Twisted $\boldsymbol{\mu_4}$-normal form for elliptic curves

David Kohel

Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France
`David.Kohel@univ-amu.fr`

Abstract. We introduce the twisted $\boldsymbol{\mu_4}$-normal form for elliptic curves, deriving in particular addition algorithms with complexity $9\mathbf{M} + 2\mathbf{S}$ and doubling algorithms with complexity $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$ over a binary field. Every ordinary elliptic curve over a finite field of characteristic 2 is isomorphic to one in this family. This improvement to the addition algorithm, applicable to a larger class of curves, is comparable to the $7\mathbf{M}+2\mathbf{S}$ achieved for the $\boldsymbol{\mu_4}$-normal form, and replaces the previously best known complexity of $13\mathbf{M} + 3\mathbf{S}$ on López-Dahab models applicable to these twisted curves. The derived doubling algorithm is essentially optimal, without any assumption of special cases. We show moreover that the Montgomery scalar multiplication with point recovery carries over to the twisted models, giving symmetric scalar multiplication adapted to protect against side channel attacks, with a cost of $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}_t + 2\mathbf{m}_c$ per bit. In characteristic different from 2, we establish a linear isomorphism with the twisted Edwards model over the base field. This work, in complement to the introduction of $\boldsymbol{\mu_4}$-normal form, fills the lacuna in the body of work on efficient arithmetic on elliptic curves over binary fields, explained by this common framework for elliptic curves in $\boldsymbol{\mu_4}$-normal form over a field of any characteristic. The improvements are analogous to those which the Edwards and twisted Edwards models achieved for elliptic curves over finite fields of odd characteristic and extend $\boldsymbol{\mu_4}$-normal form to cover the binary NIST curves.

1 Introduction

Let E be an elliptic curve with given embedding in $\mathbb{P}^r$ and identity O. The addition morphism $\mu : E \times E \to E$ is uniquely defined by the pair (E, O) but the homogeneous polynomial maps which determine μ are not unique. Let $x = (X_0, \dots, X_r)$ and $y = (Y_0, \dots, Y_r)$ be the coordinate functions on the first and second factors, respectively. We recall that an *addition law* (cf. [14]) is a bihomogenous polynomial map $\mathfrak{s} = (p_0(x, y), \dots, p_r(x, y))$ which determines μ outside of the common zero locus $p_0(x, y) = \dots = p_r(x, y) = 0$. Such polynomial addition laws play an important role in cryptography since they provide a means of carrying out addition on E without inversion in the base field.

In this work we generalize the algorithmic analysis of the $\boldsymbol{\mu_4}$-normal form to include twists. The principal improvements are for binary curves, but we are able to establish these results for a family which has good reduction and efficient arithmetic over any field k, and in fact any ring. We adopt the notation $\mathbf{M}$ and $\mathbf{S}$

for the complexity of multiplication and squaring in k, and $\mathbf{m}$ for multiplication by a fixed constant that depends (polynomially) only on curve constants.

In Section 2 we introduce a hierarchy of curves in $\boldsymbol{\mu}_4$-normal form, according to the additional 4-level structure parametrized. In referring to these families of curves, we give special attention to the so-called split and semisplit variants, while using the generic term $\boldsymbol{\mu}_4$-normal form to refer to any of the families. In particular their isomorphisms and addition laws are developed. In the specialization to finite fields of characteristic 2, by extracting square roots, we note that any of the families can be put in split $\boldsymbol{\mu}_4$-normal form, and the distinction is only one of symmetries and optimization of the arithmetic. In Section 3, we generalize this hierarchy to quadratic twists, which, in order to hold in characteristic 2 are defined in terms of Artin–Schreier extensions. The next two sections deal with algorithms for these families of curves over binary fields, particularly, their addition laws in Section 4 and their doubling algorithms in Section 6. These establish the main complexity results of this work — an improvement of the best known addition algorithms on NIST curves to $9\mathbf{M} + 2\mathbf{S}$ coupled with a doubling algorithm of $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$. These improvements are summarized in the following table of complexities (see Section 8 for details).

Curve model	Doubling	Addition	%	NIST
Lambda coordinates	$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}$	$11\mathbf{M} + 2\mathbf{S}$	100%	✓
Binary Edwards ($d_1 = d_2$)	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$16\mathbf{M} + 1\mathbf{S} + 4\mathbf{m}$	50%	✗
López-Dahab ($a_2 = 0$)	$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{m}$	$14\mathbf{M} + 3\mathbf{S}$	50%	✗
López-Dahab ($a_2 = 1$)	$2\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$	$13\mathbf{M} + 3\mathbf{S}$	50%	✓
Twisted $\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$9\mathbf{M} + 2\mathbf{S}$	100%	✓
$\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$7\mathbf{M} + 2\mathbf{S}$	50%	✗

To complete the picture, we prove in Section 7 that the Montgomery endomorphism and resulting complexity, as described in Kohel [11] carry over to the twisted families, which allows for an elementary and relatively efficient symmetric algorithm for scalar multiplication which is well-adapted to protecting against side-channel attacks. While the most efficient arithmetic is achieved for curves for which the curve coefficients are constructed such that the constant multiplications are negligible, these extensions to twists provide efficient algorithms for backward compatibility with binary NIST curves.

2   The $\boldsymbol{\mu}_4$-normal form

In this section we recall the definition and construction of the family of elliptic curves in (split) $\boldsymbol{\mu}_4$-normal form. The notion of a canonical model of level n was introduced in Kohel [9] as an elliptic curve C/k in $\mathbb{P}^{n-1}$ with subgroup scheme $G \cong \boldsymbol{\mu}_n$ (a k-rational subgroup of the n-torsion subgroup $C[n]$ whose points split in $k[\zeta_n]$, where ζ_n is an n-th root of unity in $\bar{k}$) such that for $P = (x_0 : x_1 : \cdots : x_{n-1})$ a generator S of G acts by $P + S = (x_0 : \zeta_n^1 x_1 : \cdots : \zeta_n^{n-1} x_{n-1})$. If, in addition, there exists a rational n-torsion point T such that $C[n] = \langle S, T \rangle$, we say that the model is *split* and impose the condition that T acts by a cyclic

coordinate permutation. Construction of the special cases $n = 4$ and $n = 5$ were treated as examples in Kohel [9], and the present work is concerned with a more in depth study of the former.

The Edwards curve $x^2 + y^2 = 1 + dx^2 y^2$ embeds in $\mathbb{P}^3$ (by $(1 : x : y : xy)$ as the elliptic curve

$$X_1^2 + X_2^2 = X_0^2 + dX_3^2, \ X_0 X_3 = X_1 X_2,$$

with identity $O = (1 : 0 : 1 : 0)$. Such a model was studied by Hisil et al. [8], as extended Edwards coordinates, and admits the fastest known arithmetic on such curves. The twist by a, in extended coordinates, is the twisted Edwards curve

$$aX_1^2 + X_2^2 = X_0^2 + adX_3^2, \ X_0 X_3 = X_1 X_2$$

with parameters (a, ad). For the special case $(a, ad) = (-1, -16r)$, the change of variables

$$(X_0 : X_1 : X_2 : X_3) \mapsto (X_0, X_1 + X_2, 4X_3, -X_1 + X_2).$$

has image the canonical model of level 4 above. The normalization to have good reduction at 2 (by setting $d = 16r$ and the coefficient of X_3) as well as the following refined hierarchy of curves appears in Kohel [10], and the subsequent article [11] treated only the properties of this hierarchy over fields of characteristic 2.

Definition 1. *An elliptic curve in* $\boldsymbol{\mu}_4$*-normal form is a genus one curve in the family*

$$X_0^2 - rX_2^2 = X_1 X_3, \ X_1^2 - X_3^2 = X_0 X_2$$

with base point $O = (1 : 1 : 0 : 1)$. *An elliptic curve in* semisplit $\boldsymbol{\mu}_4$*-normal form is a genus one curve in the family*

$$X_0^2 - X_2^2 = X_1 X_3, \ X_1^2 - X_3^2 = sX_0 X_2,$$

with identity $O = (1 : 1 : 0 : 1)$, *and an elliptic curve is in* split $\boldsymbol{\mu}_4$*-normal form if it takes the form*

$$X_0^2 - X_2^2 = c^2 X_1 X_3, \ X_1^2 - X_3^2 = c^2 X_0 X_2.$$

with identity $O = (c : 1 : 0 : 1)$.

Setting $s = c^4$, the transformation

$$(X_0 : X_1 : X_2 : X_3) \mapsto (X_0 : cX_1 : cX_2 : X_3)$$

maps the split $\boldsymbol{\mu}_4$-normal form to semisplit $\boldsymbol{\mu}_4$-normal form with parameter s, and setting $r = 1/s^2$, the transformation

$$(X_0 : X_1 : X_2 : X_3) \mapsto (X_0 : X_1 : sX_2 : X_3)$$

maps the semisplit $\boldsymbol{\mu}_4$-normal form to $\boldsymbol{\mu}_4$-normal form with parameter r. The names for the $\boldsymbol{\mu}_4$-normal forms of a curve C/k in $\mathbb{P}^3$, recognize the existence of $\boldsymbol{\mu}_4$ as a k-rational subgroup scheme of $C[4]$, and secondly, its role as defining the embedding class of C in $\mathbb{P}^3$, namely it is cut out by the hyperplane $X_2 = 0$ in $\mathbb{P}^3$.

Lemma 2. *Let C be a curve in $\boldsymbol{\mu}_4$-normal form, semi-split $\boldsymbol{\mu}_4$-normal form, or split $\boldsymbol{\mu}_4$-normal form, with identity $(e, 1, 0, 1)$. For any extension containing a square root i of -1, the point $S = (e : i : 0 : -i)$ is a point of order 4 acting by the coordinate scaling $(x_0 : x_1 : x_2 : x_3) \mapsto (x_0 : ix_1 : -x_2 : -ix_3)$. In particular,*

$$\{(e : 1 : 0 : 1), (e : i : 0 : -i), (e : -1 : 0 : -1), (e : i : 0 : -i)\},$$

is a subgroup of $C[4] \subseteq C(\bar{k})$.

The semisplit $\boldsymbol{\mu}_4$-normal form with square parameter $s = t^2$ admits a 4-torsion point $(1 : t : 1 : 0)$ acting by scaled coordinate permutation. After a further quadratic extension $t = c^2$, the split $\boldsymbol{\mu}_4$-normal form admits the constant group scheme $\mathbb{Z}/4\mathbb{Z}$ acting by signed coordinate permutation.

Lemma 3. *Let C/k be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form with identity $O = (c : 1 : 0 : 1)$. Then $T = (1 : c : 1 : 0)$ is a point in $C[4]$, and translation by T induces the signed coordinate permutation*

$$(x_0 : x_1 : x_2 : x_3) \longmapsto (x_3 : x_0 : x_1 : -x_2)$$

on C.

This gives the structure of a group $C[4] \cong \boldsymbol{\mu}_4 \times \mathbb{Z}/4\mathbb{Z}$, whose generators S and T are induced by the matrix actions

$$A(S) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix} \text{ and } A(T) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

on C such that $A(S)A(T) = iA(T)A(S)$. We can now state the structure of addition laws for the split $\boldsymbol{\mu}_4$-normal form and its relation to the torsion action described above.

Theorem 4. *Let C be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form:*

$$X_0^2 - X_2^2 = c^2\, X_1 X_3, \ X_1^2 - X_3^2 = c^2\, X_0 X_2, \ O = (c : 1 : 0 : 1),$$

and set $U_{jk} = X_j Y_k$. A complete basis of addition laws of bidegree $(2, 2)$ is given by:

$$\begin{aligned}
\mathfrak{s}_0 &= (U_{13}^2 - U_{31}^2, \ c(U_{13}U_{20} - U_{31}U_{02}), \ U_{20}^2 - U_{02}^2, \ c(U_{20}U_{31} - U_{13}U_{02})), \\
\mathfrak{s}_1 &= (c(U_{03}U_{10} + U_{21}U_{32}), \ U_{10}^2 - U_{32}^2, \ c(U_{03}U_{32} + U_{10}U_{21}), \ U_{03}^2 - U_{21}^2), \\
\mathfrak{s}_2 &= (U_{00}^2 - U_{22}^2, \ c(U_{00}U_{11} - U_{22}U_{33}), \ U_{11}^2 - U_{33}^2, \ c(U_{00}U_{33} - U_{11}U_{22})), \\
\mathfrak{s}_3 &= (c(U_{01}U_{30} + U_{12}U_{23}), \ U_{01}^2 - U_{23}^2, \ c(U_{01}U_{12} + U_{23}U_{30}), \ U_{30}^2 - U_{12}^2).
\end{aligned}$$

The exceptional divisor of the addition law $\mathfrak{s}_\ell$ is $\sum_{k=0}^{3} \Delta_{kS+\ell T}$, where S and T are the 4-torsion points $(c : i : 0 : -i)$ and $(1 : c : 1 : 0)$, and the divisors $\sum_{k=0}^{3}(kS+\ell T)$ are determined by $X_{\ell+2} = 0$. In particular, any pair of the above addition laws provides a complete system of addition laws.

Proof. This appears as Theorem 44 of Kohel [9] for the $\boldsymbol{\mu}_4$-normal form, subject to the scalar renormalizations indicated above. The exceptional divisor is a sum of four curves of the form Δ_P by Theorem 10 of Kohel [9], and the points P can be determined by intersection with $H = C \times \{O\}$ using Corollary 11 of Kohel [9]. Taking the particular case $\mathfrak{s}_2$, we substitute $(Y_0, Y_1, Y_2, Y_3) = (c, 1, 0, 1)$ to obtain $(U_{00}, U_{11}, U_{22}, U_{33}) = (cX_0, X_1, 0, X_3)$, and hence

$$(U_{00}^2 - U_{22}^2, \ U_{00}U_{11} - U_{22}U_{33}, \ U_{11}^2 - U_{33}^2, \ U_{00}U_{33} - U_{22}U_{11}),$$

which equals

$$(c^2 X_0^2, cX_0 X_1, X_1^2 - X_3^2, cX_0 X_3) = (c^2 X_0^2, cX_0 X_1, c^2 X_0 X_2, cX_0 X_3).$$

These coordinate functions cuts out the divisor $X_0 = 0$ with support on the points $kS + 2T$, $0 \le k < 4$, where $2T = (0 : -1 : -c : 1)$. The final statement follows since the exceptional divisors are disjoint. $\qquad\square$

The above basis of addition laws can be generated by any one of the four, by means of signed coordinate permutation on input and output determined by the action of the 4-torsion group. Denote translation by S and T by σ and τ, respectively, given by the coordinate scalings and permutations

$$\sigma(X_0 : X_1 : X_2 : X_3) = (X_0 : iX_1 : -X_2 : -iX_3),$$
$$\tau(X_0 : X_1 : X_2 : X_3) = (X_3 : X_0 : X_1 : -X_2),$$

as noted above. The set $\{\mathfrak{s}_0, \mathfrak{s}_1, \mathfrak{s}_2, \mathfrak{s}_3\}$ forms a basis of eigenvectors for the action of σ. More precisely for all (j, k, ℓ), we have

$$\mathfrak{s}_\ell = (-1)^{j+k+\ell} \sigma^{-j-k} \circ \mathfrak{s}_\ell \circ (\sigma^j \times \sigma^k).$$

Then τ, which projectively commutes with σ, acts by a scaled coordinate permutation

$$\mathfrak{s}_{\ell-j-k} = \tau^{-j-k} \circ \mathfrak{s}_\ell \circ (\tau^j \times \tau^k),$$

consistent with the action on the exceptional divisors (see Lemma 31 of Kohel [9]).

Consequently, the complexity of evaluation of any of these addition laws is computationally equivalent, since they differ only by a signed coordinate permutation on input and output.

Corollary 5. *Let C be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form. There exist algorithms for addition with complexity $9\mathbf{M} + 2\mathbf{m}$ over any ring, $8\mathbf{M} + 2\mathbf{m}$ over a ring in which 2 is a unit, and $7\mathbf{M} + 2\mathbf{S} + 2\mathbf{m}$ over a ring of characteristic 2.*

Proof. We determine the complexity of an algorithm for the evaluation of the addition law $\mathfrak{s}_2$:

$$(Z_0, Z_1, Z_2, Z_3) = (U_{00}^2 - U_{22}^2,\ c(U_{00}U_{11} - U_{22}U_{33}),\ U_{11}^2 - U_{33}^2,\ c(U_{00}U_{33} - U_{11}U_{22})\,),$$

recalling that each of the given addition laws in the basis has equivalent evaluation. Over a general ring, we make use of the equalities:

$$Z_0 = U_{00}^2 - U_{22}^2 = (U_{00} - U_{22})(U_{00} + U_{22}),$$
$$Z_2 = U_{11}^2 - U_{33}^2 = (U_{11} - U_{33})(U_{11} + U_{33}),$$

and

$$Z_1 + Z_3 = c(U_{00}U_{11} - U_{22}U_{33}) + c(U_{00}U_{33} - U_{22}U_{11}) = c(U_{00} - U_{22})(U_{11} + U_{33}),$$
$$Z_1 - Z_3 = c(U_{00}U_{11} - U_{22}U_{33}) - c(U_{00}U_{33} - U_{22}U_{11}) = c(U_{00} + U_{22})(U_{11} - U_{33}),$$

using $1\mathbf{M} + 1\mathbf{m}$ each for their evaluation.

- Evaluate $U_{jj} = X_j Y_j$, for $1 \le j \le 4$, with $4\mathbf{M}$.
- Evaluate $(Z_0,\, Z_2) = (U_{00}^2 - U_{22}^2,\, U_{11}^2 - U_{33}^2)$ with $2\mathbf{M}$.
- Evaluate $A = c(U_{00} - U_{22})(U_{11} + U_{33})$ using $1\mathbf{M} + 1\mathbf{m}$.
- Compute $Z_1 = c(U_{00}U_{11} - U_{22}U_{33})$ and set $Z_3 = A - Z_1$ with $2\mathbf{M} + 1\mathbf{m}$.

This yields the desired complexity $9\mathbf{M} + 2\mathbf{m}$ over any ring. If 2 is a unit (and assuming a neglible cost of multiplying by 2), we replace the last line with two steps:

- Evaluate $B = c(U_{00} + U_{22})(U_{11} - U_{33})$ using $1\mathbf{M} + 1\mathbf{m}$.
- Compute $(2Z_1, 2Z_3) = (A + B, A - B)$ and scale (Z_0, Z_2) by 2,

which gives a complexity of $8\mathbf{M} + 2\mathbf{m}$. This yields an algorithm essentially equivalent to that Hisil et al. [8] under the linear isomorphism with the -1-twist of Edwards normal form. Finally if the characteristic is 2, the result $7\mathbf{M} + 2\mathbf{S} + 2\mathbf{m}$ of Kohel [11] is obtained by replacing $2\mathbf{M}$ by $2\mathbf{S}$ for the evaluation of (Z_0, Z_2) in the generic algorithm. □

Before considering the twisted forms, we determine the base complexity of doubling for the split $\boldsymbol{\mu}_4$-normal form.

Corollary 6. *Let C be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form. There exist algorithms for doubling with complexity $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$ over any ring, $4\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$ over a ring in which 2 is a unit, and $2\mathbf{M} + 5\mathbf{S} + 7\mathbf{m}$ over a ring of characteristic 2.*

Proof. The specialization of the addition law $\mathfrak{s}_2$ to the diagonal gives the forms for doubling

$$(X_0^4 - X_2^4,\ c(X_0^2 X_1^2 - X_2^2 X_3^2),\ X_1^4 - X_3^4,\ c(X_0^2 X_3^2 - X_1^2 X_2^2)\,).$$

which we can evaluate as follows:

- Evaluate X_j^2, for $1 \leq j \leq 4$, with $4\mathbf{S}$.
- Evaluate $(Z_0, Z_2) = (X_0^4 - X_2^4, X_1^4 - X_3^4)$ with $2\mathbf{M}$.
- Evaluate $A = c(X_0^2 - X_2^2)(X_1^2 + X_3^2)$ using $1\mathbf{M} + 1\mathbf{m}$.
- Compute $Z_1 = c(X_0^2 X_1^2 - X_2^2 X_3^2)$ and set $Z_3 = A - Z_1$ with $2\mathbf{M} + 1\mathbf{m}$.

This gives the result of $5\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$ over any ring. As above, when 2 is a unit, we replace the last line with the two steps:

- Evaluate $B = c(X_0^2 + X_2^2)(X_1^2 - X_3^2)$ using $1\mathbf{M} + 1\mathbf{m}$.
- Compute $(2Z_1, 2Z_3) = (A + B, A - B)$ and scale (Z_0, Z_2) by 2.

This reduces the complexity by $1\mathbf{M}$. In characteristic 2, the general algorithm specializes to $3\mathbf{M} + 6\mathbf{S} + 2\mathbf{m}$, but Kohel [11] provides an algorithm with better complexity of $2\mathbf{M} + 5\mathbf{S} + 7\mathbf{m}$ (reduced by $5\mathbf{m}$ on the semisplit model). $\qquad\square$

In the next section, we introduce the twists of these $\boldsymbol{\mu}_4$-normal forms, and derive efficient algorithms for their arithmetic.

3 Twisted normal forms

A quadratic twist of an elliptic curve is determined by a non-rational isomorphism defined over a quadratic extension $k[\alpha]/k$. In odd characteristic one can take an extension defined by $\alpha^2 = a$, but in characteristic 2, the general form of a quadratic extension is $k[\omega]/k$ where $\omega^2 - \omega = a$ for some a in k. The normal forms defined above both impose the existence of a k-rational point of order 4.

Over a finite field of characteristic 2, the existence of a 4-torsion point is a weaker constraint than for odd characteristic, since if E/k is an ordinary elliptic curve over a finite field of characteristic 2, there necessarily exists a 2-torsion point. Moreover, if E does not admit a k-rational 4-torsion point and $|k| > 2$, then its quadratic twist does.

We recall that for an elliptic curve in Weierstrass form,

$$E : Y^2 Z + (a_1 X + a_3 Z)YZ = X^3 + a_2 X^2 Z + a_4 X Z^2 + a_6 Z^3,$$

the quadratic twist by $k[\omega]/k$ is given by

$$E^t : Y^2 Z + (a_1 X + a_3 Z)YZ = X^3 + a_2 X^2 Z + a_4 X Z^2 + a_6 Z^3 + a(a_1 X + a_3 Z)^2 Z,$$

with isomorphism $\tau(X : Y : Z) = (X : -Y - \omega(a_1 X + a_3 Z) : Z)$, which satisfies $\tau^\sigma = -\tau$, where σ is the nontrivial automorphism of $k[\omega]/k$. The objective here is to describe the quadratic twists in the case of the normal forms defined above.

With a view towards cryptography, the binary NIST curves are of the form $y^2 + xy = x^3 + ax^2 + b$, with $a = 1$ and group order $2n$, whose quadratic twist is the curve with $a = 0$ which admits a point of order 4. While the latter admit an isomorphism a curve in $\boldsymbol{\mu}_4$-normal form, to describe the others, we must represent them as quadratic twists.

The twisted $\boldsymbol{\mu_4}$-normal form

In what follows we let $k[\omega]/k$ be the quadratic extension given by $\omega^2 - \omega = a$, and set $\overline{\omega} = 1 - \omega$ and $\delta = \omega - \overline{\omega}$. In order to have the widest possible applicability, we describe the quadratic twists with respect to any ring or field k. The discriminant of the extension is $D = \delta^2 = 1 + 4a$. When 2 is invertible we can speak of a twist by D, but in general we refer to a as the twisting parameter. While admitting general rings, all formulas hold over a field of characteristic 2, and we investigate optimizations in this case.

Theorem 7. *Let C/k be an elliptic curve in $\boldsymbol{\mu_4}$-normal form, semisplit $\boldsymbol{\mu_4}$-normal form, or split $\boldsymbol{\mu_4}$-normal form, given respectively by*

$$X_0^2 - r\,X_2^2 = X_1 X_3,\ \ X_1^2 - X_3^2 = X_0 X_2, \quad O = (1:1:0:1),$$
$$X_0^2 - X_2^2 = X_1 X_3,\ \ X_1^2 - X_3^2 = s\,X_0 X_2, \quad O = (1:1:0:1),$$
$$X_0^2 - X_2^2 = c^2\,X_1 X_3,\ \ X_1^2 - X_3^2 = c^2\,X_0 X_2, \quad O = (c:1:0:1).$$

The quadratic twist C^t of C by $k[\omega]$, where $\omega^2 - \omega = a$, is given by

$$X_0^2 - Dr\,X_2^2 = X_1 X_3 - a(X_1 - X_3)^2,\ \ X_1^2 - X_3^2 = X_0 X_2,$$
$$X_0^2 - DX_2^2 = X_1 X_3 - a(X_1 - X_3)^2,\ \ X_1^2 - X_3^2 = s\,X_0 X_2,$$
$$X_0^2 - DX_2^2 = c^2(X_1 X_3 - a(X_1 - X_3)^2),\ \ X_1^2 - X_3^2 = c^2 X_0 X_2,$$

with identities $O = (1:1:0:1)$, $O = (1:1:0:1)$ and $O = (c:1:0:1)$, respectively. In each case, the twisting isomorphism $\tau : C \to C^t$ is given by

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (\delta X_0 : \omega X_1 - \overline{\omega} X_3 : X_2 : \omega X_3 - \overline{\omega} X_1),$$

with inverse sending $(X_0 : X_1 : X_2 : X_3)$ to $(X_0 : \omega X_1 + \overline{\omega} X_3 : \delta X_2 : \overline{\omega} X_1 + \overline{\omega} X_3)$.

Proof. Since the inverse morphism is $[-1](X_0 : X_1 : X_2 : X_3) = (X_0 : X_3 : -X_2 : X_1)$, the twisting morphism satisfies $\tau^\sigma = [-1] \circ \tau$ where σ is the nontrivial automorphism of $k[\omega]/k$. Consequently, the image C^t is a twist of C. The form of the inverse is obtained by matrix inversion. $\qquad\square$

Remark. In characteristic 2 we have $D = \delta = 1$, and the twisted split $\boldsymbol{\mu_4}$-normal form is $X_0^2 + X_2^2 = c^2(X_1 X_3 + a(X_1 + X_3)^2),\ X_1^2 + X_3^2 = c^2 X_0 X_2$, with associated twisting morphism

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (X_0 : \overline{\omega} X_1 + \omega X_3 : X_2 : \omega X_1 + \overline{\omega} X_3).$$

Over a field of characteristic different from 2, we have an isomorphism with the twisted Edwards normal form.

Theorem 8. *Let C^t be an elliptic curve in twisted $\boldsymbol{\mu_4}$-normal form*

$$X_0^2 - DrX_2^2 = X_1 X_3 - a(X_1 - X_3)^2,\ \ X_1^2 - X_3^2 = X_0 X_2,$$

with parameters (r, a) over a field of characteristic different from 2. Then C^t is isomorphic to the twisted Edwards curve

$$X_0^2 - 16DrX_3^2 = -DX_1^2 + X_2^2$$

with parameters $(-D, -16Dr)$, *via the isomorphism* $C^t \to E$:

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (4X_0 : 2(X_1 - X_3) : 2(X_1 + X_3) : X_2),$$

and inverse

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (X_0 : X_1 + X_2 : 4X_3 : -X_1 + X_2).$$

Proof. The linear transformation is the compositum of the above linear transformations with the morphism $(X_0 : X_1 : X_2 : X_3) \longmapsto (\delta X_0 : X_1 : \delta X_2 : X_3)$ from the Edwards curve to its twist. □

For completeness we provide an isomorphic model in Weierstrass form:

Theorem 9. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form with parameters (r, a). Then C^t is isomorphic to the elliptic curve*

$$y^2 + xy = x^3 + (a - 8Dr)x^2 + 2D^2 r(8r - 3)x - D^3 r(1 - 4r)$$

in Weierstrass form, where $D = 4a + 1$. The isomorphism is given by the map which sends $(X_0 : X_1 : X_2 : X_3)$ to

$$\left(D\big(U_0 - 4r(U_0 + U_2)\big) : D\big(U_1 - 2r(8U_1 + 2U_0 - U_2)\big) : U_2 - 2U_0) \right),$$

where $(U_0, U_1, U_2, U_3) = (X_1 - X_3, X_0 + X_3, X_2, X_1 + X_3)$.

Proof. A symbolic verification is carried out by the Echidna code [12] implemented in Magma [15]. □

Specializing to characteristic 2, we obtain the following corollary.

Corollary 10. *Let C^t be a binary elliptic curve in twisted $\boldsymbol{\mu}_4$-normal form*

$$X_0^2 + bX_2^2 = X_1 X_3 + aX_0 X_2, \ X_1^2 + X_3^2 = X_0 X_2,$$

with parameters $(r, a) = (b, a)$. Then C^t is isomorphic to the elliptic curve

$$y^2 + xy = x^3 + ax^2 + b,$$

in Weierstrass form via the map $(X_0 : X_1 : X_2 : X_3) \mapsto (X_1 + X_3 : X_0 + X_1 : X_2)$. On affine points (x, y) the inverse is $(x, y) \longmapsto (x^2 : x^2 + y : 1 : x^2 + y + x)$.

Proof. By the previous theorem, since $D = 1$ in characteristic 2, the Weierstrass model simplifies to $y^2 + xy = x^3 + ax^2 + b$, and the map to

$$(X_0 : X_1 : X_2 : X_3) \longmapsto (U_0 : U_1 : U_2) = (X_1 + X_3 : X_0 + X_1 : X_2).$$

The given map on affine points is easily seen to be a birational inverse, valid for $X_2 = 1$, in view of the relation $(X_1 + X_3)^2 = X_0 X_2$, well-defined outside the identity. Consequently, it extends uniquely to an isomorphism. □

As a consequence of this theorem, any ordinary binary curve (with $j = 1/b \neq 0$) can be put in twisted $\boldsymbol{\mu}_4$-normal form, via the map on affine points:

$$(x, y) \longmapsto (x^2 : x^2 + y : 1 : x^2 + y + x).$$

In particular all algorithms of this work (over binary fields) are applicable to the binary NIST curves, which permits backward compatibility and improved performance.

4 Addition algorithms

We now consider the addition laws for twisted split $\boldsymbol{\mu}_4$-normal form. In the application to prime finite fields of odd characteristic p (see below for considerations in characteristic 2), under the GRH, Lagarias, Montgomery and Odlyzko [13] prove a generalization of the result of Ankeny [1], under which we can conclude that the least quadratic nonresidue $D \equiv 1 \bmod 4$ is in $O(\log^2(p))$, and the average value of D is $O(1)$. Consequently, for a curve over a finite prime field, one can find small twisting parameters for constructing the quadratic twist. With this in mind, we ignore all multiplications by constants a and $D = 4a + 1$.

Theorem 11. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form:*

$$X_0^2 - DX_2^2 = c^2(X_1 X_3 - a(X_1 - X_3)^2), \ X_1^2 - X_3^2 = c^2 X_0 X_2.$$

over a ring in which 2 is a unit. The projections $\pi_1 : C^t \to \mathbb{P}^1$, with coordinates (X, Z), given by

$$\pi_1((X_0 : X_1 : X_2 : X_3)) = \big\{(cX_0 : X_1 + X_3), (X_1 - X_3 : cX_2)\big\},$$

and $\pi_2 : C^t \to \mathbb{P}^1$, with coordinates (Y, W), given by

$$\pi_2((X_0 : X_1 : X_2 : X_3)) = \big\{(cX_0 : X_1 - X_3), (X_1 + X_3 : cX_2)\big\},$$

determine an isomorphism $\pi_1 \times \pi_2$ with its image:

$$((c^2/2)^2 X^2 - Z^2)W^2 = D((c^2/2)^2 Z^2 - X^2)Y^2$$

in $\mathbb{P}^1 \times \mathbb{P}^1$, with inverse

$$\sigma((X : Z), (Y : W)) = (2XY : c(XW + ZY) : 2ZW : c(ZY - XW)).$$

Proof. The morphisms σ and $\pi_1 \times \pi_2$ determine isomorphisms of $\mathbb{P}^1 \times \mathbb{P}^1$ with the surface $X_1^2 - X_3^2 = c^2 X_0 X_2$ in $\mathbb{P}^3$, and substitution in the first equation for C^t yields the above hypersurface in $\mathbb{P}^1 \times \mathbb{P}^1$. $\square$

The twisted split $\boldsymbol{\mu}_4$-normal form has 2-torsion subgroup generated by $Q = (-c : 1 : 0 : 1)$ and $R = (0 : -1 : c : 1)$, with $Q + R = (0 : -1 : -c : 1)$. Over any extension containing a square root ε of $-D$, the point $S = (c : -\varepsilon : 0 : \varepsilon)$ is a point of order 4 such that $2S = Q$.

Theorem 12. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form over a ring in which 2 is a unit. The projections π_1 and π_2 determine two-dimensional spaces of bilinear addition law projections:*

$$\pi_1 \circ \mu(x, y) = \begin{cases} \mathfrak{s}_0 = (U_{13} - U_{31} : U_{20} - U_{02}), \\ \mathfrak{s}_2 = (U_{00} + DU_{22} : U_{11} + U_{33} + 2aV_{13}), \end{cases}$$

$$\pi_2 \circ \mu(x, y) = \begin{cases} \mathfrak{s}_1 = (U_{13} + U_{31} - 2aV_{13} : U_{02} + U_{20}), \\ \mathfrak{s}_3 = (U_{00} - DU_{22} : U_{11} - U_{33}), \end{cases}$$

where $U_{k\ell} = X_k Y_\ell$ and $V_{k\ell} = (X_k - X_\ell)(Y_k - Y_\ell)$. The exceptional divisors of the $\mathfrak{s}_j$ are of the form $\Delta_{T_j} + \Delta_{T_j + Q}$, where $T_0 = O$, $T_1 = S + R$, $T_2 = R$, $T_3 = S$.

Proof. The existence and dimensions of the spaces of bilinear addition law projections, as well as the form of the exceptional divisors, follows from Theorem 26 and Corollary 27 of Kohel [9], observing for j in $\{0,2\}$ that $T_j + (T_j + Q) = Q$ and for j in $\{1,3\}$ that $T_j + (T_j + Q) = O$. The correctness of the forms can be verified symbolically, and the pairs $\{T_j, T_j + Q\}$ determined by the substitution $(Y_0, Y_1, Y_2, Y_3) = (c, 1, 0, 1)$, as in Corollary 11 of Kohel [9]. In particular, for $\mathfrak{s}_0$, we obtain the tuple $(U_{13} - U_{31}, U_{20} - U_{02}) = (X_1 - X_3, cX_2)$, which vanishes on $\{O, Q\} = \{(c : 1 : 0 : 1), (-c : 1 : 0 : 1)\}$, hence the exceptional divisor is $\Delta_O + \Delta_Q$. $\qquad\square$

Composing the addition law projections of Theorem 12 with the isomorphism of Theorem 11, and dividing by 2, we obtain for the pair $(\mathfrak{s}_0, \mathfrak{s}_1)$ the tuple (Z_0, Z_1, Z_2, Z_3) with

$$Z_0 = (U_{13} - U_{31})(U_{13} + U_{31} - 2aV_{13}), \quad Z_1 + Z_3 = -c(U_{02} - U_{20})(U_{13} + U_{31} + 2aV_{13}),$$
$$Z_2 = -(U_{02} - U_{20})(U_{02} + U_{20}), \qquad Z_1 - Z_3 = -c(U_{13} - U_{31})(U_{02} + U_{20}),$$

and for the pair $(\mathfrak{s}_2, \mathfrak{s}_3)$ the tuple (Z_0, Z_1, Z_2, Z_3) with

$$Z_0 = (U_{00} + DU_{22})(U_{00} - DU_{22}), \qquad Z_1 + Z_3 = c\,(U_{11} + U_{33} + 2aV_{13})(U_{00} - DU_{22}),$$
$$Z_2 = (U_{11} + U_{33} + 2aV_{13})(U_{11} - U_{33}), \quad Z_1 - Z_3 = c(U_{00} + DU_{22})(U_{11} - U_{33}).$$

The former have efficient evaluations over a ring in which 2 is a unit, yielding $(2Z_0, 2Z_1, 2Z_2, 2Z_3)$, and otherwise we deduce expressions for (Z_1, Z_3):

$$Z_1 = c((U_{02}U_{13} - U_{02}U_{31}) - a(U_{02} - U_{20})W_{13}),$$
$$Z_3 = c((U_{02}U_{31} - U_{20}U_{13}) - a(U_{02} - U_{20})W_{13}),$$

with $W_{13} = 2(U_{13} + U_{31}) - V_{13}$, and

$$Z_1 = c(U_{00}U_{11} - DU_{22}U_{33}) - a(U_{00} - DU_{22})W_{13}),$$
$$Z_3 = c(U_{00}U_{33} - DU_{22}U_{11}) - a(U_{00} - DU_{22})W_{13}),$$

with $W_{13} = 2(U_{11} + U_{33}) - V_{13}$, respectively. We note that these expressions remain valid over any ring despite the fact that they were derived via the factorization through the curve in $\mathbb{P}^1 \times \mathbb{P}^1$ which is singular in characteristic 2.

Before evaluating their complexity, we explain the obvious symmetry of the above equations. Let τ be the translation-by-R automorphism of C^t sending $(X_0 : X_1 : X_2 : X_3)$ to

$$(X_2 : -X_3 - 2a(X_1 + X_3) : -DX_0 : X_1 + 2a(X_1 + X_3)),$$

and denote also τ for the induced automorphism

$$\tau((X : Z), (Y : W)) = ((Z : X), (-W : DY))$$

of its image in $\mathbb{P}^1 \times \mathbb{P}^1$. Then for each (i, j) in $(\mathbb{Z}/2\mathbb{Z})^2$, the tuple of morphisms $(\tau^i \times \tau^j, \tau^k)$ such that $k = i + j$ acts on the set of tuples $(\mathfrak{s}, \mathfrak{s}')$ of addition law projections:

$$(\tau^i \times \tau^j, \tau^k) \cdot (\mathfrak{s}, \mathfrak{s}') = \tau^k \circ (\mathfrak{s} \circ (\tau^i \times \tau^j), \ \mathfrak{s}' \circ (\tau^i \times \tau^j)).$$

Lemma 13. *Let C^t be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form. The tuples of addition law projections $(\mathfrak{s}_0, \mathfrak{s}_1)$ and $(\mathfrak{s}_2, \mathfrak{s}_3)$ are eigenvectors for the action of $(\tau \times \tau, 1)$ and are exchanged, up to scalars, by the action of $(\tau \times 1, \tau)$ and $(1 \times \tau, \tau)$.*

Proof. Since an addition law (projection) is uniquely determined by its exceptional divisor, up to scalars, the lemma follows from the action of $(\tau^i \times \tau^j, \tau^k)$ on the exceptional divisors given by Lemma 31 of Kohel [9], and can be established directly by substitution. □

Corollary 14. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form. There exists an algorithm for addition with complexity $11\mathbf{M} + 2\mathbf{m}$ over any ring, and an algorithm with complexity $9\mathbf{M} + 2\mathbf{m}$ over a ring in which 2 is a unit.*

Proof. Considering the product determined by the pair $(\mathfrak{s}_2, \mathfrak{s}_3)$, the evaluation of the expressions

$$Z_0 = (U_{00} - DU_{22})(U_{00} + DU_{22}),$$
$$Z_2 = (U_{11} - U_{33})(U_{11} + U_{33} + 2aV_{13}),$$

requires $4\mathbf{M}$ for the U_{ii} plus $1\mathbf{M}$ for V_{13} if $a \neq 0$, then $2\mathbf{M}$ for the evaluation of Z_0 and Z_2. Setting $W_{13} = 2(U_{11} + U_{33}) - V_{13}$, a direct evaluation of the expressions

$$Z_1 = c((U_{00}U_{11} - DU_{22}U_{33}) - a(U_{00} - DU_{22})W_{13}),$$
$$Z_3 = c((U_{00}U_{33} - DU_{22}U_{11}) - a(U_{00} - DU_{22})W_{13}),$$

requires an additional $4\mathbf{M} + 2\mathbf{m}$, saving $1\mathbf{M}$ with the relation

$$(U_{00} - DU_{22})(U_{11} + U_{33}) = (U_{00}U_{11} - DU_{22}U_{33}) + (U_{00}U_{33} - DU_{22}U_{11}),$$

for a complexity of $11\mathbf{M} + 2\mathbf{m}$. If 2 is a unit, we may instead compute

$$Z_1 + Z_3 = c\,(U_{00} - DU_{22})(U_{11} + U_{33} + 2aV_{13}),$$
$$Z_1 - Z_3 = c\,(U_{00} + DU_{22})(U_{11} - U_{33}).$$

and return $(2Z_0, 2Z_1, 2Z_2, 2Z_3)$ using $2\mathbf{M} + 2\mathbf{m}$, for a total cost of $9\mathbf{M} + 2\mathbf{m}$. □

Corollary 15. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form. There exists an algorithm for doubling with complexity $6\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$ over any ring, and an algorithm with complexity $4\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$ over a ring in which 2 is a unit.*

Proof. The specialization to $X_i = Y_i$ gives:

$$Z_0 = (X_0^2 - DX_2^2)(X_0^2 + DX_2^2),$$
$$Z_2 = (X_1^2 - X_3^2)(X_1^2 + X_3^2 + 2a(X_1 + X_3)^2).$$

The evaluation of X_i^2 costs 4**S** plus 1**S** for $(X_1 + X_3)^2$ if $a \neq 0$, rather than $4\mathbf{M} + 1\mathbf{M}$. Setting $W_{13} = 2(X_1^2 + X_3^2) - (X_1 + X_3)^2 [= (X_1 - X_3)^2]$, a direct evaluation of the expressions

$$Z_1 = c((X_0^2 X_1^2 - DX_2^2 X_3^2) - a(X_0^2 - DX_2^2)W_{13}),$$
$$Z_3 = c((X_0^2 X_3^2 - DX_2^2 X_1^2) - a(X_0^2 - DX_2^2)W_{13}),$$

requires an additional $4\mathbf{M} + 2\mathbf{m}$, as above, for a complexity of $6\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$. If 2 is a unit, we compute

$$Z_1 + Z_3 = c\,(X_0^2 - DX_2^2)(X_1^2 + X_3^2 + 2a(X_1 + X_3)^2),$$
$$Z_1 - Z_3 = c\,(X_0^2 + DX_2^2)(X_1^2 - X_3^2).$$

using $2\mathbf{M} + 2\mathbf{m}$, which gives $4\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$. $\qquad\square$

In the next section we explore efficient algorithms for evaluation of the addition laws and doubling forms in characteristic 2.

5 Binary addition algorithms

Suppose that k is a finite field of characteristic 2. The Artin-Schreier extension $k[\omega]/k$ over which we twist is determined by the additive properties of a, and half of all elements of k determine the same field (up to isomorphism) and hence an isomorphic twist. For instance, if $k/\mathbb{F}_2$ is an odd degree extension, we may take $a = 1$. As above, we assume that that multiplication by a is neglible in our complexity analyses.

Theorem 16. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form:*

$$X_0^2 + X_2^2 = c^2(X_1 X_3 + a(X_1 + X_3)^2), \ \ X_1^2 + X_3^2 = c^2 X_0 X_2,$$

over a field of characteristic 2. *A complete system of addition laws is given by the two maps* $\mathfrak{s}_0$ *and* $\mathfrak{s}_2$,

$$\big((U_{13} + U_{31})^2, c(U_{02}U_{31} + U_{20}U_{13} + aF), (U_{02} + U_{20})^2, c(U_{02}U_{13} + U_{20}U_{31} + aF)\big),$$
$$\big((U_{00} + U_{22})^2, c(U_{00}U_{11} + U_{22}U_{33} + aG), (U_{11} + U_{33})^2, c(U_{00}U_{33} + U_{11}U_{22} + aG)\big),$$

respectively, where $U_{jk} = X_j Y_k$ and

$$F = (X_1 + X_3)(Y_1 + Y_3)(U_{02} + U_{20}) \ and \ G = (X_1 + X_3)(Y_1 + Y_3)(U_{00} + U_{22}).$$

The respective exceptional divisors are $4\Delta_O$ and $4\Delta_S$ where $S = (1 : c : 1 : 0)$ is a 2-torsion point.

Proof. The addition laws $\mathfrak{s}_0$ and $\mathfrak{s}_2$ are the conjugate addition laws of Theorem 4 (as can be verified symbolically)[1] and, equivalently, are described by the reduction at 2 of the addition laws derived from the tuples of addition law projections $(\mathfrak{s}_0, \mathfrak{s}_1)$ and $(\mathfrak{s}_2, \mathfrak{s}_3)$ of Theorem 12. Since the points O and S are fixed rational points of the twisting morphism, the exceptional divisors are of the same form. As the exceptional divisors are disjoint, the pair of addition laws form a complete set. $\qquad\square$

---

[1] As is verified by the implementation in Echidna [12] written in Magma [15].

Remark. Recall that the addition laws $\mathfrak{s}_1$ and $\mathfrak{s}_3$ on the split $\boldsymbol{\mu}_4$-normal form have exceptional divisors $4\Delta_T$ and $4\Delta_{-T}$ in characteristic 2 (since $S = O$). Consequently their conjugation by the twisting morphism yields a conjugate pair over $k[\omega]$, since the twisted curve does not admit a k-rational 4-torsion point T. There exist linear combinations of these twisted addition laws which extend the set $\{\mathfrak{s}_0, \mathfrak{s}_2\}$ to a basis over k (of the space of dimension four), but they do not have such an elegant form as $\mathfrak{s}_0$ and $\mathfrak{s}_2$.

Corollary 17. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form over a field of characteristic 2. There exists an algorithm for addition with complexity $9\mathbf{M} + 2\mathbf{S} + 2\mathbf{m}$.*

Proof. Since the addition laws differ from the split $\boldsymbol{\mu}_4$-normal form only by the term aF (or aG), it suffices to determine the complexity of its evaluation. Having determined (U_{02}, U_{20}) (or (U_{00}, U_{22})), we require an additional $2\mathbf{M}$, which gives the complexity bound. $\qquad\square$

For the $\boldsymbol{\mu}_4$-normal form the addition law, after coefficient scaling, we find that the addition law with exceptional divisor $4\Delta_O$ takes the form

$$((U_{13} + U_{31})^2, U_{02}U_{31} + U_{20}U_{13} + aF, (U_{20} + U_{02})^2, U_{02}U_{13} + U_{20}U_{31} + aG),$$

and in particular does not involve multiplication by constants (other than a which we may take in $\{0, 1\}$ in cryptographic applications). This gives the following complexity result.

Corollary 18. *Let C^t be an elliptic curve in twisted $\boldsymbol{\mu}_4$-normal form over a field of characteristic 2. There exists an algorithm for addition outside of the diagonal Δ_O with complexity $9\mathbf{M} + 2\mathbf{S}$.*

6 Binary doubling algorithms

We recall the hypothesis that multiplication by a is negligible. In the cryptographic context (e.g. in application to the binary NIST curves), we may assume $a = 1$ (or $a = 0$ for the untwisted forms).

Corollary 19. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form. The doubling map is uniquely determined by*

$$\begin{aligned}
(\, (X_0 + X_2)^4 &: c((X_0X_3 + X_1X_2)^2 + a(X_0 + X_2)^2(X_1 + X_3)^2) : \\
(X_1 + X_3)^4 &: c((X_0X_1 + X_2X_3)^2 + a(X_0 + X_2)^2(X_1 + X_3)^2) \,)
\end{aligned}$$

Proof. This follows from specializing $X_j = Y_j$ in the form $\mathfrak{s}_2$ of Theorem 16. $\quad\square$

We note that in cryptographic applications we may assume that $a = 0$ (untwisted form), giving

$$((X_0 + X_2)^4 : c(X_0X_3 + X_2X_1)^2 : (X_1 + X_3)^4 : c(X_0X_1 + X_2X_3)^2),$$

and otherwise $a = 1$, in which case we have

$$((X_0 + X_2)^4 : c(X_0 X_1 + X_2 X_3)^2 : (X_1 + X_3)^4 : c(X_0 X_3 + X_2 X_1)^2).$$

It is clear that the evaluation of doubling on the twisted and untwisted normal forms is identical. This is true also for the case of general a, up to the computation of $(X_0 + X_2)^2(X_1 + X_3)^2$. We nevertheless give an algorithm which improves upon the number of constant multiplications reported in Kohel [11], in terms of polynomials in $u = c^{-1}$. With this notation, we note that the defining equations of the curve are:

$$X_1 X_3 = u^2(X_0 + X_2)^2,$$
$$X_0 X_2 = u^2(X_1 + X_3)^2.$$

These relations are important, since they permit us to replace any instances of the multiplications on the left with the squarings on the right. As a consequence, we have

$$X_0 X_1 + X_2 X_3 = (X_0 + X_3)(X_2 + X_1) + X_0 X_2 + X_1 X_3$$
$$= (X_0 + X_3)(X_2 + X_1) + u^2((X_0 + X_2)^2 + (X_1 + X_3)^2)$$
$$X_0 X_3 + X_2 X_1 = (X_0 + X_1)(X_2 + X_3) + X_0 X_2 + X_1 X_3$$
$$= (X_0 + X_1)(X_2 + X_3) + u^2((X_0 + X_2)^2 + (X_1 + X_3)^2).$$

Moreover these forms are linearly dependent with $(X_0 + X_2)(X_1 + X_3)$

$$(X_0 X_1 + X_2 X_3) + (X_0 X_3 + X_2 X_1) = (X_0 + X_2)(X_1 + X_3),$$

so that two multiplications are sufficient for the determination of these three forms. Putting this together, it suffices to evaluate the tuple

$$(u(X_0 + X_2)^4, (X_0 X_1 + X_2 X_3)^2, u(X_1 + X_3)^4, (X_0 X_3 + X_2 X_1)^2),$$

for which we obtain the following complexity for doubling.

Corollary 20. *Let C^t be a curve in twisted split $\boldsymbol{\mu}_4$-normal form. There exists an algorithm for doubling with complexity $2\mathbf{M} + 5\mathbf{S} + 3\mathbf{m}_u$.*

Using the semisplit $\boldsymbol{\mu}_4$-normal form, the complexity of $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}_u$ of Kohel [11], saving one constant multiplication, carries over to the corresponding twisted semisplit $\boldsymbol{\mu}_4$-normal form (referred to as nonsplit). By a similar argument the same complexity, $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}_u$, is obtained for the $\boldsymbol{\mu}_4$-normal form of this article.

7   Montgomery endomorphisms of Kummer products

We recall certain results of Kohel [11] concerning the Montgomery endomorphism with application to scalar multiplication on products of Kummer curves. We define the Montgomery endomorphism to be the map $\varphi : C \times C \to C \times C$ given by $(Q, R) \mapsto (2Q, Q + R)$. With a view to scalar multiplication, this induces

$$((n + 1)P, nP) \longmapsto ((2n + 2)P, (2n + 1)P),$$

and

$$(nP, (n+1)P) \longmapsto (2nP, (2n+1)P).$$

By exchanging the order of the coordinates on input and output, an algorithm for the Montgomery endomorphism computes $((2n+2)P, (2n+1)P)$ or $((2n+1)P, 2nP)$ from the input point $((n+1)P, nP)$. This allows us to construct a symmetric algorithm for the scalar multiple kP of P via a Montgomery ladder

$$((n_i+1)P, n_iP) \longmapsto ((n_{i+1}+1)P, n_{i+1}P) = \begin{cases} ((2n_i+1)P, 2n_iP), \text{ or} \\ ((2n_i+2)P, (2n_i+1)P). \end{cases}$$

It is noted that the Montgomery endomorphism sends each of the curves

$$\Delta_P = \{(Q, Q-P) \mid Q \in C(\bar{k})\}, \text{ and } \Delta_{-P} = \{(Q, Q-P) \mid Q \in C(\bar{k})\},$$

to itself, and exchange of coordinates induces $\Delta_P \to \Delta_{-P}$.

We now assume that C is a curve in split $\boldsymbol{\mu}_4$-normal form, and define the Kummer curve $\mathscr{K}(C) = C/\{\pm 1\} \cong \mathbb{P}^1$, equipped with map

$$\pi((X_0 : X_1 : X_2 : X_3)) = \begin{cases} (cX_0 : X_1 + X_3), \\ (X_1 - X_3 : cX_2). \end{cases}$$

This determines a curve $\mathscr{K}(\Delta_P)$ as the image of Δ_P in $\mathscr{K}(C) \times \mathscr{K}(C)$.

Lemma 21. *For any point P of C, the Montgomery-oriented curve $\mathscr{K}(\Delta_P)$ equals $\mathscr{K}(\Delta_{-P})$.*

Proof. It suffices to note that $(\overline{Q}, \overline{Q-P}) \in \mathscr{K}(\Delta_P)(\bar{k})$ is also a point of $\mathscr{K}(\Delta_{-P})$:

$$(\overline{Q}, \overline{Q-P}) = (\overline{-Q}, \overline{-Q+P}) = (\overline{-Q}, \overline{-Q-(-P)}) \in \mathscr{K}(\Delta_{-P}),$$

hence $\mathscr{K}(\Delta_P) \subseteq \mathscr{K}(\Delta_{-P})$ and by symmetry $\mathscr{K}(\Delta_{-P}) \subseteq \mathscr{K}(\Delta_P)$.

We conclude, moreover, that $\mathscr{K}(\Delta_P)$ is well-defined by a point on the Kummer curve.

Lemma 22. *The Montgomery-oriented curve $\mathscr{K}(\Delta_P)$ depends only on $\pi(P)$.*

Proof. The dependence only on $\pi(P)$ is a consequence of the previous lemmas, which we make explicit here. Let $P = (s_0 : s_1 : s_2 : s_3)$ and $\pi(P) = (t_0 : t_1)$. By Theorem 24 of Kohel [11], the curve $\mathscr{K}(\Delta_P)$ takes the form,

$$s_0(U_0V_1 + U_1V_0)^2 + s_2(U_0V_0 + U_1V_1)^2 = c(s_1 + s_3)U_0U_1V_0V_1,$$

but then $(s_0 : s_1 + s_3 : s_2) = (t_0^2 : c\,t_0t_1, t_1^2)$ in $\mathbb{P}^2$, hence

$$t_0^2(U_0V_1 + U_1V_0)^2 + t_1^2(U_0V_0 + U_1V_1)^2 = c^2t_0t_1U_0U_1V_0V_1.$$

which shows that the curve depends only on $\pi(P)$.

We note similarly that the Kummer curve $\mathscr{K}(C) = \mathscr{K}(C^t)$ is independent of the quadratic twist, in the sense that any twisting isomorphism $\tau : C \to C^t$ over $\bar{k}$ induces a unique isomorphism $\mathscr{K}(C) \to \mathscr{K}(C^t)$. One can verify directly the twisting isomorphism τ of Theorem 7 induces the identity on the Kummer curves with their given projections. We thus identify $\mathscr{K}(C) = \mathscr{K}(C^t)$, and denote $\pi : C \to \mathscr{K}(C)$ and $\pi^t : C^t \to \mathscr{K}(C)$ the respective covers of the Kummer curve.

Theorem 23. *Let C be a curve in split $\boldsymbol{\mu}_4$-normal form and C^t be a quadratic twist over the field k. If $P \in C^t(\bar{k})$ and $Q \in C(\bar{k})$ such that $\pi^t(P) = \pi(Q)$, then $\mathscr{K}(\Delta_P) = \mathscr{K}(\Delta_Q)$.*

It follows that we can evaluate the Montgomery endomorphism on $\mathscr{K}(\Delta_P)$, for $P \in C^t(k)$, and $\pi(P) = (t_0 : t_1)$, using the same algorithm and with the same complexity as in Kohel [11]. We recall the complexity result here, assuming a normalisation $t_0 = 1$ or $t_1 = 1$.

Corollary 24. *The Montgomery endomorphism on $\mathscr{K}(\Delta_P)$ can be computed with $4\mathbf{M} + 5\mathbf{S} + 1\mathbf{m}_t + 1\mathbf{m}_c$ or with $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}_t + 2\mathbf{m}_c$.*

By the same argument, the same Theorem 24 of Kohel [11] provides the necessary map for point recovery in terms of the input point $P = (s_0 : s_1 : s_2 : s_3)$ of $C^t(k)$.

Theorem 25. *Let C^t be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form with rational point $P = (s_0 : s_1 : s_2 : s_3)$. If P is not a 2-torsion point, the morphism $\lambda : C \to \mathscr{K}(\Delta_P)$ is an isomorphism, and defined by*

$$\pi_1 \circ \lambda(X_0 : X_1 : X_2 : X_3) = \begin{cases} (cX_0 : X_1 + X_3), \\ (X_1 + X_3 : cX_2), \end{cases}$$

$$\pi_2 \circ \lambda(X_0 : X_1 : X_2 : X_3) = \begin{cases} (s_0 X_0 + s_2 X_2 : s_1 X_1 + s_3 X_3), \\ (s_3 X_1 + s_1 X_3 : s_2 X_0 + s_0 X_2), \end{cases}$$

with inverse $\lambda^{-1}((U_0 : U_1), (V_0 : V_1))$ equal to

$$\begin{cases} ((s_1 + s_3)U_0^2 V_0 : (s_0 U_0^2 + s_2 U_1^2)V_1 + cs_1 U_0 U_1 V_0 : (s_1 + s_3)U_1^2 V_0 : (s_0 U_0^2 + s_2 U_1^2)V_1 + cs_3 U_0 U_1 V_0), \\ ((s_1 + s_3)U_0^2 V_1 : (s_2 U_0^2 + s_0 U_1^2)V_0 + cs_3 U_0 U_1 V_1 : (s_1 + s_3)U_1^2 V_1 : (s_2 U_0^2 + s_0 U_1^2)V_0 + cs_1 U_0 U_1 V_1). \end{cases}$$

This allows for the application of the Montgomery endomorphism to scalar multiplication on C^t. Using the best results of the present work, the complexity is comparable to a double and add algorithm with window of width 4.

8   Conclusion

Elliptic curves in the twisted $\boldsymbol{\mu}_4$-normal form of this article (including split and semisplit variants) provide models for curves which, on the one hand, are isomorphic to twisted Edwards curves with efficient arithmetic over nonbinary fields,

and, on the other, have good reduction and efficient arithmetic in characteristic 2.

Taking the best reported algorithms from the EFD [4], we conclude with a tabular comparison of the previously best known complexity results for doubling and addition algorithms on projective curves. We include the projective lambda model (a singular quartic model in $\mathbb{P}^2$), which despite the extra cost of doubling, admits a slightly better algorithm for addition than López-Dahab (see [16]). Binary Edwards curves [3], like the twisted $\boldsymbol{\mu}_4$-normal form of this work, cover all ordinary curves, but the best complexity result we give here is for $d_1 = d_2$ which has a rational 4-torsion point (corresponding to the trivial twist, for which the $\boldsymbol{\mu}_4$-normal form gives better performance). Similarly, the López-Dahab model with $a_2 = 0$ admits a rational 4-torsion point, hence covers the same classes, but the fastest arithmetic is achieved on the quadratic twists with $a_2 = 1$, which manage to save one squaring $\mathbf{S}$ for doubling relative to the present work, at the loss of generality (one must vary the weighted projective space according to the twist, $a_2 = 0$ or $a_2 = 1$) and with a large penalty for the cost of addition. The results stated here concern the twisted $\boldsymbol{\mu}_4$-normal form which minimize the constant multiplications. In the final columns, we indicate the fractions of ordinary curves covered by the model (assuming a binary field of odd degree), and whether the family includes the NIST curves.

Curve model	Doubling	Addition	%	NIST
Lambda coordinates	$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}$	$11\mathbf{M} + 2\mathbf{S}$	100%	✓
Binary Edwards ($d_1 = d_2$)	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$16\mathbf{M} + 1\mathbf{S} + 4\mathbf{m}$	50%	✗
López-Dahab ($a_2 = 0$)	$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{m}$	$14\mathbf{M} + 3\mathbf{S}$	50%	✗
López-Dahab ($a_2 = 1$)	$2\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$	$13\mathbf{M} + 3\mathbf{S}$	50%	✓
Twisted $\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$9\mathbf{M} + 2\mathbf{S}$	100%	✓
$\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$7\mathbf{M} + 2\mathbf{S}$	50%	✗

Table of binary doubling and addition algorithm complexities.

All curves can be represented in lambda coordinates or in $\boldsymbol{\mu}_4$-normal form. However by considering the two cases $a_2 \in \{0, 1\}$, as for the López-Dahab models, the twists of the $\boldsymbol{\mu}_4$-normal form with $a_2 = 0$ give the faster $\boldsymbol{\mu}_4$-normal form and only when $a_2 = 1$ does one need the twisted model with its reduced complexity.

By consideration of twists, we are able to describe a uniform family of curves which capture nearly optimal known doubling performance of binary curves (up to $1\mathbf{S}$), while vastly improving the performance of addition algorithms applicable to all binary curves. By means of a trivial encoding in twisted $\boldsymbol{\mu}_4$-normal form (see Corollary 10), this brings efficient arithmetic of these $\boldsymbol{\mu}_4$-normal forms to binary NIST curves.

References

1. N. C. Ankeny, The least quadratic non residue. *Annals of Mathematics, second series*, **55**, no. 1, 65–72, 1952.
2. D. J. Bernstein, T. Lange, Faster addition and doubling on elliptic curves. *Advances in cryptology—ASIACRYPT 2007, Lecture Notes in Computer Science*, **4833**, 29–50, 2007.
3. D. J. Bernstein, T. Lange, R. Rezaeian Farashahi, Binary Edwards curves. *Cryptographic hardware and embedded systems (CHES 2008, Washington, D.C.), Lecture Notes in Computer Science*, **5154**, 244–265, 2008.
4. D. J. Bernstein, T. Lange, Explicit formulas database. `http://www.hyperelliptic.org/EFD/`
5. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves. *Progress in cryptology – AFRICACRYPT 2008, Lecture Notes in Computer Science*, **5023**, 389–405, 2008.
6. D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, **7**, (4), 385–434, 1986.
7. H. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, **44**, 393–422, 2007.
8. H. Hisil, K. K.-H. Wong, G. Carter, E. Dawson, Twisted Edwards curves revisited. *Advances in cryptology – ASIACRYPT 2008, Lecture Notes in Computer Science*, **5350**, Springer, 326–343, 2008.
9. D. Kohel, Addition law structure of elliptic curves. *Journal of Number Theory* **131**, Issue 5, 894–919, 2011.
10. D. Kohel, A normal form for elliptic curves in characteristic 2. talk at *Arithmetic, Geometry, Cryptography and Coding Theory*, Luminy, 15 March 2011. `http://iml.univ-mrs.fr/~kohel/pub/normal_form.pdf`.
11. D. Kohel, Efficient arithmetic of elliptic curves in characteristic 2. *Advances in cryptology—INDOCRYPT 2012 (Kolkata, 2012), Lecture Notes in Computer Science*, **7668**, 378–398, 2012.
12. D. Kohel et al., Echidna algorithms, v.4.0, 2013. URL: `http://echidna.maths.usyd.edu.au/echidna/index.html`
13. J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, A bound for the least prime ideal in the Chebotarev density theorem, *Invent. Math.*, **54**, 271–296, 1979.
14. H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, **79** (3), 603–610, 1985.
15. Magma Computational Algebra System (Version 2.20), `http://magma.maths.usyd.edu.au/magma/handbook/`, 2015.
16. T. Oliveira, J. López, D. F. Aranha, F. Rodríguez-Henriíquez, Lambda coordiantes for binary elliptic curves, *Cryptographic Hardware and Embedded Systems - CHES 2013 Lecture Notes in Computer Science*, **8086**, 311–330, 2013.
17. W. A. Stein et al., Sage Mathematics Software (Version 6.0). The Sage Development Team, 2015, `http://www.sagemath.org`.