Pairing Computation on Twisted Edwards Form Elliptic Curves

M. Prem Laxman Das and Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road
Kolkata 700108, India
{prem_r,palash}@isical.ac.in

Abstract. A new form of elliptic curve was recently discovered by Edwards and their application to cryptography was developed by Bernstein and Lange. The form was later extended to the twisted Edwards form. For cryptographic applications, Bernstein and Lange pointed out several advantages of the Edwards form in comparison to the more well known Weierstraß form. We consider the problem of pairing computation over Edwards form curves. Using a birational equivalence between twisted Edwards and Weierstraß forms, we obtain a closed form expression for the Miller function computation.

Simplification of this computation is considered for a class of supersingular curves. As part of this simplification, we obtain a distortion map similar to that obtained for Weierstraß form curves by Barreto et al and Galbraith et al. Finally, we present explicit formulae for combined doubling and Miller iteration and combined addition and Miller iteration using both inverted Edwards and projective Edwards coordinates. For the class of supersingular curves considered here, our pairing algorithm can be implemented without using any inversion.

Keywords: elliptic curve, pairings, Edwards form, Miller function, supersingular curves.

1 Introduction

Background. Pairings on curves find many applications in cryptographic protocols. These have been used to give one-round three-party key exchange [1], identity-based encryption [2] and many other schemes. For implementing such protocols, it is essential to have curves which are pairing friendly and an efficient pairing algorithm. Construction of pairing friendly curves is itself an active area of research. See [3] for a survey.

This work concerns computing (Tate) pairing on an elliptic curve. Tate pairing was introduced in cryptology in [4]. An algorithm for finding Tate pairing on elliptic curves was first given by Miller, which was subsequently published in [5]. Tate pairing over supersingular curves was studied in [6,7]. Several techniques were described to improve the efficiency of computing the pairing.

S.D. Galbraith and K.G. Paterson (Eds.): Pairing 2008, LNCS 5209, pp. 192–210, 2008.

Edwards [8] introduced a new form of elliptic curves and gave an elegant addition rule for such curves. The work [8] considered elliptic curves over number fields. Bernstein and Lange [9] showed the usefulness of the Edwards form elliptic curves in cryptography. Among other things, they showed that, unlike the more well known Weierstraß form, the Edwards form admits a complete (and hence, unified) addition formula. This is very useful in providing resistance to side-channel attacks. Further, in [9] and [10] they developed efficient explicit formulae for doubling, addition and mixed-addition using projective and inverted coordinates. These provided the fastest methods for scalar multiplication on elliptic curves.

Motivation. Pairing based cryptographic protocols use both scalar multiplications and pairing computations. In view of the advantages of Edwards form curves, a designer may wish to implement a pairing based protocol using such curves. The problem, however, is with the pairing computation. Till date, all pairing algorithms use the more well known Weierstraß form of an elliptic curve. Thus, to implement pairings, one will have to use an isomorphism to map Edwards points to points on Weierstraß form and then compute pairing on Weierstraß form curve.

This raises several questions. Is it possible to compute pairing directly on the Edwards form? How does this compare to the cost of converting to Weierstraß form and then computing the pairing? More generally, how does pairing on Edwards form compare to the cost of computing pairing on the Weierstraß form? Are there any advantages in computing pairing directly on Edwards form?

Motivated by these questions, we make a detailed investigation of pairing on Edwards form. The basic question is of course, how to perform pairing directly on Edwards form.

Contributions. The following question is central to computing the Tate pairing on elliptic curves using Miller's algorithm: given points P_1 and P_2 on an elliptic curve, find a point P_3 and a rational function h such that

$$\mathrm{div}(h) = (P_1) + (P_2) - (P_3) - \mathcal{O},$$

where $\mathcal{O}$ is a distinguished rational point. This fact is emphasized in [4]. For Weierstraß form curve this is easy to do using the chord-and-tangent rule for addition. In this case, P_3 is taken to be the negative of the sum of P_1 and P_2 and one such step is called a Miller iteration.

The first contribution of this work is to work out a solution to the above problem for twisted Edwards form curve. Using the birational equivalence between twisted Edwards and Weierstraß form curves, we obtain the form of the rational function h over twisted Edwards form when P_3 is the sum of P_1 and P_2. In other words, we show how to perform Miller iteration directly on twisted Edwards form curve. Since the Miller iteration forms the basis of all pairing algorithms, including the Weil, Tate, Eta and Ate pairings, our work shows how to compute such pairings directly over twisted Edwards form curves.

In its general form, the expression for h looks a bit complicated. We show that for special curves, it is possible to simplify the computation. As examples, we consider supersingular curves over finite fields of characteristic greater than 3 (and hence having embedding degree 2). An important aspect in pairing computation over supersingular curves is the utilization of the so-called distortion map. For Weierstraß form, such a map was obtained in [6,7]. We obtain a similar distortion map for a class of Edwards form supersingular curves. Using this map and some further simplifications, we work out explicit formulae for combined doubling and Miller iteration and combined addition and Miller iteration using both inverted Edwards and projective Edwards coordinates.

The cost for doubling and Miller value computation is 9[M]+6[S] and for mixed addition and Miller value computation is 17[M]+1[S] using inverted Edwards coordinates. The corresponding values using projective Edwards coordinates are 9[M]+6[S] and 18[M]+1[S]. This is slower than the best known pairing algorithm for Weierstraß form supersingular curve $s^2 = r^3 + ar$ using Jacobian curves obtained in [11]. The corresponding values for general a, small a and $a = -3$ are (8[M]+6[S], 11[M]+3[S]), (7[M]+6[S], 11[M]+3[S]) and (8[M]+4[S], 11[M]+3[S]) respectively. (The Edwards form does not distinguish between different values of a.)

Comparison to Pairing on Weierstrass. In general, it is expected that pairing over Edwards form will be slower than pairing over Weierstraß form. To see this, consider the two ways of performing pairing over Edwards.

1. Convert the points to Weierstraß form and then perform the pairing on Weierstraß form. In this method, the total cost of pairing will also include the cost of converting points from Edwards form to Weierstraß form.
2. Perform pairing directly on twisted Edwards form using the required Miller function (obtained here). The form for this function is obtained by mapping Edwards points to Weierstraß points, obtaining the expression for Miller function on Weierstraß and then mapping back to obtain the Miller function on Edwards. So, the form for the Miller function on Edwards implicitly includes both the maps to and from Weierstraß. Consequently, it is unlikely that a Miller iteration on Edwards will be faster than a Miller iteration on Weierstraß.

The above seems to suggest that Edwards form should not be used for implementing pairing based protocols. The answer, however, is not that straightforward. Each algorithm in a protocol involves some scalar multiplications and some pairings. For the scalar multiplications, Edwards form is faster, especially if the implementation has to guard against side channel attacks. The pairing will be slower but, this may be compensated by the faster scalar multiplications. We believe that there is no general answer and a designer would have to look at the very specific details before making a proper selection of elliptic curve form.

Pairing on Edwards: Compute Pairing Directly or Via Weierstrass Form? Suppose a designer chooses to implement a protocol using the Edwards form. From Point 2 mentioned above, it seems that each Miller iteration on Edwards will be slower than that on Weierstraß. The direct method is faster if the cost of conversion to Weierstraß amortized over all the Miller iterations is more than the difference between the Miller iteration on Edwards and that of Weierstraß.

Inversion Free Pairing on Edwards Form. On the other hand, there is one advantange of the direct method. This arises in specific reference to the class of supersingular curves considered here. Suppose, a designer wants an inversion-free pairing algorithm, i.e., a pairing algorithm, which does not make any inversion. Then the implementation will not require an inversion module. For resource constrained devices this may be an important issue.

For the specific class of supersingular curves considered here, the pairing algorithm that we obtain is free from inversion. Hence, the inversion module is not required to implement this algorithm. In contrast, we show that if the pairing is computed by converting to Weierstraß, then the conversion itself will require an inversion (as otherwise the resulting algorithm will be inefficient).

2 Preliminaries and Notations

Throughout this paper p denotes a prime greater than 3 and q an odd prime power. The finite field of cardinality q will be denoted by $\mathbb{F}_q$.

An elliptic curve (over $\mathbb{F}_q$) in Weierstraß form is given by an equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$, where a_2, a_4 and a_6 are from $\mathbb{F}_q$. The addition rule and other properties on this form of the curve are quite well known and hence we do not repeat these here.

An elliptic curve (over $\mathbb{F}_q$) in Edwards form is given by an equation $x^2 + y^2 = c^2(1 + dx^2y^2)$, $c, d \neq 0$. Edwards introduced this form for elliptic curves over number fields and with $d = 1$. The curve parameter d was introduced by Bernstein and Lange who also studied this equation over finite fields. The additive identity is $(0, c)$; $(0, -c)$ has order 2; $(\pm c, 0)$ have order 4. The addition rule is given by the following formula.

$$(x_1, y_1) + (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{c(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - dx_1x_2y_1y_2)} \right).$$

If E is an elliptic curve defined by a bi-variate polynomial $C(x, y)$, then the set of $\mathbb{F}_q$-rational points of E is denoted by $E(\mathbb{F}_q)$ and is defined to be the set of pairs $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q$ such that $C(\alpha, \beta) = 0$. The set $E(\mathbb{F}_q)$ forms a group under a suitably defined addition law and an additive identity. For an $\mathbb{F}_q$-rational point P, the i fold sum of P is denoted by $[i]P$.

2.1 Birational Equivalence

Rational functions on a curve are important in studying the behavior of the curve. These rational functions form a field and two (forms of) elliptic curve are said to be *birationally equivalent* if their fields of rational functions are isomorphic.

Another form of elliptic curves which is also quite well known is the Montgomery form and is given by an equation of the form $Bv^2 = u^3 + Au^2 + u$, with $B \neq 0$. Birational equivalences between Weierstraß and Edwards form use the Montgomery form as an intermediate stepping stone.

It has been observed in [9] that the form $x^2 + y^2 = 1 + dx^2y^2$ is as general as the form $X^2 + Y^2 = C^2(1 + DX^2Y^2)$ in the sense that there is an isomorphism between them. The change of variables $X = Cx$ and $Y = Cy$ transforms $x^2+y^2 = 1 + dx^2y^2$ into $X^2 + Y^2 = C^2(1 + DX^2Y^2)$ with the condition that $C^4D = d$.

An extension, called the *twisted* Edwards form has been studied in [12]. The curve equation in this case has the form $ax^2 + y^2 = 1 + dx^2y^2$ for distinct non-zero elements a and d in a finite field $\mathbb{F}$ (of characteristic not equal to 2). It has been proved in [12] that the set of twisted Edwards form curves over the field $\mathbb{F}$ is birationally equivalent to the set of Montgomery form curves over $\mathbb{F}$. Then

$$(x, y) \mapsto (u, v) = ((1 + y)/(1 - y), (1 + y)(x(1 - y))) \tag{1}$$

transforms $ax^2+y^2 = 1+dx^2y^2$ to $Bv^2 = u^3+Au^2+u$, where $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$. Since a and d are distinct and non-zero, A is not 2 or -2 and B is non-zero. The inverse map is given by $(u, v) \mapsto (x, y) = (u/v, (u-1)/(u+1))$.

The case $a = 1$ in twisted Edwards curve is the Edwards curve as considered in [9]. Theorem 3.5 of [12] shows that an elliptic curve is birationally equivalent to an Edwards form curve if and only if it has a point of order 4. Assuming the curve to be in Weierstraß form $s^2 = r^3 + a_2r^2 + a_4r$ and using a point (r_1, s_1) of order 4 on this curve, it is possible to exhibit a birational equivalence between the Weierstraß and Edwards forms. The map

$$(x, y) \mapsto (r, s) = ((r_1(1 + y))/(1 - y), (s_1(1 + y))/(x(1 - y))) \tag{2}$$

transforms $x^2 + y^2 = 1 + dx^2y^2$ to $s^2 = r^3 + a_2r^2 + a_4r$, where $a_2 = s_1^2/r_1^2 - 2r_1$; $a_4 = r_1^2$ and $d = 1 - 4r_1^3/s_1^2$. This result was essentially contained in the proof of Theorem 2.1 of [9]. The actual statement and the result were more complicated because the proof missed the fact that $r_1/(1 - d)$ equals $(s_1/(2r_1))^2$ and hence, is always a square. Instead, it was required that d is a non-square (equivalently, there is a unique point of order 2), which caused some complications.

The following observation from [9] shows how to convert from $S^2 = R^3 + A_4R + A_6$ to $s^2 = r^3 + a_2r^2 + a_4r$.

Observation 1. Let E be an elliptic curve over $\mathbb{F}$ given in the Weierstraß form $S^2 = R^3 + A_4R + A_6$ such that the group $E(\mathbb{F})$ has an element $Q = (R_1, S_1)$ of order 4. Then E can be transformed into the curve E': $s^2 = r^3+a_2r^2+a_4r$ by the change of variables $r = R-R_2$, and $s = S$. Then $a_2 = 3R_2$, $a_4 = 3R_2^2+A_4$ and R_2 is the x-coordinate of $2Q$. The point Q is transformed into a point $P = (r_1, s_1)$, where $r_1 = R_1 - R_2$ and $s_1 = S_1$ leading to $2P = (0, 0)$.

2.2 Background on Pairing

In this section, we discuss basics of Tate pairing. We first recall some fundamentals on divisors on elliptic curves. Let E be an elliptic curve over $\mathbb{F}_q$, with identity $\mathcal{O}$. Points are denoted by P, Q, etcetera, while the corresponding places are denoted by (P), (Q), etcetera. The function field of E is the quotient field of the coordinate ring of E. Elements of this field are called functions over E. Places correspond to valuation rings of the function field.

Divisors of E are formal $\mathbb{Z}$-linear combinations of places. Any non-constant function has finitely many zeros and poles at places, of some finite positive order. The collection of zeros and poles of a function, expressed as a divisor is called its *principal divisor*. For a function z, its principal divisor is denoted by $\mathrm{div}(z) = (z)_0 - (z)_\infty$. The divisor $(z)_0$ is called the *zero divisor* of z and $(z)_\infty$ its pole divisor.

The computation of Tate pairing depends on the addition rule on the elliptic curve group. Following [4], the following task forms the backbone for pairing computation:

Task 1. *Given $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, points on an elliptic curve X, find a point P_3 and a function h such that* $\mathrm{div}(h) = (P_1) + (P_2) - (P_3) - (\mathcal{O})$.

Weierstraß form is the most well-studied form of elliptic curve. The task above can be easily performed using the chord-tangent rule.

Tate pairing was first introduced in cryptography in [4]. We recall the definition of Tate pairing from [7]. Let E be an elliptic curve defined over $\mathbb{F}_q$ and r be coprime to q and $r \mid \#E(\mathbb{F}_q)$. Let k be a positive integer such that the field $\mathbb{F}_{q^k}$ contains all the rth roots of unity (that is, $r \mid (q^k - 1)$).

Definition 1. *With r as above, the smallest extension field of $\mathbb{F}_q$ which contains all the rth roots of unity is denoted by L. The extension degree $[L : \mathbb{F}_q]$ is known as embedding degree.*

Following [7], the Tate pairing is defined as follows.

Definition 2. *The choices for parameters are made as discussed above. Let $G := E(\mathbb{F}_{q^k})$. The Tate pairing is defined as*

$$e_r(\cdot,\cdot) : G[r] \times G/rG \longrightarrow \mathbb{F}_{q^k}^* / \mathbb{F}_{q^k}^{*r}$$

with $e_r(P, Q) := f_P(Q)^{\frac{q^k-1}{r}}$. The function f_P is such that $\mathrm{div}(f_P) = r(P) - r(\mathcal{O})$.

The quotient group on the right hand side is the set of equivalence classes modulo the relation "$a \equiv b$ if and only if there exists $c \in \mathbb{F}_{q^k}^*$ such that $a = bc^r$". For more properties of Tate pairing refer [4]. The pairing thus defined is well-defined, non-degenerate and bilinear.

Let $h_{P,Q}$ denote the rational function corresponding to the addition of P and Q. Let $r = (r_{l-1} \cdots r_0)$ the binary representation of r. With this setup, an algorithm for computing the Tate pairing $e_r(P, Q)$ on an elliptic curve may be given. The rational function appearing in the algorithm depends on the form of the elliptic curve. See Table 1.

The algorithm in Table 1 computes in the ith iteration a function $f_{i,P}$ having divisor $\mathrm{div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O})$, called Miller's functions. At each

Table 1. Miller's algorithm for computing Tate pairing

```
Input : Points $P$ and $Q$
Output : Tate pairing of $P$ and $Q$
1. Set $f = 1$ and $P_1 = P$.
2. For $i = l - 2$ downto 0
       Set $f = f^2 \cdot h_{P,P}$ and $P_1 = 2P$.
       If $r_i = 1$ then set $f = f \cdot h_{P_1,P}$ and $P_1 = P_1 + P$.
3. Set $f = f^{\frac{q^k-1}{r}}$.
4. Return f.
```

step, the Miller's functions are evaluated at the second argument. After $l - 1$ iterations, the evaluation at Q of the function f having divisor $r(P) - r(\mathcal{O})$ is obtained.

3 Pairing over Twisted Edwards Form Curve

Pairing algorithms have been extensively studied. All such studies have used the Weierstraß form. Let us first consider how to implement pairings on Edwards form using pairings on Weierstraß form.

3.1 Pairing Via Weierstraß Form

Suppose we have a pairing friendly curve C in Weierstraß form having a point of order 4 and let E be the corresponding Edwards form. The birational equivalence between E and C is a group isomorphism between the corresponding group of points. Using this isomorphism, we can map points on Edwards form into Weierstraß form and compute the pairing on Weierstraß form. (Note that the output of the pairing is an element of an extension field and there is no issue of "going back" to Edwards form.) The cost of this procedure is the cost of applying the isomorphism from Edwards to Weierstraß form plus the cost of computing the pairing on Weierstraß form.

Suppose the input to the pairing are the points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in Edwards form. Using (2), and recalling that (r_1, s_1) is a point of order four on Weierstraß form, we have

$$\begin{aligned} (x_P, y_P) &\mapsto \left(r_1 \times \frac{1+y_P}{1-y_P}, s_1 \times \frac{1+y_P}{x_P(1-y_P)} \right), \\ (x_Q, y_Q) &\mapsto \left(r_1 \times \frac{1+y_Q}{1-y_Q}, s_1 \times \frac{1+y_Q}{x_Q(1-y_Q)} \right). \end{aligned} \tag{3}$$

The coordinates x_P, y_P of the point P are from $\mathbb{F}_q$. However, the coordinates x_Q, y_Q of the point Q are from $\mathbb{F}_{q^k}$, where k is the embedding degree. The inverses of $(1 - y_Q)$ and x_Q are required as also the inverses of $(1 - y_P)$ and x_P. While the later is easier to obtain, depending on the embedding degree, obtaining the former inverses may be rather expensive. As example, consider the value $k = 10$ which is the focus of current research on obtaining pairing friendly curves [3]. In this case, the two inversions on $\mathbb{F}_{q^{10}}$ can be computed using one $\mathbb{F}_{q^{10}}$-inversion and three $\mathbb{F}_{q^{10}}$-multiplications. The total cost will be equivalent to a few hundred multiplications over $\mathbb{F}_q$.

The above transforms an affine representation of a Edwards point into an affine representation of a Weierstraß point. In many situations, one works with other representations such as projective or Jacobian coordinates. It is possible to convert to the desired coordinate system using a few multiplications. Suppose that the Edwards form point is given in affine coordinates as (x, y) and we want the Weistraß form point in projective coordinates. The output of (3) is equal to (r, s), where $r = a/b$ and $s = c/d$ with $a = r_1(1 + y)$, $b = (1 - y)$, $c = s_1(1 + y)$ and $d = x(1 - y)$. Then, the projective representation (R, S, T) with $r = R/T$ and $s = S/T$ is obtained by setting $R = ad$, $S = cb$ and $T = bd$. After obtaining a, b, c and d, three extra multiplications convert the point to projective coordinates. Further, the representation (RT, ST^2, T) is in Jacobian coordinates and two extra multiplications and one squaring are required for this.

The point in Edwards may not be given in affine. Projective and inverted Edwards representations have been suggested in [9,10]. The representation is (X, Y, Z), where in the former case, $x = X/Z$ and $y = Y/Z$ and in the latter case, $x = Z/X$ and $y = Z/Y$. With both coordinate systems it is possible to convert to projective (and Jacobian) Weierstraß forms. We show this for the inverted Edwards coordinates, the case for projective Edwards being similar. In this case, the affine Weierstraß form is $(r = a/b, s = c/d)$ where $a = r_1(Y + Z)$, $b = Y - Z$, $c = s_1X(Y + Z)$ and $d = Z(Y - Z)$. From this affine representation the conversion to projective or Jacobian Weierstraß is as described above.

If we use (3) to convert to affine Weierstraß then an inversion is required. Converting to projective or Jacobian can avoid inversion at the cost of several extra multiplications. There are two additional issues to consider for inversion free conversion.

1. Obtaining the point P in affine Weierstraß allows mixed addition formula to be used during Miller iteration. Obtaining P in projective and Jacobian will increase the cost of mixed addition.
2. The cost of converting the point Q will require extension field multiplications. Further, most pairing algorithms on Weierstraß form require Q in affine. If Q is given in projective, this will imply extra (extension field) multiplications when the Miller function is evaluated at Q. The last point is significant, since, even one extra extension field multiplication per Miller iteration can prove to be costly.

Thus, avoiding inversions in the conversion from Edwards to Weierstraß in general pushes up the cost for pairing computation on Weierstraß form itself. On the other hand, avoiding inversions may be required for other reasons in addition to that of computational efficiency. In resource constrained devices, it is desirable to implement the algorithm in as small hardware area or software code as possible. The ability to avoid implementing the inversion routine will be useful for such scenarios.

Based on the above discussion, we consider the problem of developing a pairing algorithm which works directly over the twisted Edwards form. The main task is to compute the Miller function at each iteration.

3.2 Miller Function for Twisted Edwards Form Curve

This section deals with efficiently performing Task 1 (of Section 2.2) on twisted Edwards form elliptic curve. As already seen, the Miller function computation forms the backbone for computing Tate pairing. The result of this section gives the Miller function corresponding to addition of P_1 and P_2.

Theorem 1. *Let $\mathbb{F}_q$ be a field of characteristic not equal to 2 and $ax^2 + y^2 = 1 + dx^2y^2$ be a twisted Edwards form curve where a and d are distinct non-zero elements of $\mathbb{F}_q$. Let $P_0 = (0, 1)$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on it. Let $P_3 = (x_3, y_3)$ be the sum of P_1 and P_2. Then the Miller function $h(x, y)$ such that*

$$\mathrm{div}(h) = (P_1) + (P_2) - (P_3) - (P_0) \tag{4}$$

is given by

$$h(x, y) = \frac{(1 - y_3)}{x(y - y_3)}((1 + y) - x(\lambda(1 + y) + \theta(1 - y))). \tag{5}$$

where $A = (2(a + d))/(a - d)$, $B = 4/(a - d)$ and

$$\lambda = \begin{cases} \frac{x_1(A(y_1^2-1)-2(1+y_1+y_1^2))}{B(y_1^2-1)} & \text{if } P_1 = P_2; \\ \frac{x_1(y_1-1)(y_2+1)-x_2(y_1+1)(y_2-1)}{2x_1x_2(y_1-y_2)} & \text{if } P_1 \neq P_2. \end{cases} \tag{6}$$

and $\theta = 2(1 + y_1)/(x(1 - y_1)) - \lambda(1 + y_1)/(1 - y_1)$ is given by

$$\theta = \begin{cases} \frac{(y_1^2-1)(Ax_1^2-B)-2x_1^2(1+y_1+y_1^2)}{Bx_1(y_1^2-1)} & \text{if } P_1 = P_2; \\ \frac{(x_1-x_2)(1+y_1)(1+y_2)}{2x_1x_2(y_1-y_2)} & \text{if } P_1 \neq P_2. \end{cases} \tag{7}$$

[**Note.** There is no assumption on the embedding degree.]

Proof. The idea of the proof is simple. In the Weierstraß form it is easy to obtain a rational function $g(x, y)$ such that a relation similar to that of Equation 4 holds. Basically $g(x, y)$ is the ratio of two lines – the line passing through P_1 and P_2 and the line passing through P_3 and $-P_3$.

Let Φ be the transformation given in (1).

$$\Phi(x, y) = (u, v) \triangleq \left(\frac{1 + y}{1 - y}, \frac{(1 + y)}{x(1 - y)}\right). \tag{8}$$

Then $x = u/v$ and $y = (u-1)/(u+1)$. This transforms the curve $ax^2 + y^2 = 1 + dx^2y^2$ into the curve $Av^2 = u^3 + Bu^2 + u$, where $A = 2(a+d)/(a-d)$ and $B = 4/(a-d)$. The later curve is in Montgomery form. But, the Miller function $g(x,y)$ for Montgomery form is still the ratio of two lines as in the case of the Weierstraß form.

The idea is to first transform points P_i on Edwards form into corresponding points Q_i on Montgomery form using Φ; compute $g(x,y)$ on Montgomery form and then use the inverse of Φ to transform $g(x,y)$ into the desired rational function $h(x,y)$. For this to work we need to note that the transformation Φ extends to several isomorphisms.

1. The map $\sum n_i(P_i) \mapsto \sum n_i(\Phi(P_i))$ is an isomorphism of the set of divisors on Edwards and Montgomery form curves.
2. The map $h(x,y) \mapsto h(\Phi(x,y))$ is an isomorphism of the function fields of the Edwards and Montgomery form curves.

Let $\mathcal{O}$ be the identity on Montgomery form curve. Then $\Phi((P_1)+(P_2)-(P_3)-(P_0)) = (Q_1)+(Q_2)-(Q_3)-(\mathcal{O})$. We use (x,y) to denote Edwards coordinates and (u,v) to denote Montgomery coordinates. Let $l_1(u,v)$ be the line through Q_1 and Q_2 and $l_2(u,v)$ be the line through Q_3 and $-Q_3$. Then $l_1(u,v) = v - \lambda u - \theta$ and $l_2(u,v) = u - u_3$ where the slope λ and the constant θ are obtained later.

Define $g(u,v) = l_1(u,v)/l_2(u,v)$ and so $g(u,v) = (v - \lambda u - \theta)/(u - u_3)$. The desired function $h(x,y)$ is $g(\Phi^{-1}(u,v)) = g((1+y)/(1-y), 2(1+y)/(x(1-y)))$. We have

$$\begin{aligned} h(x,y) &= \frac{\frac{1+y}{x(1-y)} - \lambda\frac{1+y}{1-y} - \theta}{\frac{1+y}{1-y} - \frac{1+y_3}{1-y_3}} \\ &= \frac{(1-y_3)((1+y) - \lambda x(1+y) - \theta x(1-y))}{x((1+y)(1-y_3) - (1+y_3)(1-y))} \\ &= \frac{(1-y_3)}{2x(y-y_3)}((1+y) - x(\lambda(1+y) + \theta(1-y))). \end{aligned}$$

It remains to obtain the expressions for λ and θ in terms of x_1, y_1, x_2 and y_2. Recall that $u_i = \frac{1+y_i}{1-y_i}$ and $v_i = \frac{(1+y_i)}{x_i(1-y_i)}$. Also, $\theta = v_1 - \lambda u_1$. The value of λ is obtained as the slope of the line through P_1 and P_2, if they are distinct; or as the slope of the tangent through P_1, if the points are equal. In the former case, $\lambda = (v_2 - v_1)/(u_2 - u_1)$. In the later case, we have to refer to the equation of the curve. The curve in question is the Montgomery form curve $Bv^2 = u^3 + Au^2 + u$. Differentiating with respect to u we have $\lambda = (3u_1^2 + 2Au_1 + 1)/(2Bv_1)$. The expressions for λ and θ in the two cases can now be obtained by substituting the values of u_i, v_i and simplifying the resulting expressions. □

4 Supersingular Curves in Edwards Form

For $p > 3$, two supersingular curves in Weierstraß form are quite well known. We provide the corresponding Edwards form. For the map given by (2) to exist, the curve must have a point of order 4. The number of $\mathbb{F}_p$-rational points on supersingular curves of characteristics greater than 3 is known to be $p+1$. So, we require $p \equiv 3 \bmod 4$ as a necessary condition for a point of order 4 to exist.

$\boldsymbol{s^2 = r^3 + a_4 r}$**.** The condition $p \equiv 3 \bmod 4$ ensures that this curve is supersingular which is compatible with the condition for a point of order 4 to exist. Let $P = (r_1, s_1)$ be a hypothesized point of order 4 on this curve. Then $a_4 = r_1^2$ and $s_1^2 = r_1(r_1^2 + a_4) = 2a_4 r_1$. The possible values of (r_1, s_1) are $\left(\sqrt{a_4}, \pm\sqrt{2a_4^{3/2}}\right)$ and $\left(-\sqrt{a_4}, \pm\sqrt{-2a_4^{3/2}}\right)$. Since $p \equiv 3 \bmod 4$, a_4 must be a square modulo p which is a necessary and sufficient condition for transforming to Edwards form.

Since $p \equiv 3 \bmod 4$, -1 is a non-square modulo p and hence exactly one of $2a_4^{3/2}$ and $-2a_4^{3/2}$ is a square modulo p. This shows that there are exactly two points of order 4.

1. If $a_4 = 1$, then $(1, \pm\sqrt{2})$ are the points of order 4 if $(p^2-1)/8$ is even; and $(-1, \pm\sqrt{-2})$ are the points of order 4 if $(p^2-1)/8$ is odd. Later we will consider pairing over this curve.
2. If $a_4 = -3$, then the curve has a point of order 4 only if 3 is a non-square modulo p, i.e., if $p \equiv \pm 5 \bmod 12$. Determining the two actual points of order 4 requires obtaining the square root of either $\sqrt{2 \times 3^{3/2}}$ or $\sqrt{-2 \times 3^{3/2}}$. We know that one of them is a square, but the exact value of the square root depends on p.

The value of d in the Edwards form curve is determined from the relation $a_2 = 0 = s_1^2/r_1^2 - 2r_1$. Then $2r_1^3 = s_1^2$ and so, $d = 1 - (4r_1^3/s_1^2) = -1$. Thus, if a_4 is a square modulo p, then the corresponding Edwards form is

$$x^2 + y^2 = 1 - x^2y^2. \tag{9}$$

Note that d is equal to -1 irrespective of the value of a_4. Also, in (9) $a_4 = 1$ so that $A = 0$ and $B = 2$ in the Montgomery form obtained by applying (1).

Interestingly, the curve $x^2 + y^2 = 1 - x^2y^2$ was studied by Euler [13] and Edwards [8] reports that the curve was also of "great interest" to Gauss [14].

$\boldsymbol{S^2 = R^3 + \alpha}$**.** The condition $p \equiv 2 \bmod 3$ ensures that this curve is supersingular. This, along with the condition $p \equiv 3 \bmod 4$ for the point of order 4 to exist, implies that $p \equiv -1 \bmod 12$.

Here $A_4 = 0$ and $A_6 = \alpha$. Let $P = (R_1, S_1)$ be a point of order 4 on this curve and R_2 is the x-coordinate of $2P$. Since $2P$ has order 2, the y-coordinate of $2P$ must be zero and so $R_2^3 = -\alpha$. Using $2P = (R_2, 0)$, it can be shown that R_1 and S_1 are obtained by first solving $R_1^3 - 3R_2R_1 - 2\alpha = 0$ for R_1 and then solving $S_1^2 = R_1^3 + \alpha$ for S_1. So, for P to exist, first $-\alpha$ must be a cube modulo p and then these two equations should be solvable modulo p.

Once R_2 and (R_1, S_1) have been obtained, we can first apply Observation 1 followed by (2) to obtain the corresponding Edwards form.

Concrete Examples. Consider $E : y^2 = x^3 + x$ over $\mathbb{F}_p,\ p \geq 5$. In [15, Table 1], suitable values of p and r for various levels of security are given. We consider some particular values given in [15, Section 7.2]. In both cases below $p \equiv 3 \bmod 4$ and hence the curve $x^2+y^2 = 1-x^2y^2$ is supersingular over $\mathbb{F}_p$. The group $E(\mathbb{F}_p)$ has a unique element of order 2 and the points $(1, \pm\sqrt{2})$ are of order 4.

For 80-bit security level, with $k = 2$, recommended sizes of p and r are 512 and 160, respectively. A suitable set of parameters is given there as $p = 2^{520} + 2^{363} - 2^{360} - 1$, $r = 2^{160} + 2^3 - 1$.

For 128-bit security level, with $k = 2$, recommended sizes of p and r are 1536 and 256 bits respectively. A suitable set of parameters is given there as $p = 2^{1582} + 2^{1551} - 2^{1326} - 1$, $r = 2^{256} + 2^{225} - 1$.

5 Pairing Computation on $x^2 + y^2 = 1 - x^2y^2$ over $\mathbb{F}_p$, $p > 3$ and $p \equiv 3 \bmod 4$

In Section 4, we have seen that the supersingular curve $\mathcal{E} : s^2 = r^3 + ar$ over $\mathbb{F}_p$, with $p \equiv 3 \bmod 4$ transforms to $x^2 + y^2 = 1 - x^2y^2$ over $\mathbb{F}_p$, provided a is a square modulo p. Let $\mathcal{E}(\mathbb{F}_p)[r]$ be the set of all $\mathbb{F}_p$-rational r-torsion points of this curve. Let r be a prime greater than 3 and then $\langle R\rangle = \mathcal{E}(\mathbb{F}_p)[r]$. Then for any $(\alpha, \beta) \in \langle R\rangle$, $\beta \neq 0$. (If $\beta = 0$, then $\alpha = \pm 1$ and the points $(\pm 1, 0)$ are of order 4 and hence cannot be in $\langle R\rangle$; if they are, then $4|r$ which contradicts r is a prime greater than 3.)

The domain of pairing is $\mathcal{E}(\mathbb{F}_p)[r] \times \mathcal{E}(\mathbb{F}_{p^2})/r\mathcal{E}(\mathbb{F}_{p^2})$. By using a so-called "distortion map", the domain can be changed to $\mathcal{E}(\mathbb{F}_p)[r] \times \mathcal{E}(\mathbb{F}_p)[r]$. For the corresponding Weierstraß form this has been done in [6,7].

Definition 1. *[16, Section 4.2] A distortion map ϕ with respect to a cyclic group $\langle P\rangle$ of order r is an endomorphism of the curve that maps any non-zero point Q in $\langle P\rangle$ to a point $\phi(Q)$ which is independent of Q.*

The curve $s^2 = r^3 + r$ over $\mathbb{F}_p$ with $p > 3$ is supersingular for $p \equiv 3 \bmod 4$, with embedding degree $k = 2$. The map $\phi(r, s) = (-r, is)$ where $i^2 = -1$ is a distortion map for this curve. (For more details see [6].)

We obtain a distortion map for the Edwards form curve. The following result can be proved by mapping (x, y) on Edwards form curve to (r, s) on Weierstraß form; mapping (r, s) to $(-r, is)$ using the distortion map on Weierstraß form; and then mapping the resulting point back to Edwards form. The proof that we provide is more direct.

Theorem 2. *The function $\phi : \mathcal{E}(\mathbb{F}_p)[r] \rightarrow \mathcal{E}[\mathbb{F}_{p^2}]$ given by*

$$\phi(x, y) = \left(ix, \frac{1}{y}\right), \tag{10}$$

is a distortion map on the Edwards form curve $x^2 + y^2 = 1 - x^2y^2$.

Proof. First we notice that the image of ϕ is not contained in $\mathcal{E}(\mathbb{F}_p)[r]$. Next, we verify that ϕ is an endomorphism. Let $P_i = (x_i, y_i)$, for $i = 1, 2$. Let (x_3, y_3) be the sum $P_1 + P_2$. Thus, we have

$$\phi(P_1 + P_2) = \left(i\frac{x_1y_2 + x_2y_1}{1 - x_1x_2y_1y_2}, \frac{1 + x_1x_2y_1y_2}{y_1y_2 - x_1x_2} \right).$$

On the other hand,

$$\phi(P_1) + \phi(P_2) = \left(ix_1, \frac{1}{y_1} \right) + \left(ix_2, \frac{1}{y_2} \right) = \left(i\frac{x_1y_1 + x_2y_2}{x_1x_2 + y_1y_2}, \frac{1 + x_1y_1x_2y_2}{y_1y_2 - x_1x_2} \right).$$

We now verify that $(x_1y_2 + x_2y_1)(x_1x_2 + y_1y_2) = (x_1y_1 + x_2y_2)(1 - x_1x_2y_1y_2)$. Indeed, expanding the left hand side, we obtain,

$$\begin{aligned}(x_1y_2 + x_2y_1)(x_1x_2 + y_1y_2) &= x_1^2x_2y_2 + x_1x_2^2y_1 + x_1y_1y_2^2 + x_2y_1^2y_2 \\ &= x_1y_1(x_2^2 + y_2^2) + x_2y_2(x_1^2 + y_1^2) \\ &= x_1y_1(1 - x_2^2y_2^2) + x_2y_2(1 - x_1^2y_1^2) \\ &= (x_1y_1 + x_2y_2)(1 - x_1x_2y_1y_2)\end{aligned}$$

which proves the theorem. □

Under this distortion map, the output of $e(P, Q)$ is defined to be $e(P, \phi(Q))$. Each Miller iteration takes two points P_1 and P_2 and obtains P_3 to be the sum of P_1 and P_2 and evaluates $h(\phi(Q))$, where h is the rational function h given in Theorem 1. In other words, we have to evaluate

$$\begin{aligned}h\left(ix_Q, \frac{1}{y_Q}\right) &= \frac{(1 - y_3)\left(\left(1 + \frac{1}{y_Q}\right) - ix_Q\left(\lambda\left(1 + \frac{1}{y_Q}\right) + \theta\left(1 - \frac{1}{y_Q}\right)\right)\right)}{ix_Q(\frac{1}{y_Q} - y_3)} \\ &= \frac{i(y_3 - 1)}{x_Q(1 - y_Qy_3)}((y_Q + 1) - ix_Q(\lambda(y_Q + 1) + \theta(y_Q - 1))) \qquad (11) \\ &= \frac{(y_Q + 1)(y_3 - 1)}{x_Q(1 - y_Qy_3)}(x_Q\lambda + \alpha_Q\theta + i)\end{aligned}$$

where $\alpha_Q = x_Q(y_Q - 1)/(y_Q + 1)$ and λ and θ are given by Equation 6 and Equation 7 respectively. Note that the expression for α_Q is the same as that of $1/v$ obtained in transforming from Edwards to Montgomery (see (1)). The value of α_Q depends only on Q and can be computed before starting the actual pairing computation.

Inversion Free Pairing. Computing α_Q, however, requires an inversion over $\mathbb{F}_p$ per pairing computation. While this cost is not severe, as discussed earlier, in resource constrained situations, it might be desirable to altogether avoid implementing the inversion module. For this, we express $h(ix_Q, 1/y_Q)$ as

$$h\left(ix_Q, \frac{1}{y_Q}\right) = \frac{(y_3 - 1)}{x_Q(1 - y_Qy_3)}(\beta_Q\lambda + \gamma_Q\theta + i\delta_Q) \qquad (12)$$

where $\beta_Q = x_Q(y_Q + 1)$, $\gamma_Q = x_Q(y_Q - 1)$ and $\delta_Q = y_Q + 1$. The quantities β_Q, γ_Q and δ_Q do not vary with Miller iteration and can be computed using two multiplications at the beginning of the pairing computation.

Observation 2. An important observation is that in Tate pairing computation, the final output of Miller loop is raised to the power $(p^2 - 1)/r$, where r does not divide $(p - 1)$. So, $(p - 1)$ divides $(p^2 - 1)/r$ and hence, in the computation of $h(Q)$ we can freely divide or multiply by a non-zero element of $\mathbb{F}_p$. This is because for any non-zero $\alpha \in \mathbb{F}_p$, $\alpha^{p-1} = 1$. This technique has been used in [6] to speed up computation on Weierstraß form curve.

Since we can multiply and divide by non-zero elements of $\mathbb{F}_p$, we see that it is sufficient to evaluate

$$g(x_Q, \alpha_Q) = \beta_Q\lambda + \gamma_Q\theta + i\delta_Q. \tag{13}$$

In the following, we simplify this expression after substituting the values of λ and θ and using appropriate coordinates and then obtain explicit formulae for jointly computing P_3 and g.

Converting to Weierstraß and Computing the Pairing. The Weierstraß form of the supersingular curve that we are considering is $s^2 = r^3 + ar$. Explicit formulae for doubling-and-Miller and addition-and-Miller for this curve have been given in [11]. The coordinate system used was Jacobian and the pairing did not require any $\mathbb{F}_p$-inversion and still used mixed addition.

In contrast, if we use (3) to convert from Edwards to Weierstraß then an inversion is required. Due to the availability of the distortion map (for the Weierstraß form), we may assume that the coordinates of both P and Q in (3) are from $\mathbb{F}_p$. Then the four inversions can be done using 9[M] and 1[I] using Montgomery's trick ($s_1 = x_1$; $s_i = s_{i-1}x_{i-1}$, $1 \leq i \leq 4$; $y_4 = s_4^{-1}$; $x_{i+1}^{-1} = y_{i+1}s_i$, $y_i = x_{i+1}y_{i+1}$, $3 \geq i \geq 1$; this procedure generalizes to arbitrary number of x_is). The total operation (including multiplications by r_1 and s_1) count is 19[M]+1[I] for the conversion.

If we choose not to perform any inversion, then as discussed in Section 3, at the cost of some extra multiplications, we can put P in Jacobian and Q in either Jacobian or projective. As a result, the mixed addition on Weierstraß will be slower and the evaluation of each Miller function at Q will also be slower. The exact amount of slowdown for the Weierstraß form pairing due to these two factors is not clear and the entire pairing formulae for Weierstraß needs to be worked out to determine this. We do not do this; instead we work out the explicit formulae for performing inversion-free pairing directly on Edwards form. It does not appear that performing inversion-free pairing after converting to Weierstraß is likely to be faster.

In the following, by [M] *we will denote one* $\mathbb{F}_p$ *multiplication and by* [S] *we will denote one* $\mathbb{F}_p$ *squaring.*

5.1 Pairing Using Inverted Edwards Coordinates

The point (x, y) is said to be in affine representation. There are several other coordinate systems for representing a point. In [10], the inverted Edwards representation is used to represent the point (x, y) by (X, Y, Z), where $x = Z/X$ and $y = Z/Y$. The curve then transforms into $Z^4 = X^2Y^2 - Z^2(X^2 + Y^2)$. The addition and doubling formulae for the inverted Edwards representation have been given in [10].

Let $P_1 = (X_1, Y_1, Z_1)$, $P_2(X_2, Y_2, Z_2)$ and $P_3 = (X_3, Y_3, Z_3)$ such that P_3 is the sum of P_1 and P_2. It is possible to obtain unified formulae for X_3, Y_3 and Z_3, i.e., one which does not distinguish between $P_1 = P_2$ and $P_1 \neq P_2$. While this is useful for side channel resistance, a dedicated doubling formula is faster. We use the dedicated doubling formula, since in the current context the value of r (the order of the subgroup of $\mathcal{E}(\mathbb{F}_p)[r]$) is not a secret and the pairing computation will be computing rP for some point P.

Suppose that we want to compute the pairing value for P and Q. We assume that P is given as (X_1, Y_1, Z_1) with $Z_1 = 1$ and Q is given in affine as (x_Q, y_Q) so that $\phi(Q) = (ix_Q, 1/y_Q)$. As discussed above, for computing h, it is sufficient to compute g given in (13) or a product of g and some element of $\mathbb{F}_p$.

Doubling and Miller Iteration. Doubling a point and computing the Miller value are done together so that some computations can be shared. In Theorem 1, substituting the value of d to be -1 and using inverted Edwards coordinates, we obtain

$$\lambda = \frac{Z_1(Y_1^2 + Y_1Z_1 + Z_1^2)}{X_1(Y_1 - Z_1)(Y_1 + Z_1)}; \qquad \theta = \frac{(X_1^2(Y_1^2 - Z_1^2) - Z_1^2(Y_1^2 + Y_1Z_1 + Z_1^2))}{X_1(Y_1 - Z_1)^2 Z_1}.$$

At this point we need to substitute these values of λ and θ into (13) and simplify the resulting expression. During the simplification, we are free to multiply and divide by non-zero elements of $\mathbb{F}_p$ as done earlier. We have performed this simplification with the help of Mathematica [17] and the final expression for the Miller value turns out to be $\Psi = \beta_Q F + \gamma_Q G + 2i\delta_Q H$, where

$$\begin{aligned} F &= 4Z_1(Y_1 - Z_1)(Y_1^2 + Y_1Z_1 + Z_1^2) \\ G &= -4Y_1Z_1^2(Y_1 + Z_1) \\ H &= 2X_1(Y_1 + Z_1)(Y_1 - Z_1)^2. \end{aligned} \tag{14}$$

Explicit formulae for doubling using inverted Edwards coordinates have been given in [10] and requires 3[M]+4[S] operations over $\mathbb{F}_p$. This is shown in the column "doubling" in Table 2. Some of the expressions obtained during doubling can be used in the computation of Ψ. With one squaring, the value of $J = 2Y_1Z_1 = (Y_1 + Z_1)^2 - Y_1^2 - Z_1^2$ can be found. We also require $I = 2X_1Z_1 = (X_1 + Z_1)^2 - X_1^2 - Z_1^2$, which can be computed with one squaring. It may be easily seen that

$$F = (2Y_1Z_1 - 2Z_1^2)(2Y_1^2 + 2Y_1Z_1 + 2Z_1^2) = (J - 2M)(2B + J + 2M),$$

can be computed with one multiplication. The computation of $G = -J(J+2M)$ and

$$H = (2X_1Y_1 + 2X_1Z_1)(Y_1^2 - 2Y_1Z_1 + Z_1^2) = (E + I)(B - J + M)$$

Table 2. Combined explicit formula for doubling and Miller value computation using inverted Edwards coordinates. An alternative form for Ψ is $x_QF + \alpha_QG + 2iH$. Here, $\alpha_Q = x_Q(y_Q - 1)/(y_Q + 1)$, $\beta_Q = x_Q(y_Q + 1)$, $\gamma_Q = x_Q(y_Q - 1)$ and $\delta_Q = y_Q + 1$.

Doubling	Miller value
	$J = (Y_1 + Z_1)^2 - B - M,$
$A = X_1^2,\ B = Y_1^2,\ C = A + B,$	$I = (X_1 + Z_1)^2 - A - M,$
$D = A - B,\ E = (X_1 + Y_1)^2 - C = 2X_1Y_1,$	$F = (J - 2M)(2B + J + 2M),$
$M = Z_1^2,\ Z_3 = D \cdot E,\ X_3 = C \cdot D,$	$G = -J(J + 2M),$
$Y_3 = (C + 2Z_1^2)$	$H = (E + I)(B - J + M),$
	$\Psi = \beta_QF + \gamma_QG + 2i\delta_QH.$

require two multiplications. Finally, the computation of $\Psi = \beta_QF + \gamma_QG + 2i\delta_QH$ requires three additional multiplications. Thus, computing the Miller value requires an additional $6[M] + 2[S]$ operations and the combined doubling and Miller value computation require a total of $9[M] + 6[S]$ operations. The complete description is given in Table 2.

Mixed Addition and Miller Iteration. Explicit formula for computing the mixed addition of a point P_1 and a point P_2 (whose Z coordinate is 1) has been given in [9]. In the present case, the point P is taken to be P_2. (Recall that we are computing the pairing value of P and Q.) This is shown in the column "Mixed Addition" of Table 3. Proceeding as in the case of doubling, we need to compute $\Psi = \beta_QF + \gamma_QG + 2i\delta_QH$, where in this case,

$$\begin{aligned} F &= -X_2(1 + Y_2)(Y_1 - Z_1)Z_1 + X_1(-1 + Y_2)(Y_1 + Z_1) \\ G &= (1 + Y_2)(Y_1 + Z_1)(-X_1 + X_2Z_1) \\ H &= Z_1(-Y_1 + Y_2Z_1) \end{aligned} \tag{15}$$

The sequence of operations is the following. First, $J = Y_2Z_1$ and $K = X_2Z_1$ need two multiplications. This gives $J_1 = Y_1 - Y_2Z_1$, $J_2 = (Y_2 + 1)(Y_1 + Z_1)$, $J_3 = (Y_2 - 1)(Y_1 + Z_1)$, $J_4 = (Y_2 + 1)(Y_1 - Z_1)$ and $K_1 = X_2Z_1 - X_1$ without any other multiplications. Computation of $F = -X_2 \cdot J_4 + X_1 \cdot J_3$ requires two multiplications. Computations of $G = J_2 \cdot K_1$ and $H = -Z_1 \cdot J_1$ require one

Table 3. Combined explicit formula for mixed addition and Miller value computation using inverted Edwards coordinates. An alternative form for Ψ is $x_QF + \alpha_QG + 2iH$. Here, $\alpha_Q = x_Q(y_Q - 1)/(y_Q + 1)$, $\beta_Q = x_Q(y_Q + 1)$, $\gamma_Q = x_Q(y_Q - 1)$ and $\delta_Q = y_Q + 1$.

Mixed Addition	Miller Value
$B = -Z_1^2, C = X_1X_2, D = Y_1Y_2,$	$D = Y_1Y_2,\ J = Y_2Z_1,\ K = X_2Z_1,\ J = Y_1 - J,$
$E = C \cdot D, H = C - D,$	$J_2 = Y_1 + Z_1 + D + J,\ J_3 = D + J - Y_1 - Z_1,$
$I = (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D,$	$J_4 = D - J + Y_1 - Z_1,\ K_1 = K - X_1,$
$X_3 = (E + B) \cdot H, Y_3 = (E - B) \cdot I,$	$F = -X_2J_4 + X_1J_3,\ G = J_2K_1,\ H = -Z_1J_1,$
$Z_3 = A \cdot H \cdot I$	$\Psi = \beta_QF + \gamma_QG + 2i\delta_QH.$

multiplication each. Thus, the value of Ψ can be computed with $9[M]$. Thus, mixed addition plus rational function computation requires $17[M] + 1[S]$ computations. The complete formula is given in Table 3.

5.2 Pairing Using Projective Edwards Coordinates

The affine point (x, y) on a Edwards form curve can be represented in projective coordinates as (X, Y, Z), where $x = X/Z$ and $y = Y/Z$. The curve equation then changes to $X^2 + Y^2 = Z^2 - X^2Y^2$. Explicit formulae for doubling and mixed addition using projective Edwards coordinates has been given in [9]. Equation 13 can be simplified using projective coordinates and formulae obtained for combined computation of double-and-Miller value and add-and-Miller value. The simplification process for doing this is similar to that done for inverted Edwards coordinates. Hence, we do not provide the details. Instead, we provide the final formulae in Tables 4 and 5. The total number of operations are 9[M]+6[S] and 18[M]+1[S] respectively.

Table 4. Doubling and computation of Miller value using projective Edwards coordinates. An alternative form for Ψ is $x_QF + \alpha_QG + 2iH$. Here, $\alpha_Q = x_Q(y_Q - 1)/(y_Q + 1)$, $\beta_Q = x_Q(y_Q + 1)$, $\gamma_Q = x_Q(y_Q - 1)$ and $\delta_Q = y_Q + 1$.

Doubling	Miller Value
$B = (X_1 + Y_1)^2, C = X_1^2, D = Y_1^2,$ $E = C + D, M = Z_1^2, J = E - 2M,$ $X_3 = (B - E)J,\ Y_3 = E(C - D),\ Z_3 = EJ$	$B = (X_1 + Y_1)^2,\ C = X_1^2,\ D = Y_1^2,$ $L = 2X_1Z_1,\ K = 2Y_1Z_1,\ Z_1^2,$ $F = (L - B + C + D)(2D + K + 2M),$ $G = -K \cdot (L + B - C - D),$ $H = (2M + K)(M + D - K),$ $\Psi = \beta_QF + \gamma_QG + 2i\delta_QH.$

Table 5. Mixed addition and computation of Miller value using projective Edwards coordinates. An alternative form for Ψ is $x_QF + \alpha_QG + 2iH$. Here, $\alpha_Q = x_Q(y_Q - 1)/(y_Q + 1)$, $\beta_Q = x_Q(y_Q + 1)$, $\gamma_Q = x_Q(y_Q - 1)$ and $\delta_Q = y_Q + 1$.

Mixed Addition	Miller Value
$B = Z_1^2, C = X_1X_2, D = Y_1Y_2, E = -CD,$ $I = B - E, J = B + E,$ $X_3 = Z_1I((X_1 + Y_1)(X_2 + Y_2) - C - D),$ $Y_3 = Z_1J(D - C),\ Z_3 = IJ$	$C = X_1X_2,\ K = Y_2Z_1,\ L = X_2Z_1,$ $D = Y_1Y_2,\ L_1 = X_1 - L,\ K_1 = K - Y_1,$ $K_2 = D + K + Y_1 + Y_2,$ $K_3 = D + K - Y_1 - Z_1,$ $K_4 = D - K + Y_1 - Z_1,$ $F = -X_1K_4 + LK_3,\ G = -K_2L_1,$ $H = CK_1,\ \Psi = \beta_QF + \gamma_QG + 2i\delta_QH.$

6 Concluding Remarks

In this work, we have studied pairing algorithms on Edwards form elliptic curves. A general form for the function required in a Miller iteration has been obtained. For a class of supersingular curves over fields of characteristic greater than 3, the expression for the Miller function has been simplified and explicit formulae obtained for combined doubling and Miller iteration and combined addition and Miller iteration using both inverted Edwards and projective Edwards coordinates.

Acknowledgements

The authors wish to thank Prof. Tanja Lange for her extensive comments on an earlier version of this work. The authors also wish to the thank the reviewers for their comments. The fist author is supported by Ministry of Information Technology, Govt. of India.

References

1. Joux, A.: A one round protocol for tripartite Diffie-Hellman. J. Cryptology 17(4), 263–276 (2004)
2. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. SIAM J. Comput. 32(3), 586–615 (2003)
3. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372 (2006), http://eprint.iacr.org/
4. Frey, G., Rück, H.G.: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of Computation 62, 865–874 (1994)
5. Miller, V.S.: The Weil pairing and its efficient calculation. J. Cryptology 17(4), 235–261 (2004)
6. Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 354–369. Springer, Heidelberg (2002)
7. Galbraith, S.D., Harrison, K., Soldera, D.: Implementing the Tate pairing. In: Fieker, C., Kohel, D.R. (eds.) ANTS 2002. LNCS, vol. 2369, pp. 324–337. Springer, Heidelberg (2002)
8. Edwards, H.M.: A normal form for elliptic curves. Bulletin of the American Mathematical Society 44, 393–422 (2007)
9. Bernstein, D.J., Lange, T.: Faster addition and doubling on elliptic curves. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 29–50. Springer, Heidelberg (2007)
10. Bernstein, D.J., Lange, T.: Inverted Edwards coordinates. In: Boztas, S., Lu, H.F. (eds.) AAECC 2007. LNCS, vol. 4851, pp. 20–27. Springer, Heidelberg (2007)
11. Chatterjee, S., Sarkar, P., Barua, R.: Efficient computation of Tate pairing in projective coordinate over general characteristic fields. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 168–181. Springer, Heidelberg (2005)
12. Bernstein, D.J., Birkner, P., Lange, T., Peters, C.: Twisted Edwards curves. Cryptology ePrint Archive, Report 2008/013 (2008) http://eprint.iacr.org/ (Accepted in AFRICACRYPT 2008)
13. Euler, L.: Observationes de comparatione arcuum curvarum irrectificabilium. Novi Comm. Acad. Sci. Petropolitanae 6(1761), 58–84

14. Gauss, C.F.: Werke 3, 404
15. Koblitz, N., Menezes, A.: Pairing-based cryptography at high security levels. In: Smart, N. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 13–36. Springer, Heidelberg (2005)
16. Verheul, E.R.: Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. Journal of Cryptology 17, 277–296 (2004)
17. Wolfram, S.: The Mathematica Book, 5th edn. Wolfram Media (2003), `http://www.wolfram.com`