Fast Pairing-Friendly Twisted Hessian Curves

Abstract

This paper recalls explicit constructions of families of pairing-friendly twisted Hessian curves with embedding degree $k \equiv 3, 9, 15 \pmod{18}$ and $k \equiv 0 \pmod{6}$ where $18 \nmid k$ and gives explicit formulas to compute the reduced Tate pairing on these families of twisted Hessian curves. Curves generated by our constructions are guaranteed to have twists of degree 3. We also explain a method to eliminate denominators for odd embedding degrees. Our constructions provide alternative embedding degrees for a higher security level in view of the recent attacks on the discrete logarithm problem for elliptic curves over finite fields with composite embedding degree.

Keywords: twisted Hessian curves, pairing-friendly curves, Tate pairing, odd embedding degree, denominator elimination

1 Introduction

Pairings on elliptic curves have various applications in cryptography, ranging from very basic key exchange protocols, such as one round tripartite Diffie–Hellman [28] [29], to complicated protocols, such as identity-based encryption [9] [25] [22] [46]. Pairings also help to improve currently existing protocols, such as signature schemes, to have shortest possible signatures [10].

Curves that are suitable for pairings are called *pairing-friendly curves*, and these curves must satisfy specific properties. It is extremely rare that a randomly generated elliptic curve is pairing-friendly, so pairing-friendly curves have to be generated in a special way. Examples of famous and commonly used pairing-friendly curves include Barreto-Naehrig curves [6] (BN curves), Barreto-Lynn-Scott curves [5] (BLS curves), and Kachisa-Schaefer-Scott curves [31] (KSS curves).

Performance of pairing-based cryptography relies on elliptic-curve-point arithmetic, computation of line functions and pairing algorithms. A pairing is a bilinear map from two elliptic curve groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to a target group $\mathbb{G}_T$. Therefore, to achieve a good performance, as well as having an efficient pairing algorithm, it is also desirable to have a fast elliptic-curve-point arithmetic in both $\mathbb{G}_1$ and $\mathbb{G}_2$.

Security of pairings depends on the cost of solving discrete logarithm problem (DLP) in the three groups previously mentioned, namely, $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$. Since one can attack pairing-based protocols by attacking any of these three groups, the cost of solving DLP must be sufficiently high in all of these three groups.

1.1 Choice of curves and embedding degrees

One way to improve the performance of pairings is to improve the performance of the underlying point arithmetic. Since pairing computation arises naturally from a geometric representation of Weierstrass curves, most pairing formulas use curves written in Weierstrass form. However, the algorithms for performing arithmetic on elliptic curves in Weierstrass form are known to be quite slow compared to elliptic curves with special properties allowing them to be written in for example Hessian form [48] [30] or in Edwards form [18] [8].

Pairings based on Edwards curves, along with examples of pairing-friendly Edwards curves were proposed by Arene, Lange, Naehrig and Ritzenthaler [1]. They found that the computation of line functions necessary to compute the pairing is much more complicated than if the curves were written in Weierstrass form. In other words, even though Edwards curves allow faster point arithmetic, this gain is outweighed by the slower computation of line functions.

Pairings based on Hessian curves have been considered by Gu, Gu and Xie [23]. They provided a geometric interpretation of the group law on Hessian curves along with an algorithm for computing Tate pairing on elliptic curves in Hessian form. However, no pairing-friendly curves in Hessian form were given.

Bos, Costello and Naehrig [11] investigated the possibility of first using a model of a curve (such as Edwards or Hessian) allowing for fast group operations, then mapping to Weierstrass form for the computation of the pairing. They found that for every elliptic curve E in the BN-12, BLS-12, and KSS-18 families of pairing-friendly curves, if E is isomorphic over $\mathbb{F}_p$ to a curve in Hessian or Edwards form, then it is not isomorphic over $\mathbb{F}_{p^k}$ to a curve in Hessian or Edwards form, where k is the embedding degree, so that the computations in either $\mathbb{G}_1$ or $\mathbb{G}_2$ have to use slower algorithms for group operations on curves in Weierstrass form. Moreover, this idea of using different curve models comes at a cost of at least one conversion between other curve models into Weierstrass curves.

Regardless of which model of elliptic curve was being studied, most of the previous articles on this topic were considering "even" embedding degrees. In this paper, we concentrate on curves with embedding degrees divisible by 3, as pairing-friendly elliptic curves in Hessian form are equipped with natural twists of degree 3. One of the main advantages of even embedding degrees is the applicability of a denominator elimination technique in the pairing computation, which is unfortunately not available for odd embedding degrees. In spite of this, pairing algorithms for curves in Weierstrass form with odd embedding degree have been shown previously to be competitive, for example in work by Lin, Zhao, Zhang and Wang in [39], by Mrabet, Guillermin and Ionica in [42], and by Fouotsa, Mrabet and Pecha in [19]. Also, due to recent advances in number field sieve techniques for attacking the discrete logarithm problem for pairing-friendly elliptic curves over finite fields, it is necessary to increase the size of the finite fields in which we are working for pairing-friendly curves, and one way of doing this is by increasing the embedding degree. This means increasing the current standard (even) embedding degrees $k = 12$ and $k = 18$, on which we give more details below.

1.2 Attacks on solving DLP over finite fields

The series of advances in attacking the discrete logarithm problem for elliptic curves over finite fields, i.e., [33] [3] [4], have weakened the security of pairing-friendly elliptic curves by dramatically decreasing the security level on the finite field side. In order to retain the security level, either the size of the prime field or the embedding degree (or both) has to be increased. For example, BN-12 (BN curves with embedding degree 12) used to be very popular for 128-bit security level, because a 256-bit prime field maps to a 3072-bit finite field where the security on both the prime field side and the finite field side have a 128-bit security level. A recent article on "Updating key size estimations for parings" by Barbulescu and Duquesne [2] suggests that, for BN curves, the prime field has to be increased to over 400 bits in order to achieve 128-bit security level. Increasing the field size has a penalty of slowing down arithmetic operations which creates a huge impact on performance.

1.3 Our contributions

In terms of the performance of pairing-based protocols, the paper [11] by Bos, Costello and Naehrig inspires the question whether it is possible to construct pairing-friendly curves that could be represented in the same curve models, preferably with fast point arithmetic and fast computation of line functions, for both $\mathbb{G}_1$ and $\mathbb{G}_2$,

Twisted Hessian curves with faster point arithmetic have recently been proposed by Bernstein, Lange, Chuengsatiansup and Kohel [7]. This leads to questions whether the newer point arithmetic would also lead to fast formulas for computing line functions, and whether these formulas would be applicable to computing pairings on twisted Hessian curves.

We present the first construction (to our knowledge) of a pairing on curves in Hessian form with odd embedding degree. Note in particular that among the popular pairing-friendly curve families, BN-12 and KSS-18 have embedding degrees 12 and 18 respectively, which gives a large difference in field size. Our results provide an alternative of embedding degree 15, in an attempt to give a better balance between the size of the prime field and of the embedding degree. For higher security level, our constructions allow, for example, embedding degrees 21 or 33.

The setup of this article is as follows: in Section 2, we recall Miller's algorithm to compute the reduced Tate pairing on an elliptic curve in Hessian form. In Section 3, we state constructions of families of pairing-friendly elliptic curves given in [20] that can be written in twisted Hessian form and show how to use the degree 3 twists to optimize computations. In Section 4, we state explicit formulas for the computation of the reduced Tate pairing on Hessian curves based on the state-of-the-art point arithmetic formulas. In Section 5, we compare the efficiency of our algorithm with the Weierstrass case.

2 The reduced Tate pairing

Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$ where p is a prime, let r be the size of the largest prime-order subgroup of $E(\mathbb{F}_p)$, and let $\mu_r \subseteq \mathbb{F}_{p^k}^*$ be the group of r^{th} roots of unity. We define the *embedding degree* of E to be

$$\min\{k \in \mathbb{Z} : r | p^k - 1\}.$$

For an integer $0 < e \leq k$ and a point $T \in E(\mathbb{F}_{p^e})$, we define the function $f_{r,T}$ to be the unique normalized function with divisor

$$\operatorname{div}(f_{r,T}) = r[T] - [rT] - (r-1)[T_\infty],$$

where T_∞ denotes the point at infinity on E.

Definition 1. With notation as above, we define the *reduced Tate pairing on E* to be

$$\begin{array}{cccc} \tau_r : & E(\mathbb{F}_{p^k})[r] \times E(\mathbb{F}_{p^k})/[r]E(\mathbb{F}_{p^k}) & \longrightarrow & \mu_r \\ & (P, Q) & \mapsto & f_{r,P}(Q)^{\frac{p^k-1}{r}}. \end{array}$$

In this paper we address the computation of the reduced Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_2$, where

$$\mathbb{G}_1 = E[r] \cap \ker(\phi_p - [1])$$

and

$$\mathbb{G}_2 = E[r] \cap \ker(\phi_p - [p]) \subseteq E(\mathbb{F}_{p^k}).$$

Here ϕ_p denotes the p-power Frobenius morphism on E. We denote the restriction of τ_r to $\mathbb{G}_1 \times \mathbb{G}_2$ by

$$e_r : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mu_r.$$

It is easy to check on a case-by-case basis that this pairing is non-degenerate and bilinear. (Non-degeneracy and bilinearity are automatic for ordinary elliptic curves, but the curves that we consider are supersingular). The following facts, due to Miller ([41]), allow us to explicitly compute this pairing. Let $0 < e \leq k$ be an integer, and let $T, T' \in E(\mathbb{F}_{q^e})$. We will write $L_{T,T'}$ for the projective line passing through T and T', and we will write $g_{T,T'}$ for the function

$$g_{T,T'} = \frac{L_{T,T'}}{L_{T+T',-(T+T')}}.$$

Lemma 1. With notation as above, for $P \in \mathbb{G}_1$, we have that $f_{0,P} = f_{1,P} = 1$ and for $n \geq 2$, that $f_{n+1,P} = f_{n,P} g_{P,nP}$.

Proof. Straightforward computation on divisors. See [41] for more details. □

Corollary 1. With notation as above, for $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, we get that

$$e_r(P,Q) = \prod_{m=1}^{r-1} \frac{L_{P,mP}(Q)^{\frac{p^k-1}{r}}}{L_{(m+1)P,-(m+1)P}(Q)^{\frac{p^k-1}{r}}}.$$

Hence, we only need to give formulas for addition and point doubling to compute the reduced Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_2$. That is, Algorithm 1 computes $e_r(P,Q)$ for $(P,Q) \in \mathbb{G}_1 \times \mathbb{G}_2$. For a point R on E, we denote by ℓ_{2R} the tangent line at R and by $\ell_{R,P}$ the line passing through R and P.

Algorithm 1 Miller's algorithm

```
for $i := \ell - 2$ down to $0$ do
    $f \leftarrow f^2 \cdot \ell_{2R}(Q)$
    $R \leftarrow 2R$
    if $m_i = 1$ then
        $f \leftarrow f \cdot \ell_{R,P}(Q)$
        $R \leftarrow R + P$
$f \leftarrow f^{(p^k-1)/r}$
```

3 Pairing-friendly twisted Hessian curves

Recall that in Section 2, we defined

- p to be prime,

- E to be an elliptic curve over $\mathbb{F}_p$,
- r to be the size of the largest prime order subgroup of $E(\mathbb{F}_p)$, and
- k to be smallest integer for which $r|p^k - 1$.

Under these assumptions, we also defined

$$\mathbb{G}_1 = E[r] \cap \ker(\phi_p - [1]) \quad \text{and} \quad \mathbb{G}_2 = E[r] \cap \ker(\phi_p - [p]) \subseteq E(\mathbb{F}_p^k),$$

and the reduced Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_2$ was given by

$$\begin{array}{rccc} e_r : & \mathbb{G}_1 \times \mathbb{G}_2 & \longrightarrow & \mu_r \\ & (P, Q) & \mapsto & f_{r,P}(Q)^{\frac{p^k-1}{r}}. \end{array}$$

We will refer to an elliptic curve $E/\mathbb{F}_p$ where p, r, k are known and satisfy the above properties as *pairing-friendly*. To construct the reduced Tate pairing, we search for pairing-friendly elliptic curves with a point of order 3, as these can be written in Hessian form. There are many constructions of parametric families of pairing-friendly curves listed in [20]. We recall below those families for which the curves also have a point of order 3, as shown in [7, Section 5].

3.1 Construction 1: $k \equiv 3 \pmod{18}$

This construction follows Construction 6.6 in [20] under the first subcase where $k \equiv 3 \pmod 6$. Define

$$\begin{aligned} r(x) &= \Phi_{2k}(x), \\ k(x) &= x^{k/3+1} + 1, \\ q(x) &= \frac{1}{3}(x^2 - x + 1)(x^{2k/3} - x^{k/3} + 1) + x^{k/3+1}, \end{aligned}$$

where $\Phi_{2k}(x)$ denotes the cyclotomic polynomial of degree $2k$. For infinitely many $x_0 \in \mathbb{Z}$, we can construct an elliptic curve $E/\mathbb{F}_{p(x_0)}$ such that the integers $r = r(x_0)$, $k = k(x_0)$, and $p = p(x_0)$ satisfy the properties for E to be pairing-friendly. Furthermore, for such x_0, we have that $k(x_0) \equiv 3 \pmod{18}$.

3.2 Construction 2: $k \equiv 9, 15 \pmod{18}$

This construction follows Construction 6.6 in [20] under the second subcase where $k \equiv 3 \pmod 6$. Define

$$\begin{aligned} r(x) &= \Phi_{2k}(x), \\ t(x) &= -x^{k/3+1} + x + 1, \\ q(x) &= \frac{1}{3}(x + 1)^2(x^{2k/3} - x^{k/3} + 1) - x^{2k/3+1}, \end{aligned}$$

where $\Phi_{2k}(x)$ denotes the cyclotomic polynomial of degree $2k$. For infinitely many $x_0 \in \mathbb{Z}$, we can construct an elliptic curve $E/\mathbb{F}_{p(x_0)}$ such that the integers $r = r(x_0)$, $k = k(x_0)$, and $p = p(x_0)$ satisfy the properties for E to be pairing-friendly. Furthermore, for such x_0, we have that $k(x_0) \equiv 9, 15 \pmod{18}$.

3.3 Construction 3: $k \equiv 0 \pmod 6$ and $18 \nmid k$

This construction follows the last case of Construction 6.6 in [20]. Define

$$\begin{aligned} r(x) &= \Phi_k(x), \\ t(x) &= x + 1, \\ q(x) &= \frac{1}{3}(x-1)^2(x^{k/3} - x^{k/6} + 1) + x, \end{aligned}$$

where $\Phi_k(x)$ denotes the cyclotomic polynomial of degree k. For infinitely many $x_0 \in \mathbb{Z}$, we can construct an elliptic curve $E/\mathbb{F}_{p(x_0)}$ such that the integers $r = r(x_0)$, $k = k(x_0)$, and $p = p(x_0)$ satisfy the properties for E to be pairing-friendly. Furthermore, for such x_0, we have that $k(x_0) \equiv 0 \pmod 6$, where $18 \nmid k(x_0)$.

3.4 Twists of degree 3

Let E and E' be elliptic curves over $\mathbb{F}_p$. We call E' a *twist* of E if E and E' are isomorphic over some field extension of $\mathbb{F}_p$. More precisely, E' is a *degree-d twist* of E if they are isomorphic over a degree d extension and not over any smaller field. We will see below that if E is an elliptic curve over $\mathbb{F}_p$ where $p \equiv 1 \bmod 3$ and can be written in the form

$$E_a : aX^3 + Y^3 + Z^3 = 0$$

then E_a has twists of degree 3. We will also see that if the embedding degree k is divisible by 3, the existence of these twists allow us to assume without loss of generality that 2 of the 3 coordinates of the point $Q \in E(\mathbb{F}_{q^k})$ are in $\mathbb{F}_{q^{k/3}}$, reducing the cost of the computation.

Lemma 2. Suppose that

$$E : aX^3 + Y^3 + Z^3 = 0$$

is an elliptic curve defined over a field $\mathbb{F}_p$ with embedding degree k, that $p \equiv 1 \bmod 3$, and that $3|k$. Then up to $\mathbb{F}_{p^{k/3}}$-isomorphism there are exactly two degree 3 twists of E defined over $\mathbb{F}_{p^{k/3}}$. These twists are given by

$$E_{a'} : a'X^3 + Y^3 + Z^3 = 0,$$

for $a \neq a' \in \mathbb{F}^*_{p^{k/3}}/(\mathbb{F}^*_{p^{k/3}})^3$.

Proof. Every supersingular elliptic curve with a point of order 3 is of the form

$$E' : \alpha X^3 + \beta Y^3 + \gamma Z^3 = 0,$$

where $\alpha, \beta, \gamma \in \mathbb{F}_{p^{k/3}}$. Furthermore, we know that α, β, and γ are non-zero as E' is non-singular. Hence every twist of E is isomorphic over $\mathbb{F}_{p^{k/3}}$ to an elliptic curve E' of the above form with $\alpha, \beta, \gamma \in \mathbb{F}^*_{p^{k/3}}/(\mathbb{F}^*_{p^{k/3}})^3$. Let a' be a generator of the group $\mathbb{F}^*_{p^{k/3}}/(\mathbb{F}^*_{p^{k/3}})^3$, so that

$$\mathbb{F}^*_{p^{k/3}}/(\mathbb{F}^*_{p^{k/3}})^3 = \{1, a', a'^2\}.$$

The curves defined by

$$E_{a'} : a'X^3 + Y^3 + Z^3 = 0,$$

$$E_{a'^2} : a'^2X^3 + Y^3 + Z^3 = 0,$$

and

$$E_1 : X^3 + Y^3 + Z^3 = 0$$

are the only non-$\mathbb{F}_{p^{k/3}}$-isomorphic twists of E such that any two of the coefficients α, β, γ are the same. The curve E' with $\alpha = 1$, $\beta = a'$, and $\gamma = a'^2$ is isomorphic over $F_{p^{k/3}}$ to

$$E_1 : X^3 + Y^3 + Z^3 = 0.$$

□

Now, if $3|k$, where k is the embedding degree of $E/\mathbb{F}_p$, and $\#E(\mathbb{F}_p) \not\equiv 0 \bmod 3$, then by [24, Theorem 3] and the above Lemma, for any $a \in \mathbb{F}^*_p$, we have that

$$E_a(\mathbb{F}_{p^k}) \cong \bigoplus_{a' \in \mathbb{F}^*_{p^{k/3}}/(\mathbb{F}^*_{p^{k/3}})^3} E_{a'}(\mathbb{F}_{p^{k/3}}).$$

In particular, every point $Q \in E_a(\mathbb{F}_{p^k})$ is the image of a point $Q_{a'} \in E_{a'}(\mathbb{F}_{p^{k/3}})$, for some $a' \in \mathbb{F}^*_{p^{k/3}}/(\mathbb{F}^*_{p^{k/3}})^3$, under the morphism

$$\begin{array}{rccc} \phi_{a'} : & E_{a'} & \longrightarrow & E \\ & (x : y : z) & \mapsto & (b^{-1}x : y : z), \end{array}$$

where $b \in \mathbb{F}_{p^k}$ satisfies $b^3 = a'/a$. Hence, writing $Q = (x_Q : y_Q : z_Q)$, we can conclude that only x_Q is in the full extension field $\mathbb{F}_{p^k}$, as y_Q and $z_Q \in \mathbb{F}_{p^{k/3}}$.

Also, as we are currently bound to using algorithms written for curves given in Weierstrass form, when we have computed a degree 3 twist E' of a given elliptic curve E, we have to check whether it can be written in Hessian form, that is, whether or not E' contains a point of order 3. To do this, we use the formulas for the number of points on twisted curves given in [24]. The formulas for calculating the number of points on twisted curves always come in pairs as there are exactly two twists, as we proved above. For example, the formulas stated in [24] are as follows:

$$\begin{aligned} \#E'(\mathbb{F}_p) &= p + 1 - (3f - t)/2 \qquad && \textit{with} \quad t^2 - 4p = -3f^2, \\ \#E'(\mathbb{F}_p) &= p + 1 - (-3f - t)/2 \qquad && \textit{with} \quad t^2 - 4p = -3f^2. \end{aligned}$$

To determine the unique twist containing the pre-image of our point $Q \in E(\mathbb{F}_{p^k})$, we use the fact that $\#E'(\mathbb{F}_p)$ must also be divisible by r.
Note that in Constructions 1 and 2, the only twists that occur are of degree 3, even without the restriction that the resulting curve should be in Hessian form. For Construction 3, there exist twists of degrees different from 3, but the resulting curves will not be in Hessian form.

4 Computation of line functions

Let notation be as above, and let $P \in \mathbb{G}_1$. We now move to the explicit computation of the line functions $\ell_1 = L_{iP,jP}$ and $\ell_2 = L_{(i+j)P,-(i+j)P}$ given in the formula for the reduced Tate pairing; recall from Section 2 that computing these line functions is enough to compute the reduced Tate pairing. Recall also that the line ℓ_2 is in the denominator of the pairing. Inversion is expensive, so we first apply 'denominator elimination' to optimize this inversion.

4.1 Denominator elimination

We follow a similar technique as described in [39] and [42] by rewriting an inversion into a fraction for which the denominator lies in a subfield. Define a field extension $\mathbb{F}_{p^k}$ of a finite field $\mathbb{F}_p$ and suppose that $x, y \in \mathbb{F}_{p^k}$.

Observe that

$$\frac{1}{x - y} = \frac{x^2 + xy + y^2}{x^3 - y^3}.$$

As x^3 and y^3 lie in a subfield of $\mathbb{F}_{p^k}$, we have that

$$(x^3 - y^3)^{\frac{p^k-1}{r}} = 1,$$

hence after the final exponentiation in the computation of the pairing, this factor does not appear. This means that we can ignore the computation of the denominator $x^3 - y^3$, so that instead of computing $\frac{1}{x-y}$, we compute $x^2 + xy + y^2$. The cost of division by $x - y$ then becomes the cost of multiplication by $x^2 + xy + y^2$.

4.2 Explicit formulas

Recall the twisted Hessian curve equation in projective coordiates

$$\mathcal{H} : aX^3 + Y^3 = Z^3 + dXYZ.$$

This subsection shows formulas to compute point doubling, point addition, and line functions associated to these operations. These formulas work under an assumption that the curve parameter $d = 0$.

Symbols $\mathbf{m}, \mathbf{s}, \mathbf{m}_a, k, d$ denote field multiplication, field squaring, field multiplication by curve constant a, embedding degree and twist degree respectively.

4.2.1 Doubling.

Given a point $P = (X_1, Y_1, Z_1)$ on $E/\mathbb{F}_p$ and a point $Q = (X_Q, Y_Q, 1)$ on $E/\mathbb{F}_{p^k}$ where $X_Q \in \mathbb{F}_{p^k}$ and $Y_Q \in \mathbb{F}_{p^{k/d}}$, the following formulas compute the doubling of point $P = 2P = (X_3, Y_3, Z_3)$ and the line function l.

$$\begin{aligned}
&T = Y_1^2; \quad A = Y_1 \cdot T; \quad S = Z_1^2; \quad B = Z_1 \cdot S;\\
&X_3 = X_1 \cdot (A - B); \quad Y_3 = -Z_1 \cdot (2A + B); \quad Z_3 = Y_1 \cdot (A + 2B);\\
&l_1 = aX_1^2 X_Q + T \cdot Y_Q + S; \quad l_a = X_3 \cdot Y_Q + X_3;\\
&l_b = X_Q \cdot (Y_3 + Z_3); \quad l_c = l_a^2 + l_b \cdot (l_a + l_b); \quad l = l_1 \cdot l_c;
\end{aligned}$$

The total number of operations is $k(\frac{14}{3}\mathbf{m} + \frac{1}{3}\mathbf{s}) + 5\mathbf{m} + 3\mathbf{s} + 1\mathbf{m}_a$.

4.2.2 Addition.

Given points $P = (X_1, Y_1, 1)$ and $R = (X_2, Y_2, Z_2)$ on $E/\mathbb{F}_p$ and a point $Q = (X_Q, Y_Q, 1)$ on $E/\mathbb{F}_{p^k}$ where $X_Q \in \mathbb{F}_{p^k}$ and $Y_Q \in \mathbb{F}_{p^{k/d}}$, the following formulas compute the addition of points $P + R = (X_1, Y_1, 1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3)$ and the line function l.

$$\begin{aligned}
&A = X_1 \cdot Z_2; \quad C = Y_1 \cdot X_2; \quad D = Y_1 \cdot Y_2; \quad F = aX_1 \cdot X_2;\\
&G = (D + Z_2) \cdot (A - C); \quad H = (D - Z_2) \cdot (A + C);\\
&J = (D + F) \cdot (A - Y_2); \quad K = (D - F) \cdot (A + Y_2);\\
&X_3 = G - H; \quad Y_3 = K - J;\\
&Z_3 = J + K - G - H - 2(B - F) \cdot (C + E);\\
&l_1 = (Y_1 \cdot Z_2 - Y_2) \cdot (X_1 - X_Q) + (Y_Q - Y_1) \cdot (X_1 \cdot Z_2 - X_2);\\
&l_a = Y_Q \cdot X_3 + X_3; \quad l_b = X_Q \cdot (Y_3 + Z_3); \quad l_c = l_a^2 + l_a \cdot (l_b + l_b);\\
&l = l_1 \cdot l_c;
\end{aligned}$$

The total number of operations is $k(\frac{14}{3}\mathbf{m} + \frac{1}{3}\mathbf{s}) + 11\mathbf{m} + 1\mathbf{m}_a$.

5 Comparison

We would like to emphasize that:

- Most of the previous work concerned Weierstrass curves.
- Most of the previous work concerned even embedding degrees.
- There was some previous work on Hessian curves but with even embedding degrees.
- There was also some previous works with odd embedding degrees but using Weierstrass curves.

Therefore, it is difficult to have an appropriate comparison between the constructions in this article and previous work, as we are the first to consider the twisted Hessian curves with odd embedding degrees, to our knowledge. Note that even embedding degrees have the advantage of being able to completely eliminate denominators in the computation of the Tate pairing. However, with odd embedding degrees, we need to compute the denominator as it is non-trivial.

Table 1 shows the costs of the computation of pairings using our constructions in comparison with previous work. The first column gives the embedding degrees k. The second column gives the curve model, where $\mathcal{J}$, $\mathcal{P}$, $\mathcal{E}$, $\mathcal{H}$ denote the Weierstrass model with Jacobian coordinates, the Weierstrass model with projective coordinates, the Edwards model and the Hessian model respectively. Note that this work considers the generalization of Hessian curves to "twisted" Hessian curves, and that the twists are of degree 3. The third and fourth columns show the cost of doubling (DBL) and mixed addition (mADD) including the computation of the line functions for pairing computations. By 'mixed addition' we mean that the z coordinate is set to be 1. We denote the cost of field multiplication and field squaring over the base field $\mathbb{F}_p$ by $\mathbf{m}$ and $\mathbf{s}$ respectively. The cost of multiplication by curve parameters is omitted from the table.

Table 1: Cost of pairing computation

k	Curve models	DBL	mADD
even	$\mathcal{J}$, [26] [1]	$k\mathbf{m}+1\mathbf{m}+11\mathbf{s}$	$k\mathbf{m}+6\mathbf{m}+6\mathbf{s}$
	$\mathcal{J}, a=-3$, [1]	$k\mathbf{m}+6\mathbf{m}+5\mathbf{s}$	$k\mathbf{m}+6\mathbf{m}+6\mathbf{s}$
	$\mathcal{J}, a=0$, [1]	$k\mathbf{m}+3\mathbf{m}+8\mathbf{s}$	$k\mathbf{m}+6\mathbf{m}+6\mathbf{s}$
	$\mathcal{P}, a=0, b=c^2$, [15]	$k\mathbf{m}+3\mathbf{m}+5\mathbf{s}$	$k\mathbf{m}+10\mathbf{m}+2\mathbf{s}$
	$\mathcal{E}$, [1]	$k\mathbf{m}+6\mathbf{m}+5\mathbf{s}$	$k\mathbf{m}+12\mathbf{m}$
	$\mathcal{H}$, [23]	$k\mathbf{m}+3\mathbf{m}+6\mathbf{s}$	$k\mathbf{m}+10\mathbf{m}$
odd	$\mathcal{P}$, [16]	$k\mathbf{m}+6\mathbf{m}+7\mathbf{s}$	$k\mathbf{m}+13\mathbf{m}+3\mathbf{s}$
	$\mathcal{H}, d=3$, this paper	$k(\frac{14}{3}\mathbf{m}+\frac{1}{3}\mathbf{s})+5\mathbf{m}+3\mathbf{s}$	$k(\frac{14}{3}\mathbf{m}+\frac{1}{3}\mathbf{s})+11\mathbf{m}$

Let $\mathbf{M}$ and $\mathbf{S}$ denote the cost of field multiplication and field squaring over the extension field. In the doubling step (line 2 in Algorithm 1), we have to compute $f^2 \cdot l$. Therefore, the extra cost of $1\mathbf{M} + 1\mathbf{S}$ is required. Similarly, in the addition step (line 5 in Algorithm 1), we have to compute $f \cdot l$. Therefore, the extra cost of $1\mathbf{M}$ is required. These extra costs are the same for all curve models regardless of the embedding degree, hence, we omit these costs from the table.

Note that there are various advantages of our constructions that cannot be justified by the cost shown in Table 1. First of all, the costs shown in Table 1 do not reflect the total cost for the pairing-based protocols. This is because generically there are many group operations performed prior to relatively few pairing computations, and group operations on twisted Hessian curves allow faster point arithmetic operations than Weierstrass curves. Secondly, having curves represented in the same models for $\mathbb{G}_1$ and $\mathbb{G}_2$ does not induce the extra cost of conversion between curve models. (Recall that for BN, BLS, and KSS, this conversion is always necessary if one wants to take advantage of the fast point-arithmetic on Hessian or Edwards curves, as proven in [11].)

6 Concluding remarks

This paper presents concrete methods to generate pairing-friendly twisted Hessian curves. Curves generated by these methods are guaranteed to have twists of degree 3, and have embedding degree $k \equiv 3 \pmod{18}$, $k \equiv 9, 15 \pmod{18}$ or $k \equiv 0 \pmod 6$ where $18 \nmid k$. We describe techniques to eliminate intermediate denominators for odd embedding degrees, leading to faster overall computation. We also provide explicit formulas to compute line functions in pairing computations.

Although pairings on Hessian curves have already been considered, for example, by Gu, Gu, and Xie in [23] and by Li and Zhang in [38], this work is the first to explain methods to generate pairing-friendly "twisted" Hessian curves with odd embedding degree, to our knowledge. Twisted Hessian curves are a generalization of Hessian curves; using twists allows our formulas to be applied to more curves. We also take advantage of the state-of-the-art fast point arithmetic formulas from [7] available on curves in Hessian form.

The pairing-friendly families of BN, BLS, and KSS curves use primarily embedding degrees 12 or 18. Due to recent advances in the discrete logarithm problem, it has become necessary to increase the size of the finite field, which can be done either by increasing the size of the prime or by increasing the embedding degree. Our constructions address this problem by generating pairing-friendly twisted Hessian curves with embedding degrees 15 and 21.

References

[1] Christophe Arene, Tanja Lange, Michael Naehrig, and Christophe Ritzenthaler. Faster Computation of the Tate Pairing. *IACR Cryptology ePrint Archive*, 2009:155, 2009. http://eprint.iacr.org/2009/155.

[2] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *IACR Cryptology ePrint Archive*, page 334, 2017. http://eprint.iacr.org/2017/334.

[3] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In *Eurocrypt 2015 [43]*, pages 129–155, 2015.

[4] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The tower number field sieve. In *Asiacrypt 2015 [27]*, pages 31–55, 2015.

[5] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. On the Selection of Pairing-Friendly Groups. In *SAC 2003 [40]*, pages 17–25, 2003.

[6] Paulo S.L.M. Barreto and Michael Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. In *SAC 2005 [44]*, pages 319–331, 2006. http://cryptosith.org/papers/pfcpo.pdf.

[7] Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted Hessian Curves. In *LATINCRYPT 2015 [37]*, pages 269–294, 2015. http://cr.yp.to/papers.html#hessian.

[8] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *Asiacrypt 2007 [35]*, pages 29–50, 2007. http://cr.yp.to/newelliptic/newelliptic-20070906.pdf.

[9] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO 2001 [32]*, pages 213–229, 2001. http://www.iacr.org/archive/crypto2001/21390212.pdf.

[10] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004. http://crypto.stanford.edu/~dabo/pubs/papers/weilsigs.ps.

[11] Joppe W. Bos, Craig Costello, and Michael Naehrig. Exponentiating in Pairing Groups. In *SAC 2013 [36]*, 2013. http://cryptosith.org/papers/#exppair.

[12] Wieb Bosma, editor. *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2–7, 2000, proceedings*, volume 1838 of *Lecture Notes in Computer Science*. Springer, 2000.

[13] Çetin Kaya Koç, David Naccache, and Christof Paar, editors. *Cryptographic hardware and embedded systems — CHES 2001, third international workshop, Paris, France, May 14–16, 2001, proceedings*, volume 2162 of *Lecture Notes in Computer Science*. Springer, 2001.

[14] 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*. Springer, 2008.

[15] Craig Costello, Hüseyin Hisil, Colin Boyd, Juan Manuel González Nieto, and Kenneth Koon-Ho Wong. Faster pairings on special weierstrass curves. In *Pairing 2009 [47]*, pages 89–101, 2009.

[16] Craig Costello, Tanja Lange, and Michael Naehrig. Faster pairing computations on curves with high-degree twists. In *PKC 2010*, pages 224–242, 2010.

[17] Ronald Cramer, editor. *Advances in Cryptology — EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.

[18] 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.

[19] Emmanuel Fouotsa, Nadia El Mrabet, and Aminatou Pecha. Optimal ate pairing on elliptic curves with embedding degree 9, 15 and 27. *IACR Cryptology ePrint Archive*, 2016:1187, 2016. http://eprint.iacr.org/2016/1187.

[20] David Freeman, Michael Scott, and Edlyn Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *Journal of Cryptology*, 23(2):224–280, 2010. http://eprint.iacr.org/2006/372/.

[21] 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*. Springer, 2008.

[22] Craig Gentry and Alice Silverberg. Hierarchical ID-Based Cryptography. In *Asiacrypt 2002 [49]*, pages 548–566, 2002. http://www.cs.ucdavis.edu/~franklin/ecs228/pubs/extra_pubs/hibe.pdf.

[23] Haihua Gu, Dawu Gu, and WenLu Xie. Efficient pairing computation on elliptic curves in hessian form. In *ICISC 2010*, pages 169–176, 2010.

[24] Florian Hess, Nigel P. Smart, and Frederik Vercauteren. The Eta Pairing Revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006. http://eprint.iacr.org/2006/110.

[25] Jeremy Horwitz and Ben Lynn. Toward Hierarchical Identity-Based Encryption. In *Eurocrypt 2002 [34]*, pages 466–481, 2002. http://theory.stanford.edu/~horwitz/pubs/hibe.pdf.

[26] Sorina Ionica and Antoine Joux. Another approach to pairing computation in edwards coordinates. In *INDOCRYPT 2008 [14]*, pages 400–413, 2008.

[27] Tetsu Iwata and Jung Hee Cheon, editors. *Advances in Cryptology — ASIACRYPT 2015, 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 – December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*. Springer, 2015.

[28] Antoine Joux. A One Round Protocol for Tripartite Diffie-Hellman. In *ANTS-IV, [12]*, pages 385–393, 2000. http://cgi.di.uoa.gr/~aggelos/crypto/page4/assets/joux-tripartite.pdf.

[29] Antoine Joux. A One Round Protocol for Tripartite Diffie-Hellman. *Journal of Cryptology*, 17(4):263–276, 2004.

[30] Marc Joye and Jean-Jacques Quisquater. Hessian elliptic curves and side-channel attacks. In *CHES 2001 [13]*, pages 402–410, 2001. http://joye.site88.net/.

[31] Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field. In *Pairing 2008 [21]*, pages 126–135, 2008.

[32] Joe Kilian, editor. *Advances in Cryptology — CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*. Springer, 2001.

[33] Taechan Kim and Razvan Barbulescu. Extended tower number field sieve: A new complexity for the medium prime case. In *CRYPTO 2016 [45]*, pages 543–571, 2016.

[34] Lars R. Knudsen, editor. *Advances in Cryptology — EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 –*

May 2, 2002, proceedings, volume 2332 of *Lecture Notes in Computer Science*. Springer, 2002.

[35] Kaoru Kurosawa, editor. *Advances in Cryptology — ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2–6, 2007, Proceedings*, volume 4833 of *Lecture Notes in Computer Science*. Springer, 2007.

[36] Tanja Lange, Kristin Lauter, and Petr Lisonek, editors. *Selected areas in cryptography, 20th international conference, SAC 2013, Burnaby, BC, Canada, August 14–16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*. Springer, 2014.

[37] Kristin E. Lauter and Francisco Rodríguez-Henríquez, editors. *Progress in Cryptology — LATINCRYPT 2015, 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23–26, 2015, Proceedings*, volume 9230 of *Lecture Notes in Computer Science*. Springer, 2015.

[38] Liangze Li and Fan Zhang. Tate pairing computation on generalized hessian curves. In *WISA 2012*, pages 111–123, 2012.

[39] Xibin Lin, Changan Zhao, Fangguo Zhang, and Yanming Wang. Computing the Ate Pairing on Elliptic Curves with Embedding Degree $k = 9$. *IEICE Transactions*, 91-A(9):2387–2393, 2008.

[40] Mitsuru Matsui and Robert J. Zuccherato, editors. *Selected Areas in Cryptography, 10th Annual International Workshop, SAC 2003, Ottawa, Canada, August 14–15, 2003, Revised Papers*, volume 3006 of *Lecture Notes in Computer Science*. Springer, 2004.

[41] Victor S. Miller. The weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, 2004.

[42] Nadia El Mrabet, Nicolas Guillermin, and Sorina Ionica. A study of pairing computation for elliptic curves with embedding degree 15. *IACR Cryptology ePrint Archive*, 2009:370, 2009. http://eprint.iacr.org/2009/370.

[43] Elisabeth Oswald and Marc Fischlin, editors. *Advances in Cryptology — EUROCRYPT 2015, 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26–30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*. Springer, 2015.

[44] Bart Preneel and Stafford E. Tavares, editors. *Selected Areas in Cryptography, 12th International Conference, SAC 2005, Kingston, ON, Canada, August 11–12, 2005, Revised Selected Papers*, volume 3897 of *Lecture Notes in Computer Science*. Springer, 2006.

[45] Matthew Robshaw and Jonathan Katz, editors. *Advances in Cryptology — CRYPTO 2016, 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14–18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*. Springer, 2016.

[46] Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. In *Eurocrypt 2005 [17]*, pages 457–473, 2005. http://eprint.iacr.org/2004/086/.

[47] Hovav Shacham and Brent Waters, editors. *Pairing-Based Cryptography — Pairing 2009, Third International Conference, Palo Alto, California, USA, August 12–14, 2009, proceedings*, volume 5671 of *Lecture Notes in Computer Science*. Springer, 2009.

[48] Nigel P. Smart. The Hessian form of an elliptic curve. In *CHES 2001 [13]*, pages 118–125, 2001.

[49] Yuliang Zheng, editor. *Advances in Cryptology — ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1–5, 2002, Proceedings*, volume 2501 of *Lecture Notes in Computer Science*. Springer, 2002.