Compression for trace zero points on twisted Edwards curves

Giulia Bianco and Elisa Gorla*

Institut de Mathématiques, Université de Neuchâtel
Rue Emile-Argand 11, CH-2000 Neuchâtel, Switzerland

Abstract

We propose two optimal representations for the elements of trace zero subgroups of twisted Edwards curves. For both representations, we provide efficient compression and decompression algorithms. The efficiency of the algorithm is compared with the efficiency of similar algorithms on elliptic curves in Weierstrass form.

Introduction

Trace zero subgroups are subgroups of the groups of points of an elliptic curve over extension fields. They were first proposed for use in public key cryptography by Frey in [10]. A main advantage of trace zero subgroups is that they offer a better scalar multiplication performance than the whole group of points of an elliptic curve of approximately the same cardinality. This allows a fast arithmetic, which can speed up the calculations by 30% compared with elliptic curves groups (see e.g. [13] for the case of hyperelliptic curves, [3] and [8] for elliptic curves over fields of even characteristic). In addition, computing the cardinality of a trace zero subgroup is more efficient than for the group of points of an elliptic curve of approximately the same cardinality. Moreover, even if the trace zero subgroup is a proper subgroup of the group of rational points of the curve over an extension field, the Discrete Logarithm Problem (DLP) in the two groups has the same complexity. Hence, when working over non-prime fields, we may restrict to the trace zero subgroup to gain a more efficient arithmetic without compromising the security. Finally, in the context of pairings trace zero subgroups of supersingular elliptic curves offer higher security than supersingular elliptic curves of the same bit-size, as shown in [15].

The problem of how to compress the elements of the trace zero subgroup of an elliptic or hyperelliptic curve is the analogue of torus-based cryptography in finite fields. For elliptic and hyperelliptic curves this problem has been studied by many authors, see [14], [13], [17], [15], [11], and [12].

Edwards curves were first introduced by H.M. Edwards in [9] as a normal form for elliptic curves. They were proposed for use in elliptic curve cryptography by Bernstein and Lange in [4]. Twisted Edwards curves were introduced shortly after in [6]. They are relevant from

*The research reported in this paper was partially supported by the Swiss National Science Foundation under grant no. 200021_150207.

a cryptographic point of view since the group operation can be computed very efficiently and via strongly unified formulas, i.e. formulas that do not distinguish between addition and doubling. This makes them more resistant to side-channel attacks. We refer to [4], [5], and [6] for a detailed discussion of the advantages of Edwards curves.

In this paper, we provide two efficient representations for the elements of the trace zero subgroups of twisted Edwards curves. The first one follows ideas from [11] and it is based on Weil restriction of scalars and Semaev's summation polynomials. The second one follows ideas from [12] and it makes use of rational functions on the curve. Some obstacles have to be overcome in adapting these ideas to Edwards curves, especially for adapting the method from [12].

Given a twisted Edwards curve defined over a finite field $\mathbb{F}_q$ of odd characteristic and a field extension of odd prime degree $\mathbb{F}_q \subset \mathbb{F}_{q^n}$, we consider the trace zero subgroup $\mathcal{T}_n$ of the group of $\mathbb{F}_{q^n}$-rational points of the curve. We give two efficiently computable maps from $\mathcal{T}_n$ to $\mathbb{F}_q^{n-1}$, such that inverse images can also be efficiently computed. One of our maps identifies Frobenius conjugates, while the other identifies Frobenius conjugates and opposites of points. Since $\mathcal{T}_n$ has order $\mathcal{O}(q^{n-1})$, our maps are optimal representations of $\mathcal{T}_n$ modulo Frobenius equivalence. For both representations we provide efficient algorithms to compute the image and the preimage of an element, that is, to compress and decompress points. We also compare with the corresponding algorithms for trace zero subgroups of elliptic curves in short Weierstrass form.

The article is organized as follows: In Section 1 we give some preliminaries on twisted Edwards curves, finite fields, trace zero subgroups, and representations. In Section 2 we present our first optimal representation based on Weil restriction and summations polynomials, and give compression and decompression algorithms. We then make explicit computations for the cases $n = 3$ and $n = 5$, and compare execution times of our Magma implementation with those of the corresponding algorithms for elliptic curves in short Weierstrass form. In Section 3 we propose another representation based on rational functions, with the corresponding algorithms, computations, and efficiency comparison.

1 Preliminaries and notations

Let $\mathbb{F}_q$ be a finite field of odd characteristic and let $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ be a field extension of odd prime degree. Choose a normal basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If $n|q-1$, let $\mathbb{F}_{q^n} = \mathbb{F}_q[\xi]/(\xi^n - \mu)$, where μ is not a n^{th}-power in $\mathbb{F}_q$, and choose the basis $\{1, \xi, \ldots, \xi^{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Either of these choices is suitable for computation, since it produces sparse equations. When writing explicit formulas, we always assume that we are in the latter situation.

When counting the number of operations in our computations, we denote respectively by M, S, and I multiplications, squarings, and inversions in the field. We do not take into account additions and multiplications by constants. The timings for the implementation of our algorithms in Magma refer to version V2.20-7 of the software, running on a single 3 GHz core.

1.1 Twisted Edwards curves

Definition 1. A **twisted Edwards curve** over $\mathbb{F}_q$ is a plane curve of equation

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

where $a, d \in \mathbb{F}_q \setminus \{0\}$ and $a \neq d$. An **Edwards curve** is a twisted Edwards curve with $a = 1$.

Twisted Edwards curves are curves of geometric genus one with two ordinary multiple points, namely the two points at infinity. Since $E_{a,d}$ is birationally equivalent to a smooth elliptic curve, one can define a group law on the set of points of $E_{a,d}$, called the twisted Edwards addition law.

Definition 2. The sum of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ of $E_{a,d}$ is defined as

$$P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

We refer to [4, Section 3] and [6, Section 6] for a detailed discussion on the formulas and a proof of correctness. The point $\mathcal{O} = (0, 1) \in E_{a,d}$ is the neutral element of the addition, and we denote by $-P$ the additive inverse of P. If $P = (x, y)$, then $-P = (-x, y)$. We let $\mathcal{O}' = (0, -1) \in E_{a,d}$, and denote by $\Omega_1 = [1, 0, 0]$ and $\Omega_2 = [0, 1, 0]$ the two points at infinity of $E_{a,d}$.

Edwards curves were introduced in [9] as a convenient normal form for elliptic curves. Over an algebraically closed field, every elliptic curve in Weierstrass form is birationally equivalent to an Edwards curve, and vice versa. This is however not the case over $\mathbb{F}_q$, where Edwards curves represent only a fraction of elliptic curves in Weierstrass form. In [6, Theorem 3.2] it is shown that a twisted Edwards curve defined over $\mathbb{F}_q$ is birationally equivalent over $\mathbb{F}_q$ to an elliptic curve in Montgomery form, and conversely, an elliptic curve in Montgomery form defined over $\mathbb{F}_q$ is birationally equivalent over $\mathbb{F}_q$ to a twisted Edwards curve.

Proposition 3. *The twisted Edwards curve $E_{a,d}$ defined over $\mathbb{F}_q$ is birationally equivalent over $\mathbb{F}_q$ to the elliptic curve in Montgomery form $E_{A,B} : By^2 = x^3 + Ax^2 + x$, where $A = 2\frac{a+d}{a-d}$ and $B = \frac{4}{a-d}$. Let $\overline{E}_{a,d}$ and $\overline{E}_{A,B}$ be the projective closures of $E_{a,d}$ and $E_{A,B}$, respectively. The birational isomorphism $\Phi : \overline{E}_{A,B} \longrightarrow \overline{E}_{a,d}$ is defined via*

$$\phi([x, y, z]) = [x(x + z), y(x - z), y(x + z)] \quad \textit{if } [x, y, z] \notin \{\Omega_2, (0, 0)\} \quad \textit{and}$$

$$\phi([x, y, z]) = [By(x+z), By^2-x^2-Axz-z^2, By^2+x^2+Axz+z^2] \quad \textit{if } [x, y, z] \notin \{Q_1, Q_2, Q_3, Q_4\},$$

where $Q_1 = \left(\frac{\sqrt{d}+\sqrt{a}}{\sqrt{d}-\sqrt{a}}, 0\right)$, $Q_2 = \left(\frac{\sqrt{d}-\sqrt{a}}{\sqrt{d}+\sqrt{a}}, 0\right)$, $Q_3 = (-1, \sqrt{d})$, $Q_4 = (-1, -\sqrt{d}) \in E_{A,B}$.

Proof. It is easy to check that Φ is well defined and $\Phi(Q_1) = \Phi(Q_2) = \Omega_1$ and $\Phi(Q_3) = \Phi(Q_4) = \Omega_2$. Moreover Φ is injective on $\overline{E}_{A,B} \setminus \{Q_1, Q_2, Q_3, Q_4\}$, and its birational inverse is $\Psi : \overline{E}_{a,d} \setminus \{\Omega_1, \Omega_2\} \longrightarrow \overline{E}_{A,B}$ given by

$$\Psi([x, y, z]) = \begin{cases} [x(z + y), z(z + y), x(z - y)] & \text{if } [x, y, z] \neq \mathcal{O}', \\ [z(z + y)(z - y), x(az^2 - dy^2), z(z - y)^2] & \text{if } [x, y, z] \neq \mathcal{O}. \end{cases}$$

□

Moreover, the twisted Edwards addition law corresponds to the usual addition law on the birationally isomorphic elliptic curve in Montgomery form, as shown in [4, Theorem 3.2]. Similarly to elliptic curves in Montgomery or Weierstrass form, the twisted Edwards addition law has a geometric interpretation.

Proposition 4. ([2, Section 4]) *Let $P_1, P_2 \in E_{a,d}$, and let C be the projective conic passing through P_1, P_2, Ω_1, Ω_2, and $\mathcal{O}'$. Then the point $P_1 + P_2$ is the symmetric with respect to the y-axis of the eighth point of intersection between $E_{a,d}$ and C.*

1.2 Trace zero subgroups

Let $E_{a,d}$ be a twisted Edwards curve defined over $\mathbb{F}_q$. We denote by $E_{a,d}(\mathbb{F}_{q^n})$ the group of $\mathbb{F}_{q^n}$-rational points of $E_{a,d}$, by P_∞ any point at infinity of $E_{a,d}$, and by φ the Frobenius endomorphism on $E_{a,d}$:

$$\varphi : E_{a,d} \longrightarrow E_{a,d} \ , \ (x, y) \mapsto (x^q, y^q) \ , \ P_\infty \mapsto P_\infty.$$

Definition 5. The **trace zero subgroup** $\mathcal{T}_n$ of $E_{a,d}(\mathbb{F}_{q^n})$ is the kernel of the trace map

$$\mathrm{Tr} : E_{a,d}(\mathbb{F}_{q^n}) \longrightarrow E_{a,d}(\mathbb{F}_q) \ , \ P \mapsto P + \varphi(P) + \varphi^2(P) + \cdots + \varphi^{n-1}(P).$$

We can view $\mathcal{T}_n$ as the $\mathbb{F}_q$-rational points of an abelian variety of dimension $n-1$ defined over $\mathbb{F}_q$, called the trace zero variety. We refer to [1] for a construction and the basic properties of the trace zero variety. The following result is an easy consequence of [1], Proposition 7.13.

Proposition 6. *The sequence*

$$0 \longrightarrow E_{a,d}(\mathbb{F}_q) \longrightarrow E_{a,d}(\mathbb{F}_{q^n}) \stackrel{\varphi - \mathrm{id}}{\longrightarrow} \mathcal{T}_n \longrightarrow 0$$

is exact. Therefore the DLPs in $E_{a,d}(\mathbb{F}_{q^n})$ and in $\mathcal{T}_n$ have the same complexity.

1.3 Representations

Definition 7. A *representation of size ℓ* for the elements of a finite set G is a map

$$\mathcal{R} : G \longrightarrow \mathbb{F}_2^\ell.$$

Notice that, in our setup, a representation $\mathcal{R}$ is not necessarily injective. Nevertheless, any representation induces an injective representation

$$\overline{\mathcal{R}} : G/\sim \longrightarrow \mathbb{F}_2^\ell,$$

where $g \sim h$ iff $\mathcal{R}(g) = \mathcal{R}(h)$ for any $g, h \in G$.

Definition 8. Let $\mathcal{A}$ be a family of abelian varieties of fixed dimension d. An *optimal representation* for $\mathcal{A}$ is a family of representations $\mathcal{R} : A(\mathbb{F}_q) \longrightarrow \mathbb{F}_2^\ell$ for all finite fields $\mathbb{F}_q$ and for all $A \in \mathcal{A}$ defined over $\mathbb{F}_q$, with the property that

$$\ell = \ell(q) = \lceil \log_2 |A(\mathbb{F}_q)| \rceil + \mathcal{O}(1) = d \lceil \log_2 q \rceil + \mathcal{O}(1).$$

We also say that each $\mathcal{R}$ is an *optimal representation* for the elements of $A(\mathbb{F}_q)$.

Given $g \in A(\mathbb{F}_q)$, $x \in \mathrm{Im}\,\mathcal{R}$, we refer to computing $\mathcal{R}(g)$ as *compression* and $\mathcal{R}^{-1}(x)$ as *decompression*.

Intuitively, a representation is optimal if $\ell(q)$ is the smallest possible length of a binary representation of the elements of $A(\mathbb{F}_q)$, up to an additive constant. In particular, the length of a representation is regarded as a function of q, while the dimension d of the varieties is assumed to be constant. Notice moreover that, if $|\mathcal{R}^{-1}(x)| \in \mathcal{O}(1)$ as a function of q, then

$$\ell(q) = \lceil \log_2 |A(\mathbb{F}_q)| \rceil = \lceil \log_2 |A(\mathbb{F}_q)/\sim| \rceil + \mathcal{O}(1).$$

In particular, optimality of a representation does not depend on the number of elements that are identified, under the assumption that this number is upper bounded by a constant in q. Therefore Definition 8 is well-posed.

Remark 9. The problem of representing the elements of $\mathbb{F}_q$ via binary strings of length $\lceil \log_2 q \rceil$ is well studied. Therefore, an optimal representation for $\mathcal{A}$ may be given via a family of maps

$$\mathcal{R} : A(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^d \times \mathbb{F}_2^k$$

where $k \in \mathcal{O}(1)$.

The problem of finding an optimal representation has been studied for the following families of abelian varieties: elliptic curves, Jacobians of hyperelliptic curves of fixed genus, trace zero varieties of elliptic or hyperelliptic curves of fixed genus and with respect to a field extension of fixed degree. One may also let $\mathcal{A}$ consist of only one element, e.g. the multiplicative group, or its primitive subgroup. Finding an optimal representation for the latter is at the core of torus-based cryptography.

In this paper, we let $\mathcal{A}$ be the set of trace zero varieties of Edwards curves, with respect to a field extension of fixed prime degree n, $n \neq 2$. We construct two optimal representations for the elements of $\mathcal{T}_n$, with the property that each element in the image has at most $2n$, respectively n inverse images.

2 An optimal representation using summation polynomials

Let $\mathbb{F}_q$ be a finite field of odd characteristic and let $E_{a,d}$ be the twisted Edwards curve of equation

$$ax^2 + y^2 = 1 + dx^2y^2$$

where $a, d \in \mathbb{F}_q \backslash \{0\}$ and $a \neq d$. Following ideas from [11], in this section we use Weil restriction of scalars and Semaev's summation polynomials to write an equation for the subgroup $\mathcal{T}_n$. Similarly to the case of elliptic curves in Weierstrass form, a point $P = (x, y) \in E_{a,d}(\mathbb{F}_{q^n})$ can be represented via $y \in \mathbb{F}_{q^n}$. Using the curve equation, the value of x can be recovered up to sign. Hence, after choosing an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$, each pair of points $\pm P \in E_{a,d}(\mathbb{F}_{q^n})$ can be represented by the element $(y_0, \ldots, y_{n-1}) \in \mathbb{F}_q^n$ corresponding to $y \in \mathbb{F}_{q^n}$ under the isomorphism $\mathbb{F}_{q^n} \cong \mathbb{F}_q^n$ induced by the chosen basis. Having an equation for $\mathcal{T}_n$ allows us to drop one of the y_i's and represent each pair $\pm P$ via $n-1$ coordinates in $\mathbb{F}_q$, thus providing an optimal representation for the elements of $\mathcal{T}_n$. In order to make computation of the compression and decompression maps more efficient, we modify this basic idea and use the elementary symmetric functions of $y, y^q, \ldots, y^{q^{n-1}}$ instead of the vector $(y_0, \ldots, y_{n-1}) \in \mathbb{F}_q^n$.

Summation polynomials were introduced by Semaev in [16] for elliptic curves in Weierstrass form. Here we use them in the form for Edwards curves from [18].

Definition 10. The n-th **summation polynomial** is denoted by f_n and defined recursively by

$$f_3(z_1,z_2,z_3) = (z_1^2z_2^2 - z_1^2 - z_2^2 + ad^{-1})z_3^2 + 2(d-a)d^{-1}z_1z_2z_3 + ad^{-1}(z_1^2+z_2^2-1) - z_1^2z_2^2,$$

$$f_n(z_1,\ldots,z_n) = \mathrm{res}_t(f_{n-k}(z_1,\ldots,z_{n-k-1},t), f_{k+2}(z_{n-k},\ldots,z_n,t))$$

for all $n \geq 4$ and for all $1 \leq k \leq n-3$, where $\mathrm{res}_t(f_i,f_j)$ denotes the resultant of f_i and f_j with respect to t.

The next theorem summarizes the properties of summation polynomials.

Theorem 11 ([16] Section 2 and [18] Section 2.3.1)**.** *Let $n \geq 3$, let $f_n \in \mathbb{F}_q[z_1,\ldots,z_n]$ be the n-th summation polynomial. Denote by $\mathbb{F}_q \subset k$ a field extension, and by $\overline{k}$ its algebraic closure. Then:*

1. *f_n is absolutely irreducible, symmetric, and has degree 2^{n-2} in each of the variables.*
2. *$(\beta_1,\ldots,\beta_n) \in k^n$ is a root of f_n if and only if there exist $\alpha_1,\ldots,\alpha_n \in \overline{k}$ such that $P_i = (\alpha_i,\beta_i) \in E_{a,d}(\overline{k})$ and $P_1 + \ldots + P_n = \mathcal{O}$.*

By the previous theorem, if $P = (x,y) \in \mathcal{T}_n$, then

$$f_n(y, y^q, \ldots, y^{q^{n-1}}) = 0. \tag{1}$$

A partial converse and exceptions to the opposite implication are given in the next proposition.

Proposition 12. ([11, Lemma 1 and Proposition 4]) *Let $E_{a,d}$ be a twisted Edwards curve and denote by $E_{a,d}[m]$ its m-torsion points. We have:*

(1) $\mathcal{T}_3 = \{(x,y) \in E_{a,d}(\mathbb{F}_{q^3}) \mid f_3(y,y^q,y^{q^2}) = 0\}$,

(2) $\mathcal{T}_5 \cup E_{a,d}[3](\mathbb{F}_q) = \{(x,y) \in E_{a,d}(\mathbb{F}_{q^5}) \mid f_5(y,y^q,\ldots,y^{q^4}) = 0\}$,

(3) $\mathcal{T}_n \cup \bigcup_{k=1}^{\lfloor \frac{n}{2} \rfloor} E_{a,d}[n-2k](\mathbb{F}_q) \subseteq \{(x,y) \in E_{a,d}(\mathbb{F}_{q^n}) \mid f_n(y,y^q,\ldots,y^{q^{n-1}}) = 0\}$ *for $n \geq 7$.*

Proof. The proof proceeds as in Lemma 1 and Proposition 4 of [11], after observing that for any odd prime n one has $E_{a,d}[2] \cap \mathcal{T}_n = \{\mathcal{O}\}$. □

Remark 13. Proposition 12 raises the question of efficiently deciding, for each root $y \in \mathbb{F}_{q^n}$ of equation (1), whether the corresponding points $(\pm x, y) \in E_{a,d}$ are elements of $\mathcal{T}_n$. However, this issue is easily solved in the two cases of major interest $n = 3$ and $n = 5$. In fact:

- By Proposition 12 (1), $(\pm x, y) \in \mathcal{T}_3$ if and only if $x \in \mathbb{F}_{q^3}$.
- By Proposition 12 (2), $(\pm x, y) \in \mathcal{T}_5$ if and only if $x \in \mathbb{F}_{q^5}$ and $(\pm x, y) \notin E_{a,d}[3](\mathbb{F}_q) \backslash \{\mathcal{O}\}$. By storing the list $\mathcal{L}$ of the y-coordinates of the elements of $E_{a,d}[3](\mathbb{F}_q) \setminus \{\mathcal{O}\}$, one can easily decide whether a point of $E_{a,d}(\mathbb{F}_{q^5})$ of coordinates (x,y) belongs to $\mathcal{T}_5$ by checking that $y \notin \mathcal{L}$. Notice that $\mathcal{L}$ consists of at most 4 elements of $\mathbb{F}_q$.

Using the above considerations as a starting point, we can give an optimal representation for the points of $\mathcal{T}_n$ with efficient compression and decompression algorithms.

1. Denote by $e_1, \ldots, e_n$ the elementary symmetric functions in n variables. Represent $(x, y) \in \mathcal{T}_n$ via $n-1$ of the elementary symmetric functions evaluated at $y, y^q, \ldots, y^{q^{n-1}}$. We obtain an efficiently computable optimal representation

$$\begin{array}{rccc} \mathcal{R}: & \mathcal{T}_n & \longrightarrow & \mathbb{F}_q^{n-1} \\ & (x,y) & \longmapsto & (e_i(y, y^q, \ldots, y^{q^{n-1}}))_{i=1,\ldots,n-1}. \end{array} \tag{2}$$

2. Since the polynomial $f_n(z_1, \ldots, z_n)$ is symmetric, we can write it uniquely as a polynomial $g_n(e_1, \ldots, e_n) \in \mathbb{F}_q[e_1, \ldots, e_n]$. Therefore, the equation

$$g_n(e_1, \ldots, e_n) = 0$$

describes trace zero points (with the exceptions seen in Proposition 12) via the equations

$$e_1 = \tilde{e}_1(y_0, \ldots, y_{n-1}), \ldots, e_n = \tilde{e}_n(y_0, \ldots, y_{n-1}), \tag{3}$$

where the polynomials $\tilde{e_1}, \ldots, \tilde{e_n}$ are obtained from the polynomials

$$e_1(y, y^q, \ldots, y^{q^{n-1}}), \ldots, e_n(y, y^q, \ldots, y^{q^{n-1}})$$

by Weil restriction of scalars with respect to the chosen basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and reducing modulo $y_i^q - y_i$ for $i \in \{0, \ldots, n-1\}$. Notice that the reduction simplifies the equations by drastically reducing their degrees. Moreover, it does not alter their values when evaluated over $\mathbb{F}_q$.

3. For $(e_1, \ldots, e_{n-1}) \in \mathcal{R}(\mathcal{T}_n)$, we first solve $g_n(e_1, \ldots, e_{n-1}, t) = 0$ for t. For any solution $e_n \in \mathbb{F}_q$, we solve system (3) to find $(y_0, \ldots, y_{n-1}) \in \mathbb{F}_q^n$, corresponding to $y \in \mathbb{F}_{q^n}$. From y we can recover x in the usual way (see also Remark 13).

Notice that $g_n(e_1, \ldots, e_n,)$ is not linear in any of the variables for $n \geq 3$, hence in step 3 we may find more than one value for e_n. This corresponds to the fact that $\mathcal{R}$ may identify more than just opposites and Frobenius conjugates. However this is a rare phenomenon, and for a generic point $P \in \mathcal{T}_n$, $\mathcal{R}^{-1}(\mathcal{R}(P))$ consists only of $\pm P$ and their Frobenius conjugates. We come back to this discussion in Subsection 2.2, where we discuss this issue for $n = 5$.

We now give the pseudocode of a compression and decompression algorithm for the elements of $\mathcal{T}_n$.

Algorithm 1 (Compression).

Input : $P = (x, y) \in \mathcal{T}_n$
Output : $\mathcal{R}(P) \in \mathbb{F}_q^{n-1}$

1: Write $y = y_0\alpha + \ldots + y_{n-1}\alpha^{q^{n-1}}$.
2: Compute $e_i = \tilde{e}_i(y_0, \ldots, y_{n-1})$ for $i = 1, \ldots, n-1$.
3: **return** $(e_1, \ldots, e_{n-1})$

Algorithm 2 (Decompression).

Input : $(e_1, \ldots, e_{n-1}) \in \mathbb{F}_q^{n-1}$
Output : $\mathcal{R}^{-1}(e_1, \ldots, e_{n-1}) \subseteq \mathcal{T}_n$

1: Solve $g_n(e_1, \ldots, e_{n-1}, t) = 0$ for t in $\mathbb{F}_q$.
2: $T \leftarrow$ list of solutions of $g_n(e_1, \ldots, e_{n-1}, t) = 0$ in $\mathbb{F}_q$.
3: **for** $e_n \in T$, find a solution in $\mathbb{F}_q^n$of the system

$$\begin{cases} e_1 &= \tilde{e}_1(y_0, \ldots, y_{n-1}) \\ &\vdots \qquad\qquad \text{if it exists.} \\ e_n &= \tilde{e}_n(y_0, \ldots, y_{n-1}) \end{cases}$$

4: Any time a solution $(y_0, \ldots, y_{n-1})$ is found, compute $y = y_0\alpha + \cdots + y_{n-1}\alpha^{q^{n-1}}$.
5: Recover one of the corresponding x-coordinates using the curve equation.
6: **end for**
7: **if** $(x, y) \in \mathcal{T}_n$ **then**
8: Add $P = (\pm x, y)$ and all its Frobenius conjugates to the list L of output points.
9: **end if**
10: **return** L

2.1 Explicit equations, complexity, and timings for $n = 3$

In this subsection we give explicit equations for trace zero point compression and decompression on twisted Edwards curves for $n = 3$. We also estimate the number of operations needed for the computations, present some timings obtained with Magma, and compare with the results from [11] for elliptic curves in short Weierstrass form.

The symmetrized third summation polynomial for $E_{a,d}$ is

$$g_3(e_1, e_2, e_3) = e_1^2 - 1 + (d/a)(e_3^2 - e_2^2) + (2d/a)e_1e_3 - 2e_2 + ((-2a + 2d)/a)e_3, \tag{4}$$

where e_1, e_2 and e_3 are the elementary symmetric polynomials in y, y^q, y^{q^2}:

$$\begin{cases} e_1 &= y + y^q + y^{q^2} \\ e_2 &= y^{1+q} + y^{1+q^2} + y^{q+q^2} \\ e_3 &= y^{1+q+q^2}. \end{cases} \tag{5}$$

The symmetrized third summation polynomial for an elliptic curve in short Weierstrass form is

$$G_3(e_1, e_2, e_3) = e_2^2 - 4e_1e_3 - 4Be_1 - 2Ae_2 + A^2. \tag{6}$$

Notice that, while G_3 is linear in e_1 and e_3, g_3 is of degree 2 in each variable. In particular, none of e_1, e_2, e_3 is determined uniquely by the other two as is the case of elliptic curves in Weierstrass form. However, applying the change of coordinates

$$\begin{cases} t_1 &= e_1 \\ t_2 &= e_3 + e_2 \\ t_3 &= e_3 - e_2 \end{cases} \tag{7}$$

to g_3, we obtain the polynomial

$$\tilde{g}_3(t_1, t_2, t_3) = t_1^2 + (d/a)(t_2t_3 + t_1t_2 + t_1t_3) + ((d/a) - 2)t_2 + dt_3 - 1, \tag{8}$$

that is linear in both t_2 and t_3.

Applying Weil restriction of scalars to the combination of (5) and (7) (and following the conventions of Section 1) we obtain

$$\begin{cases} t_1 &= 3y_0 \\ t_2 &= y_0^3 - 3\mu y_0y_1y_2 + \mu y_1^3 + \mu^2 y_2^3 + 3y_0^2 - 3\mu y_1y_2 \\ t_3 &= y_0^3 - 3\mu y_0y_1y_2 + \mu y_1^3 + \mu^2 y_2^3 - 3y_0^2 + 3\mu y_1y_2 \end{cases} \tag{9}$$

which expresses t_1, t_2, t_3 as polynomials in y_0, y_1, y_2.

Point Compression. For compression of a point $P = (x, y) \in \mathcal{T}_3$ we use the first two coordinates from (7) and (9), obtaining

$$\mathcal{R}(P) = (t_1, t_2) = (3y_0, y_0^3 - 3\mu y_0y_1y_2 + \mu y_1^3 + \mu^2 y_2^3 + 3y_0^2 - 3\mu y_1y_2).$$

If we compute t_2 as $(y_0 + 1)(y_0^2 - 3\mu y_1y_2) + \mu y_1^3 + \mu^2 y_2^3 + 2y_0^2$, the cost of computing $\mathcal{R}(P)$ is 3S+4M in $\mathbb{F}_q$. In the case of elliptic curves in short Weierstrass form, computing the representation of a point is less expensive, as it takes 1S+1M in $\mathbb{F}_q$ or 1M in $\mathbb{F}_q$ with the two methods presented in [11, Section 5].

Point Decompression. In order to decompress $(t_1, t_2) \in \operatorname{Im}\mathcal{R}$ we proceed as follows.

1. Given $(t_1, t_2) \in \operatorname{Im}\mathcal{R}$, solve $\tilde{g}_3(t_1, t_2, t_3) = 0$ for t_3. If $t_1 + t_2 + a = 0$, then $\tilde{g}_3(t_1, t_2, t_3) = 0$ for all $t_3 \in \mathbb{F}_q$. If $t_1 + t_2 + a \neq 0$, then

$$t_3 = -\frac{((d/a) - 2)t_2 + (d/a)t_1t_2 + (t_1 + 1)(t_1 - 1)}{(d/a)(t_1 + t_2 + a)}.$$

Hence t_3 can be computed with 3M+1I in $\mathbb{F}_q$.

2. Given (t_1, t_2, t_3), we solve system (9) for y_0, y_1, y_2. Notice that, since the t_i's are obtained from the e_i's by a linear change of coordinates, all considerations from [11] apply to our situation. In particular, one can compute y from (t_1, t_2, t_3) with at most 3S+3M+1I, 1 square root and 2 cube roots in $\mathbb{F}_q$.

Summarizing, the complete decompression algorithm takes at most 3S+6M+2I, 1 square root, and 2 cube roots in $\mathbb{F}_q$. For elliptic curves in short Weierstrass form, decompression takes at most 3S+5M+2I, 1 square root, and 2 cube roots in $\mathbb{F}_q$ or 4S+4M+2I, 1 square roots and 2 cube roots in $\mathbb{F}_q$, depending on the method used. We refer the interested reader to [11, Section 5] for details on the complexity of the computation for curves in short Weierstrass form.

Remark 14. Notice that one can also use (t_1, t_3) as an optimal representation of $(x, y) \in \mathcal{T}_3$, and then solve $\tilde{g_3}$ for t_2 in order to recover y. This choice is analogous to the one we have made, and the computational cost of compression and decompression does not change.

Remark 15. The symmetry of twisted Edwards curves makes the computation of point addition on these curves more efficient than on elliptic curves in short Weierstrass form. However, the same symmetry results in summation polynomials of higher degree and with a denser support. This explains our empirical observation that the summation polynomials in the elementary symmetric functions for elliptic curves in short Weierstrass form are sparser than those for twisted Edwards curves for $n = 3, 5$, even though for both curves they have the same degree 2^{n-2}. For $n = 3$, this behavior is apparent if one compares equations (4) and (6). Therefore, one should expect that compression and decompression for a representation based on summation polynomials for twisted Edwards curves are less efficient than for elliptic curves in short Weierstrass form. This is confirmed by our findings.

The following examples and statistics have been implemented in Magma [7].

Example 16. Let $q = 2^{79} - 67$ and $\mu = 3$. We choose random curves, defined and birationally equivalent over $\mathbb{F}_q$:

$$E_{a,d} : 31468753957068040687814x^2 + y^2 = 1 + 19269782127663896649899 7x^2y^2$$

and

$$E : y^2 = x^3 + 2924678484276594994785 03x + 361361026736404004345421.$$

We choose a random point of trace zero $P' \in E(\mathbb{F}_{q^3})$, and let P be the corresponding point on $E_{a,d}$. For brevity, here we only write the x-coordinates of points of E and the y-coordinates of points of $E_{a,d}$:

$$P' = 34656092814607695931475 3\xi^2 + 45682653962853598103421 2\xi + 34416747040302665282667 2,$$

$$P = 20852071389751823621596 6\xi^2 + 45112194455021994736881 1\xi + 68041089860429901306252.$$

We represent the points of E using the compression coordinates (t_1, t_2) from [11, Section 5]. Denote by $\mathcal{R}$ and $\mathcal{R}'$ the representation maps on $E_{a,d}$ and E, respectively. We compute

$$\mathcal{R}'(P') = (344167470403026652826672, 334324534997495805088214),$$

$$\mathcal{R}(P) = (20412326958128970391875 6, 98788782936076524413527).$$

We now apply the corresponding decompression algorithms to $\mathcal{R}'(P')$ and $\mathcal{R}(P)$. We obtain

$$\mathcal{R}'^{-1}(344167470403026652826672, 334324534997495805088214) =$$

$$\{34656092814607695931475 3\xi^2 + 45682653962853598103421 2\xi + 34416747040302665282667 2,$$

$$16475949861450750318749 3\xi^2 + 36152069098819775153438 1\xi + 34416747040302665282667 2,$$

$$93142483046730124850775\xi^2 + 39057858899789544213744 9\xi + 34416747040302665282667 2\},$$

which are exactly the x-coordinate of P' and its Frobenius conjugates. Similarly

$$\mathcal{R}^{-1}(20412326958128970391875 6, 98788782936076524413527) =$$

$$\{20852071389751823621596 6\xi^2 + 45112194455021994736881 1\xi + 68041089860429901306252,$$

$$53932153696106685501116 7\xi^2 + 23743139109764296838671 9\xi + 68041089860429901306252,$$

$$46108356875604408347890 9\xi^2 + 52037248396676625895051 2\xi + 68041089860429901306252\},$$

which are exactly the y-coordinate of P and its Frobenius conjugates.

We now give an estimate of the average time of compression and decompression for groups of different bit-size. We consider primes q_1, q_2, and q_3 such that $3|q_i - 1$ for all i, of bit-length 96, 112, and 128, respectively. For each q_i, we consider five pairs of birationally equivalent curves $(E, E_{a,d})$ defined over $\mathbb{F}_{q_i}$, such that the order of $\mathcal{T}_3$ is prime of bit-length respectively 192, 224 and 256. On each pair of curves we randomly choose $20'000$ pairs of points (P', P) of trace zero, as in Example 16. For each pair of points, we compute $\mathcal{R}'(P'), \mathcal{R}(P), \mathcal{R}'^{-1}(\mathcal{R}'(P')), \mathcal{R}^{-1}(\mathcal{R}(P))$. For each computation, we consider the average time in milliseconds for each curve, and then the averages over the five curves. The average computation times are reported in the table below.

Table 1.

Bit-length of $\lvert\mathcal{T}_3\rvert$	192	224	256
Compression on E	0.006	0.005	0.006
Compression on $E_{a,d}$	0.016	0.017	0.015
Decompression on E	0.81	2.40	1.20
Decompression on $E_{a,d}$	0.88	2.44	1.17

The following table contains the ratios between the average times for point compression and decompression on elliptic curves in short Weierstrass form and twisted Edwards curves.

Table 2.

Bit-length of $\lvert\mathcal{T}_3\rvert$	192	224	256
Comp on E / Comp on $E_{a,d}$	0.375	0.294	0.400
Dec on E / Dec on $E_{a,d}$	0.920	0.984	1.026

2.2 Explicit equations, complexity, and timings for $n = 5$

In this subsection we treat in detail the case $n = 5$. We compute explicit equations for compression and decompression, give an estimate of the complexity of the computations in terms of the number of operations, and give some timings computed in Magma. We also compare with the results obtained in [11] for elliptic curves in short Weierstrass form.

The fifth Semaev polynomial f_5 for a twisted Edwards curve has degree 40, while for curves in short Weierstrass form it has degree 32. The first polynomial also contains many more terms than the second. This agrees with what we observed in Remark 15 for the case $n = 3$. The symmetrized fifth summation polynomial g_5 has degree 8 for both Weierstrass and Edwards curves. However, for Edwards curves g_5 has degree 8 in each variable, while for elliptic curves in short Weierstrass form it has degree 6 in some of the variables. Because of these reasons, we expect that compression and decompression for a trace zero subgroup coming from a twisted Edwards curve are less efficient than for one coming from a curve in short Weierstrass form.

For fields such that $16|q-1$, we perform a linear change of coordinates on the e_i's in order to obtain a polynomial $\tilde{g}_5$, of degree strictly less than 8 in some variable. The polynomial g_5 is too big to be printed here. However, denoting by $(g_5)_8$ the part of g_5 which is homogeneous

of degree 8, we have:

$$(g_5)_8(e_1,\ldots,e_5) = e_1^8 + (d/a)^4(e_2^8+e_3^8) + (d/a)^8(e_4^8+e_5^8). \tag{10}$$

Let $\mu_1 \in \overline{\mathbb{F}}_q$ be a primitive 16-th roots of unity. Then we can factor t^8+s^8 over $\mathbb{F}_q$ as

$$t^8+s^8 = (t-\mu_1 s)(t+\mu_1 s)r_6(t,s).$$

Therefore, (10) can be written in the form

$$(g_5)_8 = e_1^8 + (d/a)^4(e_2-\mu_1 e_3)(e_2+\mu_1 e_3)r_6(e_2,e_3) + (d/a)^8(e_4^8+e_5^8).$$

Hence, after performing the change of coordinates

$$\begin{cases} t_2 &= e_2-\mu_1 e_3 \\ t_3 &= e_2+\mu_1 e_3 \\ t_i &= e_i \text{ for } i=1,4,5 \end{cases}$$

we obtain a polynomial $\tilde{g}_5(t_1,\ldots,t_5)$ of degree 8 in t_1,t_4,t_5, and degree 7 in t_2,t_3.

Example 17. Let $q = 2^{10}-3$, $\mu = 2$. Consider the Edwards curve $E_{1,486}$ of equation $x^2+y^2 = 1+6x^2y^2$. Let $P \in \mathcal{T}_5$ be the point

$$P = (u,v) = (951\xi^4+338\xi^3+246\xi^2+934\xi+133, 650\xi^4+927\xi^3+301\xi^2+171\xi+973).$$

The compression of P is $\mathcal{R}(P) = (e_1,e_2,e_3,e_4) = (686,289,865,418)$. In order to decompress, we solve

$$g_5(e_1,e_2,e_3,e_4,t) = g_5(686,289,865,418,t) =$$
$$71t^8+705t^7+1007t^6+970t^5+233t^4+1014t^3+356t^2+198t+575 = 0,$$

which has a unique solution $e_5 = 790 \in \mathbb{F}_q$. In order to recover the value of y up to Frobenius conjugates, we find a root in $\mathbb{F}_{q^5}$ of

$$y^5 - e_1y^4 + e_2y^3 - e_3y^2 + e_4y - e_5 = y^5+335y^4+289y^3+156y^2+418y+231.$$

Notice that the five roots are Frobenius conjugates of each other. From one $y \in \mathbb{F}_{q^5}$ we can recompute x via the curve equation, hence recover one of the Frobenius conjugates of $\pm P$. So the decompression algorithm returns $\mathcal{R}^{-1}(\mathcal{R}(P)) = \{\pm P, \pm\varphi(P), \pm\varphi^2(P), \pm\varphi^3(P), \pm\varphi^4(P)\}$.

We now give an example that presents some indeterminacy in the decompression algorithm.

Example 18. Let $q = 2^{10}-3$ and consider the Edwards curve

$$E_{210,924} : 210x^2+y^2 = 1+924x^2y^2$$

and the point

$$P = (1020\xi^4+713\xi^3+158\xi^2+745\xi+515, 891\xi^4+557\xi^3+135\xi^2+976\xi+62) \in \mathcal{T}_5.$$

The compressed representation of P is $\mathcal{R}(P) = (e_1,e_2,e_3,e_4) = (310,887,19,660)$. The decompressing equation is

$$g_5(e_1,e_2,e_3,e_4,t) = 62t^8+502t^7+388t^6+294t^5+2t^4+466t^3+723t^2+55t+388 = 0,$$

which has solutions $e_5 = 428, e_5' = 835, e_5'' = 550 \in \mathbb{F}_q$. By solving the equation

$$y^5 - e_1y^4 + e_2y^3 - e_3y^2 + e_4y - e_5 = y^5 + 310y^4 + 887y^3 + 19y^2 + 660y + 593 = 0$$

we recover the y-coordinate of P and all its Frobenius conjugates. By solving the equation

$$y^5 - e_1y^4 + e_2y^3 - e_3y^2 + e_4y - e_5' = y^5 + 310y^4 + 887y^3 + 19y^2 + 660y + 186 = 0$$

we find roots in $\mathbb{F}_{q^5}$, which do not correspond to points of trace zero. By solving the equation

$$y^5 - e_1y^4 + e_2y^3 - e_3y^2 + e_4y - e_5'' = y^5 + 310y^4 + 887y^3 + 19y^2 + 660y + 471 = 0$$

we find $Q \in \mathcal{T}_5$ which is not a Frobenius conjugate of P. Hence in this case

$$\mathcal{R}^{-1}(\mathcal{R}(P)) = \{\pm P, \ldots, \pm\varphi^4(P), \pm Q, \ldots, \pm\varphi^4(Q)\}.$$

Denote by $\mathcal{T}_5/\sim$ the quotient of $\mathcal{T}_5$ by the equivalence relation that identifies opposite points and Frobenius conjugates. The representation (2) induces a representation

$$\mathcal{R}' : \mathcal{T}_5/\sim \longrightarrow \mathbb{F}_q^4.$$

In the previous example we show that $\mathcal{R}'$ is not injective. Nevertheless, an easy heuristic argument shows that a generic $(e_1, \ldots, e_4) \in \operatorname{Im}\mathcal{R}'$ has exactly one inverse image. In order to support the heuristics, we tested $15'000$ random points in the trace zero subgroup $\mathcal{T}_5$ of 15 Edwards curves. The groups had prime cardinality and bit-length $192, 224$, and 256. For any random point P we computed the cardinality of $\mathcal{R}'^{-1}(\mathcal{R}'(P))$, and found that it is 1 for about 91% of the points, 2 for about 8.5% of the points, and 3 for about 0.5% of the points. We also found a few points for which $|\mathcal{R}'^{-1}(\mathcal{R}'(P))| = 4$, but the percentage was less than 0.02%. Finally, we did not find any points for which $4 < |\mathcal{R}'^{-1}(\mathcal{R}'(P))| \leq 8$.

In order to test the efficiency of the compression and decompression algorithms for $n = 5$, we have implemented them in Magma [7]. We consider primes q_1, q_2, and q_3 of bit-length 48, 56, and 64, respectively. We choose primes such that $5|q_i - 1$ for all i. For each q_i we consider five pairs of birationally equivalent curves $(E, E_{a,d})$ defined over $\mathbb{F}_{q_i}$, such that the order of $\mathcal{T}_5$ is prime of bit-length 192, 224, and 256, respectively. The following table contains the average times for compression and decompression in milliseconds. Each average is computed on a set of 20'000 randomly chosen points on each of the five curves.

Table 3.

Bit-length of $\lvert\mathcal{T}_5\rvert$	192	224	256
Compression on E	0.057	0.055	0.060
Compression on $E_{a,d}$	0.049	0.058	0.053
Decompression on E	64.17	104.31	121.51
Decompression on $E_{a,d}$	63.66	104.45	121.42

The following table contains the ratios between the average times for point compression and decompression on elliptic curves in short Weierstrass form and twisted Edwards curves.

Table 4.

Bit-length of $\lvert\mathcal{T}_5\rvert$	192	224	256
Comp on E / Comp on $E_{a,d}$	1.163	0.948	1.132
Dec on E / Dec on $E_{a,d}$	1.008	0.999	1.001

3 An optimal representation using rational functions

Let $E_{a,d}$ be a twisted Edwards curve defined over $\mathbb{F}_q$. In this section, we propose another optimal representation for the trace zero subgroup $\mathcal{T}_n \subset E_{a,d}(\mathbb{F}_{q^n})$ using rational functions.

In [12] the authors propose to represent an element $P \in \mathcal{T}_n$ via the coefficients of the rational function which corresponds to the principal divisor $P + \varphi(P) + \ldots + \varphi^{n-1}(P) - n\mathcal{O}$ on the elliptic curve. Optimality of the representation depends on the fact that the rational function associated to this divisor has a special form, and can therefore be represented using $n-1$ coefficients in $\mathbb{F}_q$. If we consider a principal divisor of the form $P+\varphi(P)+\ldots+\varphi^{n-1}(P)-n\mathcal{O}$ on the twisted Edwards curve $E_{a,d}$, there are several questions that need to be answered. E.g., the rational function associated to this divisor is not a polynomial in general, so one needs to overcome some difficulties in order to successfully carry out the same strategy.

We start with some preliminary results on rational functions on a twisted Edwards curve. If h is a rational function on $E_{a,d}$, we denote by $\mathrm{div}(h)$ the divisor of the homogeneous rational function associated to h on the projective closure of $E_{a,d}$. Throughout the section we use (u, v) for the coordinates of the point and x, y for the variables of the rational functions, in order to avoid confusion.

Lemma 19. *Let $c \in k$ such that $ad^{-1} = c^2$, where $k = \mathbb{F}_q$ or $k = \mathbb{F}_{q^2}$ depending on whether ad^{-1} is a quadratic residue in $\mathbb{F}_q$ or not. Let $R(x, y) \in k(x, y)$ be a rational function on $E_{a,d}$. Then R can be written in the form*

$$R(x, y) = (y - c)^{k_1}(y + c)^{k_2}\frac{r_1(y) + xr_2(y)}{r_3(y)},$$

modulo $E_{a,d}$, where $r_1, r_2, r_3 \in k[y]$, $\gcd\{r_1, r_2, r_3\} = 1$, $r_3(\pm c) \neq 0$, and k_1, $k_2 \leq 0$.

Proof. Using the relation $x^2 = \frac{(1-y^2)}{(a-dy^2)}$, we can write $R(x, y)$ in the form

$$R(x, y) = \frac{s_1(y) + xs_2(y)}{s_3(y) + xs_4(y)},$$

where $s_i(y) \in k[y]$ for $1 \leq i \leq 4$. Multiplying and dividing by $s_3(y) - xs_4(y)$, we obtain:

$$R(x, y) = \frac{t_1(y) + xt_2(y)}{t_3(y)},$$

where $t_i(y) \in k[y]$ for $1 \leq i \leq 3$. Simplifying the fraction and factoring $y - c$ and $y + c$ as much as possible from the denominator, we obtain the thesis. □

Lemma 20. *In the setting of Lemma 19, assume that R has poles at most at the points at infinity Ω_1 and Ω_2. Then*

$$R(x,y) = (y-c)^{k_1}(y+c)^{k_2}(q_1(y) + xq_2(y)),$$

modulo $E_{a,d}$, where $q_1(y)$, $q_2(y) \in k[y]$, $q_i(\pm c) \neq 0$ for $i = 1, 2$, and $k_1, k_2 \leq 0$.

Proof. By Lemma 19 we can write

$$R(x,y) = (y-c)^{k_1}(y+c)^{k_2}\frac{r_1(y) + xr_2(y)}{r_3(y)}.$$

Since $(y-c)^{k_1} = 0$ and $(y+c)^{k_2} = 0$ have no affine zeroes on $E_{a,d}$, R has poles at most at the points at infinity if and only if the order of vanishing of r_3 on $E_{a,d}$ at each affine point is less than or equal to the order of vanishing of $r_1 + xr_2$ on $E_{a,d}$ at the same point.

Let $P = (u, v)$ be a point such that $r_3(v) = 0$. Write r_3 in the form $r_3(y) = (y-v)^m t_3(y)$, where $t_3(v) \neq 0$ and $m > 0$. The order of vanishing of r_3 on $E_{a,d}$ at P is m if $u \neq 0$, and $2m$ if $u = 0$. In fact, the only points in which $E_{a,d}$ has a horizontal tangent line are $\mathcal{O}$ and $\mathcal{O}'$. The same holds for the order of vanishing of r_3 at $-P$. From $r_1(v) + ur_2(v) = r_1(v) - ur_2(v) = 0$ we obtain that $r_1(v) = ur_2(v) = 0$. Therefore, since $\gcd\{r_1, r_2, r_3\} = 1$, we have $r_2(v) \neq 0$ and $u = 0$. The order of vanishing of $r_1 + xr_2$ on $E_{a,d}$ at P is 1, since P is a smooth point and the tangent line at P to the curve of equation $r_1(y) + xr_2(y)$ is not horizontal. But the order of vanishing of r_3 on $E_{a,d}$ at P is bigger than m, which yields a contradiction. □

One has the following characterization for rational functions on $E_{a,d}$ with zero divisor.

Lemma 21. *In the setting of Lemma 19, one has that*

$$\operatorname{div}(R) = 0 \Leftrightarrow R = (y-c)^{l+m}(y+c)^{-l}(1 - \sqrt{d}x)^m$$

where $l, m \in \mathbb{Z}$, and the equality on the right hand side holds modulo E_{ad} and up to multiplication by a nonzero constant.

Proof. If R is of the form $R = (y-c)^{l+m}(y+c)^{-l}(1-\sqrt{d}x)^m$, then a straightforward calculation shows that $\operatorname{div}(R) = 0$. In order to show the converse, let D be the divisor of $\hat{R} = R \circ \Phi$ on $E_{A,B}$, where Φ is the birational isomorphism of Proposition 3. Since $\operatorname{div}(R) = 0$, one has that $\Phi(D) = 0$, hence D is of the form $D = h(Q_1 - Q_2) + k(Q_4 - Q_3)$, where h, $k \in \mathbb{Z}$. Consider the two rational functions of $E_{a,d}$: $g_1 = (y-c)/(y+c)$ and $g_2 = (y-c)(1-\sqrt{d}x)$. One has that $\operatorname{div}(g_1 \circ \Phi) = 2(Q_1 - Q_2)$ and $\operatorname{div}(g_2 \circ \Phi) = Q_1 - Q_2 + Q_4 - Q_3$. Moreover there is no rational funcion of $E_{A,B}$ whose divisor is $Q_1 - Q_2$ or $Q_4 - Q_3$, since $Q_1 \neq Q_2$ and $Q_3 \neq Q_4$. The thesis follows from these observations and from the fact that $E_{A,B}$ is nonsingular. □

In the introduction of this section, we hinted at the difficulty that if $P \in \mathcal{T}_n$ is a point of trace zero on a twisted Edwards curve $E_{a,d}$, the rational function associated to the principal divisor $P + \varphi(P) + \ldots + \varphi^{n-1}(P) - n\mathcal{O}$ is not in general a polynomial. Lemma 20 offers a solution to this problem: considering a modified principal divisor, whose associated rational function is a polynomial.

Theorem 22. *Let $E_{a,d}$ be a twisted Edwards curve defined over $\mathbb{F}_q$ and let $P \in \mathcal{T}_n \subset E_{a,d}(\mathbb{F}_{q^n})$. Then there exists a polynomial $q_P(x,y) = q_1(y) + xq_2(y) \in \mathbb{F}_q[x,y]$, with $q_1(y), q_2(y) \in \mathbb{F}_q[y]$, such that*

1. $div(q_P) = P + \varphi(P) + \ldots + \varphi^{n-1}(P) + \mathcal{O}' - 2\Omega_1 - (n-1)\Omega_2$.

2. $\max\{\deg(q_1), \deg(q_2)\} = \frac{n-1}{2}$.

3. $q_1(y) = (1+y)\hat{q_1}(y)$, *where* $\hat{q_1} \in \mathbb{F}_q[y]$ *and* $\deg(\hat{q_1}) \leq \frac{n-3}{2}$.

4. q_2 *is not the zero polynomial.*

Proof. 1. Consider the setting of Proposition 3. Since $P = (u, v) \in \mathcal{T}_n$, one has that $P' = \Psi(P)$ is a point of trace zero of $E_{A,B}$. Then there exists $f \in E_{A,B}(\mathbb{F}_q)$ such that $\mathrm{div}(f) = \mathrm{Tr(P')}$. Let $\hat{\varphi}$ be the Frobenius endomorphism on $E_{A,B}$. For each $i \in \{1, \ldots, n-2\}$ denote with ℓ_i the line through $P' + \cdots + \hat{\varphi}^{i-1}(P')$ and $\hat{\varphi}^i(P')$, for each $i \in \{1, \ldots, n-3\}$ denote by v_i the vertical line through $P' + \cdots + \hat{\varphi}^i(P')$, finally let L and V be the products of lines $L = \prod_{i=1}^{n-2} \ell_i$ and $V = \prod_{i=1}^{n-3} v_i$. By Corollary 4.2 of [12] one has that $\mathrm{div}(L/V) = \mathrm{Tr(P')}$, from which $L/V = \lambda f \mod E_{A,B}$, where λ is a nonzero constant in the algebraic closure of $\mathbb{F}_q$. Hence posing $g = (L/V) \circ \Psi$ one has that $\mathrm{div}(g) = \mathrm{Tr(P)}$ and

$$g = \frac{\phi_1 \phi_2 \cdots \phi_{n-2}}{x^{n-2}(1-y)h_1 h_2 \cdots h_{n-3}},$$

where, for each $i \in \{1, \ldots n-2\}$, ϕ_i is the conic with

$$\mathrm{div}(\phi_i) = (P + \ldots + \varphi^{i-1}(P)) + \varphi^i(P) + (-(P + \ldots + \varphi^i(P))) + \mathcal{O}' - 2\Omega_1 - 2\Omega_2$$

and, for each $i \in \{1, \ldots, n-3\}$, h_i is the horizontal line through $P + \cdots + \varphi^i(P)$. Now consider the polynomial $H(x, y) = x(1-y)^{\frac{n-1}{2}} \in \mathbb{F}_q[x, y]$ whose divisor is $\mathrm{div}(H) = n\mathcal{O} + \mathcal{O}' - 2\Omega_1 - (n-1)\Omega_2$. Then $\mathrm{div}(gH) = P + \varphi(P) + \ldots + \varphi^{n-1}(P) + \mathcal{O}' - 2\Omega_1 - (n-1)\Omega_2$ and

$$gH = \frac{\phi_1 \phi_2 \cdots \phi_{n-2}(1-y)^{\frac{n-3}{2}}}{h_1 h_2 \cdots h_{n-3} x^{n-3}} = \frac{(a - dy^2)^{\frac{n-3}{2}}}{h(y)(1+y)^{\frac{n-3}{2}}} \prod_{i=1}^{n-2} \phi_i \tag{11}$$

modulo the curve equation, where $h(y) = \prod_{i=1}^{n-3} h_i$ and $\deg(h) = n-3$. For each $i \in \{1, \ldots, n-2\}$, ϕ_i is of the form $\phi_i = B_i(y)x + A_i(y)$, where $B_i(y)$ and $A_i(y)$ are polynomials in y of degree at most 1, hence

$$\prod_{i=1}^{n-2} \phi_i = H_{n-2}(y)x^{n-2} + H_{n-3}(y)x^{n-3} + \ldots + H_1(y)x + H_0(y),$$

where each $H_i(y)$ is a polynomial in y of degree at most $n-2$. Reducing modulo $E_{a,d}$ we obtain

$$(a - dy^2)^{\frac{n-3}{2}} \prod_{i=1}^{n-2} \phi_i(x, y) = R_1(y) + xR_2(y),$$

where each $R_i(y)$ is a polynomial of $\deg(R_i) \leq \max\{\deg(H_j)\} + n - 3 \leq 2n-5$. The denominator of (11) divides both $R_1(y)$ and $R_2(y)$ by Lemma 20, so $gH = q_P$ up to multiplication by a nonzero constant, where $q_1(y)$ and $q_2(y)$ have coefficients in $\mathbb{F}_q$ since f and H have coefficients in $\mathbb{F}_q$ and $E_{a,d}$ and $E_{A,B}$ are birationally equivalent over $\mathbb{F}_q$.

2. Using the notation of part 1, we have

$$\deg(q_i) = \deg(R_i) - \deg(1+y)^{\frac{n-3}{2}} - \deg(h) \leq 2n - 5 - \frac{(n-3)}{2} - (n-3) = \frac{n-1}{2} \quad (12)$$

for $i = 1, 2$. Moreover, by part 1

$$\operatorname{div}(q_{-P}) = (-P) + \ldots + \varphi^{n-1}(-P) + \mathcal{O}' - 2\Omega_1 - (n-1)\Omega_2,$$

and modulo $E_{a,d}$

$$q_P(x,y)q_{-P}(x,y) = q_1^2(y) - \frac{1-y^2}{a-dy^2}\, q_2^2(y).$$

Since $\operatorname{div}(a-dy^2) = 4\Omega_1 - 4\Omega_2$, the polynomial $R_P(y) = (a-dy^2)q_1^2(y) - (1-y^2)q_2^2(y)$ has

$$div(R_P) = (\pm P) + (\pm\varphi(P)) + \cdots + (\pm\varphi^{n-1}(P)) + 2\mathcal{O}' - 2(n+1)\Omega_2.$$

Hence $(1+y)\prod_{i=0}^{n-1} v^{q^i} | R_P(y)$, therefore

$$n+1 \leq \deg(R_P(y)) \leq 2 + 2\max\{\deg(q_1), \deg(q_2)\} \quad (13)$$

and part 2 follows directly from (12) and (13). We have also obtained that R_P is a polynomial of degree exactly $n+1$ with coefficients in $\mathbb{F}_q$ and roots -1, v^{q^i}, for $0 \leq i \leq n-1$: we will need this result in the sequel.

3. Since q_P vanishes at $\mathcal{O}' = (0,-1)$, then q_1 is of the form

$$q_1(y) = (1+y)\hat{q_1}(y),$$

where $\hat{q_1} \in \mathbb{F}_q[y]$ and $\deg(\hat{q_1}) \leq \frac{n-3}{2}$.

4. If q_2 was the zero polynomial, then $q_P = q_1(y)$ would vanish on $\mathcal{O}'$ with multiplicity at least 2, contradicting part 1.

□

Computation of q_P. In the proof of the previous theorem we have seen that one can compute the polynomial q_P as

$$q_P = \frac{\phi_1\phi_2\cdots\phi_{n-2}(1-y)^{\frac{n-3}{2}}}{h_1h_2\cdots h_{n-3}x^{n-3}}, \quad (14)$$

where for each $1 \leq i \leq n-2$, ϕ_i is the conic through $P + \cdots + \varphi^{i-1}(P)$, $\varphi^i(P)$, $\mathcal{O}'$, $2\Omega_1$ and $2\Omega_2$, for each $1 \leq i \leq n-3$, h_i is the horizontal line through $P + \cdots + \varphi^i(P) \in E_{a,d}$. Notice that we can easily calculate ϕ_i for each i, employing the formulas given in [2, Theorem 1 and Theorem 2].

We now discuss how to use the polynomial q_P to represent P via $(n-1)$ elements of $\mathbb{F}_q$ plus a bit. As a consequence of Theorem 22, q_P has the form

$$q_P(x,y) = (1+y)\left(a_{\frac{n-3}{2}}y^{\frac{n-1}{2}} + \cdots + a_1y + a_0\right) + x\left(b_{\frac{n-1}{2}}y^{\frac{n-1}{2}} + \cdots + b_1y + b_0\right),$$

where $a_i, b_j \in \mathbb{F}_q$ for all i, j, and $b_{\frac{n-1}{2}} \in \{0, 1\}$. We have therefore obtained an optimal representation for the elements of $\mathcal{T}_n$:

$$\begin{array}{rccc} \mathcal{R}: & \mathcal{T}_n & \longrightarrow & \mathbb{F}_q^{n-1} \times \mathbb{F}_2 \\ & P & \longmapsto & \left(a_0, \ldots, a_{\frac{n-3}{2}}, b_0, \ldots, b_{\frac{n-1}{2}}\right). \end{array} \tag{15}$$

We now give the complete algorithm for point compression.

Algorithm 3 (Compression).

Input : $P \in \mathcal{T}_n$
Output : $\mathcal{R}(P) \in \mathbb{F}_q^{n-1} \times \mathbb{F}_2$

1: Compute $q_P(x, y) = q_1(y) + xq_2(y)$ using (11) and reducing modulo $E_{a,d}$.
2: Compute $\hat{q_1}(y) = q_1(y)/(1 + y) = a_{\frac{n-3}{2}} y^{\frac{n-1}{2}} + \cdots + a_1 y + a_0$.
3: $q_2(y) = b_{\frac{n-1}{2}} y^{\frac{n-1}{2}} + \cdots + b_1 y + b_0$.
4: $\mathcal{R}(P) \leftarrow (a_0, \ldots, a_{\frac{n-3}{2}}, b_0, \ldots, b_{\frac{n-1}{2}})$.
5: **return** $\mathcal{R}(P)$.

Correctness of the compression algorithm is a direct consequence of our previous results.

Given an n-tuple $(\alpha_1, \ldots, \alpha_{n-1}, b) \in \mathbb{F}_q^{n-1} \times \mathbb{F}_2$ such that $(\alpha_1, \ldots, \alpha_{n-1}, b) = \mathcal{R}(P)$ for some $P \in \mathcal{T}_n$, we want to compute the decompression $\mathcal{R}^{-1}(\alpha_1, \ldots, \alpha_{n-1}, b)$. We start with some preliminary results. The next lemma guarantees that the x-coordinate of P can be computed from its y-coordinate and the polynomial q_P.

Lemma 23. *Let $P = (u, v) \in \mathcal{T}_n$, let $q_P(x, y) = q_1(y) + xq_2(y) \in \mathbb{F}_q[x, y]$ be the polynomial with $div(q_P) = P + \varphi(P) + \ldots + \varphi^{n-1}(P) + \mathcal{O}' - 2\Omega_1 - (n-1)\Omega_2$. Then: $q_2(v) = 0$ if and only if $P = \mathcal{O}$.*

Proof. If $q_2(v) = 0$, then $q_1(v) = 0$, hence $q_P(-u, v) = 0$. Since the affine points of the curve on which q_P vanishes are exactly $\mathcal{O}'$ and $\varphi^i(P)$ for $0 \leq i \leq n-1$ by Theorem 22 and $\mathcal{O}' \notin \mathcal{T}_n$, then $-P = \varphi^i(P)$ for some i. If $i = 0$, we have $-P = P$, hence $P = \mathcal{O}$. If $i \neq 0$, then $(-u, v) = (u^{q^i}, v^{q^i})$ for some $i \in \{1, \ldots, n-1\}$. Then $v \in \mathbb{F}_{q^i} \cap \mathbb{F}_{q^n} = \mathbb{F}_q$ and $u^{q^{2i}} = u \in \mathbb{F}_{q^{2i}} \cap \mathbb{F}_{q^n} = \mathbb{F}_q$. Hence $P \in E_{a,d}(\mathbb{F}_q)$ and $-P = \varphi^i(P) = P$, from which $P = \mathcal{O}$.

Conversely, if $P = \mathcal{O}$ then $q_P(x, y) = x(1 - y)^{\frac{n-1}{2}}$ and $q_2(1) = 0$. □

Given $q_P(x, y)$, we can compute a polynomial $Q_P(y)$ whose roots are exactly the Frobenius conjugates of the y-coordinate of P. This will be used in our decompression algorithm.

Proposition 24. *Let $P = (u, v) \in \mathcal{T}_n$, let $q_P(x, y) = (1 + y)\hat{q_1}(y) + xq_2(y) \in \mathbb{F}_q[x, y]$ be the polynomial with $div(q_P) = P + \varphi(P) + \ldots + \varphi^{n-1}(P) + \mathcal{O}' - 2\Omega_1 - (n-1)\Omega_2$. Define*

$$Q_P(y) = (a - dy^2)(1 + y)\hat{q_1}^2(y) + (y - 1)q_2^2(y).$$

Then $Q_P(y) \in \mathbb{F}_q[y]$, $\deg Q_P = n$, and its roots are $v, v^q, \ldots, v^{q^{n-1}}$.

Proof. Let $R_P = (a-dy^2)q_1^2(y) - (1-y^2)q_2^2(y) = (1+y)[(a-dy^2)\hat{q_1}(y) - (1-y)q_2^2(y)]$. Then $Q_P(y) = (1+y)^{-1} \cdot R_P(y)$, and the claim follows by Theorem 22. □

We are now ready to give the decompression algorithm.

Algorithm 4 (Decompression).

Input : $(\alpha_1, \ldots, \alpha_{n-1}, b) \in \mathbb{F}_q^{n-1} \times \mathbb{F}_2$
Output : $P = (u, v) \in \mathcal{T}_n$ with $\mathcal{R}(P) = (\alpha_1, \ldots, \alpha_{n-1}, b)$

1: $\hat{q}_1(y) \leftarrow \alpha_{\frac{n-1}{2}} y^{\frac{n-3}{2}} + \cdots + \alpha_2 y + \alpha_1$.
2: $q_2(y) \leftarrow b y^{\frac{n-1}{2}} + \alpha_{n-1} y^{\frac{n-3}{2}} + \cdots + \alpha_{\frac{n+3}{2}} y + \alpha_{\frac{n+1}{2}}$.
3: $Q_P(y) \leftarrow (a - dy^2) \cdot (1+y) \cdot \hat{q}_1^2(y) + (y-1) \cdot q_2^2(y)$.
4: $v \leftarrow$ one root of $Q_P(y)$.
5: **if** $v = 1$ **then** $u \leftarrow 0$ **else** $u \leftarrow -\frac{\hat{q}_1(v)(v+1)}{q_2(v)}$ **endif**
6: **return** (u, v).

Remark 25. Let $P \in \mathcal{T}_n$ be a point with $\mathcal{R}(P) = (\alpha_1, \ldots, \alpha_{n-1}, b)$. By Theorem 22 the Frobenius conjugates of P are the only other points of $\mathcal{T}_n$ with the same representation. Correctness of the first four lines of the algorithm follows from Proposition 24 and correctness of line 5 follows from Lemma 23. Hence the given algorithm correctly recovers the point P, up to Frobenius conjugates.

3.1 Explicit equations, complexity, and timings for $n = 3$

In this subsection we give explicit equations and perform some computations for $n = 3$. We estimate the number of operations needed for the compression and decompression, and present some timings obtained with Magma. We also make comparisons with trace zero subgroups of elliptic curves in short Weierstrass form treated in [12].

Point Compression. Let $P = (u, v) \in T_3$. By Theorem 22, we may write

$$q_P(x, y) = \hat{q_1}(y)(1+y) + x q_2(y) = a_0(1+y) + x(b_1 y + b_0),$$

where a_0, $b_0 \in \mathbb{F}_q$, $b_1 \in \{0, 1\}$.

If $P \notin E_{a,d}(\mathbb{F}_q)$, let $t = \frac{v+1}{u}$. Notice that $u \neq 0$, since $u = 0$ implies $P = \mathcal{O}$, hence $P \in E_{a,d}(\mathbb{F}_q)$.

1. If $t^q - t \neq 0$, by Theorem 1 of [2]

$$\mathcal{R}(P) = (a_0, b_0, b_1) = \left(-\frac{v^q - v}{t^q - t}, -a_0 t - v, 1 \right).$$

Computing t from u and v takes 1M+1I in $\mathbb{F}_{q^3}$. Once we have t, the situation is analogous to the case of elliptic curves in short Weierstrass form. Hence we refer to [12, Section 5.1] for

a detailed discussion of how to efficiently compute $\mathcal{R}(P)$. In particular, it is shown that one can compute a_0 and b_0 with 2S+6M +1I in $\mathbb{F}_q$. Summarizing, point compression in this case takes 1M+1I in $\mathbb{F}_{q^3}$ and 2S+6M +1I in $\mathbb{F}_q$. Due to the calculation of t, it is more expensive than that for elliptic curves in short Weierstrass form.

2. If $t^q - t = 0$, then q_P is the line passing through P and $\mathcal{O}'$ by [2, Theorem 1]. Hence

$$\mathcal{R}(P) = \left(-t^{-1}, 1, 0\right). \tag{16}$$

Since $\mathcal{O}' \notin T_3$, then $t \neq 0$. In this case point compression requires only 1M + 1I in $\mathbb{F}_{q^3}$.

If $P \in E_{a,d}(\mathbb{F}_q)$, then the computation takes place in $\mathbb{F}_q$ instead of $\mathbb{F}_{q^3}$, hence we expect the complexity to be lower. We carry on a precise operation count, as in the previous case.

3. If $du^2v - 1 \neq 0$, by [2, Theorem 1]

$$\mathcal{R}(P) = \left(\frac{u(1-v)}{du^2v-1}, \frac{v-au^2}{du^2v-1}, 1\right).$$

Therefore, point compression takes 1S+4M+1I in $\mathbb{F}_q$.

4. If $du^2v - 1 = 0$, then the situation is analogous to **2.** and $\mathcal{R}(P)$ is given by (16). Hence point compression requires 1M + 1I in $\mathbb{F}_q$.

Since **1.** is the generic case, the expected complexity of point compression is 1M+1I in $\mathbb{F}_{q^3}$ and 2S+6M +1I in $\mathbb{F}_q$.

Point Decompression. Let $(\alpha_1, \alpha_2, b) \in \mathbb{F}_q^2 \times \mathbb{F}_2$ and $P = (u, v) \in \mathcal{T}_3$ such that $\mathcal{R}(P) = (\alpha_1, \alpha_2, b)$. In order to recover P from $\mathcal{R}(P)$, we want to find the roots of

$$Q_P(y) = (b - d\alpha_1^2)y^3 + (-d\alpha_1^2 + 2\alpha_2 b - b)y^2 + (a\alpha_1^2 - 2\alpha_2 b + \alpha_2^2)y + (a\alpha_1^2 - \alpha_2^2).$$

They are the solutions to the system

$$\begin{cases} y + y^q + y^{q^2} & = & c(d\alpha_1^2 - 2\alpha_2 b + b) \\ y^{q+1} + y^{q^2+1} + y^{q^2+q} & = & c(a\alpha_1^2 - 2\alpha_2 b + \alpha_2^2) \\ y^{1+q+q^2} & = & c(-a\alpha_1^2 + \alpha_2^2) \end{cases} \tag{17}$$

where $c = (b - d\alpha_1^2)^{-1}$. Notice that $(b - d\alpha_1^2) \neq 0$, since Q_P has degree 3 by Proposition 24.

Computing the constant terms of (17) takes 2S+3M+1I in $\mathbb{F}_q$. Computing a solution of the system takes at most 3S+3M+1I, one square root and two cube roots in $\mathbb{F}_q$, as shown in [12]. Finally, computing u from v requires 2M+1I in $\mathbb{F}_{q^3}$. Summarizing, for $n = 3$ point decompression takes at most 2M+1I in $\mathbb{F}_{q^3}$ and 5S+6M+2I, one square root and two cube roots in $\mathbb{F}_q$. It is more expensive than that for elliptic curves in short Weierstrass form, which

takes at most 1M in $\mathbb{F}_{q^3}$ and 5S+4M+1I, one square root and two cube roots in $\mathbb{F}_q$.

We now give an example and some statistics implemented in Magma. We follow the same setup as in Example 16, and compare with the method for elliptic curves in short Weierstrass form proposed in [12].

Example 26. Let $q = 2^{79} - 67$ and $\mu = 3$. We choose random, birationally equivalent curves defined over $\mathbb{F}_q$:

$$E_{a,d} : 31468753957068040687814x^2 + y^2 = 1 + 19269782127663896649899 7x^2y^2$$

and

$$E : y^2 = x^3 + 2924678484276594994785 03x + 36136102673640400434542 1.$$

We choose a random point $P' \in E(\mathbb{F}_{q^3})$ of trace zero, and let P be the corresponding point on $E_{a,d}$. For brevity, we only write the x-coordinates of points of E and the y-coordinates of points of $E_{a,d}$:

$$P' = 34656092814607695931475 3\xi^2 + 45682653962853598103421 2\xi + 34416747040302665282667 2,$$

$$P = 20852071389751823621596 6\xi^2 + 45112194455021994736881 1\xi + 68041089860429901306252.$$

We denote by $\mathcal{R}$ and $\mathcal{R}'$ the representation maps on $E_{a,d}$ and E, respectively. We compute:

$$\mathcal{R}'(P') = (\gamma_0, \gamma_1) = (48823870679406912678832, 28345175156076495772030 2),$$

$$\mathcal{R}(P) = (a_1, b_0, b_1) = (31308434255223282002781 6, 53581470317932429707416 1, 1).$$

Applying the decompression algorithms to $\mathcal{R}'(P')$ and $\mathcal{R}(P)$, we obtain

$$\mathcal{R}'^{-1}(48823870679406912678832, 28345175156076495772030 2) =$$

$\{34656092814607695931475 3\xi^2 + 45682653962853598103421 2\xi + 34416747040302665282667 2,$

$16475949861450750318749 3\xi^2 + 36152069098819775153438 1\xi + 34416747040302665282667 2,$

$93142483046730124850775\xi^2 + 39057858899789544213744 9\xi + 34416747040302665282667 2\},$

which are the x-coordinates of P' and its Frobenius conjugates. Similarly

$$\mathcal{R}^{-1}(31308434255223282002781 6, 53581470317932429707416 1, 1) =$$

$\{20852071389751823621596 6\xi^2 + 45112194455021994736881 1\xi + 68041089860429901306252,$

$53932153696106685501116 7\xi^2 + 23743139109764296838671 9\xi + 68041089860429901306252,$

$46108356875604408347890 9\xi^2 + 52037248396676625895051 2\xi + 68041089860429901306252\},$

which are the y-coordinates of P and its Frobenius conjugates.

We now give an estimate of the average time of compression and decompression for groups of different bit-size. We consider primes q_1, q_2, and q_3 such that $3|q_i - 1$ for all i, of bit-length 96, 112, and 128, respectively. For each q_i, we consider five pairs of birationally equivalent curves $(E, E_{a,d})$ defined over $\mathbb{F}_{q_i}$, such that the order of $\mathcal{T}_3$ is prime of bit-length respectively 192, 224 and 256. On each pair of curves we randomly choose $20'000$ pairs of points (P', P) of trace zero which correspond to each other via the birational isomorphism between the curves. For each pair of points, we compute $\mathcal{R}'(P'), \mathcal{R}(P), \mathcal{R}'^{-1}(\mathcal{R}'(P')), \mathcal{R}^{-1}(\mathcal{R}(P))$. For each computation, we consider the average time in milliseconds for each curve, and then the averages over the five curves. The average computation times are reported in the table below.

Table 5.

Bit-length of $\lvert\mathcal{T}_3\rvert$	192	224	256
Compression on E	0.015	0.013	0.011
Compression on $E_{a,d}$	0.034	0.037	0.035
Decompression on E	0.09	0.13	0.15
Decompression on $E_{a,d}$	0.14	0.19	0.20

The next table contains the ratios of the average times for point compression and decompression on elliptic curves in short Weierstrass form and twisted Edwards curves.

Table 6.

Bit-length of $\lvert\mathcal{T}_3\rvert$	192	224	256
Comp on E / Comp on $E_{a,d}$	0.441	0.351	0.314
Dec on E / Dec on $E_{a,d}$	0.643	0.684	0.750

3.2 Explicit equations, complexity, and timings for $n = 5$

In this subsection we give explicit equations and perform computations for $n = 5$. We estimate the number of operations needed for the computations and present some timings obtained with Magma. We also make comparisons with the method proposed in [12] for elliptic curves in short Weierstrass form.

Point Compression. Let $P \in \mathcal{T}_5$. By Theorem 22, q_P is of the form

$$q_P(x, y) = (1 + y)\hat{q_1}(y) + xq_2(y) = (1 + y)(a_1y + a_0) + x(b_2y^2 + b_1y + b_0)$$

where a_0, a_1, b_0, $b_1 \in \mathbb{F}_q$, and $b_2 \in \mathbb{F}_2$. Moreover

$$(1 + y)h_1h_2q_P = \phi_1\phi_2\phi_3(a - dy^2)$$

modulo $E_{a,d}$ and up to a nonzero constant factor. We consider the generic case, where $b_2 = 1$ and ϕ_i is of the form

$$\phi_i(x, y) = p_i(y + 1) + x(y + q_i)$$

with p_i, $q_i \in \mathbb{F}_{q^5}$, and $i \in \{1, 2, 3\}$. Denote by k_1 and k_2 the y-coordinates of $P_1 + P_2$ and $P_1 + P_2 + P_3$, respectively. We have

$$\mathcal{R}(P) = (a_0, a_1, b_0, b_1, 1),$$

where

$$\begin{aligned}
a_1 &= k \cdot (d(p_1p_2p_3) + (p_1 + p_2 + p_3)),\\
a_0 &= k \cdot (3d(p_1p_2p_3) + (p_1q_2 + p_1q_3 + q_1p_2 + q_1p_3 + p_2q_3 + q_2p_3) + (p_1 + p_2 + p_3)) +\\
&\quad a_1 \cdot (k_1 + k_2 - 2),\\
b_1 &= k \cdot (d(p_1p_2q_3 + p_1p_3q_2 + p_2p_3q_1) + 2d(p_1p_2 + p_1p_3 + p_2p_3) + (q_1 + q_2 + q_3)) +\\
&\quad (k_1 + k_2 - 1),\\
b_0 &= k \cdot (2d(p_1p_2q_3 + p_1p_3q_2 + p_2p_3q_1) + (d - a)(p_1p_2 + p_1p_3 + p_2p_3) +\\
&\quad (q_1q_2 + q_1q_3 + q_2q_3)) - 1) + b_1(k_1 + k_2 - 1) + (k_1 + k_2 - k_1k_2),\\
k &= (d(p_1p_2 + p_1p_3 + p_2p_3) + 1)^{-1}.
\end{aligned}$$

Computing ϕ_1, ϕ_2, and ϕ_3 takes 2S+34M+2I in $\mathbb{F}_{q^5}$. Computing a_1, a_2, b_1, b_0 with the formulas above requires 45M+1I in $\mathbb{F}_{q^5}$. So point compression for $n = 5$ takes a total of 2S+79M+3I in $\mathbb{F}_{q^5}$. The method of [12] for elliptic curves in short Weierstrass form is less expensive, as it takes 3S+18M+3I in $\mathbb{F}_{q^5}$.

Point Decompression. Let $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, b) \in \mathbb{F}_q^4 \times \mathbb{F}_2$ and let $P = (u, v) \in \mathcal{T}_5$ such that $\mathcal{R}(P) = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, b)$. In order to decompress $\mathcal{R}(P)$, we look for the roots of

$$Q_P(y) = Q_5y^5 + Q_4y^4 + Q_3y^3 + Q_2y^2 + Q_1y + Q_0,$$

where

$$\begin{aligned}
Q_0 &= a\alpha_1^2 - \alpha_3^2\\
Q_1 &= a\alpha_1^2 + 2a\alpha_1\alpha_2 + \alpha_3^2 - 2\alpha_3\alpha_4\\
Q_2 &= -d\alpha_1^2 + 2a\alpha_1\alpha_2 + a\alpha_2^2 + 2\alpha_3\alpha_4 - 2\alpha_3b - \alpha_4^2\\
Q_3 &= -d\alpha_1^2 - 2d\alpha_1\alpha_2 + a\alpha_2^2 + 2\alpha_3b + \alpha_4^2 - 2\alpha_4b\\
Q_4 &= -2d\alpha_1\alpha_2 - d\alpha_2^2 + 2\alpha_4b - b.\\
Q_5 &= -d\alpha_2^2 + b.
\end{aligned}$$

This amounts to solving the system

$$\begin{cases}
e_1(y, y^q, \ldots, y^{q^4}) &= -Q_5^{-1}Q_4\\
e_2(y, y^q, \ldots, y^{q^4}) &= Q_5^{-1}Q_3\\
e_3(y, y^q, \ldots, y^{q^4}) &= -Q_5^{-1}Q_2\\
e_4(y, y^q, \ldots, y^{q^4}) &= Q_5^{-1}Q_1\\
e_5(y, y^q, \ldots, y^{q^4}) &= -Q_5^{-1}Q_0
\end{cases}$$

where $e_i(y, y^q, \ldots, y^{q^4})$ is the i-th elementary symmetric polynomial in $y, y^q, \ldots, y^{q^4}$. Computing the constants in the system takes 4S+7M+1I in $\mathbb{F}_q$, while solving the system requires $\mathcal{O}(\log_2 q)$ operations in $\mathbb{F}_q$ following the approach from [12]. Finally, recovering u from v takes 1S+5M+1I in $\mathbb{F}_{q^5}$. The computational cost of point decompression is comparable to that of the decompression algorithm from [12] for elliptic curves in short Weierstrass form.

In order to estimate of the average time of compression and decompression for groups of different bit-size, we consider primes q_1, q_2, and q_3 such that $3|q_i - 1$ for all i, of bit-length 96, 112, and 128, respectively. For each q_i, we consider five pairs of birationally equivalent curves $(E, E_{a,d})$ defined over $\mathbb{F}_{q_i}$, such that the order of $\mathcal{T}_3$ is prime of bit-length respectively 192, 224 and 256. On each pair of curves we randomly choose 20′000 pairs of points (P', P) of

trace zero which correspond to each other via the birational isomorphism between the curves. For each pair of points, we compute $\mathcal{R}'(P'), \mathcal{R}(P), \mathcal{R}'^{-1}(\mathcal{R}'(P')), \mathcal{R}^{-1}(\mathcal{R}(P))$. For each computation, we consider the average time in milliseconds for each curve, and then the averages over the five curves. The average computation times are reported in the table below.

Table 7.

Bit-length of $\lvert\mathcal{T}_5\rvert$	192	224	256
Compression on E	1.566	1.725	1.894
Compression on $E_{a,d}$	1.704	1.868	2.052
Decompression on E	6.10	31.69	36.99
Decompression on $E_{a,d}$	6.15	31.37	36.59

The next table contains the ratios of the average times for point compression and decompression on elliptic curves in short Weierstrass form and twisted Edwards curves.

Table 8.

Bit-length of $\lvert\mathcal{T}_5\rvert$	192	224	256
Comp on E / Comp on $E_{a,d}$	0.919	0.923	0.923
Dec on E / Dec on $E_{a,d}$	0.992	1.010	1.011

Finally, Table 9 summarizes the number of operations for point compression and decompression. We compare the operation count from this paper with the one for elliptic curves in short Weierstrass form from [12].

Table 9.

Compression, $n = 3$, elliptic	2S+6M+1I in $\mathbb{F}_q$
Compression, $n = 3$, Edwards	1M+1I in $\mathbb{F}_{q^3}$ and 2S+6M+1I in $\mathbb{F}_q$
Decompression, $n = 3$, elliptic	1M in $\mathbb{F}_{q^3}$, 5S+4M+1I, one square root, two cube roots in $\mathbb{F}_q$
Decompression, $n = 3$, Edwards	2M + 1I in $\mathbb{F}_{q^3}$, 5S+6M+2I, one square root, two cube roots in $\mathbb{F}_q$
Compression, $n = 5$, elliptic	3S+18M+3I in $\mathbb{F}_{q^5}$
Compression, $n = 5$, Edwards	2S+79M+3I in $\mathbb{F}_{q^5}$
Decompression, $n = 5$, elliptic	$\mathcal{O}(\log_2 q)$ operations in $\mathbb{F}_q$, 1S+3M+1I in $\mathbb{F}_{q^5}$
Decompression, $n = 5$, Edwards	$\mathcal{O}(\log_2 q)$ operations in $\mathbb{F}_q$, 1S+5M+1I in $\mathbb{F}_{q^5}$

References

[1] R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Mathematics and Its Applications 34, Chapman & Hall/CRC (2005).

[2] C. Aréne. T. Lange, M. Naehrig, C. Ritzenthaler, *Faster Computation of the Tate Pairing*, Journal of Number Theory 131, no. 5 (2011), 842-857.

[3] R. M. Avanzi, E. Cesena, *Trace zero varieties over fields of characteristic 2 for cryptographic applications*, Proceedings of the First Symposium on Algebraic Geometry and Its Applications – SAGA '07 (2007), 188-215.

[4] D. J. Bernstein, T. Lange, *Faster addition and doubling on elliptic curves*, Advances in Cryptology - ASIACRYPT 2007, LNCS vol. 4833, Springer-Verlag (2007), 29-50.

[5] D. J. Bernstein, T. Lange, *Inverted Edwards Coordinates*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, LNCS vol .4851, Springer-Verlag (2007), 20-27.

[6] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, *Twisted Edwards Curves*, Progress in Cryptology - AFRICACRYPT 2008, LNCS vol. 5023, Springer-Verlag (2008), 389-405.

[7] W. Bosma, J. Cannon, C.e Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235-265.

[8] E. Cesena, *Trace zero varieties in pairing-based cryptography*, Ph.D. Thesis (2010), available at `https://ricerca.mat.uniroma3.it/dottorato/Tesi/tesicesena.pdf`.

[9] H. M. Edwards, *A Normal Form for Elliptic Curves*, Bulletin of the American Mathematical Society 44 (2007), 393-422.

[10] G.Frey, *Applications of Arithmetical Geometry to Cryptographic Constructions*, Proceedings of the 5th International Conference on Finite Fields and Applications, Springer (1999),128-161.

[11] E. Gorla, M. Massierer, *Point Compression for the Trace Zero Subgroup over a Small Degree Extension Field*, Designs, Codes and Cryptography 75, no. 2 (2015), 335-357.

[12] E. Gorla, M. Massierer, *An Optimal Representation for the Trace Zero Subgroup*, available at `http://arxiv.org/abs/1405.2733`.

[13] T. Lange, *Trace zero subvarieties of genus* 2 *curves for cryptosystem*, Ramanujan Math. Soc. 19, no. 1 (2004) 15-33.

[14] N. Naumann, *Weil-Restriktion abelscher Varietäten*, Master's thesis (1999), available at `http://web.iem.uni-due.de/ag/numbertheory/dissertationen`.

[15] K. Rubin, A. Silverberg, *Using abelian varieties to improve pairing-based cryptography*, Journal of Cryptology 22, no. 3 (2009), 330-364.

[16] I. Semaev, *Summation polynomials and the discrete logarithm problem on elliptic curves*, available at `http://eprint.iacr.org/2004/013,2004`.

[17] A. Silverberg, *Compression for Trace Zero Subgroups of Elliptic Curves*, Trends in Mathematics 8 (2005), 93-100.

[18] J. C. Faugére, P. Gaudry, L. Huot, G. Renault, *Using Symmetries in the Index Calculus for Elliptic Curves Discrete Logarithm*, Journal of Cryptology 27, no. 4 (2014),595-635.