = (x_{P'}, 1)$, $Q' + P' = (x_{Q'+P'}, 1)$, $Q' + \sigma'^{-1}(P') = (x_{Q'+\sigma'^{-1}(P')}, 1)$, the $y$-coordinates of $P'$ and $Q'$, together with the inverse coordinates $(x^{-1}_{Q'-P'}, 1)$ and $(x^{-1}_{Q'-\sigma'^{-1}(P')}, 1)$ of $Q' - P'$ and $Q' - \sigma'^{-1}(P')$. The parametrized seed $x = \sum_{i=0}^{N} n_i 2^i$.
Output: The value $Z^{xp^{10}}_{[x]Q'+P'} \cdot Z_{[x]Q'+\sigma'^{-1}(P')}$.
 1: $\mathrm{tab}_1[0] \leftarrow \texttt{cDBL}(Q'), \mathrm{tab}_2[0] \leftarrow \texttt{cDIFF}(\mathrm{tab}_1[0], Q', Q'), T \leftarrow \texttt{cDIFF}(Q' + P', Q', P')$
 2: for $i = N - 2$ to $N - 10$ do
 3:     if $n_i = 0$ then
 4:         $T \leftarrow \texttt{cDIFF}(T, \mathrm{tab}_1[N - 2 - i], P')$
 5:         $\mathrm{tab}_1[N - 1 - i] \leftarrow \texttt{cDBL}(\mathrm{tab}_1[N - 2 - i])$
 6:         $\mathrm{tab}_2[N - 1 - i] \leftarrow \texttt{cDIFF}(\mathrm{tab}_1[N - 1 - i], \mathrm{tab}_1[N - 2 - i], Q')$
 7:     else
 8:         $T \leftarrow \texttt{cDIFF}(\mathrm{tab}_2[N - 2 - i], T, Q' - P')$
 9:         $\mathrm{tab}_1[N - 1 - i] \leftarrow \texttt{cDIFF}(\mathrm{tab}_2[N - 2 - i], \mathrm{tab}_1[N - 2 - i], Q')$
10:         $\mathrm{tab}_2[N - 1 - i] \leftarrow \texttt{cDBL}(\mathrm{tab}_2[N - 2 - i])$
11:     end if
12: end for
13: $T \leftarrow \texttt{cDIFF}(\mathrm{tab}_2[N - 1 - i], T, Q' - P')$
14: $\mathrm{tab}_1[N - i] \leftarrow \texttt{cDIFF}(\mathrm{tab}_2[N - 1 - i], \mathrm{tab}_1[N - 1 - i], Q')$
15: for $i = N - 12$ to $1$ do
16:     $T \leftarrow \texttt{cDIFF}(T, \mathrm{tab}_1[N - 1 - i], P')$, $\mathrm{tab}_1[N - i] \leftarrow \texttt{cDBL}(\mathrm{tab}_1[N - 1 - i])$
17: end for
18: $M \leftarrow (y_{P'} - y_{Q'}) \cdot (x_{\sigma' \circ \pi'^4(Q')} - x_{Q'}) + (y_{\sigma' \circ \pi'^4(Q')} + y_{Q'}) \cdot (x_{P'} - x_{Q'})$
19: $M \leftarrow \big(M \cdot \big(X_T \cdot Z_{\mathrm{tab}_1[N-1]} - X_{\mathrm{tab}_1[N-1]} \cdot Z_T\big)\big)^2$, $\lambda \leftarrow M^{p^{10}}$
20: $T \leftarrow \texttt{cDIFF}(Q' + \sigma'^{-1}(P'), Q', \sigma'^{-1}(P'))$
21: $T \leftarrow (\lambda \cdot X_T, \lambda \cdot Z_T)$, $(X^{-1}_{Q'-\sigma'^{-1}(P')}, Z^{-1}_{Q'-\sigma'^{-1}(P')}) \leftarrow (\lambda \cdot x^{-1}_{Q'-\sigma'^{-1}(P')}, \lambda)$
22: for $i = N - 2$ to $N - 11$ do
23:     if $n_i = 0$ then
24:         $T \leftarrow \texttt{cDIFF}(T, \mathrm{tab}_1[N - 2 - i], \sigma'^{-1}(P'))$
25:     else
26:         $T \leftarrow \texttt{cDIFF}(\mathrm{tab}_2[N - 2 - i], T, Q' - \sigma^{-1}(P'))$
27:     end if
28: end for
29: for $i = N - 12$ to $1$ do
30:     $T \leftarrow \texttt{cDIFF}(T, \mathrm{tab}_1[N - 1 - i], \sigma'^{-1}(P'))$
31: end for
32: $M' \leftarrow (y_{\sigma'^{-1}(P')} - y_{Q'}) \cdot (x_{\pi'^4(Q')} - x_{Q'}) + (y_{\pi'^4(Q')} + y_{Q'}) \cdot (x_{\sigma'^{-1}(P')} - x_{Q'})$
33: $M' = \big(M' \cdot \big(X_T \cdot Z_{\mathrm{tab}_1[N-1]} - X_{\mathrm{tab}_1[N-1]} \cdot Z_T\big)\big)^2$
34: $\lambda \leftarrow \lambda \cdot M'$
35: return $\lambda$
```

(3) Note that we scale $[2]Q' \widetilde{+ \sigma'^{-1}}(Q')$ rather than $Q' \widetilde{+ \sigma^{-1}}(Q')$ by λ (Line 21 of Algorithm 4) since we want to first derive $\lambda^{\frac{x-1}{2}} \cdot Z_{[x-1]Q'+\sigma^{-1}(P')} \cdot M'$ and

then execute a squaring on it (Line 33 of Algorithm 4). Such an adjustment allows us to eliminate one squaring.

(4) For a Montgomery curve $E_{A,B}$ switched from the quadratic twist of BW14-382, it holds that $\sigma' \circ \pi'^4(Q') = [x]Q', Q' \in E_{A,B}(\mathbb{F}_{p^{k/d}})[r]$, leading to a speedup for the last iterations (Lines 18 and 32 of Algorithm 4).

Finally, following by Equations (5)-(11) and the cost estimates in Tables 1, 3 and 4, we can derive the computational costs for Miller loops on CP5-663, CP7-512, BW14-382, BLS15-383 and BLS21-511 via biextension technique on Montgomery model switched from these curves or their twists. For simplicity, we only provide the explicit cost calculation for BW14-382, the calculation processes for other curves are similar.

BW14-382. From the parametrized seed $x = 2^{21}+2^{18}+2^{17}+2^{16}+2^{13}+2^{10}+1$, Equations (7), (8) and (12), as well as Algorithm 4, we have

$$\begin{aligned}
\mathrm{Cost}_{\mathrm{Miller}} = {} & \underbrace{\mathrm{Cost}_{\mathrm{cub}_{\mathrm{init}}} + 3\mathbf{m}_7 + 2\mathbf{s}_7}_{\text{Line 1 of Alg. 4}} + \underbrace{5\mathrm{Cost}_{\mathrm{cub}_0} + 5\mathrm{Cost}_{\mathrm{cub}_1} - (2\mathbf{m}_7 + 2\mathbf{s}_7) + 9\mathrm{Cost}_{\mathrm{dadd}_0}}_{\text{Lines 2-17 of Alg. 4}} \\
& + \underbrace{\mathrm{Cost}_{\mathrm{dadd}_{\mathrm{last1}}} + \mathbf{f}_{14}}_{\text{Lines 18-19 of Alg. 4}} + \underbrace{2\mathbf{s}_{14} + 4\mathbf{m}_7 + 14\mathbf{m} + 3\mathbf{m}_{14}}_{\text{Lines 20-21 of Alg. 4}} \\
& + \underbrace{5(2\mathbf{s}_{14} + 4\mathbf{m}_7 + 14\mathbf{m}) + 5(2\mathbf{m}_{14} + 2\mathbf{s}_{14} + 4\mathbf{m}_7) + 9(2\mathbf{s}_{14} + 4\mathbf{m}_7 + 14\mathbf{m})}_{\text{Lines 22-31 of Alg. 4}} \\
& + \underbrace{\mathrm{Cost}_{\mathrm{dadd}_{\mathrm{last1}}} + \mathbf{m}_{14}}_{\text{Lines 32-34 of Alg. 4}} \\
= {} & 7127\mathbf{m}.
\end{aligned}$$

Table 5 summarizes the computational costs for Miller loops on the selected pairing-friendly curves above by utilizing our method (biextension approach on Montgomery models translated from selected curves or their twists) and Miller's algorithm. For the cost estimations of Miller's algorithm, we refer to [25, Eq. (1)] for curves CP5-663/CP7-512/BLS15-383/BLS21-511, and [13, Eq. (6)] for BW14-382, respectively.

Table 5. Cost comparisons in terms of $\mathbb{F}_p$-multiplications for **Miller loops** on curves CP5-663, CP7-512, BW14-382, BW15-383 and BLS21-511 by leveraging our method (biextension approach on Montgomery model converted from these selected curves or their twists) and Miller's algorithm. We fix $\mathbf{m} = \mathbf{s}$ for estimation. The fourth column illustrates the ratios of computational costs between our approach and Miller's algorithm.

Curve	This work	Miller's algorithm	Ratio
CP5-663 [25, Sec. 6.1]	5499**m**	11058**m**	49.7%
CP7-512 [25, Sec. 6.1]	6535**m**	11953**m**	54.7%
BW14-382 [13, Tab. 4]	7127**m**	7998**m**	89.1%
BLS15-383 [24, Tab. 5]	7791**m**	8316**m**	93.7%
BLS21-511 [1, Tab. 5]	10911**m**	11655**m**	93.6%

Table 5 shows that our proposed method consistently outperforms Miller's algorithm across all evaluated curves. Specifically, we achieve savings of approximately **50.3**% and **45.3**% in $\mathbb{F}_p$-multiplications for the Miller loop on CP5-663 and CP7-512, respectively, compared to the results by Guillevic et al. [25]. For BW14-382, which admits a quadratic twist, the improvement reaches **10.9**% over the approach of Dai et al. [13]. Even on curves with cubic twists, BLS15-383 and BLS21-511—our method still reduces $\mathbb{F}_p$-multiplications by **6.3**% and **6.4**% compared to the Miller's algorithm-based implementations in [24] and [1], respectively. Moreover, the biextension technique is highly amenable to parallelization, as many of its computational modules operate independently. Implementing the cubical arithmetic in a multi-threaded environment can thus further enhance its efficiency. As a result, our work significantly **broadens the applicability** of the biextension approach, strengthening its competitiveness in pairing-based cryptography.

6 Conclusion and Future Work

In this paper, we first established the systematic clarity of the technical framework, and then characterized the conversion between short Weierstrass curves and Montgomery curves. New theorems and lemmas were also proposed for effectively determine whether a short Weierstrass curve or its degree-d twist can be translated to Montgomery model. Then we considered and discussed most of the pairing-friendly curves in the literature and determined those were compatible with our acceleration (those or their twists that can be transformed to Montgomery curves). Finally we selected five curves and made concrete cost analysis. The results illustrated that our optimized approach derived savings of 50.3%, 45.3%, 10.9%, 6.3% and 6.4% in terms of $\mathbb{F}_p$-multiplications for Miller loops on curves CP5-663, CP7-512, BW14-382, BLS15-383 and BLS21-511, respectively. In conclusion, our method significantly extends the practicality of biextension technique to a wider range of pairing-friendly curves, substantially narrowing the gap between this technique and Miller's algorithm, and thereby enhancing its competitiveness as an alternative in elliptic curve cryptography. Implementing the biextension method in parallel may make it outperform Miller's algorithm on more pairing-friendly curves such as the well-known family BLS24. We leave it as future work.

Acknowledgement

Jianming Lin, Chang-An Zhao and Yuhao Zheng are supported by the National Natural Science Foundation of China (No. 12441107), Guangdong Major Project of Basic and Applied Basic Research (No. 2019B030302008), and Guangdong Provincial Key Laboratory of Information Security Technology (No. 2023B1212060026). Kaizhan Lin is supported by the National Key Research and Development Program of China (No.2022YFB2701601), Shanghai Collaborative Innovation Fund (No.XTCX-KJ-2023-54), Special Fund for Key Technologies in Blockchain of Shanghai Scientific and Technological Committee (No.23511100300).

References

1. Aranha, D.F., Fotiadis, G., Guillevic, A.: A short-list of pairing-friendly curves resistant to the Special TNFS algorithm at the 192-bit security level. IACR Communications in Cryptology **1**(3), 44 (2024)
2. Barbulescu, R., Robert, D., Sarkis, N.: Models of kummer lines and galois representations (2025)
3. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: Cimato, S., Persiano, G., Galdi, C. (eds.) Security in Communication Networks. pp. 257–267. Springer Berlin Heidelberg, Berlin, Heidelberg (2003)
4. Blake, I., Seroussi, G., Smart, N., Cassels, J.W.S.: Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series). Cambridge University Press, USA (2005)
5. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) Advances in Cryptology — CRYPTO 2001. pp. 213–229. Springer Berlin Heidelberg, Berlin, Heidelberg (2001)
6. Brezing, F., Weng, A.: Elliptic curves suitable for pairing based cryptography. Designs, Codes and Cryptography **37**(1), 133–141 (2005)
7. Cai, S., Hu, Z., Yao, Z.A., Zhao, C.A.: The elliptic net algorithm revisited. Journal of Cryptographic Engineering **14**(1), 43–55 (2024)
8. Castryck, W., Decru, T.: Csidh on the surface. In: International Conference on Post-Quantum Cryptography. pp. 111–129. Springer (2020)
9. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: 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 24. pp. 395–427. Springer (2018)
10. Chen, B., Zhao, C.A.: An improvement of the elliptic net algorithm. IEEE Transactions on Computers **65**(9), 2903–2909 (2015)
11. Cocks, C., Pinch, R.: Identity-based cryptosystems based on the weil pairing. Unpublished manuscript **170** (2001)
12. Costello, C., Smith, B.: Montgomery curves and their arithmetic - the case of large characteristic fields. J. Cryptogr. Eng. **8**(3), 227–240 (2018)
13. Dai, Y., He, D., Peng, C., Yang, Z., Zhao, C.a.: Revisiting pairing-friendly curves with embedding degrees 10 and 14. In: Chung, K.M., Sasaki, Y. (eds.) Advances in Cryptology – ASIACRYPT 2024. pp. 454–485. Springer Nature Singapore, Singapore (2025)
14. Dai, Y., Lin, K., Zhao, C., Zhou, Z.: Fast subgroup membership testings for $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ on pairing-friendly curves. Des. Codes Cryptogr. **91**(10), 3141–3166 (2023)
15. Dai, Y., Zhang, F., Zhao, C.A.: Fast hashing to g 2 on pairing-friendly curves with the lack of twists. Finite Fields Appl. **91**(C) (Oct 2023)
16. De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020. pp. 64–93. Springer International Publishing, Cham (2020)
17. El Housni, Y., Guillevic, A.: "Optimized and Secure Pairing-Friendly Elliptic Curves Suitable for One Layer Proof Composition". In: Krenn, S., Shulman, H., Vaudenay, S. (eds.) Cryptology and Network Security. pp. 259–279. Springer International Publishing, Cham (2020)

18. El Housni, Y., Guillevic, A.: Families of SNARK-Friendly 2-Chains of Elliptic Curves. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022. pp. 367–396. Springer International Publishing, Cham (2022)
19. El Mrabet, N., Guillevic, A., Ionica, S.: Efficient multiplication in finite field extensions of degree 5. In: Nitaj, A., Pointcheval, D. (eds.) Progress in Cryptology – AFRICACRYPT 2011. pp. 188–205. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
20. Fotiadis, G., Martindale, C.: Optimal TNFS-secure pairings on elliptic curves with composite embedding degree. Cryptology ePrint Archive, Paper 2019/555 (2019)
21. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of cryptology **23**, 224–280 (2010)
22. Galbraith, S.D.: Mathematics of Public Key Cryptography. Cambridge University Press, USA, 1st edn. (2012)
23. Gasnier, J., Guillevic, A.: An algebraic point of view on the generation of pairing-friendly curves. SIAM Journal on Applied Algebra and Geometry **9**(2), 456–480 (2025)
24. Guillevic, A.: A short-list of pairing-friendly curves resistant to special tnfs at the 128-bit security level. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) Public-Key Cryptography – PKC 2020. pp. 535–564. Springer International Publishing, Cham (2020)
25. Guillevic, A., Masson, S., Thomé, E.: Cocks–pinch curves of embedding degrees five to eight and optimal ate pairing computation. Des. Codes Cryptography **88**(6), 1047–1081 (Jun 2020)
26. Hess, F., Smart, N., Vercauteren, F.: The Eta Pairing Revisited. IEEE Transactions on Information Theory **52**(10), 4595–4602 (2006)
27. Joux, A.: A one round protocol for tripartite Diffie–Hellman. Journal of cryptology **17**(4), 263–276 (2004)
28. Kachisa, E.J., Schaefer, E.F., Scott, M.: Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing-Based Cryptography – Pairing 2008. pp. 126–135. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
29. Lin, J., Robert, D., Zhao, C.A., Zheng, Y.: Biextensions in pairing-based cryptography. Cryptology ePrint Archive, Paper 2025/670 (2025)
30. Miller, V.S.: The weil pairing, and its efficient calculation. Journal of cryptology **17**, 235–261 (2004)
31. Okeya, K., Kurumatani, H., Sakurai, K.: Elliptic curves with the montgomery-form and their cryptographic applications. In: Imai, H., Zheng, Y. (eds.) Public Key Cryptography. pp. 238–257. Springer Berlin Heidelberg, Berlin, Heidelberg (2000)
32. Pope, G., Reijnders, K., Robert, D., Sferlazza, A., Smith, B.: Simpler and faster pairings from the montgomery ladder. IACR Communications in Cryptology **2**(2) (2025)
33. Robert, D.: Fast pairings via biextensions and cubical arithmetic. Cryptology ePrint Archive, Paper 2024/517 (2024)
34. Silverman, J.H.: The arithmetic of elliptic curves. In: Graduate texts in mathematics (1986)
35. Stange, K.: Elliptic nets and elliptic curves. Ph.D. thesis, Brown University (2008)
36. Washington, L.C.: Elliptic curves: number theory and cryptography. Chapman and Hall/CRC (2008)

37. Zheng, Y., Lin, J., an Zhao, C.: Computing pairings on elliptic curves with embedding degree two via biextensions. Cryptology ePrint Archive, Paper 2025/1652 (2025)

A Cubical and double-and-add ladders

In this section, we present cubical and double-and-add ladders for computing the cubical coordinates $Z_{[n]Q}$ and $Z_{[n]Q+P}$. Define cDBL, cDIFF and cADD to be the functions of cubical point doubling, differential addition and compatible addition, respectively.

Algorithm 5 Cubical ladder

Input: The normalized cubical points $Q = (x_Q, 1)$, $P = (x_P, 1)$, $Q + P = (x_{Q+P}, 1)$. The scalar $n = \sum_{i=0}^{N} n_i 2^i$.
Output: The cubical points $[n]Q = (X_{[n]Q}, Z_{[n]Q})$ and $[n]Q+P = (X_{[n]Q+P}, Z_{[n]Q+P})$.

```
$R \leftarrow Q$, $S \leftarrow$ cDBL($Q$), $T \leftarrow$ cDIFF($P + Q, Q, P$)
for $i = N - 1$ to $0$ do
    $U \leftarrow$ cDIFF($S, R, Q$)
    if $n_i = 0$ then
        $T \leftarrow$ cDIFF($T, R, P$), $R \leftarrow$ cDBL($R$), $S \leftarrow U$
    else
        $T \leftarrow$ cDIFF($S, T, Q - P$), $S \leftarrow$ cDBL($S$), $R \leftarrow U$
    end if
end for
return $R$, $T$
```

B Twists of elliptic curves and the Montgomery model

In this section we investigate when twists of elliptic curves have a Montgomery model. For simplicity we assume that the characteristic is either 0 or greater than 3 throughout.

B.1 Montgomery models

Our main tool is given by the following well known result which, in view of lemma 4, is a reformulation of proposition 3 (see also [31, Proposition 1], or [2, Corollary 6.3] for many more equivalent conditions):

Proposition 7. *Let E/k be an elliptic curve (over an arbitrary field k of characteristic different from 2), and let $P \in E[2]$. Then E admit a Montgomery model $By^2 = x^3 + Ax^2 + x$ with P sent to $(0, 0)$ if and only if the self Tate pairing $e_{T,2}(P, P)$ is trivial. (We say that P is of Montgomery type.)*

Algorithm 6 Double-and-add ladder

Input: The normalized cubical points $Q = (x_Q : 1),\ P = (x_P : 1),\ Q - P = (x_{Q-P} : 1)$. The scalar $n = \sum_{i=0}^{N} n_i 2^i$.

Output: $[n]Q = (X_{[n]Q} : Z_{[n]Q})$ and $[n]Q + P = (X_{[n]Q+P} : Z_{[n]Q+P})$

```
R ← Q,  S ← cDIFF(Q, P, Q − P)
for $i = N - 1$ to 0 do
    if $n_i = 0$ then
        R ← cDBL(R)
        S ← cDIFF(S, R, P)
    else
        T ← cADD(R, Q, Q − P, S)
        R ← cDIFF(T, R, Q)
        S ← cDIFF(T, S, Q − P)
    end if
end for
return R, S
```

Lemma 4. *Let $E/k : By^2 = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve, and $P = (x_P, 0) \in E[2](k)$ be a 2-torsion point. Then a representative of the non reduced self Tate pairing in $k^*/k^{*,2}$ is given by $h'(x_P) = 3x_P^2 + 2a_2x_P + a_4$.*

Proof. A normalised function with divisor $2(P) - 2(0_E)$ is given by $\frac{x-x(P)}{B}$. Since we want to evaluate it on the point P, which is a zero, we need to adjust it by a rational uniformiser π_P at P, we pick $\pi_P = y$. So we evaluate $\frac{x-x(P)}{By^2}$ at P, which gives the value $1/h'(x_P)$ where $h(x) = x^3 + a_2x^2 + a_4x + a_6$ for the non reduced self Tate pairing. Since $h'(x_P)$ is in the same class as $1/h'(x_P)$ module squares, this concludes the proof.

Corollary 2. *Let E/k be an elliptic curve with a rational 2-torsion point P. If E admit a Montgomery model over a field extension k'/k of odd degree d, then E already admits a Montgomery model over k.*

Proof. If E admit a Montgomery model over k', there is a 2-torsion point P' whose self Tate pairing is a square in k'. This point P' is already rational in k, because d is odd and E has at least one rational 2-torsion point P, which means the other 2-torsion points are either defined over k already or over an extension of even degree. Likewise, the self Tate pairing of P' is also a square in k because d is odd. So E admits a Montgomery model over k.

If we don't suppose that E has a rational point of 2-torsion, an easy adaptation of the proof above shows that the Corollary remains true if d is prime to 6. More conceptually, this is also because the Montgomery model corresponds to a rational level $\Gamma^0(4)$ structure, and the map of stacky modular curves $X(\Gamma^0(4)) \to X(1)$ is finite étale of degree 6 over $\mathbb{Z}[1/2]$. This also shows that E/k always admit a Montgomery model over an extension k'/k of degree at most 6. If $E : By^2 = x^3 + a_2x^2 + a_4x + a_6$, one can construct k' explicitly as follows: first take k_1 a field extension (of degree at most 3) that contains a root α of $x^3 + a_2x^2 + a_4x + a_6$, and then take k' of degree at most 2 over k_1 the field that contains a square root of the self Tate pairing of $P = (\alpha, 0)$.

Definition 2. *Over a finite field $k = \mathbb{F}_q$, if the self Tate pairing $e_{T,2}(P, P)$ is non trivial, we say that P is of anti-Montgomery type, and we obtain a Montgomery- model (as introduced in [8]): $E : By^2 = x^3 + Ax^2 + cx$ where c is any fixed non quadratic residue in $\mathbb{F}_q$ (for instance one can take for c the non reduced self Tate pairing $e_{T,2}(P, P)$ [2, Theorem 6.1]).*

TODO: give cubical formulas for Montgomery- model somewhere.

B.2 Twists of elliptic curves

In this section we expand on section 2.1 to give a more detailed overview on how twists of elliptic curves are built.

If E/k is an elliptic curve, and k is not of characteristic $2, 3$, its automorphism group is given by $\mathrm{Aut}(E) = \mathrm{Aut}_{\overline{k}}(E) = \mu_n$ where $n = 2, 4$ or 6. The later cases can happen iff $j(E) = 1728$ for $n = 4$ and $j(E) = 0$ for $n = 6$. The twists of E are then classified by étale μ_n-torsors and we recall that the Kummer exact sequence combined with Hilbert 90 shows that $H^1(k, \mu_n) \simeq k^*/k^{*,n}$ where the isomorphism sends $\xi \in k^*/k^{*,n}$ to the cocycle $\sigma \in \mathrm{Gal}(\overline{k}/k) \mapsto \frac{\sigma(\xi')}{\xi'} \in \mu_n$, where ξ' is a choice of n-th root of ξ. If $k = \mathbb{F}_q$ is a finite field, evaluating the cocycle at the Frobenius π_q gives an isomorphism $H^1(\mathbb{F}_q, \mu_n) \simeq \mu_n(\overline{\mathbb{F}}_q)/(\pi_q - 1)\mu_n(\overline{\mathbb{F}}_q)$.

If E' is a twist of E, and $\gamma : E' \to E$ is an isomorphism, defined over a field extension k'/k where k' is the trivialising field of the associated μ_n-torsor, then the cocycle associate to the twist E' is given by $\sigma \mapsto \xi_\sigma \in \mu_n \simeq \mathrm{Aut}(E)$, where ξ_σ is the automorphism of E given by $\sigma\gamma\sigma^{-1}\gamma^{-1}$. More concretely, let $E : By^2 = x^3 + a_2x + a_4x + a_6$ be a Weierstrass equation for E, such that the isomorphism $\mathrm{Aut}(E) \simeq \mu_n$ is given by $\zeta \in \mu_n \mapsto \big((x, y) \mapsto (\zeta^2 x, \zeta^3 y)\big) \in \mathrm{Aut}(E)$. In particular, this means that $a_2 = a_6 = 0$ if $n = 4$ and $a_2 = a_4 = 0$ if $n = 6$. Let $\xi \in k^*/k^{*,n}$, and $\xi' \in k'$ be such that ${\xi'}^n = \xi$. Then we can define $E' : By^2 = x^3 + \frac{a_2}{\xi}x^2 + \frac{a_4}{\xi^2}x + \frac{a_6}{\xi^3}$ and $\gamma : E' \to E, (x, y) \mapsto ({\xi'}^2 x, {\xi'}^3 y)$. Then the cocycle associated to the twist E' is precisely the cocycle associated to ξ via the isomorphism $H^1(k, \mu_n) \simeq k^*/k^{*,n}$ above. As a special case, if $k = \mathbb{F}_q$, we have $\gamma\pi_{E'}\gamma^{-1} = [\pi(\xi')/\xi']\pi_E$, where π is the Frobenius.

We use a slightly non standard definition for a degree d twist

Definition 3. *A twist E' of E is said to be of degree $d \mid n$ if it is induced by a μ_d-torsor via the natural map $H^1(k, \mu_d) \to H^1(k, \mu_n)$ given by the inclusion $\mu_d \subset \mu_n$. We say that E' is of primitive (or non trivial) degree d when it is not induced by a $\mu_{d'}$-torsor for $d' < d, d' \mid d$. When speaking of degree d torsor, we often implicitly assume that it is primitive, as will be clear from context.*

Remark 4. If $\mu_n(\overline{k}) = \mu_n(k)$, the maps $H^1(k, \mu_d) \to H^1(k, \mu_n)$ are injective for $d \mid n$. In that case a degree d twist E' of E becomes isomorphic over an extension

k'/k of degree d (the extension k' that trivialize the associated μ_d-torsor), and if E' is primivie it is not isomorphic to E in any extension of smaller degree.

Note however that if k does not contains μ_n, these maps may no longer be injective. See for instance remark 5 for an example where if $\mu_4(\mathbb{F}_q) = \pm 1$, then the non trivial μ_2-torsor over $\mathbb{F}_q$ induces a trivial μ_4-torsor, hence we have a quadratic twist E' of E which is isomorphic to E already over $\mathbb{F}_q$. See also **??**.

B.3 Quadratic twists

We can also build quadratic twists as follows. If $E : By^2 = x^3 + a_2 x + a_4 x + a_6$ and $E' : B' y^2 = x^3 + a_2 x + a_4 x + a_6$ are two elliptic curves over a field k, E' is a quadratic twist whenever B'/B is not a square in k. Let $\beta \in k'$ be a square root of B, then E' is isomorphic to E via $\gamma : E' \to E, (x, y) \mapsto (x, \beta y)$. We remark that E is isomorphic to $E_0 : y^2 = x^3 + \frac{a_2}{B} x + \frac{a_4}{B^2} x + a_6$ via $(x, y) \in E_0 \mapsto (Bx, By) \in E$, so this is just a variant of the construction above. If $k = \mathbb{F}_q$, we have one non trivial quadratic twist that satisfies $\gamma \pi_{E'} \gamma^{-1} = -\pi_E$, so in particular $t_{E'} = -t_E$ where t denotes the trace. where π_E is the Frobenius

From proposition 7 we immediately get:

Corollary 3. *If E/k admit a Montgomery model, then any quadratic twist admits a Montgomery model, and conversely.*

Proof. This is immediate from the equation of the Montgomery model and the construction of the quadratic twist given above. We can also check this using proposition 7 as follows. A quadratic twist do not change the rationality of a 2-torsion point P, and lemma 4 shows that it does not change the self Tate pairing too, since the value does not depend on B.

From definition 2, the same result hold for Montgomery- models.

It remain to investigate what happens for curves with j-invariant 0 and 1728 that admit non-quadratic twists.

B.4 Elliptic curves with $j = 1728$

An elliptic curve E/k with j-invariant $j(E) = 1728$ is of the form $E_a : y^2 = x^3 - ax$. Let i be a square root of -1 (possibly over a quadratic extension k' of k). The curve E has complex multiplication (over $\overline{k}$) by $\mathbb{Z}[i]$, of discriminant -4, hence it admits an automorphism $[i] : (x, y) \mapsto (-x, -iy)$. If $k = \mathbb{F}_p$, we remark that E_a is ordinary iff -1 is a square, i.e. iff $p \equiv 1 \pmod 4$, iff $\mu_4 \subset \mathrm{Aut}_{\mathbb{F}_p}(E)$.

Let $a_1, a_2 \in k$, then E_{a_2} is the twist of E_{a_1} corresponding to the class $\frac{a_1}{a_2} \in k^*/k^{*,4}$. Let α be a fourth root of a_1/a_2, then $\gamma : E_{a_2} \to E_{a_1} : (x, y) \mapsto (\alpha^2 x, \alpha^3 y)$ is an isomorphism. If a_1/a_2 is a fourth power then both curves are isomorphic, if a_1/a_2 is a square both curves are quadratic twists, and lastly if a_1/a_2 is not a square both curves are quartic twists. We note that there are two quartic twists, which are quadratic twists of each others.

If $k = \mathbb{F}_q$ and E' is the quartic twist of E such that $\gamma \pi_{E'} \gamma^{-1} = [i] \pi_E$, then $\pi' = \gamma \pi_{E'} \gamma^{-1}$ corresponds to $i\pi$ in $\mathrm{End}(E)$. Writing $\pi = a + fi$, where f is the conductor of $\mathbb{Z}[\pi]$ in $\mathbb{Z}[i]$ (so that $t^2 - 4q = -4f^2$), and the trace of E is given by $t = 2a$, then $i\pi = ia - f$ has trace $-2f$. Likewise, the trace associated to the twist corresponding to $[-i]$ is $2f$ (see also [26, Proposition 2]).

Since we are interested in ordinary curves over finite fields in this paper, in the reminder of this section we assume that -1 is a square in $\mathbb{F}_q$.

Theorem 1. *Assume that -1 is a square in $\mathbb{F}_q$ (i.e. $q \equiv 1 \pmod 4$). Let $E_a : y^2 = x^3 - ax$ be an elliptic curve over $\mathbb{F}_q$. Then E_a admits a Montgomery model iff a is a square in $\mathbb{F}_q$, iff all points of 2-torsion are rational, iff $4 \mid \#E_a(\mathbb{F}_q)$, iff $t \equiv 2 \pmod 4$ where t is the trace of the Frobenius.*

Proof. The point $P = (0, 0)$ is of 2-torsion and its non reduced self pairing is $e_{T,2}(P, P) = -a$. Since -1 is a square, this self pairing is trivial iff a is a square, if all points of 2-torsion are rational. This implies that $4 \mid \#E_a(\mathbb{F}_q)$. Conversely, if $4 \mid \#E_a(\mathbb{F}_q)$ then either all points of 2-torsion are rational, or there is a 4-torsion point P' above P. In both case this imply that the self Tate pairing of P is trivial, hence P is of Montgomery type. The last equivalence comes from the fact that $\#E_a(\mathbb{F}_q) = q + 1 - t$ and that $4 \mid q - 1$ since -1 is a square.

Since E_a always admit a point of 2-torsion $P = (0, 0)$, it always admit either a Montgomery or a Montgomery- model. Note that if P is of Montgomery type, or equivalently if $a = \alpha^2$ is a square in $\mathbb{F}_q$, then the other 2-torsion points $(\pm\alpha, 0)$ have non reduced self Tate pairing $3\alpha^2 - a = 2a$. These two points are of Montgomery type iff 2 is a square in $\mathbb{F}_q$ (i.e. iff $q \equiv 1, 7 \pmod 8$).

Corollary 4. *Let $E_{a'}$ be a quartic twist of E_a. Then $E_{a'}$ admits a Montgomery model iff E_a does not. And if E_a has a Montgomery model, then $E_{a'}$ has a Montgomery- model, and the converse holds if 2 is a square in $\mathbb{F}_q$.*

Proof. Indeed, by construction of the quartic twist, a' is a square iff a is not a square.

Corollary 5. *The elliptic curve $E : y^2 = x^3 - ax/\mathbb{F}_q$ with trace t has a quartic twist E' over $\mathbb{F}_{q^k}$ which admits a Montgomery model iff $t \equiv 0 \pmod 4$ and k is odd.*

Proof. By theorem 1 E' has a Montgomery model iff a is not a square in $\mathbb{F}_{q^k}$, which is equivalent to k being odd and a not a square in $\mathbb{F}_q$, and the later condition is equivalent to $t \equiv 0 \pmod 4$.

Remark 5. If -1 is not a square in $\mathbb{F}_q$, one needs to be careful that since $\pi_q i = -i$, we have $H^1(\mathbb{F}_q, \mu_4) \simeq \mu_4/\{\pm 1\}$. In particular the quadratic twist E' of E is isomorphic to E over $\mathbb{F}_q$. Another way to see that is that if $\gamma : E' \to E$ is the twisting isomorphism over $\mathbb{F}_{q^2}$, then $[i] \circ \gamma$ is rational, because the Frobenius conjugation acts by -1 on both. Likewise, both quartic twists are isomorphic over $\mathbb{F}_q$ (but are still non isomorphic quadratic twists over $\mathbb{F}_{q^2}$).

The point $P = (0, 0) \in E_a$ is of Montgomery type iff a is not a square in $\mathbb{F}_q$. If $a = \alpha^2$ is a square, E_a has for other two torsion points $(\pm\alpha, 0)$, whose non reduced self Tate pairing is $3\alpha^2 - a = 2a$. So in that case E_a has a Montgomery model iff 2 is a square in $\mathbb{F}_q$.

Remark 6. The results of this section are mostly an immediate consequence of the following description of the full stacky Kummer line $[E/\mu_4]$ (we distinguish the full Kummer line from the standard Kummer line $[E/\mu_2]$). Here $[E/\mu_4]$ denotes the stacky quotient, while E/μ_4 denotes the geometric scheme quotient, this is also the coarse space associated to $[E/\mu_4]$. Indeed, the map $E \to \operatorname{Spec} k$ induces a map $[E/\mu_4] \to B\mu_4$ where $B\mu_4 = [\operatorname{Spec} k/\mu_4]$ is the classifying torsor. Now the universal torsor $i : \operatorname{Spec} k \to B\mu_4$ allows to recover E by pullback $E = [E/\mu_4] \times_{B\mu_4} \operatorname{Spec} k$. By definition, a μ_4-torsor then corresponds to a map $i' : \operatorname{Spec} k \to B\mu_4$, and the pullback of $[E/\mu_4]$ by i' then give the associated twist E'. See [2, Appendix A]) for more details. In particular, the Galois action on the points of E' is completely characteristed by the Galois action on $[E/\mu_4]$ and the map to $B\mu_4$ associated to E'.

The projection map $E \to [E/\mu_4]$ factorizes as $E \to [E/\mu_2] \to [E/\mu_4]$ and the automorphism group μ_4 descends to the automorphism group μ_2 on the standard Kummer line $[E/\mu_2]$, at the level of coarse spaces the automorphism $[i]$ on E induces $x \mapsto -x$ on $K = E/\pm 1 \simeq \mathbb{P}^1$, and the map $E/\mu_2 \to E/\mu_4$ is given by $x \mapsto x^2$. In particular the Kummer line admits quadratic twists (which lifts to quartic twists of E). The action of μ_2 on K is free except at $x = 0, \infty$, so $[K/\mu_2]$ is the stacky projective line where all points are standard (representable), except the point $x = 0, \infty$ who have $B\mu_2$ as residual gerbe. Since $[E/\mu_2]$ is a stacky projective line whose stacky points (with associated residual gerbe $B\mu_2$) are given by the x-coordinates of the point of 2-torsion (and 0_E), it is easy to see that when $E = E_a$, $[E_a/\mu_4]$ is then the stacky projective line with stacky points given by $x = 0, \infty$, whose residual gerbes are $B\mu_4$, and $x = a$, whose residual gerbe is $B\mu_2$.

B.5 Elliptic curves with $j = 0$

An elliptic curve E/k with j-invariant $j(E) = 0$ is of the form $E_b : y^2 = x^3 - b$. Let j be a third root of 1 (possibly over a cubic extension k' of k). The curve E has complex multiplication (over $\overline{k}$) by $\mathbb{Z}[j]$, of discriminant -3, hence it admits an automorphism $[-j] : (x, y) \mapsto (j^2 x, -y)$. If $k = \mathbb{F}_p$, we remark that E_b is ordinary iff 1 is a non trivial cube, i.e. iff $p \equiv 1 \pmod 3$, iff $\mu_6 \subset \operatorname{Aut}_{\mathbb{F}_p}(E)$.

Let $b_1, b_2 \in k$, then E_{b_2} is the twist of E_{b_1} corresponding to the class $\frac{b_1}{b_2} \in k^*/k^{*,6}$. Let β be a sixth root of b_1/b_2, then $\gamma : E_{b_2} \to E_{b_1} : (x, y) \mapsto (\beta^2 x, \beta^3 y)$ is an isomorphism, and if $k = \mathbb{F}_q$, $\gamma \pi_{E_{b_2}} \gamma^{-1} = [\pi(\beta)/\beta]\pi_{E_{a_1}}$. If b_1/b_2 is a sixth power then both curves are isomorphic, if b_1/b_2 is a cube (but not a square) both curves are quadratic twists, if b_1/b_2 is a square (but not a cube) both curves are cubic twists, and lastly if b_1/b_2 is neither both curves are sextic twists. We note that the two sextic twists of E are quadratic twists of the two cubic twists of E.

If $k = \mathbb{F}_q$ and E' is the cubic twist of E such that $\gamma \pi_{E'} \gamma^{-1} = [j]\pi_E$, then $\pi' = \gamma \pi_{E'} \gamma^{-1}$ corresponds to $j\pi$ in $\operatorname{End}(E)$. Writing $\pi = a + fj$, where f is the conductor of $\mathbb{Z}[\pi]$ in $\mathbb{Z}[j]$ (so that $t^2 - 4q = -3f^2$), then the trace of E is given by $t = 2a - f$, and $j\pi = ja + fj^2$ has trace $-a - f = (-t - 3f)/2$. Likewise, the traces associated to the twists corresponding to $[j^2], [-j], [-j^2]$ is $(-t + 3f)/2, (t - 3f)/2, (t + 3f)/2$ respectively (see also [26, Proposition 2]).

In the reminder of this section we assume that 1 is a non trivial cube in $\mathbb{F}_q$.

Theorem 2. *Assume that* 1 *is a non trivial cube in* $\mathbb{F}_q$ *(i.e.* $q \equiv 1 \pmod 3$*). Let* $E_b : y^2 = x^3 - b$ *be an elliptic curve over* $\mathbb{F}_q$*. Then* E_b *admits a Montgomery model iff* b *is a cube and* 3 *is a square in* $\mathbb{F}_q$*, iff* $t \equiv 2 \pmod 4$ *where* t *is the trace of the Frobenius.*

Proof. The curve E_b admits a point of 2-torsion iff $b = \beta^3$ is a cube in $\mathbb{F}_q$. Then $P = (\beta, 0)$ has for non reduced self Tate pairing $3\beta^2$, which is a square iff 3 is a square in $\mathbb{F}_q$ (equivalently by quadratic reciprocity, $q \equiv 1 \pmod 4$; recall that we assume that $q \equiv 1 \pmod 3$ already). If both conditions are satisfied, then $4 \mid \#E(\mathbb{F}_q) = q + 1 - t$ since the 2-torsion is rational, and this implies $t \equiv 2 \pmod 4$. Conversely, if $t \equiv 2 \pmod 4$, then $2 \mid \#E(\mathbb{F}_q) = q + 1 - t$, so there is a rational point of 2-torsion, so all points of 2-torsion are rational, so $4 \mid \#E(\mathbb{F}_q) = q + 1 - t$, and $q \equiv 1 \pmod 4$.

Recall that we assume that 1 is a non trivial cube in $\mathbb{F}_q$.

Corollary 6. *If* 3 *is not a square in* $\mathbb{F}_q$*, none of the twists of* E_b *admit a Montgomery model. If* 3 *is a square in* $\mathbb{F}_q$*, then* E_b *admits a Montgomery model iff* b *is a cube, iff all the other cubic (or sextic) twists do not admit a Montgomery model.*

If 3 *is not a square in* $\mathbb{F}_q$*,* E_b *admits a Montgomery- model iff* b *is a cube, iff all the other cubic (or sextic) twists do not admit a Montgomery- model. If* 3 *is not a square in* $\mathbb{F}_q$*, none of the twists of* E_b *admit a Montgomery- model.*

Proof. If 3 is a square, E_b admits a Montgomery model iff the 2-torsion is rational iff b is a cube. But among the three cubic twists $E_b, E_{b'}, E_{b"}$ of E_b, exactly one of them satisfy this condition. The proof for the case of the Montgomery- model is similar.

Corollary 7. *The elliptic curve* $E : y^2 = x^3 - b/\mathbb{F}_q$ *with trace* t *has a (non trivial) cubic twist* E' *over* $\mathbb{F}_{q^k}$ *which admits a Montgomery model iff* $t \equiv 1 \pmod 2$*,* $k \not\equiv 0 \pmod 3$ *and* $t_k \equiv \pm f_k \pmod 8$ *where* t_k *is the trace of the Frobenius* π_k *of* E *over* $\mathbb{F}_{q^k}$ *and* $f_k = t_k^2 - 4q^k$ *is the conductor of* $\mathbb{Z}[\pi_k]$ *in* $\mathbb{Z}[j]$*.*

In this case $\#E'(\mathbb{F}_{q^k}) = q^k + 1 - t'_k = q^k + 1 + (t_k \pm 3f)/2$*, and its quadratic twist* E' *(a sextic twist of* E*) satisfies* $\#E"(\mathbb{F}_{q^k}) = q^k + 1 + t'_k = q^k + 1 - (t_k \pm 3f)/2$*. In particular, if* $r > 3$ *is a prime dividing* $\#E(\mathbb{F}_{q^k})$*, it also divides* $\#E'(\mathbb{F}_{q^k})$ *(resp.* $\#E"(\mathbb{F}_{q^k})$*) iff* $t_k \equiv \pm f \pmod r$ *(resp.* $t_k \equiv \mp 3f \pmod r$*).*

Proof. If t_k is even, then E has a rational 2-torsion point over $\mathbb{F}_{q^k}$, hence the full 2-torsion is rational over $\mathbb{F}_{q^k}$. Likewise if $k \equiv 0 \pmod 3$, b is a cube over $\mathbb{F}_{q^k}$ and E has full rational 2-torsion over $\mathbb{F}_{q^k}$. In both case, either 3 is a square in $\mathbb{F}_{q^k}$ so E has a Montgomery model by theorem 2, and then none of its (non trivial) cubic twist have a Montgomery model; or 3 is not a square and then no twists can have a Montgomery model. So if E' has a Montgomery model. t_k is odd and $k \not\equiv 0 \pmod 3$. This implies that t is odd, because if $2 \mid \#E(\mathbb{F}_q)$, $2 \mid \#E(\mathbb{F}_{q^k})$.

By theorem 2, t'_k, the trace of E' over $\mathbb{F}_{q^k}$ satisfies $t'_k \equiv 2 \pmod 4$. Assume that E' is the twist corresponding to $[j]$. Then we know that $t'_k = (-t_k - 3f)/2$, where $-3f^2 = t_k^2 - 4q^k$, so $-t_k - 3f \equiv 4 \pmod 8$. Since t_k is odd, f is odd, so $-4f - 4 \equiv 0 \pmod 8$ and $t_k \equiv f \pmod 8$. A similar computation shows that if E' corresponds to $[-j]$, then $t_k \equiv -f \pmod 8$.

Conversely if t is odd and $k \not\equiv 0 \pmod 3$, then b is not a cube in $\mathbb{F}_q$ and neither in $\mathbb{F}_{q^k}$, so t_k is odd, f is odd, and then $t_k \equiv \pm f \pmod 8$ implies $t'_k \equiv 2 \pmod 8$ for E' the cubic twist corresponding to $[\pm j]$.

The corresponding result for sextic twists follows by corollary 3 since they are quadratic twists of the cubic twists.

Remark 7. If 1 is not a (non trivial) cube in $\mathbb{F}_q$, then b admits a unique rational root $b = \beta^3$ in $\mathbb{F}_q$, and E_b has a Montgomery model over $\mathbb{F}_q$ iff 3 is a square. In this case all twists of E have a Montgomery model. This is because $H^1(\mathbb{F}_q, \mu_6) = \mu_6/(j)$ (see also remark 5), so the cubic twists are actually isomorphic to E over $\mathbb{F}_q$, and the sextic twists are isomorphic to the quadratic twist of E over $\mathbb{F}_q$.

Remark 8. As in remark 6, we can build the stacky general Kummer line $[E/\mu_6]$. The automorphism group μ_6 descends to the automorphism group μ_3 on $[E/\mu_2]$, where the automorphism $[-j]$ on E induces $x \mapsto j^2 x$ on the coarse space $K = E/\mu_2 \simeq \mathbb{P}^1$, and the map $E/\mu_2 \to E/\mu_4$ is given by $x \mapsto x^3$. In particular the Kummer line has cubic twists, and $[K/\mu_3]$ has for stacky points $x = 0, \infty$ with residual gerbe $B\mu_3$, and if $E = E_b$, $[E_b/\mu_6]$ has for stacky points $x = \infty$ with residual gerbe $B\mu_6$, $x = 0$ with residual gerbe $B\mu_3$, and $x = b$ with residual gerbe $B\mu_2$. (We remark that the pullback of $x = 0$ to E corresponds to the orbit under μ_6 of the only two points $\pm P$ invariant by $[j]$, and that P is of 3-torsion on E, because $[j]P = P$ implies that $3P = 0$.)