Faster Computation of Tate Pairings

Christophe Arène[1], Tanja Lange[2], Michael Naehrig[2], and Christophe Ritzenthaler[1]

[1] Institut de mathématiques de Luminy
Université de la Méditerranée
163 Avenue de Luminy Case 907, 13288 Marseille, France
{arene, ritzenth}@iml.univ-mrs.fr
[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands
tanja@hyperelliptic.org, michael@cryptojedi.org

Abstract. This paper proposes new explicit formulas for the doubling and addition step in Miller's algorithm to compute the Tate pairing. For Edwards curves the formulas come from a new way of seeing the arithmetic. We state the first geometric interpretation of the group law on Edwards curves by presenting the functions which arise in the addition and doubling. Computing the coefficients of the functions and the sum or double of the points is faster than with all previously proposed formulas for pairings on Edwards curves. They are even competitive with all published formulas for pairing computation on Weierstrass curves. We also speed up pairing computation on Weierstrass curves in Jacobian coordinates. Finally, we present several examples of pairing-friendly Edwards curves.
Keywords: Pairing, Miller function, explicit formulas, Edwards curves.

1 Introduction

Since their introduction to cryptography by Bernstein and Lange [7], Edwards curves have received a lot of attention because of their very fast group law. The group law in affine form was introduced by Edwards in [14] along with a description of the curve and several proofs of the group law. Remarkably none of the proofs provided a geometric interpretation while addition on Weierstrass curves is usually explained via the chord-and-tangent method.

Applications in discrete-logarithm-based systems such as Diffie-Hellman key exchange or digital signatures require efficient computation of scalar multiples and thus have benefited from the speedup in addition and doubling. The situation is significantly different in pairing-based cryptography where Miller's algorithm needs a function whose divisor is $(P)+(Q)-(P+Q)-(\mathcal{O})$, for two input points P and Q and their sum $P+Q$. For curves in Weierstrass form these functions are readily given by the line functions in the usual addition and doubling. Edwards curves have degree 4 and thus any line passes through 4 points instead of 3. This led many to conclude that Edwards curves provide no benefit to pairings and are doomed to be slower than the Weierstrass counterparts.

So far two papers have attempted to compute pairings efficiently on Edwards curves: Das and Sarkar [12] use the birational equivalence to Weierstrass curves to map the points on the Edwards curve to a Weierstrass curve on which the usual line functions are then evaluated. This approach comes at a huge performance penalty as these implicit pairing formulas need many more field operations to evaluate them. Das and Sarkar then focus on supersingular curves with embedding degree $k = 2$ and develop explicit formulas for that case.

* This work has been supported in part by the European Commission through the ICT Programme under Contract ICT–2007–216646 ECRYPT II, and in part by grant MTM2006-11391 from the Spanish MEC.

Ionica and Joux [22] use a different map to a curve of degree 3 and compute the 4-th power of the Tate pairing. The latter poses no problem in usage in protocols as long as both sides perform the same type of pairing computation. Their results are significantly faster than Das and Sarkar's but they are still much slower than pairings on Weierstrass curves.

In this paper we close several important gaps:

- We provide a geometric interpretation of the addition law for twisted Edwards curves.
- We study additions, doublings, and all the special cases that appear as part of the geometric addition law for twisted Edwards curves.
- We use the geometric interpretation of the group law to show how to compute the Tate pairing on twisted Edwards curves.
- We give examples of pairing-friendly Edwards curves.

Beyond that, we develop explicit formulas for computing pairings on Edwards and twisted Edwards curves that for Edwards curves

- solidly beat the results by Das–Sarkar [12] and Ionica–Joux [22];
- are as fast as the fastest published formulas for the doubling step on Weierstrass curves, namely curves with $a_4 = 0$ (e.g. Barreto-Naehrig curves) in Jacobian coordinates, and faster than other Weierstrass curves;
- need the same number of field operations as the best published formulas for mixed addition in Jacobian coordinates;
- have minimal performance penalty for non-affine base points.

In particular, for even embedding degree k the doubling step on an Edwards curve takes $1\mathbf{M} + 1\mathbf{S} + (k+6)\mathbf{m} + 5\mathbf{s}$, where $\mathbf{m}$ and $\mathbf{s}$ denote the costs of multiplication and squaring in the base field while $\mathbf{M}$ and $\mathbf{S}$ denote the costs of multiplication and squaring in the extension field of degree k. A mixed addition step takes $1\mathbf{M} + (k+12)\mathbf{m}$ and an addition step takes $1\mathbf{M} + (k+14)\mathbf{m}$.

We also speed up the addition and doubling steps on Weierstrass curves. We present the first and surprisingly fast explicit formulas for full addition steps on Weierstrass curves.

Our new formulas for Weierstrass curves are the fastest for affine base points while Edwards curves are better for projective base points – a common case in pairing-based protocols.

This paper does not consider other pairings such as the ate pairing; such pairings are particularly interesting for curves with twists of degree 4 or 6 and our example curves do not fit with that. The geometric interpretation and the explicit formulas work over any field.

2 Background on Pairings

Let p be a prime different from 2 and let $E/\mathbf{F}_p$ be an elliptic curve over $\mathbf{F}_p$ with neutral element denoted by $\mathcal{O}$. Let $n \mid \#E(\mathbf{F}_p)$ be a prime divisor of the group order and let E have embedding degree k with respect to n. For simplicity and speed we assume that $k > 1$.

Let $P \in E(\mathbf{F}_p)[n]$ and let $f_P \in \mathbf{F}_p(E)$ be such that $\mathrm{div}(f_P) = n(P) - n(\mathcal{O})$. Let $\mu_n \subset \mathbf{F}_{p^k}^*$ denote the group of n-th roots of unity. The reduced Tate pairing is given by

$$T_n : E(\mathbf{F}_p)[n] \times E(\mathbf{F}_{p^k})/nE(\mathbf{F}_{p^k}) \to \mu_n;\ (P,Q) \mapsto f_P(Q)^{(p^k-1)/n}.$$

Miller [25] suggested to compute pairings in an iterative manner. Let $n = (n_{l-1}, \ldots, n_1, n_0)_2$ be the binary representation of n and let $g_{R,P} \in \mathbf{F}_p(E)$ be the function arising in addition

on E such that $\mathrm{div}(g_{R,P}) = (R) + (P) - (R+P) - \mathcal{O}$, where $\mathcal{O}$ denotes the neutral element in the group of points and $R+P$ denotes the sum of R and P on E while additions of the form $(R)+(P)$ denote formal additions in the divisor group. Miller's algorithm starts with $R = P, f = 1$ and computes

1. for $i = l-2$ to 0 do
   (a) $f \leftarrow f^2 \cdot g_{R,R}(Q),\ R \leftarrow 2R$ //doubling step
   (b) if $n_i = 1$ then $f \leftarrow f \cdot g_{R,P}(Q),\ R \leftarrow R+P$ //addition step
2. $f \leftarrow f^{(p^k-1)/n}$

For Weierstrass curves and even k, several improvements and speedups are presented in [2] and [3]. In particular it is common to eliminate all denominators by choosing the second point Q such that its x-coordinate is in a subfield of $\mathbf{F}_{p^k}$. The functions $g_{R,P}$ are defined over $\mathbf{F}_p$ and their denominators are functions in x only. Writing $g_{R,P}(Q) = h_{R,P}(x_Q, y_Q)/s_{R,P}(x_Q)$ with polynomial functions $h_{R,P}$ and $s_{R,P}$, one sees that the complete contribution of all terms $s_{R,P}(x_Q)$ will be mapped to 1 by the final exponentiation if x_Q is in a proper subfield of $\mathbf{F}_{p^k}$. The latter is usually enforced by choosing a point Q' on a quadratic twist of E over $\mathbf{F}_{p^{k/2}}$ and defining Q as the image of Q' under the twist.

3 Formulas for Pairings on Weierstrass curves

An elliptic curve over $\mathbf{F}_p$ in short Weierstrass form is given by an equation of the form $y^2 = x^3 + a_4 x + a_6$ with $a_4, a_6 \in \mathbf{F}_p$. In this section we present new formulas for the addition and doubling step in Miller's algorithm that are faster than previous ones. Furthermore, we also cover the case of a non-affine base point.

The fastest formulas for doublings on Weierstrass curves are given in Jacobian coordinates (cf. the EFD [6]). A point is represented as $(X_1 : Y_1 : Z_1)$ which for $Z_1 \neq 0$ corresponds to the affine point (x_1, y_1) with $x_1 = X_1/Z_1^2$ and $y_1 = Y_1/Z_1^3$. To obtain the full speed of pairings on Weierstrass curves it is useful to represent a point by $(X_1 : Y_1 : Z_1 : T_1)$ with $T_1 = Z_1^2$. This allows one $\mathbf{s} - \mathbf{m}$ tradeoff in the addition step compared with the usual representation $(X_1 : Y_1 : Z_1)$. If the intermediate storage is an issue or if $\mathbf{s}$ are not much cheaper than $\mathbf{m}$, T_1 should not be cached. We present the formulas including T_1 below to have the best operation count for Weierstrass curves in the comparison; the modifications to omit T_1 are trivial.

The line function for Weierstrass curves is given by

$$g_{R,P}(X : Y : Z) = \frac{(YZ_0^3 - Y_0Z^3) - \lambda(XZ_0^2 - X_0Z^2)ZZ_0}{(X - cZ)Z^2},$$

where λ is the slope of the line through R and P (with multiplicities), $(X_0 : Y_0 : Z_0)$ is a point on the line, and c is some constant. When one computes the Tate pairing, the point $(X_0 : Y_0 : Z_0)$ and the constants λ and c are defined over the base field $\mathbf{F}_p$. The function is evaluated at a point $Q = (X_Q : Y_Q : Z_Q)$ defined over $\mathbf{F}_{p^k}$; if k is even then the field extension $\mathbf{F}_{p^k}$ is usually constructed via a quadratic subfield as $\mathbf{F}_{p^k} = \mathbf{F}_{p^{k/2}}(\alpha)$, with $\alpha^2 = \delta$ and Q is chosen to be of the form $Q = (x_Q : y_Q\alpha : 1)$ with $x_Q, y_Q \in \mathbf{F}_{p^{k/2}}$. Since the denominator is defined over a subfield, only the numerator needs to be considered and all multiplicative contributions from subfields of $\mathbf{F}_{p^k}$ can be discarded. In particular $\lambda = L_1/Z_3$ for curves in Jacobian coordinates and thus the computation simplifies to computing $Z_3(y_QZ_0^3\alpha - Y_0) - L_1(x_QZ_0^2 - X_0)Z_0$ up to factors from subfields of $\mathbf{F}_{p^k}$.

3.1 Addition

In Miller's algorithm all additions involve the base point as one input point, so in computing the line function, $(X_0 : Y_0 : Z_0)$ can be chosen as the base point P and all values depending solely on P and Q can be precomputed at the beginning of the computation. For additions, P is always stated as the second summand $P = (X_2 : Y_2 : Z_2)$.

Independent of the value of a_4, all doubling formulas compute Y_2^2. This means that $R_2 = Y_2^2$ can be cached since Miller's algorithm starts by computing $2P$. To enable an $\mathbf{m} - \mathbf{s}$ tradeoff we compute twice the value above; this does not change the result since $2 \in \mathbf{F}_p$. Multiplications with x_Q and y_Q cost $(k/2)\mathbf{m}$ each; for $k > 2$ it is thus useful to rewrite this equation as

$$l = Z_3 \cdot 2y_Q Z_2^3 \alpha - 2Z_3 \cdot Y_2 - L_1 \cdot (2(x_Q Z_2^2 - X_2)Z_2).$$

needing $(k+1)\mathbf{m}$ for precomputed $y'_Q = 2y_Q Z_2^3 \alpha$ and $x'_Q = 2(x_Q Z_2^2 - X_2)Z_2$. Additionally $1\mathbf{M}$ is needed to update the function f in Miller's algorithm.

Full addition. We use Bernstein and Lange's formulas ("add-2007-bl") from the EFD [6]. Note that pairings can be combined with windowing methods but this is rarely done because of the extra costs of $1\mathbf{M}$ of updating the step function. This means that all additions involve the base point P which is fixed throughout the computation. Therefore we can cache all values depending solely on P. In particular we precompute (or cache after the first addition) the values of $T_2 = Z_2^2$ and $S_2 = T_2 \cdot Z_2$. The numerator of λ is $r = D - C$.

$$\begin{aligned}
&A = X_1 \cdot T_2;\ B = X_2 \cdot T_1;\ C = 2Y_1 \cdot S_2;\ D = ((Y_2 + Z_1)^2 - R_2 - T_1) \cdot T_1;\\
&H = B - A;\ I = (2H)^2;\ J = H \cdot I;\ r = D - C;\ V = A \cdot I;\\
&X_3 = r^2 - J - 2V;\ Y_3 = r \cdot (V - X_3) - 2C \cdot J;\ Z_3 = ((Z_1 + Z_2)^2 - T_1 - T_2) \cdot H;\\
&T_3 = Z_3^2;\ l = Z_3 \cdot y'_Q - (Y_2 + Z_3)^2 + R_2 + T_3 - r \cdot x'_Q.
\end{aligned}$$

The formulas need $1\mathbf{M} + (k+9)\mathbf{m} + 6\mathbf{s}$ to compute the addition step. To our knowledge this is the first set of formulas for full (non-mixed) addition. If $\mathbf{m}$ is not significantly more expensive than $\mathbf{s}$, some computations should be performed differently. In particular, R_2 need not be stored, D is computed as $D = 2Y_2 \cdot Z_1 \cdot T_1$, l contains the term $-2Y_2 \cdot Z_3$ instead of $-(Y_2 + Z_3)^2 + R_2 + T_3$, and the computation of Z_3 can save some field additions.

If the values T_1, R_2, S_2, T_2, x'_Q, and y'_Q cannot be stored, different optimizations are needed; in particular the line function is computed as

$$l = ((Z_3 \cdot Z_0) \cdot Z_0^2) \cdot y_Q \alpha - Y_0 \cdot Z_3 - (L_1 \cdot Z_0) \cdot Z_0^2 \cdot x_Q + X_0 \cdot (L_1 \cdot Z_0)$$

and the computation costs end up as $(11\mathbf{m} + 5\mathbf{s}) + 1\mathbf{M} + (k+6)\mathbf{m} + 1\mathbf{s}$.

Mixed addition. Mixed addition means that the second input point is in affine representation. This happens in scalar multiplication if the base point P is given as $(x_2 : y_2 : 1)$.

We now state the mixed addition formulas based on Bernstein and Lange's formulas ("add-2007-bl") from the EFD [6]. Mixed additions are the usual case studied for pairings and the evaluation in $(k+1)\mathbf{m}$ is standard. However, most implementations miss the $\mathbf{s} - \mathbf{m}$ tradeoff in the main mixed addition formulas and do not compute the T-coordinate.

$$\begin{aligned}
&B = x_2 \cdot T_1;\ D = ((y_2 + Z_1)^2 - R_2 - T_1) \cdot T_1;\ H = B - X_1;\ I = H^2;\ E = 4I;\ J = H \cdot E;\\
&r = 2(D - Y_1);\ V = X_1 \cdot E;\ X_3 = r^2 - J - 2V;\ Y_3 = r \cdot (V - X_3) - 2Y_1 \cdot J;\\
&Z_3 = (Z_1 + H)^2 - T_1 - I; T_3 = Z_3^2;\ l = Z_3 \cdot y_Q \alpha - (y_2 + Z_3)^2 + R_2 + T_3 - r \cdot (x_Q - x_2).
\end{aligned}$$

The formulas need $1\mathbf{M} + (k+6)\mathbf{m} + 6\mathbf{s}$ to compute the mixed addition step.

3.2 Doubling

The main differences between the addition and the doubling formulas are that the doubling formulas depend on the curve coefficients and that the line function must be computed with the input to the doubling function $(X_0 : Y_0 : Z_0) = (X_1 : Y_1 : Z_1)$, which is changing at every step. So in particular $Z_0 \neq 1$ and no precomputations (like x'_Q or y'_Q in the addition step) can be done.

For arbitrary a_4 the equation of the slope is $\lambda = (3X_1^2 - a_4 Z_1^2)/(2Y_1 Z_1) = (3X_1^2 - a_4 Z_1^2)/Z_3$. Thus Z_3 is divisible by Z_1 and we can replace l by $l' = l/Z_1$ which will give the same result for the pairing computation. The value of

$$l' = (Z_3 \cdot Z_1^2) \cdot y_Q \alpha - 2Y_1^2 - L_1 \cdot Z_1^2 \cdot x_Q + X_1 \cdot L_1$$

can be computed in at worst $(k+3)\mathbf{m} + 1\mathbf{s}$.

The formulas by Ionica and Joux take into account the doubling formulas from the EFD for general Weierstrass curves in Jacobian coordinates. We thus present new formulas for the more special curves with $a_4 = -3$ and $a_4 = 0$.

Doubling on curves with $a_4 = -3$. The fastest doubling formulas are due to Bernstein (see [6] "dbl-2001-b") and need $3\mathbf{m} + 5\mathbf{s}$ for the doubling.

$$\begin{aligned} A = Y_1^2;\ B = X_1 \cdot A;\ C = 3(X_1 - T_1) \cdot (X_1 + T_1);\\ X_3 = C^2 - 8B;\ Z_3 = (Y_1 + Z_1)^2 - A - T_1;\ Y_3 = C \cdot (4B - X_3) - 8A^2;\\ l = (Z_3 \cdot T_1) \cdot y_Q \alpha - 2A - L_1 \cdot T_1 \cdot x_Q + X_1 \cdot L_1;\ T_3 = Z_3^2. \end{aligned}$$

The complete doubling step thus takes $1\mathbf{M} + 1\mathbf{S} + (k+6)\mathbf{m} + 5\mathbf{s}$.

Doubling on curves with $a_4 = 0$. The following formulas compute a doubling in $1\mathbf{m} + 7\mathbf{s}$. Note that without T_1 and computing $Z_3 = 2Y_1 \cdot Z_1$ a doubling can be computed in $2\mathbf{m} + 5\mathbf{s}$ which is always faster (see [6]) but the line functions make use of Z_1^2. Note further that here $L_1 = E = 3X_1^2$ is particularly simple.

$$\begin{aligned} A = X_1^2;\ B = Y_1^2;\ C = B^2;\ D = 2((X_1 + B)^2 - A - C);\ E = 3A;\ G = E^2;\\ X_3 = G - 2D;\ Y_3 = E \cdot (D - X_3) - 8C;\ Z_3 = (Y_1 + Z_1)^2 - B - T_1;\\ l = 2(Z_3 \cdot T_1) \cdot y_Q \alpha - 4B - 2E \cdot T_1 \cdot x_Q + (X_1 + E)^2 - A - G;\ T_3 = Z_3^2; \end{aligned}$$

The complete doubling step thus takes $1\mathbf{M} + 1\mathbf{S} + (k+3)\mathbf{m} + 8\mathbf{s}$.

4 Geometric interpretation of the group law on twisted Edwards curves

In this section K will denote a field of characteristic different from 2. A *twisted Edwards curve* over K is a curve given by an affine equation of the form $\mathrm{E}_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ for $a, d \in K^*$ and $a \neq d$. They were introduced by Bernstein et al. in [5] as a generalization of Edwards curves [7] which are included as $\mathrm{E}_{1,d}$. The addition law on $\mathrm{E}_{a,d}$ found a lot of attention in scalar multiplication. There is an addition law on points of the curve $\mathrm{E}_{a,d}$ which is given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$$

The neutral element is $\mathcal{O} = (0, 1)$, and the negative of (x_1, y_1) is $(-x_1, y_1)$. The point $\mathcal{O}' = (0, -1)$ has order 2. The points at infinity $\Omega_1 = (1 : 0 : 0)$ and $\Omega_2 = (0 : 1 : 0)$ are singular and blow up to two points each.

The name twisted Edwards curves comes from the fact that the set of twisted Edwards curves is invariant under quadratic twists while a quadratic twist of an Edwards curve is not necessarily an Edwards curve. In particular, let $\delta \in K \setminus K^2$ and let $\alpha^2 = \delta$ for some α in a quadratic extension K_2 of K. The map $\epsilon : (x, y) \mapsto (\alpha x, y)$ defines a K_2-isomorphism between the twisted Edwards curves $\mathrm{E}_{a/\delta,d/\delta}$ and $\mathrm{E}_{a,d}$. Hence, the map ϵ is the prototype of a quadratic twist. Note that twists change the x-coordinate unlike on Weierstrass curves where they affect the y-coordinate.

We now study the intersection of $\mathrm{E}_{a,d}$ with certain plane curves and explain the Edwards addition law in terms of the divisor class arithmetic. We remind the reader that the divisor class group is defined as the group of degree-0 divisors modulo the group of principal divisors in the function field of the curve, i.e. two divisors are *equivalent* if they differ by a principal divisor. For background reading on curves and Jacobians, we refer to [16] and [30].
We first consider projective lines in $\mathbb{P}^2$. A general line is of the form $L : c_X X + c_Y Y + c_Z Z = 0$ where $(c_X : c_Y : c_Z) \in \mathbb{P}^2$. A line is uniquely determined by two of its points when they are distinct. Let $P = (X_0 : Y_0 : Z_0) \in \mathbb{P}^2(K)$ with $Z_0 \neq 0$. The line through P and Ω_1 will be denoted $L_{1,P}$ and is defined by $Z_0 Y - Y_0 Z = 0$. The line through P and Ω_2 will be denoted $L_{2,P}$ and is defined by $Z_0 X - X_0 Z = 0$.

Let $\phi(X, Y, Z) = c_{X^2} X^2 + c_{Y^2} Y^2 + c_{Z^2} Z^2 + c_{XY} XY + c_{XZ} XZ + c_{YZ} YZ \in K[X, Y, Z]$ be a homogeneous polynomial of degree 2 and $C : \phi(X, Y, Z) = 0$, the associated plane (possibly degenerate) conic. Since the points $\Omega_1, \Omega_2, \mathcal{O}'$ are not on a line, a conic C passing through these points cannot be a double line and ϕ represents C uniquely up to multiplication by a scalar. Evaluating ϕ at Ω_1, Ω_2, and $\mathcal{O}'$ we see that a conic C through these points has the form

$$C : c_{Z^2}(Z^2 + YZ) + c_{XY} XY + c_{XZ} XZ = 0, \tag{1}$$

where $(c_{Z^2} : c_{XY} : c_{XZ}) \in \mathbb{P}^2(K)$.

Theorem 1. *Let $\mathrm{E}_{a,d}$ be a twisted Edwards curve over K, and let $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ be two affine, not necessarily distinct, points on $\mathrm{E}_{a,d}(K)$. Let C be the conic passing through Ω_1, Ω_2, $\mathcal{O}'$, P_1, and P_2, i. e. C is given by an equation of the form (1). If some of the above points are equal, we consider C and $\mathrm{E}_{a,d}$ to intersect with at least that multiplicity at the corresponding point. Then the coefficients in (1) of the equation ϕ of the conic C are uniquely (up to scalars) determined as follows:*

(a) If $P_1 \neq P_2$, $P_1 \neq \mathcal{O}'$ and $P_2 \neq \mathcal{O}'$, then

$$\begin{aligned} c_{Z^2} &= X_1 X_2 (Y_1 Z_2 - Y_2 Z_1), \\ c_{XY} &= Z_1 Z_2 (X_1 Z_2 - X_2 Z_1 + X_1 Y_2 - X_2 Y_1), \\ c_{XZ} &= X_2 Y_2 Z_1^2 - X_1 Y_1 Z_2^2 + Y_1 Y_2 (X_2 Z_1 - X_1 Z_2). \end{aligned}$$

(b) If $P_1 \neq P_2 = \mathcal{O}'$, then $c_{Z^2} = -X_1$, $c_{XY} = Z_1$, $c_{XZ} = Z_1$.
(c) If $P_1 = P_2$, then

$$\begin{aligned} c_{Z^2} &= X_1 Z_1 (Z_1 - Y_1), \\ c_{XY} &= d X_1^2 Y_1 - Z_1^3, \\ c_{XZ} &= Z_1 (Z_1 Y_1 - a X_1^2). \end{aligned}$$

Proof. If the points are distinct, the coefficients are obtained by evaluating the previous equation at the points P_1 and P_2. We obtain two linear equations in c_{Z^2}, c_{XY}, and c_{XZ}

$$\begin{aligned} c_{Z^2}(Z_1^2 + Y_1Z_1) + c_{XY}X_1Y_1 + c_{XZ}X_1Z_1 = 0, \\ c_{Z^2}(Z_2^2 + Y_2Z_2) + c_{XY}X_2Y_2 + c_{XZ}X_2Z_2 = 0. \end{aligned}$$

The formulas in (a) follow from the (projective) solutions

$$c_{Z^2} = \begin{vmatrix} X_1Y_1 & X_1Z_1 \\ X_2Y_2 & X_2Z_2 \end{vmatrix}, \; c_{XY} = \begin{vmatrix} X_1Z_1 & Z_1^2 + Y_1Z_1 \\ X_2Z_2 & Z_2^2 + Y_2Z_2 \end{vmatrix}, \; c_{XZ} = \begin{vmatrix} Z_1^2 + Y_1Z_1 & X_1Y_1 \\ Z_2^2 + Y_2Z_2 & X_2Y_2 \end{vmatrix}.$$

If $P_1 = P_2 \neq \mathcal{O}'$, we start by letting $Z_1 = 1, Z = 1$ in the equations. The tangent vectors at the non singular point $P_1 = (X_1 : Y_1 : 1)$ of $\mathrm{E}_{a,d}$ and of C are

$$\begin{pmatrix} dX_1^2Y_1 - Y_1 \\ aX_1 - dX_1Y_1^2 \end{pmatrix}, \quad \begin{pmatrix} -c_{Z^2} - c_{XY}X_1 \\ c_{XY}Y_1 + c_{XZ} \end{pmatrix}.$$

They are collinear if the determinant of their coordinates is zero which gives us a linear condition in the coefficients of ϕ. We get a second condition by $\phi(X_1, Y_1, 1) = 0$. Solving the linear system, we get the projective solution

$$\begin{aligned} c_{Z^2} &= X_1^3(-dY_1^2 + a) = X_1(1 - Y_1^2) = X_1(Y_1 + 1)(1 - Y_1), \\ c_{XY} &= 2dX_1^2Y_1^2 - Y_1 - Y_1^2 + dX_1^2Y_1 - aX_1^2 \\ &= -1 - Y_1 + dX_1^2Y_1^2 + dX_1^2Y_1 = (Y_1 + 1)(dX_1^2Y_1 - 1), \\ c_{XZ} &= -dX_1^2Y_1^3 - aX_1^2 + Y_1^2 + Y_1^3 = (Y_1 + 1)(Y_1 - aX_1^2) \end{aligned}$$

using the curve equation $aX_1^2 + Y_1^2 = 1 + dX_1^2Y_1^2$ to simplify. Finally, since $P_1 \neq \mathcal{O}'$, we can divide by $1 + Y_1$ and homogenize to get the result which provides the formulas as stated. The same formulas hold if $P_1 = \mathcal{O}'$ since intersection multiplicity greater than or equal to 3 at $\mathcal{O}'$ is achieved by setting $\phi = X(Y + Z) = XY + XZ$.

Assume now that $P_1 \neq P_2 = \mathcal{O}'$. Note that the conic C is tangent to $\mathrm{E}_{a,d}$ at $\mathcal{O}'$ if and only if $(\partial\phi/\partial x)(0, -1, 1) = (c_{XY}y + c_{XZ}z)(0, -1, 1) = 0$, i.e. $c_{XY} = c_{XZ}$. Then $\phi = (Y + Z)(c_{Z^2}Z + c_{XY}X)$. Since $P_1 \neq \mathcal{O}'$, it is not on the line $Y + Z = 0$. Then we get $c_{Z^2}Z_1 + c_{XY}X_1 = 0$ and the coefficients as in (b). □

Let P_1 and P_2 be two affine K-rational points on a twisted Edwards curve $\mathrm{E}_{a,d}$, and let $P_3 = (X_3 : Y_3 : Z_3) = P_1 + P_2$ be their sum. Let

$$l_1 = Z_3Y - Y_3Z, \quad l_2 = X$$

be the polynomials of the horizontal line L_{1,P_3} and the vertical line $L_{2,\mathcal{O}}$ respectively, and let

$$\phi = c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ$$

be the unique polynomial (up to multiplication by a scalar) defined by Theorem 1. The following theorem shows that the twisted Edwards group law indeed has a geometric interpretation involving the above equations. It gives us an important ingredient to compute Miller functions.

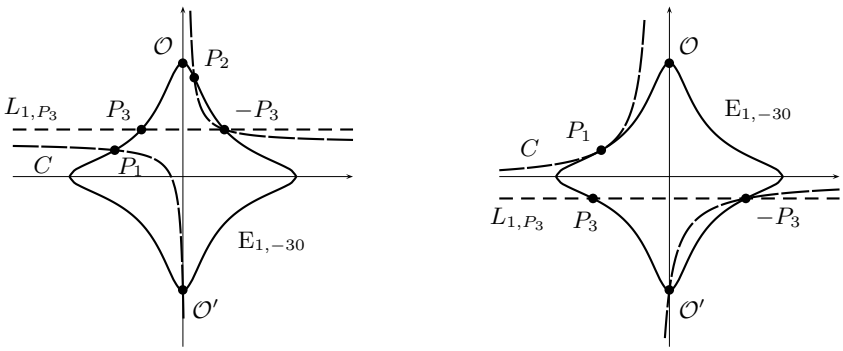
Theorem 2. *Let $a, d \in K^*$, $a \neq d$ and $\mathrm{E}_{a,d}$ be a twisted Edwards curve over K. Let $P_1, P_2 \in \mathrm{E}_{a,d}(K)$. Define $P_3 = P_1 + P_2$. Then we have*

$$\mathrm{div}\left(\frac{\phi}{l_1 l_2}\right) \sim (P_1) + (P_2) - (P_3) - (\mathcal{O}). \tag{2}$$

Proof. Let us consider the intersection divisor $(C \cdot \mathrm{E}_{a,d})$ of the conic $C : \phi = 0$ and the singular quartic $\mathrm{E}_{a,d}$. Bezout's Theorem [17, p. 112] tells us that the intersection of C and $\mathrm{E}_{a,d}$ should have $2 \cdot 4 = 8$ points counting multiplicities over $\overline{K}$. We note that the two points at infinity Ω_1 and Ω_2 are singular points of multiplicity 2. Moreover, by definition of the conic C, $(P_1) + (P_2) + (\mathcal{O}') + 2(\Omega_1) + 2(\Omega_2) \leq (C \cdot \mathrm{E}_{a,d})$. Hence there is an eighth point Q in the intersection. Let $L_{1,Q} : l_Q = 0$ be the horizontal line going through Q. Since the inverse for addition on twisted Edwards curves is given by $(x, y) \mapsto (-x, y)$, we see that $(L_{1,Q} \cdot \mathrm{E}_{a,d}) = (Q) + (-Q) + 2(\Omega_2)$. On the other hand $(L_{2,\mathcal{O}} \cdot \mathrm{E}_{a,d}) = (\mathcal{O}) + (\mathcal{O}') + 2(\Omega_1)$. Hence by combining the above divisors we get $\mathrm{div}\left(\frac{\phi}{l_Q l_2}\right) \sim (P_1) + (P_2) - (-Q) - (\mathcal{O})$. By unicity of the group law with neutral element $\mathcal{O}$ on the elliptic curve $\mathrm{E}_{a,d}$ [30, Prop.3.4], the last equality means that $P_3 = -Q$. Hence $(L_{1,P_3} \cdot \mathrm{E}_{a,d}) = (P_3) + (-P_3) + 2(\Omega_2) = (-Q) + (Q) + 2(\Omega_2)$ and $l_1 = l_Q$. So $\mathrm{div}\left(\frac{\phi}{l_1 l_2}\right) \sim (P_1) + (P_2) - (P_3) - (\mathcal{O})$. □

Remark 3. From the proof, we see that $P_1 + P_2$ is obtained as the mirror image with respect to the y-axis of the eighth intersection point of $\mathrm{E}_{a,d}$ and the conic C passing through $\Omega_1, \Omega_2, \mathcal{O}', P_1$ and P_2.

Example 4. As an example we consider the Edwards curve $\mathrm{E}_{1,-30} : x^2 + y^2 = 1 - 30x^2y^2$ over the set of real numbers $\mathbb{R}$. We choose the point P_1 with x-coordinate $x_1 = -0.6$ and P_2 with x-coordinate $x_2 = 0.1$. Figure 1(a) shows addition of different points P_1 and P_2, and Figure 1(b) shows doubling of the point P_1.



(a) $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$, $P_3 = P_1 + P_2$ (b) $P_1 = P_2 \neq \mathcal{O}'$, $P_3 = 2P_1$

Fig. 1. Geometric interpretation of the group law on $x^2 + y^2 = 1 - 30x^2y^2$ over $\mathbb{R}$.

5 Formulas for Pairings on Edwards Curves

In this section we show how to use the geometric interpretation of the group law to compute pairings. We assume that k is even and that the second input point Q is chosen by using the tricks in [2] and [3]: Let $\mathbf{F}_{p^k}$ have basis $\{1, \alpha\}$ over $\mathbf{F}_{p^{k/2}}$ with $\alpha^2 = \delta \in \mathbf{F}_{p^{k/2}}$ and let

$Q' = (X_0 : Y_0 : Z_0) \in \mathrm{E}_{a\delta,d\delta}(\mathbf{F}_{p^{k/2}})$. Twisting Q' with α ensures that the second argument of the pairing is on $\mathrm{E}_{a,d}(\mathbf{F}_{p^k})$ (and no smaller field) and is of the form $Q = (X_0\alpha : Y_0 : Z_0)$, where $X_0, Y_0, Z_0 \in \mathbf{F}_{p^{k/2}}$.

By Theorem 2 we have $g_{R,P} = \frac{\phi}{l_1 l_2}$. So the update in the Miller loop computes $g_{R,P}$, evaluates it at $Q = (X_0\alpha : Y_0 : Z_0)$ and updates f as $f \leftarrow f \cdot g_{R,P}(Q)$ (addition) or as $f \leftarrow f^2 \cdot g_{R,R}(Q)$ (doubling). Given the shape of ϕ and the point $Q = (X_0\alpha : Y_0 : Z_0)$, we see that we need to compute

$$\begin{aligned}\frac{\phi}{l_1 l_2}(X_0\alpha : Y_0 : Z_0) &= \frac{c_{Z^2}(Z_0^2 + Y_0 Z_0) + c_{XY} X_0 \alpha Y_0 + c_{XZ} X_0 Z_0 \alpha}{(Z_3 Y_0 - Y_3 Z_0) X_0 \alpha} \\ &= \frac{c_{Z^2}\frac{Z_0+Y_0}{X_0\delta}\alpha + c_{XY} y_0 + c_{XZ}}{Z_3 y_0 - Y_3}, \\ &\in (c_{Z^2}\eta\alpha + c_{XY} y_0 + c_{XZ})\mathbf{F}^*_{p^{k/2}},\end{aligned}$$

where $(X_3 : Y_3 : Z_3)$ are coordinates of the point $R+P$ or $R+R$, $y_0 = Y_0/Z_0$, and $\eta = \frac{Z_0+Y_0}{X_0\delta}$. Note that $\eta \in \mathbf{F}_{p^{k/2}}$ and that it is fixed for the whole computation, so it can be precomputed. The coefficients c_{Z^2}, c_{XY}, and c_{XZ} are defined over $\mathbf{F}_p$, so the evaluation at Q given the coefficients of the conic can be computed in $k\mathbf{m}$ (multiplications by η and y_0 need $\frac{k}{2}\mathbf{m}$ each).

5.1 Addition

Hisil et al. presented new addition formulas for twisted Edwards curves in extended Edwards form at Asiacrypt 2008 [21]. Let $P_3 = P_1 + P_2$ for two different points $P_1 = (X_1 : Y_1 : Z_1 : T_1)$ and $P_2 = (X_2 : Y_2 : Z_2 : T_2)$ with $Z_1, Z_2 \neq 0$ and $T_i = X_i Y_i / Z_i$. Theorem 1 (a) states the coefficients of the conic section for addition. We use T_1, T_2 to shorten the formulas.

$$\begin{aligned}c_{Z^2} &= X_1 X_2 (Y_1 Z_2 - Y_2 Z_1) = Z_1 Z_2 (T_1 X_2 - X_1 T_2), \\ c_{XY} &= Z_1 Z_2 (X_1 Z_2 - Z_1 X_2 + X_1 Y_2 - Y_1 X_2), \\ c_{XZ} &= X_2 Y_2 Z_1^2 - X_1 Y_1 Z_2^2 + Y_1 Y_2 (X_2 Z_1 - X_1 Z_2) \\ &= Z_1 Z_2 (Z_1 T_2 - T_1 Z_2 + Y_1 T_2 - T_1 Y_2).\end{aligned}$$

Note that all coefficients are divisible by $Z_1 Z_2 \neq 0$ and so we scale the coefficients. The explicit formulas for computing $P_3 = P_1 + P_2$ and $(c_{Z^2}, c_{XY}, c_{XZ})$ are given as follows:

$$\begin{aligned}A &= X_1 \cdot X_2;\ B = Y_1 \cdot Y_2;\ C = Z_1 \cdot T_2;\ D = T_1 \cdot Z_2;\ E = D + C; \\ F &= (X_1 - Y_1) \cdot (X_2 + Y_2) + B - A;\ G = B + aA;\ H = D - C;\ I = T_1 \cdot T_2; \\ c_{Z^2} &= (T_1 - X_1) \cdot (T_2 + X_2) - I + A;\ c_{XY} = X_1 \cdot Z_2 - X_2 \cdot Z_1 + F; \\ c_{XZ} &= (Y_1 - T_1) \cdot (Y_2 + T_2) - B + I - H; \\ X_3 &= E \cdot F;\ Y_3 = G \cdot H;\ T_3 = E \cdot H;\ Z_3 = F \cdot G.\end{aligned}$$

With these formulas P_3 and $(c_{Z^2}, c_{XY}, c_{XZ})$ can be computed in $1\mathbf{M} + (k+14)\mathbf{m} + 1\mathbf{m_a}$, where $\mathbf{m_a}$ denotes the costs of a multiplication by a. If the base point P_2 has $Z_2 = 1$, the above costs reduce to $1\mathbf{M} + (k+12)\mathbf{m} + 1\mathbf{m_a}$. We used Sage [31] to verify the explicit formulas.

5.2 Doubling

Theorem 1 (c) states the coefficients of the conic section in the case of doubling. To speed up the computation we multiply each coefficient by $-2Y_1/Z_1$; remember that ϕ was unique up to scaling. Note also that $Y_1, Z_1 \neq 0$ because we assume that all points have odd order. The multiplication by Y_1/Z_1 reduces the overall degree of the equations since we can use the curve equation to simplify the formula for c_{XY}; the factor 2 is useful in obtaining an $\mathbf{s} - \mathbf{m}$ tradeoff in the explicit formulas below. We obtain:

$$\begin{aligned} c_{Z^2} &= X_1(2Y_1^2 - 2Y_1Z_1), \\ c_{XY} &= 2(Y_1Z_1^3 - dX_1^2Y_1^2)/Z_1 = 2(Y_1Z_1^3 - Z_1^2(aX_1^2 + Y_1^2) + Z_1^4)/Z_1 \\ &= Z_1(2(Z_1^2 - aX_1^2 - Y_1^2) + 2Y_1Z_1), \\ c_{XZ} &= Y_1(2aX_1^2 - 2Y_1Z_1). \end{aligned}$$

Of course we also need to compute $P_3 = 2P_1$. We use the explicit formulas from [5] for the doubling and reuse subexpressions in computing the coefficients of the conic. The formulas were checked for correctness with Sage [31]. Since the input is given in extended form as $P_1 = (X_1 : Y_1 : Z_1 : T_1)$ we can use T_1 in the computation of the conic as

$$\begin{aligned} c_{Z^2} &= X_1(2Y_1^2 - 2Y_1Z_1) = 2Z_1Y_1(T_1 - X_1), \\ c_{XY} &= Z_1(2(Z_1^2 - aX_1^2 - Y_1^2) + 2Y_1Z_1), \\ c_{XZ} &= Y_1(2aX_1^2 - 2Y_1Z_1) = 2Z_1(aX_1T_1 - Y_1^2), \end{aligned}$$

and then scale the coefficients by $1/Z_1$. The computation of $P_3 = (X_3 : Y_3 : Z_3 : T_3)$ and $(c_{Z^2}, c_{XY}, c_{XZ})$ is then done in $1\mathbf{M} + 1\mathbf{S} + (k+6)\mathbf{m} + 5\mathbf{s} + 2\mathbf{m_a}$ as

$$\begin{aligned} &A = X_1^2;\ B = Y_1^2;\ C = Z_1^2; D = (X_1 + Y_1)^2;\ E = (Y_1 + Z_1)^2; \\ &F = D - (A + B);\ G = E - (B + C);\ H = aA;\ I = H + B;\ J = C - I; \\ &K = J + C;\ c_{Z^2} = 2Y_1 \cdot (T_1 - X_1);\ c_{XY} = 2J + G;\ c_{XZ} = 2(aX_1 \cdot T_1 - B); \\ &X_3 = F \cdot K;\ Y_3 = I \cdot (B - H);\ Z_3 = I \cdot K;\ T_3 = F \cdot (B - H). \end{aligned}$$

Note that like in [21] we can save $1\mathbf{m_a}$ per doubling by changing to the extended representation only before an addition. Morain [26] showed that a can always be chosen as $a = 1$ when constructing a pairing-friendly curve. So the effective cost of multiplying by a is $\mathbf{m_a} = 0$.

6 Operation counts

We give an overview of the best formulas in the literature for pairing computation on Edwards curves and for the different forms of Weierstrass curves in Jacobian coordinates. We compare the results with our new pairing formulas for Weierstrass and Edwards curves.

Throughout this section we assume that k is even, that Q is given in affine coordinates, and that quadratic twists are used so that multiplications with η and y_Q take $(k/2)\mathbf{m}$ each.

6.1 Overview

Chatterjee, Sarkar, and Barua [8] study pairings on Weierstrass curves in Jacobian coordinates. Their paper does not distinguish between multiplications in $\mathbf{F}_p$ and in $\mathbf{F}_{p^k}$ but their

results are easily translated. For mixed addition their formulas need $1\mathbf{M} + (k+9)\mathbf{m} + 3\mathbf{s}$. For doublings they need $1\mathbf{M} + (k+7)\mathbf{m} + 1\mathbf{S} + 4\mathbf{s}$ if $a_4 = -3$. For doubling on general Weierstrass curves (no condition on a_4) the formulas by Ionica and Joux [22] are fastest with $1\mathbf{M} + (k+1)\mathbf{m} + 1\mathbf{S} + 11\mathbf{s}$.

Actually, any mixed addition (mADD) or addition (ADD) needs $1\mathbf{M} + k\mathbf{m}$ for the evaluation at Q and the update of f; each doubling (DBL) needs $1\mathbf{M} + k\mathbf{m} + 1\mathbf{S}$ for the evaluation at Q and the update of f. In the following we do not comment on these costs since they do not depend on the chosen representation and are a fixed offset. We also do not report these expenses in the overview table.

Hankerson, Menezes, and Scott [20] study pairing computation on Barreto-Naehrig [4] curves. All BN curves have the form $y^2 = x^3 + a_6$ and are thus more special than curves with $a_4 = -3$ or Edwards curves. They need $6\mathbf{m} + 5\mathbf{s}$ for a doubling step and $9\mathbf{m} + 3\mathbf{s}$ for a mixed addition step. Very recently, Costello et al. presented explicit formulas for pairing on curves of the form $y^2 = x^3 + b^2$, i.e. $a_4 = 0$ and a_6 is a square. The representation is in projective rather than Jacobian coordinates.

Das and Sarkar [12] were the first to publish pairing formulas for Edwards curves. We do not include them in our overview since their study is specific to supersingular curves with $k = 2$. Ionica and Joux [22] proposed the thus far fastest pairing formulas for Edwards curves. Note that they actually compute the 4th power $T_n(P,Q)^4$ of the Tate pairing. This has almost no negative effect for usage in protocols. So we include their result as pairings on Edwards curves.

We denote Edwards coordinates by $\mathcal{E}$, projective coordinates by $\mathcal{P}$, and Jacobian coordinates by $\mathcal{J}$. Morain [26] showed that 2-isogenies reach $a = 1$ from any twisted Edwards curve; we therefore omit $\mathbf{m_a}$ in the table.

	DBL	mADD	ADD
$\mathcal{J}$, [22], [8]	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m_{a_4}}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}$, [22], this paper	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m_{a_4}}$	$6\mathbf{m} + 6\mathbf{s}$	$9\mathbf{m} + 6\mathbf{s}$
$\mathcal{J}, a_4 = -3$, [8]	$7\mathbf{m} + 4\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = -3$, this paper	$6\mathbf{m} + 5\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$9\mathbf{m} + 6\mathbf{s}$
$\mathcal{J}, a_4 = 0$, [9], [8]	$6\mathbf{m} + 5\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = 0$, this paper	$3\mathbf{m} + 8\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$9\mathbf{m} + 6\mathbf{s}$
$\mathcal{P}, a_4 = 0, a_6 = b^2$ [11]	$3\mathbf{m} + 5\mathbf{s}$	$10\mathbf{m} + 2\mathbf{s} + 1\mathbf{m_b}$	$13\mathbf{m} + 2\mathbf{s} + 1\mathbf{m_b}$
$\mathcal{E}$, [22]	$8\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	$14\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	—
$\mathcal{E}$, this paper	$6\mathbf{m} + 5\mathbf{s}$	$12\mathbf{m}$	$14\mathbf{m}$

6.2 Comparison

It is common in the literature to assume $\mathbf{s} = 0.8\mathbf{m}$; however, this is for extremely sparse primes such as generalized Mersenne primes allowing extremely fast reduction. The construction of pairing-friendly curves rarely lead to very sparse primes p and thus $\mathbf{s}/\mathbf{m}$ is closer to 1. Note also that additions appear far less frequently than doublings since the constructions lead to n with low Hamming weight.

The overview shows that our new formulas for Edwards curves solidly beat all previous formulas published for pairing computation on Edwards curves.

Our new formulas for pairings on arbitrary Edwards curves are faster than all formulas previously known for Weierstrass curves except for the very special curves with $a_4 = 0$. Specifically mixed additions on Edwards curves are slower by some $\mathbf{s} - \mathbf{m}$ tradeoffs but doublings are much more frequent and gain at least an $\mathbf{s} - \mathbf{m}$ tradeoff each.

The curves considered in [11] are extremely special: For $p \equiv 2 \bmod 3$ these curves are supersingular and thus have $k = 2$ and for $p \equiv 1 \bmod 3$ a total of 3 isomorphism classes is covered by this curve shape. They have faster doublings but slower additions and mixed additions than Edwards curves.

Our own improvements to the doubling and addition formulas for Weierstrass curves beat our new formulas for Edwards curves with affine base point by several $\mathbf{s}-\mathbf{m}$ tradeoffs. However, in many protocols the pairing input P is the output of some scalar multiplication and is thus naturally provided in non-affine form. Converting P to affine form is more expensive than proceeding in non-affine form so that all additions are full additions. A full addition on an Edwards curve needs one field operation less than on Weierstrass curves. Depending on the frequency of addition and the $\mathbf{s}/\mathbf{m}$ ratio the special curves with $a_4 = 0$ might or might not be faster. For all other curves, the Edwards form is the best representation. Furthermore, scalar multiplications on Edwards curves are significantly faster than on Weierstrass curves.

To the best of our knowledge no full addition formulas were published for Weierstrass curves before this paper. Our new formulas for Weierstrass curves are faster than all previous ones by several $\mathbf{s} - \mathbf{m}$ tradeoffs.

7 Construction of Pairing-Friendly Edwards Curves

The previous chapter showed that pairing computation can benefit from Edwards curves. Most constructions of pairing-friendly elliptic curves in the literature aim at a prime group order and thus in particular do not lead to curves with cofactor 4 that can be transformed to Edwards curves. Galbraith, McKee, and Valença [18] showed how to use the MNT construction to produce curves with small cofactor. Some other constructions that allow to find curves with cofactor divisible by 4 are described by Freeman, Scott, and Teske [15].

For efficient implementation, we aim at balancing the difficulty of the DLPs on the curve and in the multiplicative group of the finite field $\mathbf{F}_{p^k}$. Following the ECRYPT recommendations [13], the "optimal" bitsizes of the primes p and n for curves $E/\mathbf{F}_p$ with $n \mid \#E(\mathbf{F}_p)$ and n prime are shown in Table 1 for the most common security levels. For these parameters, the DLP in the subgroup of $E(\mathbf{F}_p)$ of order n is considered equally hard as the DLP in $\mathbf{F}^*_{p^k}$. In order to transform the curve to an Edwards curve, we need to have $\#E(\mathbf{F}_p) = 4hn$ for some cofactor h. It follows that the rho-value $\rho = \log(p)/\log(n)$ of E is always larger than 1. The recommendations imply a desired value for $\rho \cdot k$ as displayed in Table 1, which preferably should be achieved with an even embedding degree to favor efficient implementation and ρ close to 1. In the appendix we present five examples of pairing-friendly Edwards curves with

n	160	192	224	256	320	512
p^k	1248	1776	2432	3248	4800	15424
$\rho \cdot k$	7.80	9.25	10.86	12.67	15	30.13

Table 1. "Optimal" bitsizes for the primes n and p and the corresponding values for $\rho \cdot k$.

embedding degrees $k \in \{6, 8, 10, 22\}$, thus covering a range of security parameters.

References

1. Roberto M. Avanzi, Henri Cohen, Christophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *The Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC, 2005.
2. Paulo S. L. M. Barreto, Hae Yong Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. In *CRYPTO 2002 [33]*, pages 354–368, 2002.
3. Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Efficient implementation of pairing-based cryptosystems. *J. Cryptology*, 17:321–334, 2004.
4. Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In *SAC 2005 [29]*, pages 319–331, 2006.
5. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In *Africacrypt [32]*, pages 389–405, 2008. http://cr.yp.to/papers.html#twisted.
6. Daniel J. Bernstein and Tanja Lange. Explicit-formulas database. http://www.hyperelliptic.org/EFD.
7. Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *ASIACRYPT 2007 [24]*, pages 29–50, 2007. http://cr.yp.to/newelliptic/.
8. Sanjit Chatterjee, Palash Sarkar, and Rana Barua. Efficient computation of Tate pairing in projective coordinate over general characteristic fields. In *ICISC 2004 [27]*, pages 168–181, 2005.
9. Zhaohui Cheng and Manos Nistazakis. Implementing pairing-based cryptosystems. In *3rd International Workshop on Wireless Security Technologies IWWST-2005*, 2005.
10. Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors. *Progress in Cryptology - INDOCRYPT 2008, 9th International Conference on Cryptology in India, Kharagpur, India, December 14-17, 2008, proceedings*, volume 5365 of *Lecture Notes in Computer Science*, Berlin, 2008. Springer.
11. Craig Costello, Huseyin Hisil, Colin Boyd, Juan Manuel Gonzalez Nieto, and Kenneth Koon-Ho Wong. Faster pairings on special weierstrass curves. Technical report, ePrint, 2009.
12. M. Prem Laxman Das and Palash Sarkar. Pairing computation on twisted Edwards form elliptic curves. In *Pairing 2008 [19]*, pages 192–210, 2008.
13. Mats Näslund (editor). ECRYPT yearly report on algorithms and keysizes (2007-2008). Technical report, ECRYPT – European Network of Excellence in Cryptology, EU FP6, IST-2002-507932, 2008. published as deliverable D.SPA.28 http://www.ecrypt.eu.org/ecrypt1/documents/D.SPA.28-1.1.pdf.
14. Harold M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007. http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html.
15. David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006. update 2008, http://eprint.iacr.org/.
16. Gerhard Frey and Tanja Lange. *Background on Curves and Jacobians*, chapter 13 in [1], pages 45–85. 2005.
17. William Fulton. *Algebraic Curves*. W. A. Benjamin, Inc., 1969.
18. Steven D. Galbraith, James F. McKee, and Paula C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields and their Applications*, 13:800–814, 2007.
19. Steven D. Galbraith and Kenneth G. Paterson, editors. *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008, Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, Berlin, 2008. Springer.
20. Darrel Hankerson, Alfred J. Menezes, and Michael Scott. Software implementation of pairings. In *Identity-Based Cryptography [23]*, pages 188–206, 2009.
21. Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In *ASIACRYPT 2008 [28]*, pages 326–343, 2008.
22. Sorina Ionica and Antoine Joux. Another approach to pairing computation in Edwards coordinates. In *INDOCRYPT 2008 [10]*, pages 400–413, 2008. http://eprint.iacr.org/2008/292.
23. Marc Joye and Gregory Neven, editors. *Identity-Based Cryptography*, volume 2 of *Cryptology and Information Security Series*. IOS Press, 2009.
24. Kaoru Kurosawa, editor. *Advances in Cryptology — ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, Berlin Heidelberg, 2007. Springer.
25. Victor S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17:235–261, 2004.
26. Francois Morain. Edwards curves and cm curves. Technical report, arXiv, 2009.
27. Choonsik Park and Seongtaek Chee, editors. *Information Security and Cryptology - ICISC 2004, 7th International Conference, Seoul, Korea, December 2-3, 2004, Revised Selected Papers*, volume 3506 of *Lecture Notes in Computer Science*. Springer, 2005.
28. Josef Pieprzyk, editor. *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, volume 5350 of *Lecture Notes in Computer Science*, Berlin, 2008. Springer.

29. Bart Preneel and Stafford E. Tavares, editors. *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers*, volume 3897 of *Lecture Notes in Computer Science*. Springer, 2006.
30. Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Graduate texts in mathematics. Springer-Verlag, 1986.
31. William Stein. Sage mathematics software (version 2.8.12), 2008. The Sage Group, http://www.sagemath.org.
32. Serge Vaudenay, editor. *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008, proceedings.*, Lecture Notes in Computer Science, Berlin, 2008. Springer.
33. Moti Yung, editor. *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*. Springer, 2002.

8 Appendix: Examples of Pairing-Friendly Edwards Curves

This appendix presents pairing-friendly Edwards curves. Note that they were constructed for applications in the Tate pairing so that the curve over the ground field has a point of order 4 (rather than for the ate pairing for which the twist of the curve should be birationally equivalent to a curve in Edwards form. The rho-values are stated with the curves. Notation is as before, where the number of $\mathbf{F}_p$-rational points on the curve is $4hn$.

$k = 6, \rho = 1.22$ following [18]: $D = 7230$, $\lceil \log(n) \rceil = 165, \lceil \log(h) \rceil = 34, \lceil \log(p) \rceil = 201$

$$\begin{aligned} p &= 2051613663768129606093583432875887398415301962227490187508801, \\ n &= 4481254541330857991395743820133138543474344236627 7, \\ h &= 7 \cdot 733 \cdot 2230663, \\ d &= 889556570662354157210639662153375862261205379822879716332449. \end{aligned}$$

$k = 6, \rho = 1.48$ following [18]: $D = 4630$, $\lceil \log(n) \rceil = 191, \lceil \log(h) \rceil = 90, \lceil \log(p) \rceil = 283$

$$\begin{aligned} p &= 1207642247325762099962277292422023053565510428560082635785607017961903151061588636160 1, \\ n &= 2498886235887409414948289020220476887707263210939845485839, \\ h &= 11161 \cdot 19068349 \cdot 5676957216676051, \\ d &= 459700868786641293497037849824546593293161507789317870532074459230552713530050277819 0. \end{aligned}$$

$k = 8, \rho = 1.50$ following Example 6.10 in [15]:
$D = 1$, $\lceil \log(n) \rceil = 267, \lceil \log(h) \rceil = 133, \lceil \log(p) \rceil = 401$

$$\begin{aligned} p &= 3268160001953756839814226928408095055564196036053442104675179095037921817537848577548206 867473587369969429214840474559317, \\ n &= 1333924868013886151119696464826683826609085298781760137526173900750680368723648 81, \\ h &= 5 \cdot 7730839564540529681 \cdot 15845840683775553774, \\ d &= 2123127426004088514407260044332673251624085348705495887018005315725392532299918749170138 112572498450762627364652443 8. \end{aligned}$$

$k = 10, \rho = 1.49$ following Construction 6.5 in [15]:

$D = 1$, $\lceil \log(n) \rceil = 328, \lceil \log(h) \rceil = 160, \lceil \log(p) \rceil = 490$

$p = 319667071934078971315677746964738362812713703914060344412320604868708613896665173327525$
$2543330209754427990875101879841425427646115157594515629491249,$
$n = 546812704438652190176048473638362779688423061794499756311925945545462152449512232744941$
$959488864241,$
$h = 2^4 \cdot 70199^4 \cdot 7831391^4,$
$d = -1.$

$k = 22, \rho = 1.39$ following Construction 6.6 in [15]:
$D = 3$, $\lceil \log(n) \rceil = 519, \lceil \log(h) \rceil = 204, \lceil \log(p) \rceil = 724$

$p = 793243907836538225101919663581953770913765580662849594203574636874518836858270555160144$
$920983827280386815433912190214824741372960533715598691121880716182459140439367767771926$
$661771139435864150449118516697852906546951 23,$
$n = 962131187808560377898569195262572710988984869464755002509459666178069262628367282191252$
$973105101373704953818660670550658659790389637917606342501732923486369,$
$h = 3^5 \cdot 7 \cdot 13^2 \cdot 19^2 \cdot 37^2 \cdot 6421^2 \cdot 7291 \cdot 3498559^2 \cdot 22526869^2 \cdot 78478074679,$
$d = 264414627547939780810839826727395383259987444981352560753582877086320074680650633780571$
$920373615518032509200852332864216413041328949865016666759728218019456097204687710831048$
$176560920168796149011602454439457862563995 18.$