Efficient Pairings Computation on Jacobi Quartic Elliptic Curves*

Sylvain Duquesne[1], Nadia El Mrabet[2], and Emmanuel Fouotsa[3]

[1] IRMAR, UMR CNRS 6625, Université Rennes 1,
Campus de Beaulieu 35042 Rennes cedex, France
sylvain.duquesne@univ-rennes1.fr

[2] Université Paris 8, Laboratoire d'Informatique Avancé de Saint-Denis,
93526 Saint Denis Cedex, France
elmrabet@ai.univ-paris8.fr

[3] Département de Mathématiques, Université de Bamenda
Ecole Normale Supérièure, BP 5052 Bamenda, Cameroun
emmanuel.fouotsa@prmais.org

Abstract. This paper proposes the computation of the Tate pairing, Ate pairing and its variations on the special Jacobi quartic elliptic curve $Y^2 = dX^4 + Z^4$. We improve the doubling and addition steps in Miller's algorithm to compute the Tate pairing. We use the birational equivalence between Jacobi quartic curves and Weierstrass curves, together with a specific point representation to obtain the best result to date among curves with quartic twists. For the doubling and addition steps in Miller's algorithm for the computation of the Tate pairing, we obtain a theoretical gain up to 27% and 39%, depending on the embedding degree and the extension field arithmetic, with respect to Weierstrass curves [2] and previous results on Jacobi quartic curves [3]. Furthermore and for the first time, we compute and implement Ate, twisted Ate and optimal pairings on the Jacobi quartic curves. Our results are up to 27% more efficient, comparatively to the case of Weierstrass curves with quartic twists [2].

Keywords: Jacobi quartic curves, Tate pairing, Ate pairing, twists, Miller function.

1 Introduction

Bilinear pairings were first used to solve the discrete logarithm problem on elliptic curve groups [4, 5]. But they are now useful to construct many public key protocols for which no other efficient implementation is known [6, 7]. A survey of some of these protocols can be found in [8]. The efficient computation of pairings

* This work was supported in part by French ANR projects no. 12-BS01-0010-01 "PEACE", INS 2012 SIMPATIC project and LIRIMA 2013 MACISA project. This work is an improved and extended version of the work [1] appeared in the proceedings of Pairing 2012.

depends on the model chosen for the elliptic curve. Pairing computation on the Edwards model of elliptic curves has been done successively in [9, 10] and [11]. The recent results on pairing computation using elliptic curves of Weierstrass form can be found in [12, 2]. Recently in [3], Wang et al. have computed the Tate pairing on Jacobi quartic elliptic curves using the geometric interpretation of the group law. In this paper, we focus on the special Jacobi quartic elliptic curve $Y^2 = dX^4 + Z^4$ over fields of large characteristic $p \geq 5$ not congruent to 3 modulo 4.

For pairing computation with embedding degree divisible by 4, we define and use the quartic twist of the curve $Y^2 = dX^4 + Z^4$. Our results improve those obtained by Wang et al. in [3] and they are more efficient than those concerning the Tate pairing computation in Weierstrass elliptic curves [2].

Furthermore, the Miller algorithm is the main tool in the Tate pairing computation, and its efficiency has been successfully improved in the last years leading to other pairings such as:

- The Eta-pairing [13] on supersingular elliptic curves.
- Ate and twisted Ate pairings introduced in [14] that are closely related to the Eta-pairing, but can be used efficiently with ordinary elliptic curves. These pairings can be more efficient than the Tate pairing, essentially due to the reduction of the number of iterations in the Miller algorithm.
- In [15] and [16], Vercauteren and Hess generalize the method with the notion of optimal pairings and pairings lattices that can be computed using the smallest number of basic Miller's iterations.

The computation of these different pairings has been done by Costello et al. [2] in the case of Weierstrass curves. As a second contribution of this work, we extend the results on the special Jacobi quartic in [1] to the computation of Ate pairing and its variations. We show that among known curves with quartic twists, the Jacobi model $Y^2 = dX^4 + Z^4$ offers the best performances for all these different pairings.

The rest of this paper is organized as follows: Section 2 provides a background on the Jacobi elliptic curve, and notions on pairings that are useful in the paper. In Section 3, we present the computation of the Tate pairing on the Jacobi quartic curve mentioned above using birational equivalence and we compare our results to others in the literature. In Section 4, we determine the Miller function and rewrite the addition formulas for Ate pairing. We also provide a comparative study of these pairings on the curves in Jacobi and Weierstrass forms. In Section 5 we provide an example of pairing friendly curve of embedding degree 8. An implementation of the Tate, Ate and optimal Ate pairings based on this example has been done using the Magma computer algebra system. This enable to verify all the formulas given in this paper. Finally, we conclude in Section 6.

The following notations are used in this work.

$\mathbb{F}_q$: A finite field of characteristic $p \geq 5$, not congruent to 3 modulo 4.

m_k, s_k : Cost of multiplication and squaring in the field $\mathbb{F}_{q^k}$, for any integer k

mc: Cost of the multiplication by a constant in $\mathbb{F}_q$

2 Background on Pairings and on Jacobi Elliptic Curves

In this section, we briefly review pairings on elliptic curves and the Jacobi quartic curves. We also define twists of Jacobi's curves.

2.1 The Jacobi Quartic Curve

A Jacobi quartic elliptic curve over a finite field $\mathbb{F}_q$ is defined by

$$E_{d,\mu} : y^2 = dx^4 + 2\mu x^2 + 1$$

with discriminant $\triangle = 256d(\mu^2 - d)^2 \neq 0$. In [17] Billet and Joye proved that if the Weierstrass curve $E : y^2 = x^3 + ax + b$ has a rational point of order 2 denoted $(\theta, 0)$, then it is birationally equivalent to the Jacobi quartic $E_{d,\mu}$ with $d = -(3\theta^2 + 4a)/16$ and $\mu = -3\theta/4$. In the remainder of this paper, we will focus our interest on the special Jacobi quartic curve

$$E_{d,0} : y^2 = dx^4 + 1$$

because this curve has interesting properties such as a quartic twist which will contribute to an efficient computation of pairings.
The addition and doubling formulas on $E_{d,0}$ are deduced from [18].
The point addition $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ is given by :

$$x_3 = \frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2} \text{ and } y_3 = \frac{(x_1 - x_2)^2}{(x_1 y_2 - y_1 x_2)^2}(y_1 y_2 + 1 + dx_1^2 x_2^2) - 1.$$

The point doubling $(x_3, y_3) = 2(x_1, y_1)$ on $E_{d,0}$ is given by:

$$x_3 = \frac{2y_1}{2 - y_1^2} x_1 \text{ and } y_3 = \frac{2y_1}{2 - y_1^2}\left(\frac{2y_1}{2 - y_1^2} - y_1\right) - 1.$$

The birational equivalence, deduced from [17], between the Weierstrass curve $W_d : y^2 = x^3 - 4dx$ and the Jacobi quartic curve $E_{d,0}$ is given by

$$\begin{array}{rll} \varphi : E_{d,0} & \longrightarrow & W_d \\ (0,1) & \longmapsto & P_\infty \\ (0,-1) & \longmapsto & (0,0) \\ (x,y) & \longmapsto & \left(2\frac{y+1}{x^2}, 4\frac{y+1}{x^3}\right) \end{array} \quad \text{and} \quad \begin{array}{rll} \varphi^{-1} : W_d & \longrightarrow & E_{d,0} \\ P_\infty & \longmapsto & (0,1) \\ (0,0) & \longmapsto & (0,-1) \\ (x,y) & \longmapsto & \left(\frac{2x}{y}, \frac{2x^3 - y^2}{y^2}\right) \end{array}$$

From now on, and for efficiency reasons, we adopt for the first time in pairings computation a specific points representation namely $(x, y) = (\frac{X}{Z}, \frac{Y}{Z^2})$. The curve $E_{d,0}$ is then equivalent to

$$E_d : Y^2 = dX^4 + Z^4.$$

The addition and doubling formulas on E_d are as follows. The point addition $[X_3 : Y_3 : Z_3] = [X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]$ on E_d is given by :

$$\begin{cases} X_3 = X_1^2 Z_2^2 - Z_1^2 X_2^2, \\ Z_3 = X_1 Z_1 Y_2 - X_2 Z_2 Y_1, \\ Y_3 = (X_1 Z_2 - X_2 Z_1)^2 (Y_1 Y_2 + (Z_1 Z_2)^2 + d(X_1 X_2)^2) - Z_3^2. \end{cases}$$

The point doubling $[X_3 : Y_3 : Z_3] = 2[X_1 : Y_1 : Z_1]$ on E_d is given by :

$$\begin{cases} X_3 = 2X_1 Y_1 Z_1, \\ Z_3 = Z_1^4 - dX_1^4, \\ Y_3 = 2Y_1^4 - Z_3^2. \end{cases}$$

The birational equivalence between the projective model $E_d : Y^2 = dX^4 + Z^4$ and the Weierstrass curve $W_d : y^2 = x^3 - 4dx$ becomes

$$\begin{array}{rcl} \varphi : \quad E_d & \longrightarrow & W_d \\ [0:1:1] & \longmapsto & P_\infty \\ [0:-1:1] & \longmapsto & (0,0) \\ [X:Y:Z] & \longmapsto & \left(2\frac{Y+Z^2}{X^2}, 4\frac{Z(Y+Z^2)}{X^3}\right) \end{array} \quad . \quad \begin{array}{rcl} \varphi^{-1} : \quad W_d & \longrightarrow & E_d \\ P_\infty & \longmapsto & [0:1:1] \\ (0,0) & \longmapsto & [0:-1:1] \\ (x,y) & \longmapsto & [2x : 2x^3 - y^2 : y]. \end{array}$$

The Sage software code to verify the correctness of our formulas is available here: `http://www.prmais.org/Implementation-Pairings-Jacobi.txt`.

2.2 Pairings on Elliptic Curves

In this section, we first recall the Tate pairing. Then, the notion of twists of elliptic curves is defined to recall the definition of Ate pairing ant its variations. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. The neutral element of the additive group law defined on the set of rational points of E is denoted P_∞. Let r be a large prime divisor of the group order $\sharp E(\mathbb{F}_q)$ and k be the embedding degree of E with respect to r, i.e. the smallest integer such that r divides $q^k - 1$. The set $E\left(\overline{\mathbb{F}_q}\right)[r] = \{P \in E\left(\overline{\mathbb{F}_q}\right) : [r]P = P_\infty\}$ is the set of $r-$torsion points with coordinates in an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$, where $[\ ] : P \longmapsto [r]P$ is the endomorphism defined on $E(\mathbb{F}_q)$ which consists to add P to itself r times. The integer k is also the smallest integer such that $E\left(\overline{\mathbb{F}_q}\right)[r] \subset E(\mathbb{F}_{q^k})$ and this is the main property that we use in this work.

The Tate pairing. Consider a point $P \in E(\mathbb{F}_q)[r]$ and the divisor $D = r(P) - r(P_\infty)$, then according to [19, Corollary 3.5, Page 67], D is principal and so there is a function $f_{r,P}$ with divisor Div $(f_{r,P}) = D$. Let Q be a point of order r with coordinates in $\mathbb{F}_{q^k}$ and μ_r be the group of r-th roots of unity in $\mathbb{F}_{q^k}^*$. The reduced Tate pairing e_r is a bilinear and non degenerate map defined as

$$\begin{array}{rl} e_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] & \to \mu_r, \\ (P, Q) & \mapsto f_{r,P}(Q)^{\frac{q^k-1}{r}}. \end{array}$$

The value $f_{r,P}(Q)$ can be determined efficiently using Miller's algorithm [20]. Indeed, for an integer i, consider the divisor $D_i = i(P) - ([i]P) - (i-1)(P_\infty)$. We observe that D_i is a principal divisor and so there is a function $f_{i,P}$ such that $\mathrm{Div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(P_\infty)$. Observe that

$$\text{for } i = r \text{ one has } D_r = r(P) - r(P_\infty) = \mathrm{Div}(f_{r,P}).$$

Thus, to obtain the value of $f_{r,P}(Q)$, it suffices to apply an iterative algorithm using an *addition chain* for r, that is, a sequence $(1, i_1, i_2, ..., r)$ such that each i_k is the sum of two previous terms of the sequence. This is justified by the fact that the functions $f_{i,P}$ are satisfying the following conditions:

$$f_{1,P} = 1 \text{ and } f_{i+j,P} = f_{i,P} f_{j,P} h_{[i]P,[j]P} \tag{1}$$

where $h_{R,S}$ denotes a rational function such that

$$\mathrm{Div}(h_{R,S}) = (R) + (S) - (S+R) - (P_\infty),$$

with R and S two arbitrary points on the elliptic curve. In the case of elliptic curves in Weierstrass form, $h_{R,S} = \frac{\ell_{R,S}}{v_{R+S}}$ where $\ell_{R,S}$ is the straight line defining $R+S$ and v_{R+S} is the corresponding vertical line passing through $R+S$.

Miller uses the *double-and-add* method as the addition chains for r (see [21, Chapter 9] for more details on addition chains) and the properties of $f_{i,P}$ to compute $f_{r,P}(Q)$. The Miller algorithm that computes efficiently the pairing of two points is given in Algorithm 1.

```
Algorithm 1: Miller's Algorithm
Input : $P \in E(\mathbb{F}_q)[r]$, $Q \in E(\mathbb{F}_{q^k})[r]$, $r = (1, r_{n-2}, ....r_1, r_0)_2$.
Output: The reduced Tate pairing of $P$ and $Q$ : $f_{r,P}(Q)^{\frac{q^k-1}{r}}$
Set $f \leftarrow 1$ and $R \leftarrow P$
For $i = n-2$ down to $0$ do
        $f \leftarrow f^2 \cdot h_{R,R}(Q)$
        $R \leftarrow 2R$
    if $r_i = 1$ then
        $f \leftarrow f \cdot h_{R,P}(Q)$
        $R \leftarrow R + P$
    end if
end for
return $f^{\frac{q^k-1}{r}}$
```

Fig. 1. The Miller algorithm for the computation of the reduced Tate pairing

More informations on pairings can be found in [22] and [23].

Let us now define twists of elliptic curves and specialise to the case of Jacobi quartic curves. This notion of twists enable to work on smaller base fields for pairings computations.

Twists of elliptic curves. A twist of an elliptic curve E defined over a finite field $\mathbb{F}_q$ is an elliptic curve E' defined over $\mathbb{F}_q$ that is isomorphic to E over an algebraic closure of $\mathbb{F}_q$. The smallest integer δ such that E and E' are isomorphic over $\mathbb{F}_{q^\delta}$ is called the degree of the twist.
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve in Weierstrass form defined over $\mathbb{F}_q$. The equation defining the twist E' has the form $y^2 = x^3 + a\omega^4 x + b\omega^6$ where ω belongs to an extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ and the isomorphism between E' and E is

$$\begin{array}{rccc} \psi : & E' & \longrightarrow & E \\ & (x', y') & \longmapsto & (x'/\omega^2, y'/\omega^3). \end{array}$$

More details on twists can be found in [2].

Twist of Jacobi quartic curves. To obtain the twist of the Jacobi quartic curve $Y^2 = dX^4 + Z^4$, we use the birational maps defined in Subsection 2.1 and the twist of Weierstrass curves defined above. Let k be an integer divisible by 4.

Definition 1 *[1] A quartic twist of the Jacobi quartic curve $Y^2 = dX^4 + Z^4$ defined over the extension $\mathbb{F}_{q^{k/4}}$ of $\mathbb{F}_q$ is a curve given by the equation*

$$E_d^\omega : Y^2 = d\omega^4 X^4 + Z^4$$

where $\omega \in \mathbb{F}_{q^k}$ is such that $\omega^2 \in \mathbb{F}_{q^{k/2}}$, $\omega^3 \in \mathbb{F}_{q^k} \backslash \mathbb{F}_{q^{k/2}}$ and $\omega^4 \in \mathbb{F}_{q^{k/4}}$.
In other terms $\{1, \omega, \omega^2, \omega^3\}$ is a basis of $\mathbb{F}_{q^k}$ as a vector space over $\mathbb{F}_{q^{k/4}}$.

Proposition 1 *Let E_d^ω defined over $\mathbb{F}_{q^{k/4}}$ be a twist of E_d. The $\mathbb{F}_{q^k}$-isomorphism between E_d^ω and E_d is given by*

$$\begin{array}{rccc} \psi : & E_d^\omega & \rightarrow & E_d, \\ & [X : Y : Z] & \mapsto & [\omega X : Y : Z] \,. \end{array}$$

We explain in Section 2.3 and in Section 3.1 how twists are very useful for an efficient computation of pairings.

Ate pairing and its variations. In this section, we briefly define Ate and twisted Ate pairings. The results in this section are very well described in the original article of Hess et al. [14]. We recall that $f_{i,R}$ is the function with divisor

$$\mathrm{Div}(f_{i,R}) = i(R) - ([i]R) - (i-1)(P_\infty).$$

Let

$$\begin{array}{rcl} \pi_q : E\left(\overline{\mathbb{F}_q}\right) & \rightarrow & E\left(\overline{\mathbb{F}_q}\right) \\ (x, y) & \mapsto & (x^q, y^q) \end{array}$$

be the Frobenius endomorphism on the curve, and t be its trace. The characteristic polynomial of π_q is $X^2 - tX + q$, see [24, Chapter 4]. Using the fact that π_q satisfies its characteristic polynomial (Cayley Hamilton theorem), we have the following equality:

$$\pi_q^2 - t\pi_q + q = 0.$$

The relation between the trace t of the Frobenius endomorphism and the group order is given by [24, Theorem 4.3]:

$$\sharp E(\mathbb{F}_q) = q + 1 - t.$$

The Frobenius endomorphism π_q has exactly two eigenvalues. Indeed, using the Lagrange theorem in the multiplicative group $(\mathbb{F}_q^*, \times)$, it is clear that 1 is an eigenvalue. We then use the characteristic polynomial to conclude that q is the other one. This enables to consider $P \in \mathbb{G}_1 = E\left(\overline{\mathbb{F}_q}\right)[r] \cap \text{ Ker}(\pi_q - [1]) = E(\mathbb{F}_q)[r]$ and $Q \in \mathbb{G}_2 = E\left(\overline{\mathbb{F}_q}\right)[r] \cap \text{ Ker}(\pi_q - [q])$. The Ate pairing is defined as follows:

Definition 2 *(The Ate pairing) The reduced Ate pairing is the map:*

$$\begin{aligned} e_A : \mathbb{G}_2 \times \mathbb{G}_1 &\to \mu_r, \\ (Q, P) \ &\mapsto f_{T,Q}(P)^{\frac{q^k-1}{r}}, \end{aligned}$$

where $T = t - 1$.

The following theorem gives some properties of Ate pairing, in particular its relation with the Tate pairing. This relation makes sense to Definition 2: Ate pairing is a power of the Tate pairing and therefore is a pairing. A complete proof can be found in [14]

Theorem 1 *[14] Let $N = gcd(T^k - 1, q^k - 1)$ and $T^k - 1 = LN$. We have*

- *$e_A(Q, P)^{rc} = (f_{r,Q}(P)^{(q^k-1)/r})^{LN}$ where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1}$ mod r.*
- *for $r \nmid L$, Ate pairing e_A is non-degenerate.*

Remark 1. The Tate pairing is defined on $\mathbb{G}_1 \times E(\mathbb{F}_{q^k})$, while Ate pairing is defined on $\mathbb{G}_2 \times \mathbb{G}_1$ with $\mathbb{G}_2 \subseteq E(\mathbb{F}_{q^k})$. This means that during the execution of the Miller algorithm in Ate pairing computation, the point addition is performed in an extension field of $\mathbb{F}_q$ whereas it was performed in $\mathbb{F}_q$ in the case of the Tate pairing. As the arithmetic over $\mathbb{F}_{q^k}$ is much more expensive than the arithmetic over $\mathbb{F}_q$, each step of Ate pairing is more expensive than a step of the Tate pairing. However the Miller loop length in the case of Ate pairing is $\log_2 T$ which is less (generally the half) than $\log_2 r$, the loop length for the Tate pairing.

Observe that if Ate pairing were defined on $\mathbb{G}_1 \times \mathbb{G}_2$, then it will be faster than the Tate pairing since its Miller loop length will be approximately halved. This remark yields to the definition of the twisted Ate pairing [14].

Definition 3 *(The twisted Ate pairing) [14] Assume that E has a twist of degree δ and $m = gcd(k, \delta)$. Let $e = k/m$ and $T_e = T^e$ mod r, then the reduced twisted Ate pairing is defined as follows:*

$$\begin{aligned} e_{T_e} : \mathbb{G}_1 \times \mathbb{G}_2 &\to \mu_r, \\ (P, Q) &\mapsto f_{T_e,P}(Q)^{\frac{q^k-1}{r}}. \end{aligned}$$

As in the case of Ate pairing, the following theorem ensures that e_{T_e} is a pairing.

Theorem 2 *[14]*

- *$e_{T_e}(P, Q)^{rc} = e_T(P, Q)^{LN}$ where $e_T(P, Q)$ is the Tate pairing and $c = \sum_{i=0}^{m-1} T^{e(m-1-i)} q^{ei} \equiv mq^{e(m-1)}$ mod r.*
- *for $r \nmid L$, twisted Ate pairing e_{T_e} is non-degenerate.*

Remark 2. The reduced Tate and twisted Ate pairings are defined on $\mathbb{G}_1 \times E(\mathbb{F}_{q^k})$ and $\mathbb{G}_1 \times \mathbb{G}_2$ respectively. So they have the same complexity for each iteration of the Miller algorithm but the Miller loop parameter is T^e mod r for the reduced twisted Ate pairing and r for the Tate pairing. Consequently, the twisted Ate pairing will be more efficient than the reduced Tate pairing only for curves with trace t such that T^e mod r is significatively less than r.

Optimal pairings. The reduction of Miller's loop length is an important way to improve the computation of pairings. The latest work is a generalized method to find the shortest loop when possible, which leads to the concept of optimal pairing [15]. Indeed, observe that if k is the embedding degree with respect to r, then $r|q^k - 1$ but $r \nmid q^i - 1$ for any $1 \leq i < k$. This implies that $r|\Phi_k(q)$ where Φ_k is the $k-th$ cyclotomic polynomial. Since $T \equiv q$ mod r where $T = t - 1$, we have $r|\Phi_k(T)$. More generally, if we consider Ate$-i$ pairing, which is a generalisation of Ate pairing with Miller function $f_{T_i,Q}$ where $T_i \equiv q^i$ mod r, then

$$r|\Phi_{k/g}(T_i), \text{ where } g = gcd(i, k)$$

so that the minimal value for T_i is $r^{1/\varphi(k/g)}$ (where φ is the Euler's totient function) and the lowest bound is $r^{1/\varphi(k)}$, obtained for $g = 1$. We then give the following definition of optimal pairing, this is a pairing that can be computed with the smallest number of iterations in the Miller loop.

Definition 4 *[15] Let $e : G_1 \times G_2 \longrightarrow G_T$ be a non-degenerate, bilinear pairing with $|G_1| = |G_2| = |G_T| = r$, where the field of definition of G_T is $\mathbb{F}_{q^k}$. e is called an optimal pairing if it can be evaluated with about at most $(\log_2 r)/\varphi(k) + \varepsilon(k)$ Miller iterations, where $\varepsilon(k)$ is less than $\log_2 k$.*

The lowest bound is attained for several families of elliptic curves. The following theorem gives the construction of an optimal pairing.

Theorem 3 *[15, Theorem 4] Let E be an elliptic curve defined over $\mathbb{F}_q$. The embedding degree with respect to a large integer r dividing the order of the group $\sharp E(\mathbb{F}_q)$ is denoted k. Let $\lambda = mr$ be a multiple of r such that $r \nmid m$ and write $\lambda = \sum_{i=0}^{l} c_i q^i$. Remember $h_{R,S}$ is the function with divisor $\mathrm{Div}(h_{R,S}) = (R) + (S) - (S+R) - (P_\infty)$ where R and S are two arbitrary points on the elliptic curve E. If $s_i = \sum_{j=i}^{l} c_j q^j$, the map $e_o : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$ defined as*

$$(Q, P) \longmapsto \left(\prod_{i=0}^{l} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{l-1} h_{[s_{i+1}]Q,[c_i q^i]Q}(P) \right)^{\frac{q^k-1}{r}}$$

defines a bilinear pairing. Furthermore, the pairing is non degenerate if

$$mkq^k \neq ((q^k - 1)/r) \cdot \sum_{i=0}^{l} i c_i q^{i-1} \ mod\ r.$$

In Section 5, we apply the previous theorem to provide an example of optimal pairing on Jacobi quartic curves of embedding degree 8. Observe that the computation of optimal pairings follows the same approach as the computation of the Ate pairing.

2.3 Use of Twists for Efficient Computation of Pairings

For the applications of twists, observe that the points input of the Tate pairing, Ate pairing, twisted Ate or optimal pairing on a curve of embedding degree k take the form $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$. In the case of the Tate pairing and the twisted Ate pairing, the evaluation of the Miller function is done at the point Q in the full extention $\mathbb{F}_{q^k}$ whereas in the case of Ate and Optimal Ate pairings, it is the addition of point that is performed there. In both cases, this can affect the efficiency of computations. However many authors (see for example [25] or [2]) have shown that one can use the isomorphism between the curve and its twist of degree δ to take the point Q in a particular form which allows to perform some computations more efficiently in the sub-field $\mathbb{F}_{q^{k/\delta}}$ instead of $\mathbb{F}_{q^k}$. More precisely, if E is an elliptic curve defined over $\mathbb{F}_q$, E' its twist of degree δ defined over $\mathbb{F}_{q^{k/\delta}}$ and $\psi : E' \longrightarrow E$ the isomorphism between E and E', then the point Q is taken as the image by ψ of a point on the twisted curve $E'(\mathbb{F}_{q^{k/\delta}})$. In this case, the present form of Q allows many computations either for additon of points or evaluation of the Miller functions to be done more efficiently in the subfield $\mathbb{F}_{q^{k/\delta}}$. For example in the present case of this work and from Proposition 1, instead of taking Q with full coordinates in $\mathbb{F}_{q^k}$, it can be taken in the form $[\omega X : Y : Z]$ where $X, Y, Z \in \mathbb{F}_{q^{k/4}}$. In this work, we use this technic for the computation of the Tate, Ate, twisted Ate and Optimal pairings. As a consequence, the twists can be use to eliminate the denominator of the function $h_{R,S}$ in the Miller algorithm. See Section 3.1 for applications.

3 The Tate Pairing and Twisted Ate Pairing Computation on $E_d : Y^2 = dX^4 + Z^4$

Wang et al. in [3] considered pairings on Jacobi quartics and gave the geometric interpretation of the group law. We use a different way, namely the birational equivalence between Jacobi quartic curves and Weierstrass curves, of obtaining the formulas. We specialise to the particular curves $E_d : Y^2 = dX^4 + Z^4$ to obtain better results for these up to 39% improvement compared to results in [3]. The results in this section are from [1].

Given two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on the Weierstrass curve $W_d : y^2 = x^3 - 4dx$ such that $P_3 = (x_3, y_3) = P_1 + P_2$, consider $R = [X_1 : Y_1 : Z_1]$, $S = [X_2 : Y_2 : Z_2]$ and $[X_3 : Y_3 : Z_3] = [X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]$ the corresponding points on the Jacobi quartic E_d. To derive the Miller function $h_{R,S}(X, Y, Z)$ for E_d, we first write the Miller function $h_{P_1,P_2}(x, y)$ on the Weierstrass curve W_d:

$$h_{P_1,P_2}(x, y) = \frac{y - \lambda x - \alpha}{x - x_3},$$

where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ if $P_1 \neq P_2$, $\lambda = \dfrac{3x_1^2 - 4d}{2y_1}$ if $P_1 = P_2$ and $\alpha = y_1 - \lambda x_1$.

Using the birational equivalence, the Miller function for the Jacobi quartic $E_d : Y^2 = dX^4 + Z^4$ is given by $h_{R,S}(X, Y, Z) = h_{P_1,P_2}(\varphi(X, Y, Z))$. We have:

$$h_{R,S}(X, Y, Z) = \frac{4X_3^2X^2}{2X_3^2(Y + Z^2) - 2X^2(Y_3 + Z_3^2)} \left(\frac{ZY+Z^3}{X^3} - \frac{1}{2}\lambda\left(\frac{Y + Z^2}{X^2}\right) - \frac{\alpha}{4}\right).$$

where

$$\lambda = \begin{cases} \dfrac{-2X_1^3Z_2(Y_2 + Z_2^2) + 2X_2^3Z_1(Y_1 + Z_1^2)}{X_1X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]} & \text{if } P_1 \neq P_2, \\ \dfrac{Y_1 + 2Z_1^2}{X_1Z_1} & \text{if } P_1 = P_2, \end{cases} \tag{2}$$

and

$$\alpha = \begin{cases} \dfrac{-4(Y_1 + Z_1^2)(Y_2 + Z_2^2)(Z_2X_1 - Z_1X_2)}{X_1X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]} & \text{if } P_1 \neq P_2, \\ \dfrac{-2Y_1(Y_1 + Z_1^2)}{X_1^3Z_1} & \text{if } P_1 = P_2. \end{cases} \tag{3}$$

Remark 3. It is simple to verify that our formulas obtained by change of variables is exactly the same result obtained by Wang et al. in [3] using the geometric interpretation of the group law.

Indeed, by setting $x_1 = \frac{X_1}{Z_1}$, $x_2 = \frac{X_2}{Z_2}$, $y_1 = \frac{Y_1}{Z_1^2}$ and $y_2 = \frac{Y_2}{Z_2^2}$ in their Miller function obtained for the curve $E_{d,\mu} : y^2 = dx^4 + 2\mu x + 1$ (by taking $\mu = 0$), we get exactly the same result that we found above. However, we take an advantage based on our coordinates system to obtain more efficient formulas in pairings computation.

The correctness of the formulas in this work can be checked at
`http://www.prmais.org/Implementation-Pairings-Jacobi.txt`.

3.1 Simplification of the Miller Function

We apply the twist technique described in Section 2.3 to the present case of quartic twist (see the isomorphism in Proposition 1). This enables the point Q in the Tate and twisted Ate pairings computation to be chosen as $[\omega X_Q : Y_Q : Z_Q]$ or $[x_Q\omega : y_Q : 1]$ in affine coordinates where X_Q, Y_Q, Z_Q, x_Q and y_Q are in $\mathbb{F}_{q^{k/4}}$. Thus

$$h_{R,S}(x_Q\omega, y_Q, 1) = \frac{2X_3^2 x_Q^2 \omega^2}{X_3^2(y_Q+1) - x_Q^2\omega^2(Y_3+Z_3^2)} \left(-\tfrac{1}{2}\lambda \left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2 + \left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega - \frac{\alpha}{4}\right).$$

Write $-\frac{\alpha}{4} = \frac{A}{D}$ and $-\frac{1}{2}\lambda = \frac{B}{D}$ then

$$h_{R,S}(x_Q\omega, y_Q, 1) = \frac{2X_3^2 x_Q^2 \omega^2}{D(X_3^2(y_Q+1) - x_Q^2\omega^2(Y_3+Z_3^2))} \left(B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2 + D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega + A\right).$$

We can easily see that the denominator $D(X_3^2(y_Q+1) - x_Q^2\omega^2(Y_3+Z_3^2))$ and the factor $2X_3^2x_Q^2\omega^2$ of $h_{R,S}$ belong to $\mathbb{F}_{q^{k/2}}$. As $q^{k/2}-1$ divides q^k-1, they are sent to 1 during the final exponentiation (last step in the Algorithm 1). So they can be discarded in pairing computation and we only have to evaluate

$$\tilde{h}_{R,S}(x_Q\omega, y_Q, 1) = B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)\omega^2 + D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)\omega + A.$$

Since $Q = (x_Q\omega, y_Q, 1)$ is fixed during pairing computation, the quantities $\frac{y_Q+1}{x_Q^3\omega^4}$ and $\frac{y_Q+1}{x_Q^2\omega^4}$ can be precomputed in $\mathbb{F}_{q^{k/4}}$, once for all steps. Note that each of the multiplications $D\left(\frac{y_Q+1}{x_Q^3\omega^4}\right)$ and $B\left(\frac{y_Q+1}{x_Q^2\omega^4}\right)$ costs $\frac{k}{4}m_1$, since $A, B, D \in \mathbb{F}_q$.

Efficient computation of the main multiplication in Miller's algorithm Depending on the form of the function $\tilde{h}_{R,S}$ and the field $\mathbb{F}_{q^k}$, the main multiplication in Miller's algorithm which enables to update the function f can be done efficiently. In this work, the expression of $\tilde{h}_{R,S}$ has a nice form: the term ω^3 is absent and $A \in \mathbb{F}_q$. So, The multiplication by $\tilde{h}_{R,S}$ will be more efficient than the multiplication with an ordinary element of $\mathbb{F}_{q^k}$ (which is denoted m_k)

- If the schoolbook multiplication is used for the multiplication in $\mathbb{F}_{q^k}$, the cost of the multiplication by $\tilde{h}_{R,S}$ is not m_k but $\left(\frac{1}{k}+\frac{1}{2}\right)m_k$. See Appendix A for details.

- if we are using pairing friendly fields for elliptic curves with quartic twists, the embedding degree will be of the form $k = 2^i$ (see [25]). Then we follow [26] and the cost of a multiplication or a squaring in the field $\mathbb{F}_{q^k}$ is 3^i multiplications or squaring in $\mathbb{F}_q$ using Karatsuba multiplication method. Thus, the cost of a multiplication by $\tilde{h}_{R,S}$ is $\left(\frac{2\cdot 3^{i-1}+2^{i-1}}{3^i}\right)m_k$. See Appendix A for details.

In the following of this section β stands for $\frac{1}{k} + \frac{1}{2}$ or $\frac{2 \cdot 3^{i-1} + 2^{i-1}}{3^i}$ so that the cost of the multiplication of the function f in the Miller algorithm by $\tilde{h}_{R,S}$ is βm_k instead of m_k for an ordinary multiplication in $\mathbb{F}_{q^k}$.
In what follows, we will compute A, B and D. For efficiency the point is represented by $(X : Y : Z : X^2 : Z^2)$ with $Z \neq 0$. This is the first time that this representation is used when $d \neq 1$. Thus we will use the points $P_1 = (X_1 : Y_1 : Z_1 : U_1 : V_1)$ and $P_2 = (X_2 : Y_2 : Z_2 : U_2 : V_2)$ where $U_i = X_i^2$, $V_i = Z_i^2$, $i = 1, 2$.

Remark 4. Note that if X^2 and Z^2 are known, then expressions of the form XZ can be computed using the formula $((X + Z)^2 - X^2 - Z^2)/2$. This allows the replacement of a multiplication by a squaring presuming a squaring and three additions are more efficient than a multiplication. The operations concerned with this remark are followed by $*$ in Tables 1 and 2.

3.2 Doubling Step in the Miller Algorithm

When $P_1 = P_2$, from Equations (2) and (3), we have

$$\begin{aligned} A &= Y_1(Y_1 + Z_1^2), \\ B &= -X_1^2(Y_1 + 2Z_1^2), \\ D &= 2X_1^3 Z_1. \end{aligned}$$

The computation of A, B, D and the point doubling can be done using the algorithm in Table 1 with $3m_1 + 7s_1 + 1mc$ (or $4m_1 + 6s_1 + 1mc$ according to the Remark 4). Thus, the doubling step in the Miller algorithm requires a total of $\beta m_k + 1s_k + \left(\frac{k}{2} + 3\right) m_1 + 7s_1 + 1mc$ (or $\beta m_k + 1s_k + \left(\frac{k}{2} + 4\right) m_1 + 6s_1 + 1mc$).

Operations	*Values*	*Cost*
$U := U_1^2$	$U = X_1^4$	$1s_1$
$V := V_1^2$	$V = Z_1^4$	$1s_1$
$Z_3 := V - dU$	$Z_3 = Z_1^4 - dX_1^4$	$1mc$
$E := ((X_1 + Z_1)^2 - U_1 - V_1)/2 \quad *$	$E = X_1 Z_1$	$1s_1$ (or $1m_1$)
$D := 2U_1 E$	$D = 2X_1^3 Z_1$	$1m_1$
$A := (2Y_1 + V_1)^2/4 - U$	$A = Y_1(Y_1 + Z_1^2)$	$1s_1$
$B := -U_1(Y_1 + 2V_1)$	$B = -X_1^2(Y_1 + 2Z_1^2)$	$1m_1$
$X_3 := 2EY_1$	$X_3 = 2X_1 Y_1 Z_1$	$1m_1$
$V_3 := Z_3^2$	$V_3 = Z_3^2$	$1s_1$
$Y_3 := 2V - Z_3$	$Y_3 = dX_1^4 + Z_1^4 = Y_1^2$	-
$Y_3 := 2Y_3^2 - V_3$	$Y_3 = 2Y_1^4 - Z_3^2$	$1s_1$
$U_3 := X_3^2$	$U_3 = X_3^2$	$1s_1$
Total cost: $3m_1 + 7s_1 + 1mc$ (or $4m_1 + 6s_1 + 1mc$)		

Table 1. Combined formulas for the doubling step.

3.3 Addition step in the Miller algorithm

When $P_1 \neq P_2$, from Equations (2) and (3), we have

$$\begin{aligned} A &= (Y_1 + Z_1^2)(Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1), \\ B &= X_1^3Z_2(Y_2 + Z_2^2) - X_2^3Z_1(Y_1 + Z_1^2), \\ D &= X_1X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]. \end{aligned}$$

Using the algorithm in Table 2 the computation of A, B, D and the point addition can be done in $12m_1 + 11s_1 + 1mc$ (or $18m_1 + 5s_1 + 1mc$ according to Remark 4). Applying mixed addition ($Z_2 = 1$) which can always be done in our case, this cost is reduced to $12m_1 + 7s_1 + 1mc$ (or $15m_1 + 4s_1 + 1mc$).

Operations	*Values*	*Cost*
$U := Y_1 + V_1$	$U = Y_1 + Z_1^2$	-
$V := Y_2 + V_2$	$V = Y_2 + Z_2^2$	-
$R := ((Z_2 + X_1)^2 - V_2 - U_1)/2$ *	$R = Z_2X_1$	$1s_1$ (or $1m_1$)
$S := ((Z_1 + X_2)^2 - V_1 - U_2)/2$ *	$S = Z_1X_2$	$1s_1$ (or $1m_1$)
$A := S - R$	$A = Z_1X_2 - Z_2X_1$	-
$A := AV$	$A = (Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1)$	$1m_1$
$A := AU$	$A = (Y_1 + Z_1^2)(Y_2 + Z_2^2)(Z_1X_2 - Z_2X_1)$	$1m_1$
$U := U_2U$	$U = X_2^2(Y_1 + Z_1^2)$	-
$V := U_1V$	$V = X_1^2(Y_2 + Z_2^2)$	$1m_1$
$B := RV - SU$	$B = X_1^3Z_2(Y_2 + Z_2^2) - X_2^3Z_1(Y_1 + Z_1^2)$	$2m_1$
$D := ((X_1 + X_2)^2 - U_1 - U_2)/2$ *	$D = X_1X_2$	$1s_1$ (or $1m_1$)
$E := dD^2$	$E = d(X_1X_2)^2$	$1mc + 1s_1$
$D := D(U - V)$	$D = X_1X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]$	$1m_1$
$X_3 := (R + S)(R - S)$	$X_3 = X_1^2Z_2^2 - Z_1^2X_2^2$	$1m_1$
$W_1 := ((X_1 + Z_1)^2 - U_1 - V_1)/2$ *	$W_1 = X_1Z_1$	$1s_1$ (or $1m_1$)
$W_2 := ((X_2 + Z_2)^2 - U_2 - V_2)/2$ *	$W_2 = X_2Z_2$	$1s_1$ (or $1m_1$)
$Z_3 := W_1Y_2 - W_2Y_1$	$Z_3 = X_1Z_1Y_2 - X_2Z_2Y_1$	$2m_1$
$U := Y_1Y_2$	$U = Y_1Y_2$	$1m_1$
$V := ((Z_1 + Z_2)^2 - V_1 - V_2)/2$ *	$V = Z_1Z_2$	$1s_1$ (or $1m_1$)
$V := V^2 + E$	$V = (Z_1Z_2)^2 + d(X_1X_2)^2$	$1s_1$
$E := (R - S)^2$	$E = (X_1Z_2 - X_2Z_1)^2$	$1s_1$
$U_3 := X_3^2$	$U_3 = X_3^2$	$1s_1$
$V_3 := Z_3^2$	$V_3 = Z_3^2$	$1s_1$
$Y_3 := E(U + V) - V_3$	$Y_3 = (X_1Z_2 - X_2Z_1)^2(Y_1Y_2 + (Z_1Z_2)^2 +$ $d(X_1X_2)^2) - Z_3^2$	$1m_1$
Total cost: $12m_1 + 11s_1 + 1mc$ (or $18m_1 + 5s_1 + 1mc$)		

Table 2. Combined formulas for the addition step.

Thus, the addition step in the Miller algorithm requires a total of $\beta m_k + \left(\frac{k}{2} + 12\right) m_1 + 7s_1 + 1mc$ (or $\beta m_k + \left(\frac{k}{2} + 15\right) m_1 + 4s_1 + 1mc$).

3.4 Comparison

The comparison of results is summarized in Table 3 and Table 4. The costs presented are for one iteration of the Miller algorithm and are both for the Tate and twisted Ate pairings and curves with a quartic twist. In each case, we also present an example of comparison in the cases $k = 8$ and $k = 16$ since these values are the most appropriate for cryptographic applications when a quartic twist is used [25]. In Table 3, we assume that Schoolbook multiplication method is used for the arithmetic in the extension fields $\mathbb{F}_{q^k}$.

Curves	Doubling		Mixed Addition	
Weierstrass (b=0)[2]	$1m_k + 1s_k + (\frac{k}{2} + 2)m_1 + 8s + 1mc$		$1m_k + (\frac{k}{2} + 9)m_1 + 5s_1$	
Jacobi quartic (a=0)[3]	$1m_k + 1s_k + (\frac{k}{2} + 5)m_1 + 6s_1$		$1m_k + (\frac{k}{2} + 16)m_1 + 1s_1 + 1mc$	
This work	$(\frac{1}{k} + \frac{1}{2})m_k + 1s_k + (\frac{k}{2} + 3)m_1 + 7s_1 + 1mc$		$(\frac{1}{k} + \frac{1}{2})m_k + (\frac{k}{2} + 12)m_1 + 7s_1 + 1mc$	
Example 1	$k = 8$	$m_1 = s_1 = mc$	$k = 8$	$m_1 = s_1 = mc$
Weierstrass (b=0)[2]	$98m_1 + 16s_1 + 1mc$	$115m_1$	$77m_1 + 5s_1$	$82m_1$
Jacobi quartic (a=0)[3]	$101m_1 + 14s_1$	$115m_1$	$84m_1 + 1s_1 + 1mc$	$86m_1$
This work	$75m_1 + 15s_1 + 1mc$	$91m_1$	$57m_1 + 6s_1 + 1mc$	$64m_1$
Example 2	$k = 16$	$m_1 = s_1 = mc$	$k = 16$	$m_1 = s_1 = mc$
Weierstrass (b=0)[2]	$386m_1 + 24s_1 + 1mc$	$407m_1$	$273m_1 + 5s_1$	$278m_1$
Jacobi quartic (a=0)[3]	$389m_1 + 22s_1$	$411m_1$	$280m_1 + 1s_1 + 1mc$	$282m_1$
This work	$275m_1 + 23s_1 + 1mc$	$299m_1$	$144m_1 + 27s_1 + 1mc$	$172m_1$

Table 3. Comparison of our Tate and twisted Ate pairings formulas with the previous fastest formulas using Schoolbook multiplication method

Remark 5. If we assume that $m_1 = s_1 = mc$ and $k = 16$ then we obtain in this work a theoretical gain of 26% and 27% with respect to Weierstrass curves and previous work on Jacobi quartic curves for the doubling step. Similarly, for the addition step we obtain a theoretical gain of 38% and 39% over Weierstrass and Jacobi quartic curves respectively. In the case $k = 8$, the theoretical gain is 22% and 26% with respect to Weierstrass curves and Jacobi quartic curves for the addition step and 26% for the doubling step, see Table 3.

In Table 4, we assume that Karatsuba method is used for the arithmetic in $\mathbb{F}_{q^k}$ for curves with $k = 2^i$.

Remark 6. We assume again that $m_1 = s_1 = mc$. For $k = 8$ and for the doubling step we obtain a theoretical gain of 8% over Weierstrass curves and Jacobi quartic curves (a=0)[3]. For the addition step, the improvement is up to 6% over the result on Jacobi quartic curves in [3]. When $k = 16$ the gain is 11% for the doubling step over Weierstrass curves. The improvement is 16% in addition step over Jacobi quartic curves, see Table 4.

Remark 7. The security and the efficiency of pairing-based systems requires using pairing-friendly curves. The Jacobi models of elliptic curves studied in this

Curves	Doubling		Mixed Addition	
Weierstrass (b=0)[2]	$1m_k + 1s_k + (\frac{k}{2} + 2)m_1 + 8s + 1mc$		$1m_k + (\frac{k}{2} + 9)m_1 + 5s_1$	
Jacobi quartic (a=0)[3]	$1m_k + 1s_k + (\frac{k}{2} + 5)m_1 + 6s_1$		$1m_k + (\frac{k}{2} + 16)m_1 + 1s_1 + 1mc$	
This work	$\left(\frac{2\cdot 3^{i-1}+2^{i-1}}{3^i}\right) m_k + 1s_k + (\frac{k}{2} + 3)m_1 + 7s_1 + 1mc$		$\left(\frac{2\cdot 3^{i-1}+2^{i-1}}{3^i}\right) m_k + (\frac{k}{2} + 12)m_1 + 7s_1 + 1mc$	
Example 1	$k = 8$	$m_1 = s_1 = mc$	$k = 8$	$m_1 = s_1 = mc$
Weierstrass (b=0)[2]	$33m_1 + 35s_1 + 1mc$	$69m_1$	$40m_1 + 5s_1$	$45m_1$
Jacobi quartic (a=0)[3]	$36m_1 + 33s_1$	$69m_1$	$47m_1 + 1s_1 + 1mc$	$49m_1$
This work	$29m_1 + 34s_1 + 1mc$	$64m_1$	$38m_1 + 7s_1 + 1mc$	$46m_1$
Example 2	$k = 16$	$m_1 = s_1 = m_c$	$k = 16$	$m_1 = s_1 = m_c$
Weierstrass (b=0)[2]	$91m_1 + 89s_1 + 1mc$	$181m_1$	$98m_1 + 5s_1$	$103m_1$
Jacobi quartic (a=0)[3]	$94m_1 + 87s_1$	$181m_1$	$105m_1 + 1s_1 + 1mc$	$107m_1$
This work	$73m_1 + 88s_1 + 1mc$	$162m_1$	$82m_1 + 7s_1 + 1mc$	$90m_1$

Table 4. Comparison of our formulas for theTate and twisted Ate pairings with the previous fastest formulas using Karatsuba multiplication method.

work are isomorphic to Weierstrass curves. Thus we can obtain pairing friendly curves of such models using the construction given by Galbraith et al.[27] or by Freeman et al.[25]. Some examples of pairing friendly curves of Jacobi quartic form can be found in [3].

4 Formulas for Ate Pairing and Optimal Pairing on the Jacobi Quartic Elliptic Curve $Y^2 = dX^4 + Z^4$

In this section, we extend the results of the previous section to the computation of Ate pairing and optimal pairing. Our results show that among known curves with quartic twists, the Jacobi model $Y^2 = dX^4 + Z^4$ offers the best performances for these different pairings. The section is divided as follows: In Section 4.1, we rewrite the Miller function and the addition formulas for Ate and optimal pairings. In Section 4.2 we give the cost of Ate pairing. The Section 4.3 is devoted to a comparative study of these pairings on the curves of Jacobi and Weierstrass forms.

4.1 Ate Pairing Computation on $E_d : Y^2 = dX^4 + Z^4$

According to the definition of Ate and optimal pairing, the point addition and point doubling are performed in $\mathbb{F}_{q^k}$. But thanks to the twist we will consider the points $[\omega X_i : Y_i : Z_i]$ where X_i, Y_i and Z_i belong to $\mathbb{F}_{q^{k/4}}$, $i = 1, 2, 3$ (see Proposition 1). We also know that for Ate and optimal pairings the point P is fixed during computations and has its coordinates in the base field $\mathbb{F}_q$. Thus this point can be taken as $[x_P : y_P : 1]$.

Point addition and point doubling on $\boldsymbol{E_d}$ for Ate and optimal pairings. We rewrite here formulas for point doubling and point addition on the curve E_d from those in Section 2.1 with the difference that points have the form $[\omega X_i : Y_i : Z_i]$ where X_i, Y_i and Z_i belong to $\mathbb{F}_{q^{k/4}}$, $i = 1, 2, 3$.

Doubling. $[\omega X_3 : Y_3 : Z_3] = 2[\omega X_1 : Y_1 : Z_1]$ such that

$$\begin{aligned} X_3 &= 2X_1Y_1Z_1, \\ Z_3 &= Z_1^4 - dX_1^4\omega^4, \\ Y_3 &= 2Y_1^4 - Z_3^2. \end{aligned}$$

Addition. $[\omega X_3 : Y_3 : Z_3] = [\omega X_1 : Y_1 : Z_1] + [\omega X_2 : Y_2 : Z_2]$ such that

$$\begin{aligned} X_3 &= X_1^2Z_2^2 - Z_1^2X_2^2, \\ Z_3 &= X_1Z_1Y_2 - X_2Z_2Y_1, \\ Y_3 &= (X_1Z_2 - X_2Z_1)^2(Y_1Y_2 + (Z_1Z_2)^2 + d\omega^4(X_1X_2)^2) - Z_3^2. \end{aligned}$$

The Miller function for Ate and optimal pairings computation on $\boldsymbol{E_d}$. The Miller function on the Jacobi quartic E_d is given in Section 3:

$$h_{R,S}(X,Y,Z) = \frac{4X_3^2X^2}{2X_3^2(Y+Z^2) - 2X^2(Y_3+Z_3^2)}\left(\frac{ZY+Z^3}{X^3} - \frac{1}{2}\lambda\left(\frac{Y+Z^2}{X^2}\right) - \frac{\alpha}{4}\right).$$

We follow the notations of Section 3.1 by setting $-\dfrac{\alpha}{4} = \dfrac{A}{D}$ and $-\dfrac{1}{2}\lambda = \dfrac{B}{D}$. When we replace $[X_i : Y_i : Z_i]$ by $[\omega X_i : Y_i : Z_i]$ and $[X : Y : Z]$ by $[x_P : y_P : 1]$, a carefully calculation yields to:

$$h_{R,S}(x_P, y_P, 1) =$$
$$\frac{2X_3^2x_P^2}{D\omega^2[X_3^2(y_P+1) - x_P^2(Y_3+Z_3^2)]}\left(B\left(\tfrac{y_P+1}{x_P^2}\right)\omega^3 + A\omega + D\omega^4\left(\tfrac{y_P+1}{x_P^3}\right)\right).$$

The factors A, B and D are exactly the same as in the case of the Tate pairing but with the main difference that they are in $\mathbb{F}_{q^{k/4}}$ instead of $\mathbb{F}_q$. The addition and doubling formulas for $(\omega X_i : Y_i : Z_i)$ where X_i, Y_i and Z_i belong to $\mathbb{F}_{q^{k/4}}$, $i = 1, 2, 3$ clearly show that X_3^2 and $Y_3 + Z_3^2$ are also in $\mathbb{F}_{q^{k/4}}$ such that $\dfrac{2X_3^2x_P^2}{D\omega^2[X_3^2(y_P+1) - x_P^2(Y_3+Z_3^2)]} \in \mathbb{F}_{q^{k/2}}$. Then it can be discarded in pairing computation thanks to the final exponentiation, as we explained in the case of the Tate pairing. Thus we only have to evaluate

$$\bar{h}_{R,S}(x_P, y_P, 1) = B\left(\frac{y_P+1}{x_P^2}\right)\omega^3 + A\omega + D\omega^4\left(\frac{y_P+1}{x_P^3}\right).$$

Since $P = (x_P, y_P, 1)$ is fixed during pairing computation, the quantities $\dfrac{(y_P+1)}{x_P^3}$ and $\dfrac{(y_P+1)}{x_P^2}$ can be precomputed in $\mathbb{F}_q$ once for all steps. Note that each of the multiplications $D\left(\dfrac{y_P+1}{x_P^3}\right)$ and $B\left(\dfrac{y_P+1}{x_P^2}\right)$ costs $\dfrac{k}{4}m_1$.

Remark 8. We can use the fact that in the expression of $\bar{h}$ the term ω^2 is absent. In this case, in Miller's algorithm, the cost of the main multiplication in $\mathbb{F}_{q^k}$ is not $1m_k$ but $(3/4)m_k$ if we use schoolbook method and is $(8/9)m_k$ if we use Karatsuba multiplication with pairing friendly curves, i.e $k = 2^i$. See Appendix B for details.

Remark 9. Since the coefficients of the Miller function for Ate pairing are the same as for the Tate pairing, these coefficients and points operations can be computed in the same manner it was done in the previous section with the main difference that computations are done in $\mathbb{F}_{q^{k/4}}$.

4.2 Cost of Ate and Optimal Pairing on E_d

In Table 5 and Table 6, we summarise and compare the costs for one iteration for both Ate and optimal Ate pairings on the Jacobi curve $E_d : Y^2 = dX^4 + Z^4$ and on the Weierstrass curve $W_d : y^2 = x^3 - 4dx$. We also present these costs in the cases of elliptic curves of embedding degrees 8 and 16.
In Table 5 we assume that computations are made in $\mathbb{F}_{q^k}$ using schoolbook method.

Pairings	Doubling		Mixed Addition	
Ate(Q,P) Weierstrass (b=0)[2]	$1m_k + 1s_k + 2m_e + 8s_e +$ $2em_1 + 1mc$		$1m_k + 9m_e + 5s_e + 2em_1$	
Ate(Q,P) **(This work)**	$3/4m_k + 1s_k + 3m_e + 7s_e +$ $2em_1 + 1mc$		$3/4m_k + 12m_e + 7s_e +$ $2em_1 + 1mc$	
Example 1	$k = 8$	$m_1 = s_1 = mc$	$k = 8$	$m_1 = s_1 = mc$
Ate(Q,P) Weierstrass (b=0)[2]	$112m_1 + 24s_1 + 1mc$	$137m_1$	$109m_1 + 10s_1$	$119m_1$
This work	$99m_1 + 22s_1 + 1mc$	$122m_1$	$107m_1 + 14s_1 + 1mc$	$122m_1$
Example 2	$k = 16$	$m_1 = s_1 = m_c$	$k = 16$	$m_1 = s_1 = m_c$
Ate(Q,P) Weierstrass (b=0)[2]	$464m_1 + 48s_1 + 1mc$	$513m_1$	$438m_1 + 20s_1$	$458m_1$
This work	$410m_1 + 44s_1 + 1mc$	$455m_1$	$430m_1 + 28s_1 + 1mc$	$459m_1$

Table 5. Comparisons of Ate and optimal Ate pairings formulas on Jacobi quartic and Weierstrass elliptic curves using Schoolbook method

In Table 6 we assume that computations are made in $\mathbb{F}_{q^k}$ using Karatsuba method.

Remark 10. If we assume that $m_1 = s_1 = mc$ and Schoolbook multiplication method is used then for Ate pairing computation we obtain in this work a theoretical gain of 11% with respect to Weierstrass curves for the doubling step. The improvement is 4% when Karatsuba method is used. Our addition step is not better. See Table 5 and Table 6.

4.3 Comparison

Let us now compare different pairings on Jacobi quartic curves and Weierstrass elliptic curves with quartic twists. Especially we determine the operation counts

Pairings	Doubling		Mixed Addition	
Ate(Q,P) Weierstrass (b=0)[2]	$1m_k + 1s_k + 2m_e + 8s_e + 2em_1 + 1mc$		$1m_k + 9m_e + 5s_e + 2em_1$	
Ate(Q,P) **(This work)**	$8/9m_k + 1s_k + 3m_e + 7s_e +$ $2em_1 + 1mc$		$8/9m_k + 12m_e + 7s_e +$ $2em_1 + 1mc$	
Example 1	$k = 8$	$m_1 = s_1 = mc$	$k = 8$	$m_1 = s_1 = mc$
Ate(Q,P) Weierstrass (b=0)[2]	$37m_1 + 51s_1 + 1mc$	$89m_1$	$58m_1 + 15s_1$	$73m_1$
Ate(Q,P) **This work**	$37m_1 + 48s_1 + 1mc$	$85m_1$	$64m_1 + 21s_1 + 1mc$	$86m_1$
Example 2	$k = 16$	$m_1 = s_1 = m_c$	$k = 16$	$m_1 = s_1 = m_c$
Ate(Q,P) Weierstrass (b=0)[2]	$107m_1 + 153s_1 + 1mc$	$261m_1$	$170m_1 + 45s_1$	$215m_1$
Ate(Q,P)**This work**	$107m_1 + 144s_1 + 1mc$	$252m_1$	$188m_1 + 63s_1 + 1mc$	$252m_1$

Table 6. Comparisons of Ate and optimal Ate pairings formulas on Jacobi quartic and Weierstrass elliptic curves using Karatsuba method

for the Tate, twisted Ate, Ate and optimal Ate pairings in a full loop of Miller's algorithm, based on the fastest operations counts summarized in Tables 3, 4, 5 and 6. We suppose that we are in the context of optimized pairing such that we can restricted ourselves to the cost of the doubling step. Indeed, in this case r is chosen to have a lower Hamming weight such that the computation in Miller algorithm can be done quickly by skipping many addition steps. For elliptic curves with embedding degrees $k = 8$, we consider the parameters for 112 bits and 128 bits security level. We also consider elliptic curves with embedding degrees $k = 16$ at 128 bits and 192 bits security levels. These values have been selected such that we obtain approximately the same security level both in the elliptic curve defined over the base field $\mathbb{F}_q$ and in the multiplicative group of the finite field $\mathbb{F}_{q^k}$.
For these parameters we give the approximate number of operations in the base field for all the Miller iterations. For the Miller loop in Ate pairing computation we consider an average trace $t \sim \sqrt{q}$. For the values in Table 7, we assume that $m_1 = s_1 = mc$. The rows with abbreviation **Kar** means that the values in these rows are obtained using Karatsuba multiplication method whereas the rows started with **Sco** means that the values in these rows are obtained using schoolbook multiplication method. W and J stand for Weierstrass [2] and Jacobi elliptic (this work) curves models respectively, since this work is the first that present the computation of Ate pairing and its variations on Jacobi elliptic curves.

From the values in Table 7 we draw the following observation: The different pairings computed in this work are always faster in the Jacobi quartic elliptic curves with respect to the Weierstrass elliptic curves. The gain obtained is up to 27% and depends on the method used for multiplications and the security level.

			Tate		twisted Ate		Ate		Optimal Ate	
Parameters	Sec. levels	Arith. in $\mathbb{F}_{q^k}$	W [2]	J (This work)	W [2]	J (This work)	W [2]	J (This work)	W [2]	J (This work)
$k = 8, r \approx 2^{224}$ $q \approx 2^{336}$	112	Kar.	15456	14336	23184	21504	14952	14448	4984	4816
		Sco.	25760	20384	38640	30576	23016	20496	7672	6832
$k = 8, r \approx 2^{256}$ $q \approx 2^{384}$	128	Kar.	17664	16384	26496	24576	17088	16512	5696	5504
		Sco.	29440	23296	44160	34944	26304	23424	8768	7808
$k = 16, r \approx 2^{256}$ $q \approx 2^{320}$	128	Kar.	46336	41472	115840	103680	41760	40320	8352	8064
		Sco.	105216	76544	263040	191360	82080	72800	16416	14560
$k = 16, r \approx 2^{384}$ $q \approx 2^{480}$	192	Kar.	69504	62208	173760	155520	62640	60480	12528	12096
		Sco.	157824	114816	394560	287040	123120	109200	24624	21840

Table 7. Comparison of the cost of the various Miller algorithms for pairings on Jacobi quartic curves and Weierstrass curves: $s_1 = m_1 = mc$

5 Implementation and Example

In this section we consider the familly of elliptic curves of embedding degree 8 described in [28] to verify our formulas and to implement the Tate, Ate and optimal Ate pairings. This familly of curves has the following parameters:

$$\begin{aligned}
r &= 82x^4 + 108x^3 + 54x^2 + 12x + 1,\\
q &= 379906x^6 + 799008x^5 + 705346x^4 + 333614x^3 + 88945x^2 + 12636x + 745,\\
t &= -82x^3 - 108x^2 - 54x - 8.
\end{aligned}$$

For $x = 24000000000010394$, the values of r, q, the trace t and the curve coefficient d are:

$$\begin{aligned}
r =\ & 272056320000471307161600306182614014808404525177076771934828454 76\\
& 817,\\
q =\ & 726011672004446604951703464791789328991217313776602768811505320697\\
& 5815675478784229870364764019632259 0069,\\
d =\ & 453757295002779128094814665494868330619510821110376730507190825 4359\\
& 884797174240143668977977512270161 8793,\\
t =\ & -1133568000001472850432000637893917136092090964291460.
\end{aligned}$$

We recall that $\mathbb{G}_1 = E(\mathbb{F}_q)[r]$ and $\mathbb{G}_2 = E\left(\overline{\mathbb{F}_q}\right)[r] \cap \text{Ker}(\pi_q - [q])$. To obtain an optimal pairing in the Jacobi quartic curve E_d with embedding degree 8, we follow the approach described by Vercauteren in [15]. Applying the `ShortestVectors()` function in Magma [29] to the lattice

$$L = \begin{pmatrix} r & 0\,0\,0 \\ -q & 1\,0\,0 \\ -q^2 & 0\,1\,0 \\ -q^3 & 0\,0\,1 \end{pmatrix},$$

we obtain the following vector

$$V = [c_0, c_1, c_2, c_3] = [x, 0, 0, 3x + 1].$$

An optimal pairing is then given by:

$$\begin{aligned}
e_o : \mathbb{G}_2 \times \mathbb{G}_1 \rightarrow &\qquad \mu_r\\
(Q, P) \ \mapsto &\left(f_{x,Q}^{3q^3+1}(P) \cdot H_1\right)^{\frac{q^8-1}{r}},
\end{aligned}$$

where $H_1 = (\overline{h}_{[x]Q,[x]Q}(P) \cdot \overline{h}_{[x]Q,[2x]Q}(P) \cdot \overline{h}_{[3x]Q,[1]Q}(P))^{q^3}$ and $s_1 = (3x+1)q^3$. Indeed, this is a straightforward application of Theorem 3. From that theorem we have $c_0 = x, c_1 = c_2 = 0, c_3 = 3x+1$ and $s_i = \sum_{j=i}^{3} c_j q^j$. Observe that for our example $s_1 = s_2 = s_3 = c_3 q^3 = (3x+1)q^3$. We then apply Theorem 3 to obtain the following

$$e_o(Q,P) = \left(f_{x,Q}(P) \cdot f_{3x+1,Q}^{q^3}(P) \cdot h_{[s_1]Q,[x]Q}(P) \cdot h^2_{[s_1]Q,P_\infty}(P) \right)^{\frac{q^8-1}{r}} .$$

Observe also that $f_{1,Q} = 1$ and $h^2_{[s_1]Q,P_\infty}(P) = 1$. Also, $h_{[s_1]Q,[x]Q}(P)$ will be sent to 1 during the final exponentiation because from $\lambda = mr = \sum_{i=0}^{l} c_i q^i = x + s_1$, we get $[s_1]Q + [x]Q = P_\infty$. We then apply the Property 1 to express $f_{3x+1,Q}$ in terms of $f_{x,Q}$ as follows: $f_{3x+1,Q} = f^3_{x,Q} \cdot h_{[x]Q,[x]Q} \cdot h_{[x]Q,[2x]Q} \cdot h_{[3x]Q,[1]Q}$. Finally, by using the explanation in Section 4.1, the function $h_{R,S}$ is simplified to $\overline{h}_{R,S}$. We can also observe that, if x is negative then by using the divisors we can take $f_{x,Q} = 1/(f_{-x,Q} \cdot h_{[x]Q,[-x]Q})$ and $h_{[x]Q,[-x]Q}$ is also sent to 1 during the final exponentiation. We remark that for this example, we have log $_2(x) \approx 54$ iterations of Miller's algorithm which is equal to $\log_2(r)/\varphi(8)$, and this agree with the definition of an optimal pairing.
The Magma code for the implementation of the Tate, Ate and optimal Ate pairings is available at
`http://www.prmais.org/Implementation-Pairings-Jacobi.txt`.

6 Conclusion

In this paper we have computed and implemented the Tate, Ate, twisted Ate and optimal pairings on the Jacobi quartic curve $E_d : Y^2 = dX^4 + Z^4$. The result in Tate pairing computation is a significative improvement up to 39% of the results of Wang et al. [3] on the same curve. Comparatively to the Weierstrass curve, our result is 27% more efficient. Ate pairing, twisted and optimal Ate pairings are computed on this curve for the first time. Our results are 27% more faster than in the case of Weierstrass curves [2]. According to our results the Jacobi quartic curve is then, to date, the best curve among curves with quartic twists which gives the most efficient result in pairings computation.

Acknowledgements The authors thank the anonymous referees and the program committee of Pairing 2012 for their useful comments on the first version of this work.

References

1. Duquesne, S., Fouotsa, E.: Tate pairing computation on Jacobi's elliptic curves. Pairing-Based Cryptography, Pairings 2012, LNCS Springer verlag. **vol. 7708, pp. 254-269** (2013)

2. Costello, C., Lange, T., Naehrig, M.: Faster pairing computations on curves with high-degree twists. PKC 2010, LNCS **vol. 6056, pp. 224-242** (2010)
3. Wang, H., Wang, K., Zhang, L., Li, B.: Pairing computation on elliptic curves of jacobi quartic form. Chinese Journal of electronics **vol. 20(4), pp. 655-661** (2011)
4. Menezes, A., Okamoto, T., Vanstone, S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory **vol. 39(5), pp. 1639-1646** (1993)
5. Frey, G., Muller, M., Ruck, H.: The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. IEEE Transactions on Information Theory **vol. 45(5), pp. 1717-1719** (1999)
6. Joux, A.: A one-round protocol for tripartite diffie-hellman. In Algorithmic Number Theory Symposium- ANTS IV, LNCS **vol. 1838, pp. 385-394** (2000)
7. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. SIAM Journal of Computing **vol. 32(3), pp. 586-615** (2003)
8. Dutta, R., Barua, R., Sarkar, P.: Pairing-based cryptography : A survey. Cryptology ePrint Archive **Report 2004/064** (2004)
9. Das, M., Sarkar, P.: Pairing computation on twisted Edwards form elliptic curves. Pairing 2008, LNCS **vol. 5209, pp. 192-210** (2008)
10. Ionica, S., Joux, A.: Another approach to pairing computation in edwards coordinates. INDOCRYPT 2008, LNCS **vol. 5365, pp. 400-413** (2008)
11. Arene, C., Lange, T., Naehrig, M., Ritzenthaler, C.: Faster computation of the tate pairing. Journal of number theory **vol. 131(5), pp. 842-857** (2011)
12. Costello, C., Hisil, H., Boyd, C., Nieto, J., Wong, K.: Faster pairings on special weierstrass curves. Pairing 2009, LNCS **vol. 5671, pp. 89-101** (2009)
13. Barreto, P.S.L.M., Galbraith, S., OhEigeartaigh, C., Scott, M.: Efficient pairing computation on supersingular abelian varieties. Designs, Codes and Cryptography **vol. 42(3), pp. 239-271** (2007)
14. Hesse, F., Smart, N., Vercauteren, F.: The eta pairing revisited. IEEE Transactions on Information Theory **vol. 52(10), pp. 4595-4602** (2006)
15. Vercauteren, F.: Optimal pairings. IEEE Transactions on Information Theory **vol. 56(1), pp. 455-461** (2010)
16. Hess, F.: Pairing lattices. Pairing-Based Cryptography - Pairing 2008, LNCS **vol. 5209, pp. 18-38** (2008)
17. Billet, O., Joye, M.: The jacobi model of an elliptic curve and side-channel analysis. AAECC 2003, LNCS **vol. 2643, pp. 34-42** (2003)
18. Hisil, H., K.K., W., Carter, G., Dawson, E.: Jacobi quartic curves revisited. ACISP 2009, LNCS, Springer **vol. 5594, pp. 452-468** (2009)
19. Silvermann, J.: The arithmetic of elliptic curves. Graduate texts in Mathematics, Springer-Verlag **vol. 106** (1986)
20. Miller, V.: Short programs for functions on curves. Unpublished manuscript available at http://crypto.stanford.edu/miller/miller.pdf. **vol.** (1986)
21. Avanzi, R., Cohen, H., Doche, C., Frey, G., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of elliptic and hyperelliptic curve cryptography. Discrete Math. Aplli. Chapman and Hall (2006)
22. Galbraith, S.: Pairings. London Mathematics Society Lecture Note Series - Cambridge University Press **vol. 317, pp. 183-213** (2005)
23. Duquesne, S., Frey, G.: Background on pairings. In [21] **pp. 115-124** (2005)
24. Washington, L.: Elliptic curves, number theory and cryptography. Discrete Math .Aplli, Chapman and Hall (2008)

25. Freeman, D., M., S., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of cryptology **vol. 23(2), pp. 224-280** (2010)
26. Koblitz, N., Menezes, A.: Pairing-based cryptography at high security levels. Cryptography and Coding, LNCS **vol. 3796, pp. 13-36** (2005)
27. Galbraith, S., McKee, J., Valenca, P.: Ordinary abelian varieties having small embedding degree. Finite Fields Applications **vol. 13, pp. 800-814** (2007)
28. Tanaka, S., Nakamula, K.: More constructing pairing-friendly elliptic curves for cryptography. **vol. , pp.** (2007)
29. Bosma, W., C.J., Playout, C.: The magma algebra system i. the user language. J. Symbolic Comput. **vol. 24(3-4), pp. 235-265** (1997)

A Cost of the Main Multiplication in Miller's Algorithm for the Tate and Twisted Ate pairings

The main multiplication in Miller's algorithm is of the form $f \cdot \tilde{h}$ where f and $\tilde{h}$ are in $\mathbb{F}_{q^k}$. Since $\mathbb{F}_{q^k}$ is a $\mathbb{F}_{q^{k/4}}$-vector space with basis $\{1, \omega, \omega^2, \omega^3\}$, f and $\tilde{h}$ can be written as : $f = f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3$ and $\tilde{h} = h_0 + h_1\omega + h_2\omega^2 + h_3\omega^3$ with f_i and h_i in $\mathbb{F}_{q^{k/4}}$, $i = 0, 1, 2, 3$. However in our case $h_3 = 0$, $h_0 \in \mathbb{F}_q$ and $k = 2^i$.

Schoolbook method: A full multiplication $f.\tilde{h}$ costs k^2 multiplications in the base field $\mathbb{F}_q$ using schoolbook method. But thanks to the particular form of h_0 and h_3, each of the multiplications $f_i \cdot h_0$ costs $\frac{k}{4}m_1$ and each of the multiplications $f_i \cdot h_1$, $f_i \cdot h_2$ costs $\frac{k^2}{16}m_1$. The final cost of the product $f \cdot \tilde{h}$ in the base field $\mathbb{F}_q$ is $(8\frac{k^2}{16} + 4\frac{k}{4})m_1 = (\frac{k^2}{2} + k)m_1$. Finally the ratio of the cost in this case by the cost of the general multiplication is $\frac{\frac{k^2}{2}+k}{k^2} = \frac{1}{2} + \frac{1}{k}$.

Karatsuba method: The computation of $f \cdot \tilde{h}$ is done here using a particular Karatsuba multiplication. Instead of writing $f \cdot \tilde{h}$ in the classical way (see for example Appendix B), we write it as follows:

$$f \cdot \tilde{h} = (f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3)(h_0 + h_1\omega + h_2\omega^2) =$$
$$(f_0 + f_1\omega + (f_2 + f_3\omega)\omega^2)(h_0 + (h_1 + h_2\omega)\omega)$$

In this form, the product is obtained using the following three products computed using a classical Karatsuba multiplication: $h_0(f_0+f_1\omega)$ which costs $2^{i-1}m_1$, $(f_2+f_3\omega)(h_1+h_2\omega)$ which costs $3(3^{i-2})m_1$ and $(f_0+f_2+(f_1+f_3)\omega)(h_1+(h_0+h_2)\omega)$ which costs $3(3^{i-2})m_1$. The final cost is then $2 \cdot 3^{i-1} + 2^{i-1}$.
The ratio is $\frac{2 \cdot 3^{i-1} + 2^{i-1}}{3^i}$.

B Cost of the Main Multiplication in Miller's Algorithm for Ate pairing

The main multiplication in Miller's algorithm is of the form $f \cdot \bar{h}$ where f and $\bar{h}$ are in $\mathbb{F}_{q^k}$. Since $\mathbb{F}_{q^k}$ is a $\mathbb{F}_{q^{k/4}}$-vector space with basis $\{1, \omega, \omega^2, \omega^3\}$, f and $\bar{h}$

can be written as : $f = f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3$ and $\bar{h} = h_0 + h_1\omega + h_2\omega^2 + h_3\omega^3$ with f_i and h_i in $\mathbb{F}_{q^{k/4}}$, $i = 0, 1, 2, 3$ and $h_2 = 0$.

Schoolbook method: A full multiplication $f.\bar{h}$ in $\mathbb{F}_{q^k}$ costs k^2 multiplications in the base field $\mathbb{F}_q$ using schoolbook method. But thanks to the fact that $h_2 = 0$, each of the 12 multiplications $f_i \cdot h_i$ costs $\frac{k^2}{16}m_1$, $i = 0, 1, 2, 3$. Then the total cost of the product $f \cdot \bar{h}$ is $12\frac{k^2}{16}m_1 = \frac{3k^2}{4}m_1$. Finally the ratio of the cost in this case by the cost of the general multiplication is $\frac{\frac{3k^2}{4}}{k^2} = \frac{3}{4}$.

Karatsuba method: $k = 2^i$. A full multiplication $f.\bar{h}$ in $\mathbb{F}_{q^k}$ is computed using Karatsuba multiplication as follows :

$$\begin{aligned} f \cdot \bar{h} = (f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3)(h_0 + h_1\omega + h_2\omega^2 + h_3\omega^3) = \\ (f_0 + f_1\omega + (f_2 + f_3\omega)\omega^2)(h_0 + h_1\omega + (h_2 + h_3\omega)\omega^2) \end{aligned}$$

In this form, this product is obtained by computing the three products $u_1 = (f_0 + f_1\omega)(h_0 + h_1\omega)$, $v_1 = (f_2 + f_3\omega)(h_2 + h_3\omega)$ and $w_1 = (f_0 + f_2 + (f_1 + f_3)\omega)(h_0 + h_2 + (h_1 + h_3)\omega)$. Applying again Karatsuba multiplication to u_1, v_1 and w_1, this costs $3(3^{i-2})m_1$ for each product such that the cost of the main multiplication $f \cdot \bar{h}$ using Karatsuba is $3^i m_1$.
Now in our case, $h_2 = 0$ so that the computation of v_1 costs only $2(3^{i-2})$ and the total cost for computing $f \cdot \bar{h}$ is $8 \cdot 3^{i-2}m_1$.
The ratio is then 8/9.