Efficient computation of pairings on Jacobi quartic elliptic curves

Sylvain Duquesne, Nadia El Mrabet, Emmanuel Fouotsa

J. Math. Cryptol., Ahead of Print
DOI 10.1515/jmc-2013-0033

Efficient computation of pairings on Jacobi quartic elliptic curves

Sylvain Duquesne, Nadia El Mrabet and Emmanuel Fouotsa

Communicated by Neal Koblitz

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 and previous results on Jacobi quartic curves. 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 compared to the case of Weierstrass curves with quartic twists.

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

2010 Mathematics Subject Classification. 14H52.

1 Introduction

Bilinear pairings were first used to solve the discrete logarithm problem on elliptic curve groups [14, 24]. But they are now useful to construct many public key protocols for which no other efficient implementation is known [5, 21]. A survey of some of these protocols can be found in [12]. The efficient computation of pairings depends on the model chosen for the elliptic curve. Pairing computation on the Edwards model of elliptic curves has been done successively in [9], [20] and [1]. The recent results on pairing computation using elliptic curves of Weierstrass form can be found in [7, 8]. Recently in [30], Wang et al. have computed the Tate pairing on Jacobi quartic elliptic curves using the geometric interpretation of the

This work was supported in part by French ANR project no. 12-BS01-0010-01 "PEACE", INS 2012 SIMPATIC project and LIRIMA 2013 MACISA project. This work is an improved and extended version of [10].

group law. An earlier work in the same direction as the previous one is done by Kaondera in [22]. Kaondera's work appears to be the first that tried to completely describe the geometric interpretation of the group law on Jacobi curves. But that work lacks some codes or an implementation for the verification of the correctness of the formulas obtained. In the present 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 [30] and they are more efficient than those concerning the Tate pairing computation in Weierstrass elliptic curves [8].

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:

- The Eta-pairing [3] on supersingular elliptic curves.
- Ate and twisted Ate pairings introduced in [18] 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.
- Vercauteren [29] and Hess [17] generalize the method with the notion of optimal pairings and pairing lattices that can be computed using the smallest number of basic Miller iterations.

The computation of these different pairings has been done by Costello et al. [8] in the case of Weierstrass curves. As a second contribution of this work, we extend the results on the special Jacobi quartic in [10] to the computation of the 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 the 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 a 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 enables us 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 $\Delta = 256d(\mu^2 - d)^2 \neq 0$. In [4], 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 [19].

The point addition $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ is given by

$$x_3 = \frac{x_1^2 - x_2^2}{x_1 y_2 - y_1 x_2}, \quad y_3 = \frac{(x_1 - x_2)^2}{(x_1 y_2 - y_1 x_2)^2}(y_1 y_2 + 1 + d x_1^2 x_2^2) - 1.$$

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

$$x_3 = \frac{2y_1}{2 - y_1^2} x_1, \quad y_3 = \frac{2y_1}{2 - y_1^2}\Big(\frac{2y_1}{2 - y_1^2} - y_1\Big) - 1.$$

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

$$\varphi : E_{d,0} \to W_d, \quad (0,1) \mapsto P_\infty, \quad (0,-1) \mapsto (0,0),$$
$$(x, y) \mapsto \Big(2\frac{y+1}{x^2}, 4\frac{y+1}{x^3}\Big),$$

$$\varphi^{-1} : W_d \to E_{d,0}, \quad P_\infty \mapsto (0,1), \quad (0,0) \mapsto (0,-1),$$
$$(x,y) \mapsto \Big(\frac{2x}{y}, \frac{2x^3 - y^2}{y^2}\Big).$$

From now on and for efficiency reasons, we adopt, for the first time in the computation of pairings, a specific representation of points, 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

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

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

$$X_3 = 2X_1 Y_1 Z_1, \quad Z_3 = Z_1^4 - dX_1^4, \quad Y_3 = 2Y_1^4 - Z_3^2.$$

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

$$\begin{aligned} \varphi : E_d \to W_d, \quad & [0:1:1] \mapsto P_\infty, \quad [0:-1:1] \mapsto (0,0), \\ & [X:Y:Z] \mapsto \Big(2\frac{Y+Z^2}{X^2}, 4\frac{Z(Y+Z^2)}{X^3}\Big), \\ \varphi^{-1} : W_d \to E_d, \quad & P_\infty \mapsto [0:1:1], \quad (0,0) \mapsto [0:-1:1], \\ & (x,y) \mapsto [2x : 2x^3 - y^2 : y]. \end{aligned}$$

The Sage software code to verify the correctness of our formulas is available at [26].

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 the Ate pairing and 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 by 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 $E(\overline{\mathbb{F}_q})[r] = \{P \in E(\overline{\mathbb{F}_q}) : [r]P = P_\infty\}$ is the set of r-torsion points with coordinates in an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$, where $[\,] : P \mapsto [r]P$ is the endomorphism defined on $E(\mathbb{F}_q)$ which consists of adding P to itself r times. The integer k is also the smallest integer such that $E(\overline{\mathbb{F}_q})[r] \subset E(\mathbb{F}_{q^k})$; this is the main property that we use in this work.

2.2.1 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 [28, Corollary 3.5, p. 67], D is principal and so there is a function $f_{r,P}$ with divisor $\mathrm{Div}(f_{r,P}) = D$. 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

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

The value $f_{r,P}(Q)$ can be determined efficiently using Miller's algorithm [25]. Indeed, for any 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 for $i = r$ 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 $(1, i_1, i_2, \ldots, r)$ such that each i_k is the sum of two previous terms of the sequence. This is justified by the fact that the functions $f_{i,P}$ satisfy the following conditions:

$$f_{1,P} = 1 \quad \text{and} \quad f_{i+j,P} = f_{i,P} f_{j,P} h_{[i]P,[j]P}, \tag{2.1}$$

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 for the addition chains for r and the properties of $f_{i,P}$ to compute $f_{r,P}(Q)$ (for more details on addition chains see [2, Chapter 9]). The Miller algorithm that computes efficiently the pairing of two points is given in Algorithm 1.

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

Input: $P \in E(\mathbb{F}_q)[r]$, $Q \in E(\mathbb{F}_{q^k})[r]$, $r = (1, r_{n-2}, \ldots, r_1, r_0)_2$.

Output: The reduced Tate pairing of P and Q : $f_{r,P}(Q)^{(q^k-1)/r}$

1: Set $f \leftarrow 1$ and $R \leftarrow P$
2: **for** $i = n-2$ **down to** 0 **do**
3: $\quad f \leftarrow f^2 \cdot h_{R,R}(Q)$
4: $\quad R \leftarrow 2R$
5: $\quad$ **if** $r_i = 1$ **then**
6: $\quad\quad f \leftarrow f \cdot h_{R,P}(Q)$
7: $\quad\quad R \leftarrow R + P$
8: $\quad$ **end if**
9: **end for**
10: **return** $f^{(q^k-1)/r}$

More information on pairings can be found in [11, 15].

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

2.2.2 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

$$\psi : E' \to E, \quad (x', y') \mapsto (x'/\omega^2, y'/\omega^3).$$

More details on twists can be found in [8].

2.2.3 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 Section 2.1 and the twist of Weierstrass curves defined above. Let k be an integer divisible by 4.

Definition 2.1 ([10]). 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 $\omega^2 \in \mathbb{F}_{q^{k/2}}$, $\omega^3 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/2}}$ 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 2.2. *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*

$$\psi : E_d^\omega \to E_d, \quad [X : Y : Z] \mapsto [\omega X : Y : Z].$$

In Sections 2.3 and 3.1, we explain why twists are useful for an efficient computation of pairings.

2.2.4 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. [18]. 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

$$\pi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q}), \quad (x, y) \mapsto (x^q, y^q)$$

be the Frobenius endomorphism on the curve, and t be its trace. The characteristic polynomial of π_q is $X^2 - tX + q$, see [31, 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

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

see [31, Theorem 4.3]. 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 us to consider

$$P \in \mathbb{G}_1 = E(\overline{\mathbb{F}_q})[r] \cap \mathrm{Ker}(\pi_q - [1]) = E(\mathbb{F}_q)[r],$$
$$Q \in \mathbb{G}_2 = E(\overline{\mathbb{F}_q})[r] \cap \mathrm{Ker}(\pi_q - [q]).$$

The Ate pairing is defined as follows:

Definition 2.3 (Ate pairing). The reduced Ate pairing is the map

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

where $T = t - 1$.

The following theorem gives some properties of the Ate pairing, in particular its relation with the Tate pairing. This relation shows that the Ate pairing is a power of the Tate pairing and therefore is a pairing. A complete proof can be found in [18].

Theorem 2.4 ([18]). *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 $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \bmod r$. Moreover, for $r \nmid L$, the Ate pairing e_A is non-degenerate.

Remark 2.5. The Tate pairing is defined on $\mathbb{G}_1 \times E(\mathbb{F}_{q^k})$, while the 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 the computation of the Ate pairing, 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 the Ate pairing is more expensive than a step of the Tate pairing. However the Miller loop length in the case of the 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 the Ate pairing were defined on $\mathbb{G}_1 \times \mathbb{G}_2$, then it would be faster than the Tate pairing since its Miller loop length would approximately be halved. This remark leads to the following definition of the twisted Ate pairing [18].

Definition 2.6 (Twisted Ate pairing [18]). Assume that E has a twist of degree δ and $m = \gcd(k, \delta)$. Let $e = k/m$ and $T_e = T^e \bmod r$. Then the reduced twisted Ate pairing is defined by

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

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

Theorem 2.7 ([18]). *For the Tate pairing $e_T(P, Q)$ we have*

$$e_{T_e}(P, Q)^{rc} = e_T(P, Q)^{LN},$$

where $c = \sum_{i=0}^{m-1} T^{e(m-1-i)} q^{ei} \equiv mq^{e(m-1)} \bmod r$. Moreover, for $r \nmid L$, the twisted Ate pairing e_{T_e} is non-degenerate.

Remark 2.8. 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 $T^e \bmod r$ 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 $T^e \bmod r$ is significantly less than r.

2.2.5 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 [29]. Indeed, observe that if k is the embedding degree with respect to r, then $r \mid q^k - 1$ but $r \nmid q^i - 1$ for any $1 \leq i < k$. This implies that $r \mid \Phi_k(q)$, where Φ_k is the k-th cyclotomic polynomial. Since $T \equiv q \bmod r$, where $T = t - 1$, we have $r \mid \Phi_k(T)$. More generally, if we consider the Ate-i pairing, which is a generalization of the Ate pairing with Miller function $f_{T_i,Q}$, where $T_i \equiv q^i \bmod r$, then

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

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

Definition 2.9 ([29]). Let $e : G_1 \times G_2 \to G_T$ be a non-degenerate, bilinear pairing with $|G_1| = |G_2| = |G_T| = r$, where the field of definition of G_T is $\mathbb{F}_{q^k}$. Then 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 2.10 ([29, 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

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

and R, S being 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

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

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

$$mkq^k \neq \frac{q^k-1}{r} \cdot \sum_{i=0}^{l} i c_i q^{i-1} \bmod r.$$

In Section 5, we apply Theorem 2.10 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 point addition of the Tate pairing, Ate pairing, twisted Ate or optimal pairing on a curve of embedding degree k takes 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 extension $\mathbb{F}_{q^k}$ whereas in the case of Ate and optimal Ate pairings, it is the point addition that is performed there. In both cases, this can affect the efficiency of computations. However many authors (see, e.g., [8, 13]) 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 subfield $\mathbb{F}_{q^{k/\delta}}$ 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 $\psi : E' \to E$ 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 point addition 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 2.2, 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 technique for the computation of the Tate, Ate, twisted Ate

and optimal pairings. As a consequence, the twists can be used 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 $E_d : Y^2 = dX^4 + Z^4$

In [30], Wang et al. considered pairings on Jacobi quartics and gave the geometric interpretation of the group law. We use a different way to obtain the formulas, namely the birational equivalence between Jacobi quartic curves and Weierstrass curves. We specialize to the particular curves $E_d : Y^2 = dX^4 + Z^4$ to obtain better results for these up to 39% improvement compared to the results in [30]. The results in this section are from [10].

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

$$R = [X_1 : Y_1 : Z_1], \quad S = [X_2 : Y_2 : Z_2],$$
$$[X_3 : Y_3 : Z_3] = [X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2],$$

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

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2, \\ \frac{3x_1^2 - 4d}{2y_1} & \text{if } P_1 = P_2, \end{cases} \quad \text{and} \quad \alpha = y_1 - \lambda x_1.$$

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

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

where

$$\lambda = \begin{cases} \frac{-2X_1^3 Z_2(Y_2 + Z_2^2) + 2X_2^3 Z_1(Y_1 + Z_1^2)}{X_1 X_2[-X_1^2(Y_2 + Z_2^2) + X_2^2(Y_1 + Z_1^2)]} & \text{if } P_1 \neq P_2, \\ \frac{Y_1 + 2Z_1^2}{X_1 Z_1} & \text{if } P_1 = P_2, \end{cases} \tag{3.1}$$

$$\alpha = \begin{cases} \frac{-4(Y_1+Z_1^2)(Y_2+Z_2^2)(Z_2X_1-Z_1X_2)}{X_1X_2[-X_1^2(Y_2+Z_2^2)+X_2^2(Y_1+Z_1^2)]} & \text{if } P_1 \neq P_2, \\ \frac{-2Y_1(Y_1+Z_1^2)}{X_1^3Z_1} & \text{if } P_1 = P_2. \end{cases} \tag{3.2}$$

Remark 3.1. It is easy to verify that our formulas obtained by change of variables are exactly the same obtained by Wang et al. in [30] using the geometric interpretation of the group law. Indeed, by setting

$$x_1 = \frac{X_1}{Z_1}, \quad x_2 = \frac{X_2}{Z_2}, \quad y_1 = \frac{Y_1}{Z_1^2}, \quad y_2 = \frac{Y_2}{Z_2^2}$$

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 have an advantage based on our coordinates system to obtain more efficient formulas in the computation of pairings. The correctness of the formulas in this work can be checked using the code provided at [26].

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 2.2). This enables the point Q in the computation of Tate and twisted Ate pairings 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

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

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

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

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 Algorithm 1). So they can

be discarded in the computation of the pairing and we only have to evaluate

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

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

$$D\Big(\frac{y_Q+1}{x_Q^3\omega^4}\Big) \quad \text{and} \quad B\Big(\frac{y_Q+1}{x_Q^2\omega^4}\Big)$$

costs $\frac{k}{4}m_1$, since $A, B, D \in \mathbb{F}_q$.

3.1.1 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 us 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 by 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 $(\frac{1}{k}+\frac{1}{2})m_k$. See Appendix A for details.
- If we use pairing friendly fields for elliptic curves with quartic twists, the embedding degree will be of the form $k = 2^i$ (see [13]). Then we follow [23] 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's multiplication method. Thus, the cost of a multiplication by $\tilde{h}_{R,S}$ is

  $$\Big(\frac{2\cdot 3^{i-1}+2^{i-1}}{3^i}\Big)m_k.$$

  See Appendix A for details.

In the remainder of Section 3, 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

$$P_1 = (X_1 : Y_1 : Z_1 : U_1 : V_1) \quad \text{and} \quad P_2 = (X_2 : Y_2 : Z_2 : U_2 : V_2),$$

where $U_i = X_i^2$, $V_i = Z_i^2$, $i = 1, 2$.

Remark 3.2. 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. In Tables 1 and 2, the operations concerned with this remark are indicated by *.

3.2 Doubling step in the Miller algorithm

When $P_1 = P_2$, from equations (3.1) and (3.2), we have

$$A = Y_1(Y_1 + Z_1^2), \quad B = -X_1^2(Y_1 + 2Z_1^2), \quad D = 2X_1^3 Z_1.$$

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 Remark 3.2). Thus, the doubling step in the Miller algorithm requires a total of $\beta m_k + 1s_k + (\frac{k}{2} + 3)m_1 + 7s_1 + 1mc$ (or $\beta m_k + 1s_k + (\frac{k}{2} + 4)m_1 + 6s_1 + 1mc$).

3.3 Addition step in the Miller algorithm

When $P_1 \neq P_2$, from equations (3.1) and (3.2), we have

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

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 3.2). 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 $15m_1 + 4s_1 + 1mc$). Thus, the addition step in the Miller algorithm requires a total of $\beta m_k + (\frac{k}{2} + 12)m_1 + 7s_1 + 1mc$ (or $\beta m_k + (\frac{k}{2} + 15)m_1 + 4s_1 + 1mc$).

3.4 Comparison

The comparison of results is summarized in Tables 3 and 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 [13]. In Table 3, we assume that the schoolbook multiplication method is used for the arithmetic in the extension fields $\mathbb{F}_{q^k}$.

Operations	Values	Cost
$U := U_1^2$	$U = X_1^4$	$1s_1$
$V := V_1^2$	$V = Z_1^4$	$1s_1$
$Z_3 := V - dU$	$Z_3 = Z_1^4 - dX_1^4$	$1mc$
$E := ((X_1 + Z_1)^2 - U_1 - V_1)/2$ *	$E = X_1 Z_1$	$1s_1$ (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.

Remark 3.3. 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's method is used for the arithmetic in $\mathbb{F}_{q^k}$ for curves with $k = 2^i$.

Remark 3.4. 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 ($a = 0$); see [30]. For the addition step, the improvement is up to 6% over the result on Jacobi quartic curves in [30]. When $k = 16$, the gain is 11% for the doubling step over Weierstrass curves. The improvement is 16% in the addition step over Jacobi quartic curves, see Table 4.

Remark 3.5. The security and the efficiency of pairing-based systems require using pairing-friendly curves. The Jacobi models of elliptic curves studied in this work are isomorphic to Weierstrass curves. Thus we can obtain pairing friendly

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 $1m_1$)
$V := V^2 + E$	$V = (Z_1Z_2)^2 + d(X_1X_2)^2$	$1s_1$
$E := (R - S)^2$	$E = (X_1Z_2 - X_2Z_1)^2$	$1s_1$

continued on next page

Operations	Values	Cost
$U_3 := X_3^2$	$U_3 = X_3^2$	$1s_1$
$V_3 := Z_3^2$	$V_3 = Z_3^2$	$1s_1$
$Y_3 := E(U+V) - V_3$	$Y_3 = (X_1Z_2 - X_2Z_1)^2(Y_1Y_2 + (Z_1Z_2)^2 + d(X_1X_2)^2) - Z_3^2$	$1m_1$
Total cost: $12m_1 + 11s_1 + 1mc$ (or $18m_1 + 5s_1 + 1mc$)		

Table 2. Combined formulas for the addition step.

Curves	Doubling		Mixed addition	
Weierstrass ($b = 0$) [8]	$1m_k + 1s_k + (\frac{k}{2} + 2)m_1 + 8s + 1mc$		$1m_k + (\frac{k}{2} + 9)m_1 + 5s_1$	
Jacobi quartic ($a = 0$) [30]	$1m_k + 1s_k + (\frac{k}{2} + 5)m_1 + 6s_1$		$1m_k + (\frac{k}{2} + 16)m_1 + 1s_1 + 1mc$	
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 ($b = 0$) [8]	$98m_1 + 16s_1 + 1mc$	$115m_1$	$77m_1 + 5s_1$	$82m_1$
Jacobi quartic ($a = 0$) [30]	$101m_1 + 14s_1$	$115m_1$	$84m_1 + 1s_1 + 1mc$	$86m_1$
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 ($b = 0$) [8]	$386m_1 + 24s_1 + 1mc$	$407m_1$	$273m_1 + 5s_1$	$278m_1$
Jacobi quartic ($a = 0$) [30]	$389m_1 + 22s_1$	$411m_1$	$280m_1 + 1s_1 + 1mc$	$282m_1$
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 pairing formulas with the previous fastest formulas using the schoolbook multiplication method.

Curves	Doubling		Mixed addition	
Weierstrass ($b = 0$) [8]	$1m_k + 1s_k + (\frac{k}{2} + 2)m_1 + 8s + 1mc$		$1m_k + (\frac{k}{2} + 9)m_1 + 5s_1$	
Jacobi quartic ($a = 0$) [30]	$1m_k + 1s_k + (\frac{k}{2} + 5)m_1 + 6s_1$		$1m_k + (\frac{k}{2} + 16)m_1 + 1s_1 + 1mc$	
This work	$(\frac{2\cdot 3^{i-1}+2^{i-1}}{3^i})m_k + 1s_k + (\frac{k}{2}+3)m_1 + 7s_1 + 1mc$		$(\frac{2\cdot 3^{i-1}+2^{i-1}}{3^i})m_k + (\frac{k}{2} + 12)m_1 + 7s_1 + 1mc$	
Example 1	$k = 8$	$m_1 = s_1 = mc$	$k = 8$	$m_1 = s_1 = mc$
Weierstrass ($b = 0$) [8]	$33m_1 + 35s_1 + 1mc$	$69m_1$	$40m_1 + 5s_1$	$45m_1$
Jacobi quartic ($a = 0$) [30]	$36m_1 + 33s_1$	$69m_1$	$47m_1 + 1s_1 + 1mc$	$49m_1$
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 ($b = 0$) [8]	$91m_1 + 89s_1 + 1mc$	$181m_1$	$98m_1 + 5s_1$	$103m_1$
Jacobi quartic ($a = 0$) [30]	$94m_1 + 87s_1$	$181m_1$	$105m_1 + 1s_1 + 1mc$	$107m_1$
This work	$73m_1 + 88s_1 + 1mc$	$162m_1$	$82m_1 + 7s_1 + 1mc$	$90m_1$

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

curves of such models using the construction given by Galbraith et al. [16] or by Freeman et al. [13]. Some examples of pairing friendly curves of Jacobi quartic form can be found in [30].

4 Formulas for the 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 the 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 the Ate pairing. 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 2.2). 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 $[x_P : y_P : 1]$.

4.1.1 Point addition and point doubling on E_d for Ate and optimal pairings

We rewrite the formulas from Section 2.1 for point doubling and point addition on the curve E_d 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 $\mathbb{F}_{q^{k/4}}$, $i = 1, 2, 3$.

4.1.2 Doubling

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

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

4.1.3 Addition

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

$$\begin{aligned}
X_3 &= X_1^2 Z_2^2 - Z_1^2 X_2^2,\\
Z_3 &= X_1 Z_1 Y_2 - X_2 Z_2 Y_1,\\
Y_3 &= (X_1 Z_2 - X_2 Z_1)^2\big(Y_1 Y_2 + (Z_1 Z_2)^2 + d\omega^4 (X_1 X_2)^2\big) - Z_3^2.
\end{aligned}$$

4.1.4 Miller function for the computation of Ate and optimal pairings on E_d

The Miller function on the Jacobi quartic E_d is given in Section 3:

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

We follow the notations of Section 3.1 by setting $-\frac{\alpha}{4} = \frac{A}{D}$ and $-\frac{1}{2}\lambda = \frac{B}{D}$. 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 careful calculation yields

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

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

$$\frac{2X_3^2 x_P^2}{D\omega^2[X_3^2(y_P + 1) - x_P^2(Y_3 + Z_3^2)]} \in \mathbb{F}_{q^{k/2}}.$$

Then it can be discarded in the computation of the pairing thanks to the final exponentiation, as we explained in the case of the Tate pairing. Thus we only have to evaluate

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

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

$$D\Big(\frac{y_P + 1}{x_P^3}\Big) \quad \text{and} \quad B\Big(\frac{y_P + 1}{x_P^2}\Big)$$

costs $\frac{k}{4}m_1$.

Remark 4.1. 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 the schoolbook method and is $(8/9)m_k$ if we use Karatsuba's multiplication with pairing friendly curves, i.e., $k = 2^i$. See Appendix B for details.

Remark 4.2. Since the coefficients of the Miller function for the Ate pairing are the same as for the Tate pairing, these coefficients and point 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 Tables 5 and 6, we summarize 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 the schoolbook method. In Table 6 we assume that computations are made in $\mathbb{F}_{q^k}$ using Karatsuba's method.

Remark 4.3. If we assume that $m_1 = s_1 = mc$ and if the schoolbook multiplication method is used, then for the computation of the Ate pairing 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's method is used. Our addition step is not better. See Tables 5 and 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 for the Tate, twisted Ate, Ate and optimal Ate pairings in a full loop of Miller's

Pairings	Doubling		Mixed addition	
Ate(Q, P) Weierstrass $(b = 0)$ [8]	$1m_k + 1s_k + 2m_e + 8s_e + 2em_1 + 1mc$		$1m_k + 9m_e + 5s_e + 2em_1$	
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 $(b = 0)$ [8]	$112m_1+24s_1+1mc$	$137m_1$	$109m_1 + 10s_1$	$119m_1$
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 $(b = 0)$ [8]	$464m_1+48s_1+1mc$	$513m_1$	$438m_1 + 20s_1$	$458m_1$
This work	$410m_1+44s_1+1mc$	$455m_1$	$430m_1+28s_1+1mc$	$459m_1$

Table 5. Comparisons of Ate and optimal Ate pairing formulas on Jacobi quartic and Weierstrass elliptic curves using the schoolbook method.

Pairings	Doubling		Mixed addition	
Ate(Q, P) Weierstrass $(b = 0)$ [8]	$1m_k + 1s_k + 2m_e + 8s_e + 2em_1 + 1mc$		$1m_k + 9m_e + 5s_e + 2em_1$	
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 $(b = 0)$ [8]	$37m_1 + 51s_1 + 1mc$	$89m_1$	$58m_1 + 15s_1$	$73m_1$
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 $(b = 0)$ [8]	$107m_1 + 153s_1 + 1mc$	$261m_1$	$170m_1 + 45s_1$	$215m_1$
This work	$107m_1 + 144s_1 + 1mc$	$252m_1$	$188m_1 + 63s_1 + 1mc$	$252m_1$

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

Parameters	Sec. levels	Arith. in $\mathbb{F}_{q^k}$	Tate		Twisted Ate		Ate		Optimal Ate	
			W [8]	J (this work)	W [8]	J (this work)	W [8]	J (this work)	W [8]	J (this work)
$k = 8, r \approx 2^{224}$, $q \approx 2^{336}$	112	Karat	15456	14336	23184	21504	14952	14448	4984	4816
		School	25760	20384	38640	30576	23016	20496	7672	6832
$k = 8, r \approx 2^{256}$, $q \approx 2^{384}$	128	Karat	17664	16384	26496	24576	17088	16512	5696	5504
		School	29440	23296	44160	34944	26304	23424	8768	7808
$k = 16, r \approx 2^{256}$, $q \approx 2^{320}$	128	Karat	46336	41472	115840	103680	41760	40320	8352	8064
		School	105216	76544	263040	191360	82080	72800	16416	14560
$k = 16, r \approx 2^{384}$, $q \approx 2^{480}$	192	Karat	69504	62208	173760	155520	62640	60480	12528	12096
		School	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: $s_1 = m_1 = mc$.

algorithm, based on the fastest operation counts summarized in Tables 3–6. We suppose that we are in the context of optimized pairing such that we can restrict 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's 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 the computation of the Ate pairing, we consider an average trace $t \sim \sqrt{q}$. For the values in Table 7, we assume that $m_1 = s_1 = mc$. The label "Karat" means that the values in these rows are obtained using Karatsuba's multiplication method, whereas "School" means that the values are obtained using the schoolbook multiplication method. The letters W and J stand for the Weierstrass [8] and the Jacobi elliptic (this work) curve model, respectively, since this work is the first that presents the computation of the 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.

5 Implementation and example

In this section we consider the family of elliptic curves of embedding degree 8 described in [27] to verify our formulas and to implement the Tate, Ate and optimal Ate pairings. This family of curves has the following parameters:

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

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

$$r = 27205632000047130716160030618261401480840452517707677193482845476817,$$
$$q = 72601167200444660495170346479178932899121731377660276881150532069758156754787842298703647640196322590069,$$
$$d = 45375729500277912809481466549486833061951082111037673050719082543598847971742401436689779775122701618793,$$
$$t = -113356800000147285043200063789391713609209096429146 0.$$

We recall that $\mathbb{G}_1 = E(\mathbb{F}_q)[r]$ and $\mathbb{G}_2 = E(\overline{\mathbb{F}_q})[r] \cap \mathrm{Ker}(\pi_q - [q])$. To obtain an optimal pairing in the Jacobi quartic curve E_d with embedding degree 8, we follow the approach described by Vercauteren [29]. Applying the `ShortestVectors()` function in Magma [6] 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 vector

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

An optimal pairing is then given by

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

where

$$H_1 = \left(\overline{h}_{[x]Q,[x]Q}(P) \cdot \overline{h}_{[x]Q,[2x]Q}(P) \cdot \overline{h}_{[3x]Q,[1]Q}(P)\right)^{q^3}$$

and $s_1 = (3x + 1)q^3$.

Indeed, this is a straightforward application of Theorem 2.10. 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 2.10 to obtain

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

Observe also that

$$f_{1,Q} = 1 \quad \text{and} \quad h_{[s_1]Q,P_\infty}^2(P) = 1.$$

Moreover, $h_{[s_1]Q,[x]Q}(P)$ 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 property (2.1) to express $f_{3x+1,Q}$ in terms of $f_{x,Q}$ as follows:

$$f_{3x+1,Q} = f_{x,Q}^3 \cdot h_{[x]Q,[x]Q} \cdot h_{[x]Q,[2x]Q} \cdot h_{[3x]Q,[1]Q}.$$

Finally, by using the explanation in Section 4.1.4, 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 agrees with the definition of an optimal pairing.

The Magma code for the implementation of the Tate, Ate and optimal Ate pairings is available at [26].

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 the computation of the Tate pairing is a significant improvement of up to 39% compared to the results of Wang et al. [30] on the same curve. Compared 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% faster than in the case of Weierstrass curves [8]. According to our results the Jacobi quartic curve is then, to date, the best curve among the curves with quartic twists which gives the most efficient result in the computation of pairings.

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

$$f = f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3, \quad \tilde{h} = h_0 + h_1\omega + h_2\omega^2 + h_3\omega^3$$

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 $k = 2^i$.

A.1 Schoolbook method

A full multiplication $f \cdot \tilde{h}$ costs k^2 multiplications in the base field $\mathbb{F}_q$ using the 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

$$\Big(8\frac{k^2}{16} + 4\frac{k}{4}\Big)m_1 = \Big(\frac{k^2}{2} + k\Big)m_1.$$

Finally the ratio of the cost in this case by the cost of the general multiplication is

$$\frac{\frac{k^2}{2} + k}{k^2} = \frac{1}{2} + \frac{1}{k}.$$

A.2 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:

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

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 the 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

$$f = f_0 + f_1\omega + f_2\omega^2 + f_3\omega^3, \quad \bar{h} = h_0 + h_1\omega + h_2\omega^2 + h_3\omega^3$$

with f_i and h_i in $\mathbb{F}_{q^{k/4}}$, $i = 0, 1, 2, 3$ and $h_2 = 0$.

B.1 Schoolbook method

A full multiplication $f \cdot \bar{h}$ in $\mathbb{F}_{q^k}$ costs k^2 multiplications in the base field $\mathbb{F}_q$ using the 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

$$\frac{\frac{3k^2}{4}}{k^2} = \frac{3}{4}.$$

B.2 Karatsuba method

We have $k = 2^i$. A full multiplication $f \cdot \bar{h}$ 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 $8/9$.

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

Bibliography

[1] C. Arene, T. Lange, M. Naehrig and C. Ritzenthaler, Faster computation of the Tate pairing, *J. Number Theory* **131** (2011) 842–857.

[2] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Math. Appl., Chapman & Hall, Boca Raton, 2006.

[3] P. S. L. M. Barreto, S. Galbraith, C. Ó'hEigeartaigh and M. Scott, Efficient pairing computation on supersingular abelian varieties, *Des. Codes Cryptogr.* **42** (2007), 239–271.

[4] O. Billet and M. Joye, The Jacobi model of an elliptic curve and side-channel analysis, in: *AAECC 2003*, Lecture Notes in Comput. Sci. 2643, Springer, Berlin (2003), 34–42.

[5] D. Boneh and M. Franklin, Identity-based encryption from the weil pairing, *SIAM J. Comput.* **32** (2003), 586–615.

[6] W. Bosma, J. Cannon and C. Playout, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[7] C. Costello, H. Hisil, C. Boyd, J. Nieto and K. Wong, Faster pairings on special Weierstrass curves, in: *Pairing 2009*, Lecture Notes in Comput. Sci. 5671, Springer, Berlin (2009), 89–101.

[8] C. Costello, T. Lange and M. Naehrig, Faster pairing computations on curves with high-degree twists, in: *PKC 2010*, Lecture Notes in Comput. Sci. 6056, Springer, Berlin (2010), 224–242.

[9] M. Das and P. Sarkar, Pairing computation on twisted Edwards form elliptic curves, in: *Pairing 2008*, Lecture Notes in Comput. Sci. 5209, Springer, Berlin (2008), 192–210.

[10] S. Duquesne and E. Fouotsa, Tate pairing computation on Jacobi's elliptic curves, in: *Pairing-Based Cryptography* (Pairings 2012), Lecture Notes in Comput. Sci. 7708, Springer, Berlin (2013), 254–269.

[11] S. Duquesne and G. Frey, Background on pairings, in: [2] (2006), 115–124.

[12] R. Dutta, R. Barua and P. Sarkar, Pairing-based cryptography: A survey, preprint (2004), `http://eprint.iacr.org/2004/064`.

[13] D. Freeman, S. M. and E. Teske, A taxonomy of pairing-friendly elliptic curves, *J. Cryptology* **23** (2010), 224–280.

[14] G. Frey, M. Muller and H. Ruck, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, *IEEE Trans. Inform. Theory* **45** (1999), 1717–1719.

[15] S. Galbraith, Pairings, in: *Advances in Elliptic Curve Cryptography*, London Math. Soc. Lecture Note Ser. 317, Cambridge University Press, Cambridge (2005), 183–213.

[16] S. Galbraith, J. McKee and P. Valenca, Ordinary abelian varieties having small embedding degree, *Finite Fields Appl.* **13** (2007), 800–814.

[17] F. Hess, Pairing lattices, in: *Pairing-Based Cryptography. Pairing 2008*, Lecture Notes in Comput. Sci. 5209, Springer, Berlin (2008), 18–38.

[18] F. Hesse, N. Smart and F. Vercauteren, The eta pairing revisited, *IEEE Trans. Inform. Theory* **52** (2006), 4595–4602.

[19] H. Hisil, K. K.-H. Wong, G. Carter and E. Dawson, Jacobi quartic curves revisited, in: *ACISP 2009*, Lecture Notes in Comput. Sci. 5594, Springer, Berlin (2009), 452–468.

[20] S. Ionica and A. Joux, Another approach to pairing computation in Edwards coordinates, in: *INDOCRYPT 2008*, Lecture Notes in Comput. Sci. 5365, Springer, Berlin (2008), 400–413.

[21] A. Joux, A one-round protocol for tripartite Diffie–Hellman, in: *Algorithmic Number Theory Symposium ANTS IV*, Lecture Notes in Comput. Sci. 1838, Springer, Berlin (2000), 385–394.

[22] S. R. Kaondera, *Pairing computation using Jacobi quartic curves*, Master thesis, Mzuzu University, Malawi, 2010.

[23] N. Koblitz and A. Menezes, Pairing-based cryptography at high security levels, in: *Cryptography and Coding*, Lecture Notes in Comput. Sci. 3796, Springer, Berlin (2005), 13–36.

[24] A. Menezes, T. Okamoto and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory* **39** (1993), 1639–1646.

[25] V. Miller, Short programs for functions on curves, preprint 1986, `http://crypto.stanford.edu/miller/miller.pdf`.

[26] Sage software code, `www.camercrypt.org/Implementation-Pairings-Jacobi.txt`.

[27] T. Satoru and N. Ken, More constructing pairing-friendly elliptic curves for cryptography, preprint (2007), `http://arxiv.org/abs/0711.1942`.

[28] J. Silvermann, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, Berlin, 1986.

[29] F. Vercauteren, Optimal pairings, *IEEE Trans. Inform. Theory* **56** (2010), 455–461.

[30] H. Wang, K. Wang, L. Zhang and B. Li, Pairing computation on elliptic curves of Jacobi quartic form, *Chinese J. Electron.* **20** (2011), 655–661.

[31] L. Washington, *Elliptic Curves, Number Theory and Cryptography*, Discrete Math. Appl., Chapman & Hall, Boca Raton, 2008.

Received September 16, 2013; revised April 22, 2014; accepted July 3, 2014.

Author information

Sylvain Duquesne, IRMAR, UMR CNRS 6625, Université Rennes 1,
Campus de Beaulieu, 35042 Rennes cedex, France.
E-mail: sylvain.duquesne@univ-rennes1.fr

Nadia El Mrabet, Laboratoire d'Informatique Avancé de Saint-Denis,
Université Paris 8, 93526 Saint Denis cedex, France.
E-mail: elmrabet@ai.univ-paris8.fr

Emmanuel Fouotsa, Department of Mathematics, Higher Teacher Training College,
University of Bamenda, P.O. Box 5052, Bamenda, Cameroon.
E-mail: emmanuelfouotsa@camercrypt.org