Twisted μ_4-normal form for elliptic curves

David Kohel
Institut de Mathématiques de Marseille

Eurocrypt 2017, Paris, 1 May 2017

Elliptic Curves over Binary Fields

Standards for elliptic curve Diffie-Hellman or ElGamal require an ordinary (non-supersingular) elliptic curve over a finite field k.

If k is characteristic 2 then the degree of k over $\mathbb{F}_2$ should be odd.

Such an ordinary binary elliptic curve E can be written in the form

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

Its j-invariant is b^{-1} and the parameter a is the quadratic twist, which can be taken in $\{0, 1\}$: the curves

$$y^2 + xy = x^3 + b \text{ and } y^2 + xy + x^2 = x^3 + b,$$

for $a = 0$ and $a = 1$, respectively, become isomorphic $(y \mapsto y + \omega x)$ over the quadratic extension $k[\omega]$, where $\omega^2 + \omega + 1 = 0$.

Elliptic Curves over Binary Fields

The parameter a ($= 0$ or 1) gives a simple characterization of the pair of twists (over a binary odd degree field):

$$y^2 + xy = x^3 + b \text{ and } y^2 + xy + x^2 = x^3 + b.$$

Namely, $a = 0$ if and only if $E(k)$ has a point of order 4.

Recall that every binary ordinary elliptic curve has even order; the closest we can get to prime order is $|E(k)| = 2n$ for n prime, and consequently,

$$\begin{aligned} |E(k)| &\equiv 2 \bmod 4 \quad \text{if } a = 1, \\ |E(k)| &\equiv 0 \bmod 4 \quad \text{if } a = 0. \end{aligned}$$

Specifically, if $a = 0$, then then point $(c : c^2 : 1)$, where $c^4 = b$, is a point of order 4.

Elliptic Curves over Binary Fields

As was noted for Hessian curves, Edwards normal form, and the $\boldsymbol{\mu}_4$-normal form (which we generalize here to twists), the existence of a small order point results in curves with symmetries, and yields families with efficient arithmetic and side channel resistance.

Unfortunately, 20th-century standards focused on nearly prime order $|E(k)| = hn$, where n is prime and cofactor h as small as possible, ignorant of the benefits of a point of small order $h > 2$.

Hence for backwards compatibility, standard (NIST, SEC, etc.) curves can not be put in Hessian, Edwards, or $\boldsymbol{\mu}_4$-normal form, which have points of order $h = 3$, 4 (non-binary field), and 4.

Elliptic Curves over Binary Fields

So Edwards curves are not backward compatible with 20th century curve standards. Worse, over prime fields, there is a geometric restriction to having a point of order 4 — if the order $|E(k)|$ is odd (e.g. prime) then so is the order of its quadratic twist: in short, twisted Edwards curves can not bridge this gap.

In view of the above dichotomy, the situation for binary curves is much better — if $|E(k)| \equiv 2 \bmod 4$ then it is a twist of a curve with 4-torsion point, which can be put in $\boldsymbol{\mu}_4$-normal form, that is, E can be put in *twisted $\boldsymbol{\mu}_4$-normal form*.

The objective of this work is to introduce these twists of the $\boldsymbol{\mu}_4$-normal form in order to combine the most efficient arithmetic with backward compatibility to binary curve standards.

Previous State of the Art

Previous models which covered the case of standard curves $(a = 1)$ include López-Dahab $(a = 1)$ model, and the more recent Lambda coordinates, for which we compare known complexities $(\mathbf{S} \sim 0)$:

López-Dahab $(a = 1)$:

Advantages:	Best known doubling	$2\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$
Disadvantages:	Slow addition	$13\mathbf{M} + 3\mathbf{S}$

Lambda coordinates:

Disadvantages:	Slow doubling	$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}$
Advantages:	Better addition	$11\mathbf{M} + 2\mathbf{S}$

Reference complexities for the $\boldsymbol{\mu}_4$-normal form are:

$\boldsymbol{\mu}_4$-normal form:

Advantages:	Best known doubling*	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$
	Best known addition	$7\mathbf{M} + 2\mathbf{S}$
Disadvantages:	Not standards compatible.	

Previous State of the Art

In table form we summarize the previous state of the art, and the results we present here for twisted $\boldsymbol{\mu}_4$-normal form.

Curve model	Doubling	Addition	NIST
Lambda coordinates	$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}$	$11\mathbf{M} + 2\mathbf{S}$	yes
López-Dahab ($a = 0$)	$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{m}$	$14\mathbf{M} + 3\mathbf{S}$	no
López-Dahab ($a = 1$)	$2\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$	$13\mathbf{M} + 3\mathbf{S}$	yes
$\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$7\mathbf{M} + 2\mathbf{S}$	no
Twisted $\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$9\mathbf{M} + 2\mathbf{S}$	yes

Remark. Standard curves (NIST, SEC, etc.) have large constants. For backward compatibility one should equate $1\mathbf{M} = 1\mathbf{m}$, and the various models have complexity $\sim 4\mathbf{M}$ for doubling, modulo neglibible cost of squaring $\mathbf{S} \sim 0$ using normal bases.

The μ_4-normal form: Edwards origins

An elliptic curve $E/k \subset \mathbb{P}^3$ in twisted Edwards normal form is

$$\boxed{X_0^2 + dX_3^2 = cX_1^2 + X_2^2,\ X_0X_3 = X_1X_2,\ \mathrm{O} = (1:0:1:0),}$$

and an elliptic curve $C/k \subset \mathbb{P}^3$ in μ_4-normal form is defined by

$$\boxed{X_0^2 - rX_2^2 = X_1X_3,\ X_1^2 - X_3^2 = X_0X_2,\ \mathrm{O} = (1:1:0:1).}$$

For $(c,d) = (-1,-16r)$ — a twist by -1, we have an isomorphism

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

Thus, when 2 is invertible, we recognize the μ_4-normal form as a -1-twist of Edwards. Only the latter model is valid over binary fields (has good reduction at 2).

Split $\boldsymbol{\mu}_4$-normal form: properties

When $r = 1/c^4$ (always true for binary finite fields), we can rescale the variables to put C/k in split $\boldsymbol{\mu}_4$-normal form, defined by

$$\boxed{X_0^2 - X_2^2 = c^2 X_1 X_3,\ X_1^2 - X_3^2 = c^2 X_0 X_2,\ \mathrm{O} = (c : 1 : 0 : 1).}$$

Properties:

1. The point $T = (1 : c : 1 : 0)$ is 4-torsion.
2. The translation–by–T morphism is given by:
$$\tau_T(X_0 : X_1 : X_2 : X_3) = (X_3 : X_0 : X_1 : X_2).$$
3. The inverse morphism is defined by:
$$[-1](X_0 : X_1 : X_2 : X_3) = (X_0 : X_3 : X_2 : X_1).$$

Consequently the $\boldsymbol{\mu}_4$-normal form has order divisible by 4.

The twisted μ_4-normal form

Twists of an elliptic curve in characteristic 2 (or of a family in any characteristic, respecting good reduction at 2) should be with respect to a quadratic field extension $k[\omega] = k[x]/(x^2 - x - a)$.

The discriminant of this extension is $D = 1 + 4a$, and the quadratic twist of C/k by the extension $k[\omega]$ is

$$X_0^2 - D r\, X_2^2 = X_1 X_3 - a(X_1 - X_3)^2, \; X_1^2 - X_3^2 = X_0 X_2.$$

In characteristic 2, we have $D = 1$, and this gives the binary twisted μ_4-normal form

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

with identity $(1 : 1 : 0 : 1)$.

Addition laws on $\boldsymbol{\mu}_4$-normal form

Recall: the $\boldsymbol{\mu}_4$-normal form yields an efficient addition algorithm.

Theorem (K. Indocrypt 2012)

Let C/k be an elliptic curve in split $\boldsymbol{\mu}_4$-normal form over a binary field. Setting $U_{ij} = X_iY_j$, the following is a basis for bidegree $(2,2)$-addition laws:

$$\begin{aligned}\big(\,&(U_{13}+U_{31})^2, c(U_{02}U_{31}+U_{20}U_{13}),\\ &(U_{02}+U_{20})^2, c(U_{02}U_{13}+U_{20}U_{31})\,\big),\end{aligned}$$

and

$$\begin{aligned}\big(\,&c(U_{03}U_{10}+U_{21}U_{32}), (U_{10}+U_{32})^2,\\ &c(U_{03}U_{32}+U_{10}U_{21}), (U_{03}+U_{21})^2\,\big),\end{aligned}$$

and their rotations (substitutions $U_{ij} \mapsto U_{i-1,j+1}$).

Addition laws on twisted $\boldsymbol{\mu}_4$-normal form

Theorem (K. Eurocrypt 2017)

Let C^t/k be an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form over a binary field. Setting $U_{ij} = X_i Y_j$, the following is a complete system of two addition laws:

$$\begin{aligned}&((U_{13}+U_{31})^2, c(U_{02}U_{31}+U_{20}U_{13}+aF),\\ &\ (U_{02}+U_{20})^2, c(U_{02}U_{13}+U_{20}U_{31}+aF)),\end{aligned}$$

and (by substituting $U_{ij} \mapsto U_{i-1,j+1}$)

$$\begin{aligned}&((U_{00}+U_{22})^2, c(U_{00}U_{11}+U_{22}U_{33}+aG),\\ &\ (U_{11}+U_{33})^2, c(U_{00}U_{33}+U_{11}U_{22}+aG)),\end{aligned}$$

where $F = V_{13}(U_{02}+U_{20})$ and $G = V_{13}(U_{00}+U_{22})$, for

$$V_{13} = (X_1+X_3)(Y_1+Y_3).$$

Complexity results for μ_4-normal forms

Corollary (K. Indocrypt 2012)

Addition of generic points on an elliptic curve in μ_4-normal form can be computed with $7\mathbf{M} + 2\mathbf{S} + 2\mathbf{m}$.

The extra cost of computing one of the the forms

$$F = V_{13}(U_{02} + U_{20}) \text{ or } G = V_{13}(U_{00} + U_{22}),$$

where $V_{13} = (X_1 + X_3)(Y_1 + Y_3)$ and where the respective cofactor $U_{02} + U_{20}$ or $U_{00} + U_{22}$ is known, adds two multiplications:

Corollary (K. Eurocrypt 2017)

Addition of generic points on an elliptic curve in twisted μ_4-normal form can be computed with $9\mathbf{M} + 2\mathbf{S} + 2\mathbf{m}$.

Efficient doubling

As a consequence of the addition laws we find doubling formulas.

Corollary (K. Eurocrypt 2017)

Doubling on an elliptic curve C in twisted split $\boldsymbol{\mu}_4$-normal form sends $(X_0 : X_1 : X_2 : X_3)$ to

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

if $a = 0$, and to

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

if $a = 1$.

And the complexity of doubling remains the same (twisted or not):

Corollary (K. Eurocrypt 2017)

Doubling on an elliptic curve in twisted split $\boldsymbol{\mu}_4$-normal form with $a \in \{0, 1\}$ can be computed with $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$.

Tabular comparison with known results

We recall the tabular summary of best known complexities for arithmetic:

Curve model	Doubling	Addition	NIST
Lambda coordinates	$3\mathbf{M} + 4\mathbf{S} + 1\mathbf{m}$	$11\mathbf{M} + 2\mathbf{S}$	yes
López-Dahab ($a = 0$)	$2\mathbf{M} + 5\mathbf{S} + 1\mathbf{m}$	$14\mathbf{M} + 3\mathbf{S}$	no
López-Dahab ($a = 1$)	$2\mathbf{M} + 4\mathbf{S} + 2\mathbf{m}$	$13\mathbf{M} + 3\mathbf{S}$	yes
$\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$7\mathbf{M} + 2\mathbf{S}$	no
Twisted $\boldsymbol{\mu}_4$-normal form	$2\mathbf{M} + 5\mathbf{S} + 2\mathbf{m}$	$9\mathbf{M} + 2\mathbf{S}$	yes

Remark. Lambda coordinates can be viewed as a singular version of the twisted $\boldsymbol{\mu}_4$-normal form, projected to $\mathbb{P}^2$. By carrying around four variables (in $\mathbb{P}^3$) rather than three (in $\mathbb{P}^2$), one obtains faster algorithms.

Conclusions

The faster complexity of $\boldsymbol{\mu}_4$-normal form should be used when one can choose the binary curve and its parameters:

- The $\boldsymbol{\mu}_4$-normal form, when a 4-torsion point exists ($a = 0$), previously reduced the complexity of addition on López-Dahab from $14\mathbf{M} + 3\mathbf{S}$ to $7\mathbf{M} + 2\mathbf{S}$.
- The twisted $\boldsymbol{\mu}_4$-normal form defined here reduces the complexity of addition, $13\mathbf{M} + 3\mathbf{S}$ for López-Dahab ($a = 1$) or $11\mathbf{M} + 2\mathbf{S}$ for Lambda coordinates, to $9\mathbf{M} + 2\mathbf{S}$, coupled with doubling essentially as efficient as López-Dahab (up to $1\mathbf{S}$).

When backwards compatibility with binary NIST and SEC standard curves is required, twisted $\boldsymbol{\mu}_4$-normal form should be used.

Thanks for your attention!