Guide to Pairing-Based Cryptography

by

Nadia El Mrabet and Marc Joye, Eds.

3

Pairings

Sorina Ionica
Université de Picardie Jules Verne

Damien Robert
INRIA Bordeaux Sud-Ouest, Université de Bordeaux

We recall from Section 1.2 that a pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ between finite abelian groups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$, that satisfies the following conditions:

- e is bilinear, which means that $e(P+Q,R) = e(P,R) \times e(Q,R)$ and $e(P,Q+R) = e(P,Q) \times e(P,R)$;
- e is non-degenerate, which means that for any $P \in \mathbb{G}_1$ there is a $Q \in \mathbb{G}_2$ such that $e(P,Q) \neq 1$, and for any $Q \in \mathbb{G}_2$ there is a $P \in \mathbb{G}_1$ such that $e(P,Q) \neq 1$.

A pairing e is suitable for use in cryptography when furthermore it is easy to compute, but difficult to invert. Inverting a pairing e means given $z \in \mathbb{G}_T$ to find $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ such that $e(P,Q) = z$.

The most efficient cryptographic pairings currently known come from elliptic curves (or higher dimensional algebraic varieties). Starting from an elliptic curve E defined over a finite field $\mathbb{F}_q$, we consider the Weil pairing and the Tate pairing associated to it. This allowed cryptographers to construct a map such that:

- $\mathbb{G}_1$ and $\mathbb{G}_2$ are subgroups of the rational points of E defined over an extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$;
- $\mathbb{G}_T$ is the group $(\mathbb{F}_{q^k}^*, \times)$ where the group law is given by the field multiplication on $\mathbb{F}_{q^k}$ (or more precisely $\mathbb{G}_T = \mu_r \subset \mathbb{F}_{q^k}^*$ is the subgroup of r-roots of unity);

- The pairing e can be efficiently computed using Miller's algorithm (see Algorithm 3.2);
- Currently the most efficient way to invert e is to solve the Diffie-Helman problem on $\mathbb{G}_1$, $\mathbb{G}_2$ or $\mathbb{G}_T$.

In this chapter we introduce pairings associated to an elliptic curve E over a finite field $\mathbb{F}_q$ and explain how to compute them efficiently, via an algorithm which evaluates functions on points of the curve. We first explain in Section 3.1 how to represent functions efficiently by looking at their associated divisors, and then give Miller's algorithm which allows to evaluate them.

In Section 3.2 we present the general theory of the Weil and Tate pairing and we review main recent optimizations for their computation: the Ate, twisted Ate and optimal pairings, which are preferred in implementations nowadays. Finally, we give concrete formulae to compute them in practice in Section 3.3. Since the group $\mathbb{G}_T$ is a subgroup of the multiplicative group of $\mathbb{F}_{q^k}$, security requirements involve choosing a base field $\mathbb{F}_q$ with large characteristic (see [2] or Chapter 9).

For simplicity, in Section 3.1 and 3.2 points on the elliptic curve are represented in affine coordinates. Using this representation, formulae for pairing computation are easy to write down. However, note that affine coordinates involve divisions and are not efficient for a practical implementation. We study more efficient representations of points in Section 3.3.

For the cryptographic usage of pairings, only a specific version of Miller's algorithm and the Weil and Tate pairing need to be presented. This is the version we give in Section 3.1 and 3.2, where we omit most proofs. For the sake of completness, we give the general version of the pairings along with complete proofs in Section 3.4.

Notation.

We recall that an elliptic curve defined over a field with characteristic greater than 5 can always be given in short Weierstrass form, as explained in Chapter 2. In the remainder of this chapter, all elliptic curves are defined over a field K with characteristic greater than 5 and will be given by a short Weierstrass equation. We denote this equation by $y^2 = H(x)$, with $H(x) = x^3 + ax + b$ and $a, b \in K$.

3.1 Functions, Divisors and Miller's algorithm

3.1.1 Functions and divisors on curves

Pairing computations will rely crucially on evaluating functions on points of elliptic curves. A convenient way to represent functions is by their divisor. We first give a gentle introduction to the theory of divisors by looking at examples of functions on the line before considering elliptic curves.

Let $\mathbb{A}^1$ be the affine line over an algebraically closed field $\overline{K}$. Adding the point at infinity means that we work on the projective line $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. Rational functions $\overline{K}(\mathbb{P}^1)$ on $\mathbb{A}^1$ are simply the rational functions $\overline{K}(t)$. Let $f = P/Q = \frac{\prod (t-x_i)^{n_i}}{\prod (t-y_i)^{m_i}} \in \overline{K}(t)$ be such a rational function, where the numerator P and the denominator Q are assumed to be prime with each other. Then the points x_i are *zeroes* of f with multiplicity m_i and the points y_i are *poles* of f with multiplicity n_i. This allows us to define a multiplicity $\mathrm{ord}_x(f)$ for every point $x \in \mathbb{P}^1(\overline{K})$

$$\mathrm{ord}_x(f) = \begin{cases} n & \text{if } x \text{ is a zero of } f \text{ with multiplicity } n, \\ -n & \text{if } x \text{ is a pole of } f \text{ of multiplicity } n, \\ 0 & \text{if } x \text{ is neither a zero or a pole.} \end{cases}$$

For example, f has no pole in $\mathbb{A}^1$ if and only if it is a polynomial $P(t)$.

Given a rational function $f = P/Q$ as above, we can also define the evaluation of f on the point at infinity ∞. Here is how to compute the evaluation of f at ∞: the change of variables $u = 1/t$ sends ∞ to 0. Define g by $g(u) = f(1/u)$. This gives the relation $f(t) = g(u)$ when $t = 1/u$. We can then define the *order* of f at ∞ as the order of g at 0, and when the order is 0 we can define the *value* of f at ∞ as the value of g at 0. One can then easily check that $\mathrm{ord}_\infty(f) = -\deg f = \deg Q - \deg P$.

We associate a formal sum to a function f:

$$\mathrm{div}(f) = \sum_{x \in \mathbb{P}^1(\overline{K})} \mathrm{ord}_x(f)[x],$$

where we use the notation $[x]$ to represent the point $x \in \mathbb{P}^1(\overline{K})$ in the formal sum. This formal sum is called the divisor of f. Since there is only a finite number of poles or zeroes, it is in fact finite. Moreover f is characterized by $\mathrm{div}(f)$ up to the multiplication by a constant: if f_1 and f_2 are two rational functions such that $\mathrm{div}(f_1) = \mathrm{div}(f_2)$, then f_1 and f_2 have the same poles and zeroes so they differ by a multiplicative constant.

More generally, a divisor D is defined to be a formal sum of a finite number of points:

$$D = \sum_{x \in \mathbb{P}^1(\overline{K})} n_i[x_i].$$

To a divisor D one can associate its degree $\deg(D) = \sum n_i$. By the remark above concerning the multiplicity of f at ∞, we get that $\deg \mathrm{div}(f) = 0$. Conversely, given a divisor D of degree 0 it is easy to construct a rational function f such that $\mathrm{div}\, f = D$.

The whole theory extends when we replace the line $\mathbb{P}^1$ by a (geometrically connected smooth) curve C. If $P \in C(\overline{K})$ is a point of C, then there is always a uniformiser t_P, that is a rational function on C with a simple zero at P. Thus if $f \in \overline{K}(C)$ is a rational function on C, then we can always write $f = t_P^m \cdot g$ where g is a function having no poles nor zeroes at P. We then define the *multiplicity* $\mathrm{ord}_P(f)$ of f at P to be m. If the multiplicity $\mathrm{ord}_P(f)$ is zero, that is if P is neither a pole nor a zero of f, then one can define the *value* of f at P to be $f(P)$.

In the case of the projective line $\mathbb{P}^1$, a uniformiser at x is $t - x$ and a uniformiser at ∞ is $u = \frac{1}{t}$. Hence this new notion of multiplicity coincides with the one introduced above.

For an elliptic curve E we have the following uniformisers

- $t_P = x - x_P$, except when $H(x_P) = 0$;
- $t_P = y - y_P$, except when $H'(x_P) = 0$;
- $t_{0_E} = x/y$.

We denote by $\mathrm{Disc}\, P$ the discriminant of a polynomial P, we recall that the discriminant is non zero if and only if P does not admit a double root. Since E is an elliptic curve, $\mathrm{Disc}\, H \neq 0$ and we cannot have $H(x_P) = 0$ and $H'(x_P) = 0$ at the same time. Hence there is indeed a uniformiser for every point $P \in E(\overline{K})$.

One can also define a *divisor* on E as a formal finite sum of geometric points $D = \sum n_i[P_i]$ of E, and associate to a rational function $f \in \overline{K}(E)$ a divisor $\mathrm{div}(f) = \sum_{P \in E(\overline{K})} \mathrm{ord}_P(f)[P]$. One can check that $\mathrm{ord}_P(f) = 0$ for all but a finite number of P so we get a well defined divisor. The degree $\deg D$ of a divisor $D = \sum n_i[P_i]$ is $\sum n_i$. A divisor D is said to be *principal* when there exists a function f such that $D = \mathrm{div}(f)$. Two divisors D_1 and D_2 are said to be *linearly equivalent* when there exists a function f such that $D_1 = D_2 + \mathrm{div}(f)$. It is easy to check that a divisor D is principal if and only if it is equivalent to the zero divisor, and that two divisors D_1 and D_2 are linearly equivalent if and only if $D_1 - D_2$ is linearly equivalent to the zero divisor.

PROPOSITION 3.1 *Let E be an elliptic curve over an algebraically closed field $\overline{K}$.*

1. *Given $f, g \in \overline{K}(E)$ two rational functions, then* $\mathrm{div}(f) = \mathrm{div}(g)$ *if and only* g *differs from* f *by a multiplicative constant;*
2. *If $f \in \overline{K}(E)$ is a rational function, then* $\mathrm{div}(f)$ *is a divisor of degree* 0*;*
3. *Conversely if $D = \sum n_i[P_i]$ is a divisor on E of degree* 0*, then D is the divisor of a function $f \in \overline{K}(E)$ (ie D is a principal divisor) if and only if $\sum n_i P_i = 0_E \in E(\overline{K})$ (where the last sum is not formal but comes from the addition on the elliptic curve).*

Proof. See [22, Proposition 3.4]. In fact, for the last item, given a divisor $D = \sum n_i[P_i]$ of degree 0, we give in Section 3.4.2 an explicit algorithm which constructs a rational function f such that $D = [P] - [0_E] + \mathrm{div}(f)$ and $P = \sum n_i P_i \in E(\overline{K})$. If $P = 0_E$ then $D = \mathrm{div}(f)$ is a principal divisor. It remains to show that if $P \neq 0_E$ then the divisor $[P] - [0_E]$ is not principal. But if we had a function f such that $\mathrm{div}(f) = [P] - [0_E]$, then the morphism $E \to \mathbb{P}^1_{\overline{K}} : x \mapsto (1 : f(x))$ associated to f would be birational. (Indeed since f has one simple zero and one simple pole, one could get every degree zero divisors as the divisor of a suitable rational function of f. So the function field of $k(E)$ would be $k(f)$.) But this is absurd: E is an elliptic curve so it has genus 1, it cannot have genus 0. □

An elliptic curve E defined over $\mathbb{F}_q$ can also be seen as an elliptic curve $E_{\overline{\mathbb{F}_q}}$ over the algebraic closure $\overline{\mathbb{F}_q}$. We say that a divisor $D = \sum n_i[P_i]$ of $E_{\overline{\mathbb{F}_q}}$ is rational when it is invariant under the action of the Frobenius automorphism π. If $f \in \mathbb{F}_q(E)$ is a rational function defined over $\mathbb{F}_q$, then $\mathrm{div}(f)$ is rational. Conversely if $f \in \overline{\mathbb{F}_q}(E)$ has a rational divisor $\mathrm{div}(f)$, then there exists a nonzero constant λ such that $\lambda f \in \mathbb{F}_q(E)$ [22, Chapter II §2].

3.1.2 Miller's algorithm

Let F be a principal divisor. Then by definition there is a rational function f on E such that $F = \mathrm{div}\, f$. Then f is uniquely determined up to a constant. If 0_E is neither a pole or a zero of f, then one can uniquely define f by requiring that $f(0_E) = 1$. More generally, we can define the normalized function associated to a principal divisor as follow: since $\mathrm{ord}_{0_E}(x/y) = 1$, $(x/y)^{\mathrm{ord}_{0_E}(f)}$ has the same order at 0_E as f. In particular the function $\left(\frac{f}{(x/y)^{\mathrm{ord}_{0_E}(F)}}\right)$ is defined at 0_E, and we can normalize f uniquely by requiring that the above function has value 1 at 0_E. This gives the following definition.

DEFINITION 3.1 Let F be a principal divisor. We define f_F to be the unique function such that $F = \mathrm{div}\, f_F$ and $\left(\frac{f_F}{(x/y)^{\mathrm{ord}_{0_E}(F)}}\right)(0_E) = 1$. Such a function is called normalized at 0_E (or simply normalized). If F is rational, then f_F is rational too.

If P and Q are points in E, then $[P] + [Q] - [P+Q] - [0_E]$ is principal. Indeed it has degree 0 and $P + Q - 2 0_E - (P+Q) + 0_E = 0_E$ so by Proposition 3.1 there exists a function $\mu_{P,Q}$ such that $\mathrm{div}(\mu_{P,Q}) = [P] + [Q] - [P+Q] - [0_E]$.

DEFINITION 3.2 We denote by $\mu_{P,Q}$ the normalized function with principal divisor $[P] + [Q] - [P+Q] - [0_E]$.

If E is given by a short Weierstrass equation, we can construct $\mu_{P,Q}$ explicitly: if $P = -Q$ then $P + Q = 0_E$ and we can choose

$$\mu_{P,Q} = x - x_P. \tag{3.1}$$

Otherwise let $l_{P,Q}$ be the line going through P and Q (if $P = Q$ then we take $l_{P,Q}$ to be the tangent to the elliptic curve at P). Then by definition of the addition law on E, we have that $\mathrm{div}(l_{P,Q}) = [P] + [Q] + [-P - Q] - 3[0_E]$. Now let $v_{P,Q} = x - x_{P+Q}$ be the vertical line going through $P + Q$ and $-P - Q$. Then $\mathrm{div}(v_{P,Q}) = [P + Q] + [-P - Q] - 2[0_E]$, so that $\mathrm{div}(\frac{l_{P,Q}}{v_{P,Q}}) = [P] + [Q] - [P + Q] - [0_E]$ and one can take $\mu_{P,Q} = \frac{l_{P,Q}}{v_{P,Q}}$.

To compute x_{P+Q}, we know that $-P - Q$ is the third intersection point between the line $l_{P,Q} : y = \alpha x + \beta$ and the elliptic curve $E : y^2 = x^3 + ax + b$. So x_{-P-Q}, x_P, x_Q are all roots of the degree three equation $x^3 + ax + b - (\alpha x + \beta)^2 = 0$, and we get that $x_{P+Q} = x_{-P-Q} = \alpha^2 - x_P - x_Q$. Putting everything together we finally obtain

$$\mu_{P,Q} = \frac{y - \alpha(x - x_P) - y_P}{x + (x_P + x_Q) - \alpha^2} \tag{3.2}$$

with $\alpha = \frac{y_P - y_Q}{x_P - x_Q}$ when $P \neq Q$ and $\alpha = \frac{H'(x_P)}{2y_P}$ when $P = Q$.

One can check that the functions $\mu_{P,Q}$ defined above are normalized (see Section 3.4). Let $R \in E$. The following lemma explains how to evaluate $\mu_{P,Q}$ on R (in the usual cases encountered in cryptographic applications, we refer to Lemma 3.4 for the remaining cases).

LEMMA 3.1 (Evaluating $\mu_{P,Q}$) *Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, and $R = (x_R, y_R)$ be points on E.*

- *Suppose that P, Q and $P + Q$ all different from 0_E. Then $\mu_{P,Q} = \frac{l_{P,Q}}{v_{P,Q}}$ where $l_{P,Q} = y - \alpha x - \beta$ with $\alpha = \frac{y_P - y_Q}{x_P - x_Q}$ when $P \neq Q$ and $\alpha = \frac{H'(x_P)}{2y_P}$ when $P = Q$, $\beta = y_P - \alpha x_P = y_Q - \alpha x_Q$ and $v_{P,Q} = x - x_{P+Q}$ with $x_{P+Q} = \alpha^2 - x_P - x_Q$.*
  Assume that R is not equal to P, Q, $P + Q$, $-P - Q$ or 0_E then we have

$$\mu_{P,Q}(R) = \frac{y_R - \alpha x_R - \beta}{x_R - x_{P+Q}}. \tag{3.3}$$

  (If $R = -P - Q$ and $-P - Q \neq P, Q, P + Q, 0_E$ then $\mu_{P,Q}$ is well defined on R, but computing the exact value requires more work, see Lemma 3.4 for the formula.)
- *If $P = -Q$ (but $P \neq 0_E$) so that $P + Q = 0_E$, then $\mu_{P,Q} = x - x_P$.*
  Assume that R is different from 0_E, then $\mu_{P,Q}(R) = x_R - x_P$.
- *If $P = 0_E$ or $Q = 0_E$ then $\mu_{P,Q} = 1$.*

Let $P \neq 0_E$ a point of r-torsion on E. Then $r[P] - r[0_E]$ is a principal divisor (by cite[Corollary III.3.5]Silverman09). As a consequence, we have the following definition.

DEFINITION 3.3 We denote by $f_{r,P}$ the normalized function with principal divisor $r[P] - r[0_E]$.

All pairing computations will involve the following key computation: *given $P \neq 0_E$ a point of r-torsion on E, and $Q \neq P, 0_E$ a point of the elliptic curve, evaluate $f_{r,P}(Q)$.* To explain how to compute $f_{r,P}$ we need first to extend its definition.

DEFINITION 3.4 Let $\lambda \in \mathbb{N}$ and $P \in E(K)$; we define $f_{\lambda,P} \in K(E)$ to be the function normalized at 0_E such that

$$\mathrm{div}(f_{\lambda,P}) = \lambda[P] - [\lambda P] - (\lambda - 1)[0_E].$$

Note that if $r \in \mathbb{N}$ and $P \in E[r]$, then $f_{r,P}$ is indeed the normalized function with divisor $r[P] - r[0_E]$.

PROPOSITION 3.2 *Let P be as above, and $\lambda, \nu \in \mathbb{N}$. We have*

$$f_{\lambda+\nu,P} = f_{\lambda,P} f_{\nu,P} \mathbf{f}_{\lambda,\nu,P},$$

where $\mathbf{f}_{\lambda,\nu,P} = \mu_{\lambda P,\nu P}$ is the function associated to the divisor $[(\lambda+\nu)P] - [\lambda P] - [\nu P] + [0_E]$ and normalized at 0_E.

Proof. We have seen in Lemma 3.1 that the function $\mu_{\lambda X,\nu X}$ defined in Equations (3.1) and (3.2) is normalized and has for associated divisor $[(\lambda+\nu)X] - [(\lambda)X] - [(\nu)X] + [0_E]$. By definition of $f_{\lambda,X}$, we have that $\operatorname{div} f_{\lambda+\nu,X} = (\lambda+\nu)[X] - [(\lambda+\nu)X] - (\lambda+\nu-1)[0_E] = \lambda[X] - [\lambda X] - (\lambda-1)[0_E] + \nu[X] - [\nu X] - (\nu-1)[0_E] + [(\lambda+\nu)X] - [(\lambda)X] - [(\nu)X] + [0_E] = \operatorname{div} f_{\lambda,X} f_{\nu,X} \mathbf{f}_{\lambda,\nu,X}$. So $f_{\lambda+\nu,X} = f_{\lambda,X} f_{\nu,X} \mathbf{f}_{\lambda,\nu,X}$ since they have the same associated divisor and are both normalized at 0_E. □

Proposition 3.2 is the main ingredient that we need to compute $f_{r,P}$, using a double-and-add algorithm, whose pseudocode is described in Algorithm 3.2. Here is how this algorithms works: given $P \in E[r]$, we compute rP as we would with a standard double-and-add algorithm. If the current point is $T = \lambda P$, then at each step in the loop we perform a doubling $T \mapsto 2T$, and whenever the current bit of r is a 1, we also do an extra addition $T \mapsto T + P$. The only difference between Miller's algorithm and scalar multiplication is that, at each step in the Miller loop, we also keep track of the function $f_{\lambda,P}$ (corresponding to the principal divisor $\lambda[P] - [T] - (\lambda-1)[0_E]$). During the doubling and addition step we increment this function using Proposition 3.2, until in the end we obtain $f_{r,P}$, which we can evaluate on Q. Note that in practice we do the evaluations directly at each step because representing the full function $f_{r,P}$ would be too expensive.

ALGORITHM 3.1 Miller's algorithm (general version).

Input: $r \in \mathbb{N}$, $I = [\log r]$, $P = (x_P, y_P) \in E[r](K), Q = (x_Q, y_Q) \in E(K)$.

Output: $f_{r,P}(Q)$.

1. Compute the binary decomposition: $r := \sum_{i=0}^{I} b_i 2^i$. Let $T = P, f = 1$.
2. For i in $[I-1..0]$ compute
   (a) $f = f^2 \mu_{T,T}(Q)$;
   (b) $T = 2T$;
   (c) If $b_i = 1$, then compute
      i. $f = f \mu_{T,P}(Q)$;
      ii. $T = T + P$.

Return f.

Remark 3.1

- One should be careful that at the last step, the sum (whether it is a doubling or an addition) gives 0_E, so the corresponding Miller function is simply $x - x_T$.

- There is one drawback in evaluating directly the intermediate Miller functions $\mu_{\lambda P,\nu P}$ directly on Q: if $Q \notin \{0_E, P\}$, then $f_{r,P}(Q)$ is well defined. But if Q is a zero or pole of $\mu_{\lambda P,\nu P}$, then Algorithm 3.1 fails to give the correct result. A solution to compute $f_{r,P}(Q)$ anyway is to change the addition chain used to try to get other Miller functions $\mu_{\lambda P,\nu P}$ that do not have a pole or zero on Q. Another solution is given in Section 3.4. We note that this situation can happen only when Q is a multiple of P.

Using Lemma 3.1 we get an explicit version of Algorithm 3.1, for an elliptic curve $y^2 = x^3 + ax + b$. For efficiency reasons, we only do one division at the end.

ALGORITHM 3.2 Miller's algorithm for affine short Weierstrass coordinates

Input: $r \in \mathbb{N}$, $I = [\log r]$, $P = (x_P, y_P) \in E[r](K), Q = (x_Q, y_Q) \in E(K)$.

Output: $f_{r,P}(Q)$.

1. Compute the binary decomposition: $r := \sum_{i=0}^{I} b_i 2^i$. Let $T = P, f_1 = 1, f_2 = 1$.
2. For i in $[I - 1..0]$ compute (except at the last step)
   (a) $\alpha = \frac{3x_T^2 + a}{2y_T}$, the slope of the tangent of E at T;
   (b) $x_{2T} = \alpha^2 - 2x_T$, $y_{2T} = -y_T - \alpha(x_{2T} - x_T)$;
   (c) $f_1 = f_1^2(y_Q - y_T - \alpha(x_Q - x_T))$, $f_2 = f_2^2(x_Q + 2x_T - \alpha^2)$;
   (d) $T = 2T$.
   (e) If $b_i = 1$, then compute
      i. $\alpha = \frac{y_T - y_P}{x_T - x_P}$, the slope of the line going through P and T;
      ii. $x_{T+P} = \alpha^2 - x_T - x_P$, $y_{T+P} = -y_T - \alpha(x_{T+P} - x_T)$;
      iii. $f_1 = f_1(y_Q - y_T - \alpha(x_Q - x_T))$, $f_2 = f_2(x_Q + (x_P + x_T) - \alpha^2)$;
      iv. $T = T + P$.
3. At the last step: $f_1 = f_1(x_Q - x_T)$.

Return

$$\frac{f_1}{f_2}.$$

3.2 Pairings on elliptic curves

3.2.1 The Weil pairing

The first pairing on elliptic curves has been defined by Weil. Although it is usually not used in practice for cryptography (rather the Tate pairing, or variants of the Tate pairing is), it is important for historical reasons, and also because the original construction of the Tate pairing uses the Weil pairing.

THEOREM 3.1 *Let E be an elliptic curve defined over a finite field K, $r \geq 2$ an integer*

prime to the characteristic of K and P and Q two points of r-torsion on E. Then

$$e_{W,r} = (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)} \tag{3.4}$$

is well defined when $P \neq Q$ and $P, Q \neq 0_E$. One can extend the application to the domain $E[r] \times E[r]$ by requiring that $e_{W,r}(P, 0_E) = e_{W,r}(0_E, P) = e_{W,r}(P, P) = 1$. Furthermore, the application $e_{W,r} : E[r] \times E[r] \to \mu_r$ obtained in this way is a pairing, called the Weil pairing. The pairing $e_{W,r}$ is alternate, which means that $e_{W,r}(P, Q) = e_{W,r}(Q, P)^{-1}$.

Proof. See [22, Section III.8] or Section 3.4.3. □

Note that the Weil pairing is defined over any field K of characteristic prime to r, and takes its values in $\mu_r \subset \overline{K}$. For cryptographic applications, we consider $K = \mathbb{F}_q$, with q a prime number, and we define the *embedding degree* k to be such that $\mathbb{F}_{q^k}$ is the smallest field containing μ_r. In other words, $\mathbb{F}_{q^k} = \mathbb{F}_q(\mu_r)$ or alternatively, k is the smallest integer such that $r \mid q^k - 1$.

Computing the Weil pairing

To compute the Weil pairing in practice we use Algorithm 3.2 twice to compute $f_{r,P}(Q)$ and $f_{r,Q}(P)$. Note that in this case, by Remark 3.1, whenever Miller's algorithm fails because we have an intermediate zero or pole, then Q is a multiple of P so $e_{W,r}(P, Q) = 1$. Indeed, if $Q = \lambda P$ then $e_{W,r}(P, Q) = e_{W,r}(P, P)^{\lambda} = 1$ because $e_{W,r}(P, P) = 1$ ($e_{W,r}$ is alternate).

3.2.2 The Tate pairing

The Tate pairing was defined by Tate for number fields in [24, 18] and used by Frey and Rück in the case of finite fields [7]. For simplicity, we assume that $K = \mathbb{F}_q$, with q prime, and that k is the embedding degree corresponding to r (although the construction is valid for any finite field).

THEOREM 3.2 *Let E be an elliptic curve, r a prime number dividing $\#E(\mathbb{F}_q)$, $P \in E[r](\mathbb{F}_{q^k})$ a point of r-torsion defined over $\mathbb{F}_{q^k}$ and $Q \in E(\mathbb{F}_{q^k})$ a point of the elliptic curve defined over $\mathbb{F}_{q^k}$. Let R be any point in $E(\mathbb{F}_{q^k})$ such that $\{R, Q + R\} \cap \{P, 0_E\} = \emptyset$.*
Then

$$e_{T,r}(P, Q) = \left(\frac{f_{r,P}(Q + R)}{f_{r,P}(R)} \right)^{\frac{q^k - 1}{r}} \tag{3.5}$$

is well defined and does not depend on R.

Furthermore, the application

$$\begin{aligned} E[r](\mathbb{F}_{q^k}) \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) &\to \mu_r \\ (P, Q) &\mapsto e_{T,r}(P, Q) \end{aligned}$$

is a pairing, called the Tate pairing.

Proof. See [7]. We give an elementary proof in Section 3.4.4 when all the r-torsion is rational over $\mathbb{F}_{q^k}$. □

When $E(\mathbb{F}_{q^k})$ does not contain a point of r^2-torsion (which is always the case in the cryptographic setting because r is a large prime), then the Tate pairing restricted to the r-torsion is also non-degenerate.

PROPOSITION 3.3 *Assume that $E[r] \subset E(\mathbb{F}_{q^k})$ and that there are no points of r^2-torsion in $E(\mathbb{F}_{q^k})$. Then the inclusion $E[r](\mathbb{F}_{q^k}) \subset E(\mathbb{F}_{q^k})$ induces an isomorphism $E[r] \simeq E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ so the Tate pairing $e_{T,r}$ is a non-degenerate pairing*

$$E[r] \times E[r] \to \mu_r.$$

Proof. Suppose that $P \in E[r](\mathbb{F}_{q^k})$ is equivalent to 0 in $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$. Then by definition there exists a point $P_0 \in E(\mathbb{F}_{q^k})$ such that $P = rP_0$. This means that P_0 is a point of r^2-torsion. By hypothesis there are no non-trivial points of r^2-torsion in $E(\mathbb{F}_{q^k})$, hence we deduce that $E[r] \to E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ is injective. Since both groups have cardinality r^2 (this is shown in the proof of Theorem 3.11), the injection is an isomorphism. □

Computing the Tate pairing

In practice to compute the Tate pairing, when Q is not a multiple of P (for instance when $P \in \mathbb{G}_1$ and $\mathbb{Q} \in \mathbb{G}_2$) one can take $R = 0_E$ so that

$$e_{T,r}(P,Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}}. \tag{3.6}$$

(We can't apply Theorem 3.2 directly with $R = 0_E$, but Theorem 3.11 will show that formula (3.6) is correct). We use Algorithm 3.2 to compute $f_{r,P}(Q)$ and then we do the final exponentiation by a fast exponentiation algorithm. By Remark 3.1 there are no problems during the execution of Miller's algorithm.

Unlike for the Weil pairing, $e_{T,r}(P,P)$ may not be trivial, so if we want to compute $e_{T,r}(P,P)$, or $e_{T,r}(P,Q)$ with Q a multiple of P, then we need to use Equation 3.18 with R a random point in $E(\mathbb{F}_{q^k})$. If we are unlucky and get an intermediate zero or pole, we restart the computation with another random R. An alternative method is to use the general Miller's algorithm described in Section 3.4.2 to compute the Tate pairing.

3.2.3 Using the Weil and the Tate pairing in cryptography

For the applications of the Weil and Tate pairing to cryptography, we will always consider an elliptic curve E defined over $\mathbb{F}_q$ and a large prime number r such that $r \mid \#E(\mathbb{F}_q)$. When the embedding degree k is greater than one, then $E[r]$ is defined over $\mathbb{F}_{q^k}$, and we can define two subgroups $\mathbb{G}_1$ and $\mathbb{G}_2$ of interest for pairing computations.

LEMMA 3.2 (The central setting for cryptography) *Let E be an elliptic curve defined over $\mathbb{F}_q$, r a large prime number such that $r \mid \#E(\mathbb{F}_q)$, and π_q the Frobenius endomorphism. Let k be the embedding degree relative to r, and assume that $k > 1$. Then $E[r] = \mathbb{G}_1 \times \mathbb{G}_2 \subset E(\mathbb{F}_{q^k})$ where*

$$\mathbb{G}_1 = E[r](\mathbb{F}_q) = \{P \in E[r] \mid \pi_q P = P\} \tag{3.7}$$

$$\mathbb{G}_2 = \{P \in E[r] \mid \pi_q P = [q]P\}. \tag{3.8}$$

$\mathbb{G}_1$ is called the rational subgroup of $E[r]$, while $\mathbb{G}_2$ is called the trace zero subgroup.

Proof. The characteristic polynomial of the Frobenius modulo r is the degree two polynomial $X^2 - tX + q$ modulo r where t is the trace. Let λ_1 and λ_2 be the two eigenvalues. Since $r \mid \#E(\mathbb{F}_q)$, there is a rational point of r-torsion in $E(\mathbb{F}_q)$ so that $\lambda_1 = 1$. This implies that $\lambda_2 = q$. Furthermore since $k > 1$, then $q \neq 1 \pmod r$. The two eigenvalues are then distinct, so the action of π_q on $E[r]$ is diagonalisable, and we have

$$E[r] = \mathrm{Ker}(\pi_q - \mathrm{Id}) \oplus \mathrm{Ker}(\pi_q - q\,\mathrm{Id}) = \mathbb{G}_1 \oplus \mathbb{G}_2.$$

Furthermore, let ϕ be the endomorphism given by the trace of the Frobenius (i.e. $\phi = 1 + \pi_q + \cdots + \pi_q^{k-1}$). Then ϕ acts on $\mathbb{G}_1$ by multiplication by k (which in the cryptographic setting will be prime to r), and on $\mathbb{G}_2$ the trace acts by multiplication by $\frac{q^k-1}{q-1}$. Since the embedding degree k is greater than 1 by hypothesis, then $r \mid q^k - 1$ and $r \nmid q - 1$. Hence $r \mid \frac{q^k-1}{q-1}$. We conclude that the trace restricted to $E[r]$ has $\mathbb{G}_2$ as kernel and $\mathbb{G}_1$ as image [3, 4]. This explains the name trace zero subgroup for $\mathbb{G}_2$. □

In practice, when using pairing friendly elliptic curves to compute pairings for cryptographic applications, we will always be in the situation of Lemma 3.2. It will be convenient to restrict the Tate pairing to the subgroups $\mathbb{G}_1$ and $\mathbb{G}_2$ rather than to deal with the full r-torsion. Under some additional hypotheses (which always hold in the cryptographic setting), the Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_2$ or to $\mathbb{G}_2 \times \mathbb{G}_1$ is non-degenerate.

PROPOSITION 3.4 *Assume that we are in the situation of Lemma 3.2. Then the restriction of $e_{W,r}$ to $\mathbb{G}_1 \times \mathbb{G}_2$ or to $\mathbb{G}_2 \times \mathbb{G}_1$ is non-degenerate. If furthermore there are no points of r^2-torsion in $E(\mathbb{F}_{q^k})$, then the restriction of $e_{T,r}$ to $\mathbb{G}_1 \times \mathbb{G}_2$ or to $\mathbb{G}_2 \times \mathbb{G}_1$ is also non-degenerate. More generally, if $\mathbb{G}_3$ is any cyclic subgroup of $E[r]$ different from $\mathbb{G}_1$ and $\mathbb{G}_2$, then the Weil and Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_3$, $\mathbb{G}_3 \times \mathbb{G}_1$, $\mathbb{G}_2 \times \mathbb{G}_3$ and $\mathbb{G}_3 \times \mathbb{G}_2$ is non-degenerate.*

Proof. Note that the Weil pairing is non-degenerate on $E[r]$, but is trivial on $\mathbb{G}_1 \times \mathbb{G}_1$ and $\mathbb{G}_2 \times \mathbb{G}_2$ (because these groups are cyclic and the Weil pairing is alternate). Then since $E[r] = \mathbb{G}_1 \times \mathbb{G}_2$, the Weil pairing has to be non degenerate on $\mathbb{G}_1 \times \mathbb{G}_2$ and $\mathbb{G}_2 \times \mathbb{G}_1$. Given $P \in \mathbb{G}_1$ there exists $Q \in \mathbb{G}_2$ such that $e_{W,r}(P, Q) \neq 1$. There exists $T \in \mathbb{G}_1$ such that $Q + T \in \mathbb{G}_3$, and $e_{W,r}(P, Q + T) = e_{W,r}(P, Q) \neq 1$. Hence the Weil pairing on $\mathbb{G}_1 \times \mathbb{G}_3$ is non degenerate. The same reasoning holds for the other groups. We refer to Section 3.4.4 for the proof for the Tate pairing. □

In the remainder of this chapter, we will always assume that we are in the setting of Proposition 3.4. Moreover, we focus on the optimization of the computation of the Tate pairing, since it is now preferred to the Weil pairing in cryptographic settings. This choice is explained by the fact that the Miller loop only needs to compute the evaluation of a single $f_{r,P}$ function.

Denominator elimination

The final exponentiation of the Tate pairing kills any element γ which lives in a strict subfield of $\mathbb{F}_{q^k}$. In particular we see that replacing $f_{r,P}$ by $\gamma f_{r,P}$ in Equation (3.5) does not change the result. In the execution of Algorithm 3.2, we can then modify the Miller functions $\mathbf{f}_{\lambda,\nu,P}$ by a factor γ in a strict subfield of $\mathbb{F}_{q^k}$ without affecting the final result.

Suppose that P and Q are in $\mathbb{G}_1$ or $\mathbb{G}_2$ and the embedding degree k is even. Remember that by Lemma 3.1, the Miller function $\mathbf{f}_{\lambda,\nu,P} = \mu_{\lambda P,\nu P} = \frac{l_{\lambda P,\nu P}}{v_{\lambda P,\nu P}}$. Then by Lemma 3.3 below, $v_{\lambda P,\nu P}(Q) = x_Q - x_{(\lambda+\nu)P}$ lives in a strict subfield of $\mathbb{F}_{q^k}$ so this factor will be killed by the final exponentiation. Hence in this situation we don't need to compute the division by $v_{\lambda P,\nu P}(Q)$ in Miller's algorithm for the Tate pairing, this is called denominator elimination.

LEMMA 3.3 *Let E be an elliptic curve defined over $\mathbb{F}_q$, be such that $E[r] \subset E(\mathbb{F}_{q^k})$ with k **even**. Let $Q \in \mathbb{G}_1$ or $Q \in \mathbb{G}_2$. Then $x_Q \in \mathbb{F}_{q^{k/2}}$.*

Proof. If $Q \in \mathbb{G}_1$ then $Q \in E(\mathbb{F}_q)$ so both x_Q and y_Q are in $\mathbb{F}_q \subset \mathbb{F}_{q^{k/2}}$. Now if $Q \in \mathbb{G}_2$, then by definition of $\mathbb{G}_2$ we know that $\pi_q^{k/2}(Q) = q^{k/2}Q$. By definition of the embedding degree k, $q^k = 1 \mod r$, so $q^{k/2} = \pm 1 \mod r$. But since k is the smallest integer such that $q^k = 1 \mod r$, we

then have $q^{k/2} = -1 \mod r$. So $\pi_q^{k/2}(Q) = -Q$, and in particular $\pi_q^{k/2}(x_Q) = x_{-Q} = x_Q$. So x_Q is fixed by $\pi_q^{k/2}$, which means that $x_Q \in \mathbb{F}_{q^{k/2}}$. □

To sum up, denominator elimination yields Algorithm 3.3 to compute the Tate pairing over $\mathbb{G}_1 \times \mathbb{G}_2$ or $\mathbb{G}_2 \times \mathbb{G}_1$.

ALGORITHM 3.3 Tate's pairing over $\mathbb{G}_1 \times \mathbb{G}_2$ or $\mathbb{G}_2 \times \mathbb{G}_1$.

Input: $r \in \mathbb{N}$ an odd prime dividing $\#E(\mathbb{F}_q)$ s.t. $k > 1$ is the corresponding embedding degree, k is even and there are no points of r^2-torsion in $E(\mathbb{F}_{q^k})$, $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ (or $P \in \mathbb{G}_2$, $Q \in \mathbb{G}_1$).

Output: The reduced Tate pairing $e_{T,r}(P,Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}}$.

1. Compute the binary decomposition: $r := \sum_{i=0}^{I} b_i 2^i$. Let $T = P, f = 1$.
2. For i in $[I-1..0]$ compute (except at the last step)
   (a) $\alpha = \frac{3x_T^2+a}{2y_T}$, the slope of the tangent of E at T.
   (b) $x_{2T} = \alpha^2 - 2x_T$, $y_{2T} = -y_T - \alpha(x_{2T} - x_T)$;
   (c) $f = f^2 l_{T,T}(Q) = f^2(y_Q - y_T - \alpha(x_Q - x_T))$,
   (d) $T = 2T$,
   (e) If $b_i = 1$, then compute
      i. $\alpha = \frac{y_T - y_P}{x_T - x_P}$, the slope of the line going through P and T;
      ii. $x_{T+P} = \alpha^2 - x_T - x_P$, $y_{T+P} = -y_T - \alpha(x_{T+P} - x_T)$;
      iii. $f = f l_{T,P}(Q) = f(y_Q - y_T - \alpha(x_Q - x_T))$
      iv. $T = T + P$,
3. At the last step: $f = f(x_Q - x_T)$.

Return
$$f^{\frac{q^k-1}{r}}.$$

Finding a non trivial pairing

For all cryptographic applications of pairings, one needs to find two points P and Q on the elliptic curve such that $e(P,Q) \neq 1$. For instance the original use of the Weil pairing was used in [19] as an attack method by reducing the DLP from elliptic curves to finite fields: the MOV attack (see Chapter 9). For the reduction to work, given $P \in E[r](\mathbb{F}_q)$ one need to find a point Q such that $e_{W,r}(P,Q) \neq 1$. Then the DLP between (P, nP) over $E(\mathbb{F}_q)$ reduces to a DLP between $(e_{W,r}(P,Q), e_{W,r}(P,Q)^n)$ over a finite field.

When the embedding degree k is greater than 1 as in Lemma 3.2, then taking any $Q \in G_2 \setminus 0_E$ gives a non degenerate pairing $e_{W,r}(P,Q)$. The same is true for the Tate pairing by Proposition 3.4. However when the embedding degree k is 1, and $E[r](\mathbb{F}_q) =< P >$ is cyclic, then $e_{W,r}(P,P) = 1$. To get a non-degenerate Weil pairing one need to find a $Q \in E[r] \setminus E[r](\mathbb{F}_q)$, and such a point lives over an extension of degree r. But if we replace the Weil pairing by the Tate pairing, then in this case $e_{T,r}(P,P) \neq 1$ by Section 3.4.4. This property was the original reason for the use of the Tate pairing in the article [7].

Pairings of type I,II,III

We conclude the discussion in this section by explaining how to instantiate pairings used in cryptographic protocols, following the classification into three types introduced in Section 1.2.2.

- Type III: The Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_2$ (indeed it is non degenerate by Proposition 3.4).
- Type II: Let $P \in E[r]$ be a point neither in $\mathbb{G}_1$ nor in $\mathbb{G}_2$ and define $\mathbb{G}_3 =< P >$ to be the cyclic subgroup generated by P. Then by Proposition 3.4 the Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_3$ is non-degenerate. Furthermore, since the trace of the Frobenius has image $\mathbb{G}_1$ and kernel $\mathbb{G}_2$, the restriction of the trace to $\mathbb{G}_3$ is an isomorphism between $\mathbb{G}_3$ and $\mathbb{G}_1$, so the the Tate pairing on $\mathbb{G}_1 \times \mathbb{G}_3$ is of Type II.
- Type I: An instantiation of Type I pairings is given by the Tate pairing on $\mathbb{G} \times \mathbb{G}$, where $\mathbb{G} = E[r](\mathbb{F}_q)$, when the embedding degree $k = 1$ and $E[r](\mathbb{F}_q)$ is cyclic as discussed in the paragraph above and in Section 3.4.4.
  Another example is given by supersingular elliptic curves, in the situation of Lemma 3.2. Indeed for a supersingular elliptic curve E there exists a *distorsion map* $\psi : \mathbb{G}_1 = E[r](\mathbb{F}_q) \to E[r](\mathbb{F}_{q^k})$ such that $\psi(\mathbb{G}_1) \neq \mathbb{G}_1$. In particular $e_{W,r}(P, \psi(P)) \neq 1$ and $e_{T,r}(P, \psi(P)) \neq 1$, so composing the Weil or Tate pairing with the distorsion map gives a pairing on $\mathbb{G}_1 \times \mathbb{G}_1$. We refer to [26, 8] for more details on the construction of ψ.

3.2.4 Ate and optimal Ate pairings

Miller's basic algorithm described in the previous section is an extension of the double-and-add method for finding a point multiple. With the inception of pairing-based protocols in the early 2000s, the cryptographic community put in a lot of effort in simplifying and optimizing this algorithm. The complexity of Miller's algorithm heavily depends on the length of the Miller loop. Major progress in pairing computation was made in 2006, with the introduction of the loop shortening technique. This construction, called the eta pairing, was first proposed by Barreto et al. on supersingular curves and further simplified and extended to ordinary curves by Hess et al. In this section, we detail this construction (the ate pairing) and give explicit formulae for its implementation.

By definition when $Q \in \mathbb{G}_2$, $\pi_q(Q) = qQ$. So one can use the Frobenius endomorphism π_q to speed up the scalar multiplication $Q \mapsto rQ$. Since Miller's algorithm is an extended version of the scalar multiplication, one can try to use this property of the Frobenius to speed up the computation of the Miller function $f_{r,Q}$. The first idea was to replace r by $q^k - 1$ (which is a multiple of r), and use the Frobenius to speed up the computation of $f_{q^k,Q}$. This leads to the following result given by Hess et al. [10].

THEOREM 3.3 *Let E be an elliptic curve defined over $\mathbb{F}_q$ and r a large prime with $r|\#E(\mathbb{F}_q)$. Let $k > 1$ be the embedding degree and let $\mathbb{G}_1 = E[r] \cap Ker(\pi_q - \mathrm{Id})$ and $\mathbb{G}_2 = E[r] \cap Ker(\pi_q - q\,\mathrm{Id})$. Let $\lambda \equiv q \pmod r$ and $m = (\lambda^k - 1)/r$. For $Q \in \mathbb{G}_2$ and $P \in \mathbb{G}_1$ we have*

(i) $(Q, P) \mapsto (f_{\lambda,Q}(P))^{(q^k-1)/r}$ *defines a bilinear map on $\mathbb{G}_2 \times \mathbb{G}_1$.*

(ii) *Then* $e_{T,r}(Q, P)^m = f_{\lambda,Q}(P)^{c(q^k-1)/r}$ *where* $c = \sum_{i=0}^{k-1} \lambda^{k-1-i} q^i \equiv kq^{k-1} \pmod r$, *so this map is non degenerate if $r \nmid m$.*

In particular, let t be the trace of the Frobenius, $T = t - 1$ and $L = (T^k - 1)/r$. Then $T \equiv q \pmod r$ so

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

defines a pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ when $r \nmid L$, which we call the Ate pairing.

By Hasse's theorem 2.9, the trace of the Frobenius t is such that $|t| \leq 2\sqrt{q}$. If t is suitably small with respect to r, then the Ate pairing can be computed using a Miller loop of shorter size and are thus faster than the Tate pairing. The exact same algorithm as Algorithm 3.3 allows to compute the Ate pairing by replacing r with T (since denominator elimination holds too).

Other pairings may be obtained from Theorem 3.3, by setting $\lambda \equiv q^i \pmod r$ [27]. Pushing the idea further, one may look at a multiple of cr of r so that we can write $cr = \sum c_i q^i$ with c_i small coefficients. When $Q \in \mathbb{G}_2$, computing the scalar multiplication by cr requires computing the points $c_i Q$, using the Frobenius to compute the $c_i q^i Q$ and then summing everything. The same idea applied to pairings shows that one can then use a suitable combination of Miller functions $f_{c_i,Q}$ to construct a bilinear pairing which is a power m of the Tate pairing. Once again when $r \nmid m$ we get a new pairing.

THEOREM 3.4 *Let $\lambda = \sum_{i=0}^{\phi(k)-1} c_i q^i$ such that $\lambda = mr$, for some integer m. Then $a_{[c_0,\ldots,c_l]} : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$ defined as*

$$(Q,P) \to \left(\prod_{i=0}^{\phi(k)-1} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{\phi(k)-1} \frac{l_{s_{i+1}Q,c_i q^i Q}(P)}{v_{s_i Q}(P)} \right)^{(q^k-1)/r}, \tag{3.9}$$

with $s_i = \sum_{j=i}^{\phi(k)-1} c_j q^j$ defines a bilinear map. This pairing is non-degenerate if and only if $mkq^{k-1} \neq ((q^k-1)/r) \sum_{i=0}^{\phi(k)-1} i c_i q^{i-1} \pmod r$ and we call it the optimal Ate pairing.

Proof. The optimal Ate pairing was proposed by Vercauteren [25]. See Section 3.4.5 where we follow the lines of his proof. □

3.2.5 Using twists to speed up pairing computations

The group $\mathbb{G}_1$ is defined over the base field $\mathbb{F}_q$ so it admits an efficient representation. In particular when computing the Tate pairing over $\mathbb{G}_1 \times \mathbb{G}_2$, the Miller functions are defined over $\mathbb{F}_q$, so most of the operations during the computation are performed in $\mathbb{F}_q$.

We explain here why $\mathbb{G}_2$ also admits an efficient representation: it is isomorphic to a subgroup of order r on a twist defined over a subfield of $\mathbb{F}_{q^k}$. We prove this result here and we will show in the next section that this allows to do part of the pairing computations in a subfield $\mathbb{F}_{q^e}$, with $e \mid k$, rather than in $\mathbb{F}_{q^k}$.

THEOREM 3.5 *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ admitting a twist of degree d. Assume that r is an integer such that $r || \#E(\mathbb{F}_q)$ and let $k > 2$ be the embedding degree. Then there is a unique twist E' such that $r || \#E'(\mathbb{F}_{q^e})$, where $e = k/\gcd(k,d)$. Furthermore, if we denote by $\mathbb{G}_2'$ the unique subgroup of order r of $E'(\mathbb{F}_q)$ and by $\Psi : E' \to E$ the twisting isomorphism, the subgroup $\mathbb{G}_2$ is given by $\mathbb{G}_2 = \phi(\mathbb{G}_2')$ and verifies the equation*

$$\mathbb{G}_2 = E[r] \cap Ker([\xi_d]\pi_{q^e} - \mathrm{Id}),$$

where $[\xi_d]$ is an automorphism of order dividing d.

Proof. Replacing d by $\gcd(k,d)$ we can assume that $d \mid k$ and that $e = k/d$. Take $Q \in \mathbb{G}_2$. By the definition of $\mathbb{G}_2$ we know that $\pi^e(Q) = q^e Q$. But since k is the smallest integer such that $q^k = 1 \pmod r$, we have that $q^e = \xi_d \pmod r$, where ξ_d is d-th primitive root of unity in $\mathbb{F}_{q^k}$.

Note that we have an isomorphism $[] : \mu_d \to \mathrm{Aut}(E)$ ([22, Corollary III.10.2]). Points in $\mathbb{G}_2$ are eigenvectors for any endomorphism on the curve and we denote by $[\xi_d]$ the automorphism such that $[\xi_d]Q = \xi_d^{-1}Q \pmod r$.

Let E' be a twist of degree d of E, defined over $\mathbb{F}_{q^e}$, such that $\Psi \circ (\Psi^{-1})^\sigma$ (with $\cdot^\sigma$ the action of the Frobenius on the coefficients of the automorphism) is the automorphism $[\xi_d]$ on E. If we denote by π_{q^e} the Frobenius morphism on E', we observe that $\Psi \circ \pi_{q^e} \circ \Psi^{-1} = \Psi \circ (\Psi^{-1})^\sigma \circ \pi_{q^e}$. Therefore we have

$$\mathbb{G}_2 = \mathrm{Ker}([\xi_d]\pi_{q^e} - \mathrm{Id}).$$

Let $\mathbb{G}_2' = \Psi^{-1}(\mathbb{G}_2)$. Then $\Psi \circ \pi_{q^e} \circ \Psi^{-1}(\mathbb{G}_2) = \mathbb{G}_2$. It follows that $\mathbb{G}_2'$ is invariant under π_{q^e}, hence it is defined over $\mathbb{F}_{q^e}$. □

Using the result one can compute the Miller loop for the Ate (or optimal Ate) pairing $a_T(Q, P)$ by working over $\mathbb{G}_2'$ to compute the multiples of $\Psi^{-1}(Q)$, and going back to $\mathbb{G}_2$ only to evaluate the Miller functions on P. Alternatively one can do the full computation on the twist E', as shown in [6].

THEOREM 3.6 *Let E be an elliptic curve defined over $\mathbb{F}_q$ Assume that r is an integer such that $r||\#E(\mathbb{F}_q)$ and let $k > 2$ be the embedding degree. Let E' be the twist of degree d and $\Psi : E' \to E$ the associated twist isomorphism, as in Theorem 3.5. Consider $Q \in \mathbb{G}_2$, $P \in \mathbb{G}_1$, and let $Q' = \Psi^{-1}(Q)$ and $P' = \Psi^{-1}(P)$. Let $a_T(Q, P)$ be the Ate pairing of Q and P. Then*

$$a_T(Q, P)^{\gcd(d,6)} = a_T(Q', P')^{\gcd(d,6)}$$

where $a_T(Q', P') = f_{T,Q'}(P')^{(q^k-1)/r}$ uses the same parameter loop.

This shows that the pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ may be seen as a $\mathbb{G}_1 \times \mathbb{G}_2$ pairing on a twist defined over $\mathbb{F}_{q^e}$. Indeed since $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}([\xi_d]\pi_{q^e} - \mathrm{Id})$ by Theorem 3.5, $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}([\xi_d]\pi_{q^e} - q^e \mathrm{Id})$, so $\Psi^{-1}(\mathbb{G}_2) = \mathbb{G}_1(E')$ and $\Psi^{-1}(\mathbb{G}_1) = \mathbb{G}_2(E')$, with $\mathbb{G}_1(E')$ and $\mathbb{G}_2(E')$ are the subgroups giving the eigenvectors of the Frobenius on E'

The twist improves the Ate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ by giving an efficient representation of $\mathbb{G}_2$. Alternatively, it can be used to give a shorter Miller loop for pairings on $\mathbb{G}_1 \times \mathbb{G}_2$ [13].

THEOREM 3.7 *Let $\lambda \equiv q \pmod r$ and $m = (\lambda^k - 1)/r$. Assume that E has a twist of degree d and set and set $n = \gcd(k, d)$, $e = k/n$.*

(i) $(P, Q) \mapsto (f_{\lambda^e,P}(Q))^{(q^k-1)/r}$ *defines a bilinear map on* $\mathbb{G}_1 \times \mathbb{G}_2$.

(ii) $e_{T,r}(P, Q)^L = f_{\lambda^e,P}(Q)^{c(q^k-1)/N}$ *where* $c = \sum_{i=0}^{n-1} \lambda^{e(n-1-i)} q^{ei} \equiv nq^{e(n-1)} \pmod r$, *so this map is non-degenerate if* $r \nmid m$.

In particular, if t is the trace of the Frobenius, $T = t - 1$, and $L = (T^k - 1)/r$, then $(P, Q) \mapsto (f_{T^e,P}(Q))^{(q^k-1)/r}$ defines a pairing if $r \nmid L$, which we call the twisted Ate pairing.

One can also define a twisted optimal Ate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$. This was given by Hess [12], using a general formula for the pairing function. We present it here in a simplified way, better suited for implementations.

THEOREM 3.8 *Assume that E has a twist of degree d and set $n = \gcd(k, d)$, $e = k/n$. Let $\lambda = \sum_{i=0}^{\phi(k)/e-1} c_i q^{ie}$ such that $\lambda = mr$, for some integer m. Then*

$$\begin{aligned} a_{[c_0,\ldots,c_l]} : \mathbb{G}_1 \times \mathbb{G}_2 &\rightarrow \mu_r \\ (P,Q) &\rightarrow \left(\prod_{i=0}^{\phi(k)/e-1} f_{c_i,P}^{q^{ie}}(Q) \cdot \prod_{i=0}^{\phi(k)/e-1} \frac{l_{s_{i+1}P,c_i q^{ie} P}(Q)}{v_{s_i P}(Q)} \right)^{(q^k-1)/r}, \end{aligned} \tag{3.10}$$

where $s_i = \sum_{j=i}^{\phi(k)/e-1} c_j q^{je}$, defines a bilinear map on $\mathbb{G}_1 \times \mathbb{G}_2$. This pairing is non-degenerate if and only if $mkq^{k-1} \neq ((q^k-1)/r) \sum_{i=0}^{\phi(k)/e-1} i c_i q^{e(i-1)} \pmod r$.

Proof. See Section 3.4.5. □

3.2.6 The optimal Ate and twisted optimal Ate in practice

In order for the optimal Ate and twisted optimal Ate pairings to give a short Miller loop, we would like the coefficients c_i to be as small as possible. The idea is to search for the coefficients c_i in Equations 3.9 and 3.10 by computing short vectors in the following lattice

$$\begin{pmatrix} r & 0 & 0 & \ldots & 0 \\ -q & 1 & 0 & \ldots & 0 \\ -q^2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -q^l & 0 & 0 & \ldots & 1 \end{pmatrix}, \tag{3.11}$$

where l is either $\phi(k) - 1$ in the optimal Ate pairing case, and $\phi(k)/e - 1$, in the twisted Ate case. The volume of this lattice is r, hence by Minkowski's theorem there is a short vector v in the lattice such that $||v||_\infty \leq r^{1/l+1}$.

Starting from this bound and Theorem 3.4, Vercauteren discusses the existence of pairings that may be computed with a Miller loop of size $(\log r)/\phi(k)$. Note that Theorem 3.4 does not guarantee that the pairing defined in Equation 3.9 can be computed in $(\log r)/\phi(k)$ operations. If the procedure described above produces a short vector with several c_i coefficients different from zero, then computing each $f_{c_i,Q}(P)$ separately costs $O((\log r)/\phi(k))$ operations. Possible optimizations would be to use multi-exponentiation techniques or a parallel version of Miller's algorithm to compute all the $f_{c_i,Q}(P)$ functions at once. However, in the case of parametric families introduced in Chapter 4, the entire computation can be carried with a single basic Miller loop and the pairing given in Theorem 3.4 is indeed optimal, thanks to the special form of the short vectors we obtain. To explain this idea, we give explicit formulae for this computation in the case of several Brezing-Weng type constructions of pairing-friendly curves. Since k is small, these formulae can be obtained by computing short vectors for the lattice given by the matrix 3.11, by using an available implementation of the LLL algorithm. We recommend using for instance the functions `LLL()` or `BKZ()` in Sage [23].

Example 3.1 [25, Vercauteren] We consider the Barreto-Naehrig family of curves, that was introduced in **??**. We briefly remind here that these families have embedding degree 12 are given by the following parametrizations:

$$\begin{aligned} r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t(x) &= 6x^2 + 1, \\ q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1. \end{aligned}$$

By Theorem 3.3, the length of Miller's loop for the Ate pairing is $\frac{\log_2 r}{2}$. We will show that the complexity of the computation of the optimal Ate pairing for this family is $O(\frac{\log_2 r}{4})$. Indeed, in order to apply Theorem 3.4, we compute the following short vector:

$$[6x+2, 1, -1, 1].$$

Note that in this case, 3 out of the 4 coefficients in the short vector are trivial. We conclude that the optimal twisted Ate pairing for this family of curves is given by the simple formula:

$$(f_{6x+2,Q}(P) \cdot l_{Q_3,-Q_2}(P) l_{-Q_2+Q_3,Q_1}(P) l_{Q_1-Q_2+Q_3,[6x+2]Q}(P))^{\frac{q^{12}-1}{r}},$$

where $Q_i = Q^{q^i}$, for $i = 1, 2, 3$. Note that the evaluation at Q of the vertical line $v_{(x^3-x^2+1)tP}$ can actually be ignored because of the final exponentiation. The only costly computation is that of $f_{6x+2,Q}(P)$ and costs $O(\log r/2)$ operations. While the twisted Ate has loop length $\log r$, a search for a short vector giving the optimal twisted Ate pairing gives

$$[6x^2 + 2x, 2x + 1].$$

Hence we need to compute $f_{x,P}(Q)$, $f_{x^2,P}(Q)$ and the complexity of computation is $O(\log r/2)$.

Example 3.2 We consider here the family of curves with $k = 18$ proposed by *Kachisa et al.*, whose construction is given in Chapter 4. We briefly recall that this family is parametrized by the following polynomials

$$\begin{aligned} r(x) &= x^6 + 37x^3 + 343, \\ t(x) &= \frac{1}{7}(x^4 + 16x + 7), \\ q(x) &= \frac{1}{21}(x^8 + 5x^7 + 7x^6 + 37x^5 + 188x^4 + 259x^3 + 343x^2 + 1763x + 2401). \end{aligned}$$

A similar search for the optimal pairing on curves with embedding degree 18 gives, for example, the short vector

$$[1, x^3 + 18].$$

Hence the complexity of Miller's algorithm is $\frac{\log_2 r}{2}$. The optimal Ate pairing computation for curves with $k = 18$ has complexity $\mathcal{O}(\frac{\log r}{6})$.

Building on these results, Vercauteren [25] introduces the concept of optimal pairing, i.e. a pairing that is computed in $\log r/\phi(k)$ Miller iterations. He puts forward the following conjecture:

Optimality conjecture: Any non-degenerate pairing on an elliptic curve without any efficiently computable endomorphisms different from the powers of the Frobenius requires at least $O(\log r/\phi(k))$ basic Miller iterations.

Hess [12] proved the optimality conjecture for all known pairing functions. The pairings given by the formulae in Theorem 3.4 are the fastest known pairings at the time of this writing. On curves endowed with efficiently computable endomorphisms other than the Frobenius (such as automorphisms), it is currently not known how to use the action of these endomorphisms to improve on pairing computation.

Choosing the right pairing

Assume that we are in the situation of Proposition 3.4, and let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. Then one may choose among the Tate pairing $e_{r,W}(P,Q)$, the Ate (or Optimal Ate) pairing $a_{r,T}(P,Q)$, the twisted Ate pairing ... Furthermore, when k is even, we can apply denominator elimination for the Tate pairing thanks to the final exponentiation. On the downside, one should remember that the final exponentiation may be expensive too. Indeed, the loop length of the final exponentiation is around $k \log q$ compared to $\log q$ for the Miller step. So the implementation of the final exponentiation step should not be neglected and we will give in Chapter 7 efficient algorithms for its computation.

We conclude that the choice of parameters for applications is a complex matter, with multiple aspects to take into account. Therefore, we devote the whole Chapter 10 to discussing this problem. In the remainder of this chapter, we give optimized formulae for computing one step of a Miller loop.

3.3 Formulae for pairing computation

One of the most efficient ways of computing pairings on an elliptic curve given by a Weierstrass equation is to use Jacobian coordinates [17] [9]. A point $[X,Y,Z]$ in Jacobian coordinates represents the affine point $(X/Z^2, Y/Z^3)$ on the elliptic curve. A point in projective coordinates $[X,Y,Z]$ represents the point $(X/Z, Y/Z)$ on the elliptic curve.

In this section we denote by $\mathbf{s}$ and $\mathbf{m}$ the costs of squaring and multiplication in $\mathbb{F}_q$ and by $\mathbf{S}$ and $\mathbf{M}$ the costs of these operations in the extension field $\mathbb{F}_{q^k}$, if $k > 1$. We denote by $\mathbf{d}_a$ the cost of the multiplication by a constant a. Sometimes, if q is a sparse prime (such as a generalized Mersenne prime), we may assume that $\mathbf{s}/\mathbf{m} = 0.8$. However, when constructing pairing friendly curves, it is difficult to obtain such primes. Hence, we generally have $\mathbf{s}/\mathbf{m} \approx 1$.

3.3.1 Curves with twists of degree 2

In the remainder of this section, we suppose that the embedding degree is even and that E has a twist of order 2 defined over $\mathbb{F}_{q^{k/2}}$. From Theorem 3.5 and by using the equations of twists given in Subsection 2.3.6, we derive an efficient representation of points in $\mathbb{G}_2$. It follows that the subgroup $\mathbb{G}_2 = \langle Q \rangle \subset E(\mathbb{F}_{q^k})$ can be chosen such that the x-coordinates of all its points lie in $\mathbb{F}_{q^{k/2}}$ and the y-coordinates are products of elements of $\mathbb{F}_{q^{k/2}}$ with $\sqrt{\beta}$, where β is not a square in $\mathbb{F}_{q^{k/2}}$ and $\sqrt{\beta}$ is a fixed square root in $\mathbb{F}_{q^k}$.

For curves with twists of degree 2, the fastest known formulae for Miller's algorithm doubling [14] and addition steps [1] are in Jacobian coordinates. Therefore we represent the point T as $T = [X_1, Y_1, Z_1, W_1]$, where $[X_1, Y_1, Z_1]$ are the Jacobian coordinates of the point T on the Weierstrass curve and $W_1 = Z_1^2$.

The doubling step

We will look at the doubling step in the Miller loop. We represent the point T as $T = (X_1, Y_1, Z_1, W_1)$, where (X_1, Y_1, Z_1) are the Jacobian coordinates of the point T on the Weierstrass curve and $W_1 = Z_1^2$. We compute $2T = (X_3, Y_3, Z_3, W_3)$ as:

$$\begin{aligned} X_3 &= (3X_1^2 + aW_1^2)^2 - 8X_1Y_1^2, \\ Y_3 &= (3X_1^2 + aW_1^2)(4X_1Y_1^2 - X_3) - 8Y_1^4, \\ Z_3 &= 2Y_1Z_1 \\ W_3 &= Z_3^2. \end{aligned}$$

We write the normalized function $l_{T,T}$ that appears in Algorithm (3.3) as :

$$l_{T,T}(x_Q, y_Q) = (Z_3W_1y - 2Y_1^2 - (3X_1^2 + aW_1^2)(W_1x - X_1))/(Z_3W_1)$$

Thanks to elimination in the final exponentiation, the term Z_3W_1 can be ignored. For $k = 2$, we have that $x \in \mathbb{F}_q$ and we can compute the function $l_{T,T}$ as

$$l_{T,T}(x, y) = Z_3W_1y - 2Y_1^2 - (3X_1^2 + aW_1^2)(W_1x - X_1).$$

For $k > 2$, we have that x is in $\mathbb{F}_{q^{k/2}}$ and the computation is slightly different

$$l_{T,T}(x, y) = Z_3W_1y - 2Y_1^2 - W_1(3X_1^2 + aW_1^2)x + X_1(3X_1^2 + aW_1^2).$$

The computations are done in the following order:

$$\begin{aligned}
A &= W_1^2,\ B = X_1^2,\ C = Y_1^2,\ D = C^2, E = (X_1 + C)^2 - B - D,\\
F &= 3B + aA,\ G = F^2, X_3 = -4E + G,\ Y_3 = -8D + F \cdot (2E - X_3),\\
Z_3 &= (Y_1 + Z_1)^2 - C - W_1, W_3 = Z_3^2,\ H = (Z_3 + W_1)^2 - W_3 - A,\ I = H \cdot y,\\
J &= (F + W_1)^2 - G - A,\ K = J \cdot x,\ L = (F + X_1)^2 - G - B\\
l_{T,T} &= I - 4C - K + L, f = f^2 \cdot l_{T,T}.
\end{aligned}$$

The operation count gives $10\mathbf{s}+3\mathbf{m}+1\mathbf{a}+1\mathbf{S}+1\mathbf{M}$ for $k = 2$ and $11\mathbf{s}+(k+1)\mathbf{m}+1\mathbf{d}_a+1\mathbf{S}+1\mathbf{M}$ if $k > 2$.

The mixed addition step

In implementations, it is often possible to choose the point P such that its Z-coordinate is 1, in order to save some operations. The addition of two points $T = [X_1, Y_1, Z_1]$ and $P = [X_2, Y_2, 1]$ is called *mixed addition*.

The result of the addition of $T = [X_1, Y_1, Z_1, W_1]$ and $P = [X_2, Y_2, 1]$ is $T+P = [X_3, Y_3, Z_3, W_3]$ with

$$\begin{aligned}
X_3 &= (X_1 + X_2Z_1^2)(X_1 - X_2Z_1^2)^2 + (Y_2Z_1^3 - Y_1)^2,\\
Y_3 &= (Y_2Z_1^3 - Y_1)(X_1(X_1 - X_2Z_1^2)^2 - X_3) + Y_1(X_1 - X_2Z_1^2)^2,\\
Z_3 &= Z_1(X_2Z_1^2 - X_1),\\
W_3 &= Z_3^2,\\
T_3 &= W_3x_Q - X_3.
\end{aligned}$$

The line $l_{T,P}$ is given by the equation:

$$l_{T,P} = Z_3y_Q - Y_2Z_3 - (2Y_2Z_1^3 - 2Y_1)(x_Q - X_2).$$

The computations are done in the following order:

$$\begin{aligned}
A &= Y_2^2, B = X_2 \cdot W_1, D = ((Y_2 + Z_1)^2 - A - W_1) \cdot W_1, H = B - X_1, I = H^2\\
E &= 4I, J = H \cdot E, L_1 = D - 2Y_1, V = X_1 \cdot E, X_3 = L_1^2 - J - 2V, Y_3 = (D - Y_1) \cdot (V - X_3) - 2Y_1 \cdot I\\
Z_3 &= (Z_1 + H)^2 - W_1 - I, W_3 = Z_3^2, l_{T,P} = 2Z_3 \cdot y_Q - (Y_2 + Z_3)^2 + A + W_3 - 2L_1 \cdot (x_Q - X_2)
\end{aligned}$$

The operation count gives $6\mathbf{s} + 6\mathbf{m} + k\mathbf{m} + 1\mathbf{M}$ [1].

3.3.2 Curves with equation $y^2 = x^3 + ax$

These curves have twists of degree 4. Therefore, by using the equations for twists given in Section 2.3.6 and Theorem 3.5, we derive that a point $Q \in \mathbb{G}_2$ may be written as

$$(x_Q, y_Q) = (x'_Q \nu^{1/2}, y'_Q \nu^{3/4})$$

where $x_{Q'}, y_{Q'}, \nu \in \mathbb{F}_{q^{k/4}}$ and $X^4 - \nu$ is an irreducible polynomial. Moreover, thanks to the simple form of the Weierstrass equation, the doubling and addition formulae for these curves are simpler and faster than in the case of curves allowing only twists of degree 2. The fastest formulae for pairing computation on these curves [6] use Jacobian coordinates. In the doubling step, we compute $2T$ as

$$\begin{aligned} X_3 &= (X_1^2 - aZ_1^2)^2 \\ Y_3 &= 2Y_1(X_1^2 - aZ_1^2)((X_1^2 + aZ_1^2)^2 + 4aZ_1^2X_1^2) \\ Z_3 &= 4Y_1^2. \end{aligned}$$

The line function is

$$l_{T,T} = -2(3X_1^2Z_1 + aZ_1^3)x_Q + (4Y_1Z_1)y_Q + 2(X_1^3 - aZ_1^2X_1)$$

The computation is done using the following sequence of operations:

$$\begin{aligned} A &= X_1^2, B = Y_1^2, C = Z_1^2, D = aC, X_3 = (A - D)^2, \\ E &= 2(A + D)^2 - X^3, F = ((A - D + Y_1)^2 - B - X_3), Y_3 = E \cdot F, Z_3 = 4B \\ G &= -2Z_1(3 \cdot A + D), H = 2((Y_1 + Z_1)^2 - B - C), II = (X_1 + A - D)^2 - X_3 - A, \\ l_{T,T} &= G \cdot x_Q + H \cdot y_Q + II. \end{aligned}$$

The total cost is $(2k/d + 2)\mathbf{m} + 8\mathbf{s} + 1\mathbf{d}_a$. In the mixed addition step of $T = (X_1, Y_1, Z_1)$ and $P = (X_2, Y_2, 1)$ is $T + P = (X_3, Y_3, Z_3)$ with

$$\begin{aligned} X_3 &= (Y_1 - Y_2Z_1^2)^2 - (X_1 + X_2Z_1)S, \\ Y_3 &= ((Y_1 - Y_2Z_1^2)(X_1S - X_3) - Y_1SU)UZ_1, \\ Z_3 &= (UZ_1)^2, \end{aligned}$$

where $S = (X_1 - X_2Z_1)^2Z_1$ and $U = X_1 - X_2Z_1$. This is computed with the following operations

$$\begin{aligned} A &= Z_1^2, E = X_2 \cdot Z_1, G = Y_2 \cdot A, H = D - E, I = 2(Y_1 - G), II = I^2, J = 2Z_1 \cdot H \\ K &= 4J \cdot H, X_3 = 2II - (X_1 + E) \cdot K, Z_3 = J^2 \\ Y_3 &= ((J + I)^2 - Z_3 - II) \cdot (X_1 \cdot K - X_3) - Y_1 \cdot K^2, Z_3 = 2Z_3 \\ l_{T,P} &= I \cdot X_2 - I \cdot x_Q + J \cdot y_Q - J \cdot Y_2 \end{aligned}$$

The total cost of the computation is $((2k/d) + 9)\mathbf{m} + 5\mathbf{s}$.

3.3.3 Curves with equation $y^2 = x^3 + b$

These curves have twists of degree 6. Therefore, by using the equations for twists given in Section 2.3.6 and Theorem 2.12, we derive that a point $Q \in \mathbb{G}_2$ may be written as

$$(x_Q, y_Q) = (x'_Q \nu^{1/3}, y'_Q \nu^{1/2}),$$

TABLE 3.1 Cost of one step in Miller's algorithm for even embedding degree

	Doubling		Mixed addition
	$k=2$	$k \geq 4$	
$\mathcal{J}$ [14],[1]	$3\mathbf{m}+10\mathbf{s}+1\mathbf{a}+1\mathbf{M}+1\mathbf{S}$	(1+k)$\mathbf{m}$+11$\mathbf{s}$+1$\mathbf{a}$+1$\mathbf{M}$+1$\mathbf{S}$	(6+k)$\mathbf{m}$+6$\mathbf{s}$+1$\mathbf{M}$
$\mathcal{J}$,$y^2=x^3+b$ $e=2,6$ [6]	(2k/e+2)$\mathbf{m}$+7$\mathbf{s}$+1$\mathbf{a}$+1$\mathbf{M}$+1$\mathbf{S}$	(2k/e+2)$\mathbf{m}$+7$\mathbf{s}$+1$\mathbf{a}$+1$\mathbf{M}$+1$\mathbf{S}$	(2k/e+9)$\mathbf{m}$+2$\mathbf{s}$+1$\mathbf{M}$
$\mathcal{J}$, $y^2=x^3+ax$ $e=2,4$ [6]	(2k/e+2)$\mathbf{m}$+8$\mathbf{s}$+1$\mathbf{a}$+ 1$\mathbf{M}$+1$\mathbf{S}$	(2k/e+2)$\mathbf{m}$+8$\mathbf{s}$+1$\mathbf{a}$+ 1$\mathbf{M}$+1$\mathbf{S}$	(2k/e+12)$\mathbf{m}$+4$\mathbf{s}$+1$\mathbf{M}$

where $x_{Q'}, y_{Q'}, \nu \in \mathbb{F}_{q^{k/6}}$ and $X^6-\nu$ is an irreducible polynomial. The fastest existing formulae on these curves use projective coordinates. Following [6], we compute $2T$ as:

$$\begin{aligned} X_3 &= 2X_1Y_1(Y_1^2-9bZ_1^2) \\ Y_3 &= Y_1^4+18bY_1^2Z_1^2-27b^2Z_1^4 \\ Z_3 &= 8Y_1^3Z_1 \end{aligned}$$

The line equation is

$$l_{T,T} = 3X_1^2 \cdot x_Q - 2Y_1Z_1 \cdot y_Q + 3bZ_1^2 - Y_1^2.$$

The computation is performed in the following order:

$$\begin{aligned} A &= X_1^2, B = Y_1^2, C = Z_1^2, D = 3bC, E = (X_1+Y_1)^2 - A - B, \\ F &= (Y_1+Z_1)^2 - B - C, G = 3D, X_3 = E \cdot (B-G), \\ Y_3 &= (B+G)^2 - 12D^2, Z_3 = 4B \cdot F, H = 3A, I = -F, J = D - B. \\ l_{T,T} &= H \cdot x_Q + I \cdot y_Q + J. \end{aligned}$$

The total count for the above sequence of operations is $(2k/d)\mathbf{m}+5\mathbf{s}+1\mathbf{d}_b$. In the mixed addition step of $T=(X_1,Y_1,Z_1)$ and $P=(X_2,Y_2,1)$ is $T+P=(X_3,Y_3,Z_3)$ with

$$\begin{aligned} X_3 &= (X_1-Z_1X_2)(Z_1(Y_1-Z_1Y_2)^2 - c(X_1+Z_1X_2)(X-Z_1X_2)^2), \\ Y_3 &= (Y_1-Z_1Y_2)(c(2X_1+Z_1X_2)(X_1Z_2-Z_1X_2)^2 - Z_1(Y_1-Z_1Y_2)^2) - cY_1(X_1Z_2-Z_1X_2)^3, \\ Z_3 &= cZ_1(X_1-Z_1X_2)^3, \end{aligned}$$

where $c=1/b$. The line formula is given by

$$l_{T,P} = (Y_1-Z_1Y_2)\cdot(X_2-x_Q) - (X_1-Z_1X_2)\cdot Y_2 + (X_1-Z_1X_2)\cdot Z_2 y_Q$$

The computation is performed using the following sequence of operations :

$$\begin{aligned} t_1 &= Z_1 \cdot X_2, t_1 = X_1 - t_1, t_2 = Z_1 \cdot Y_2, t_2 = Y_2 - t_2, g = c_1 \cdot t_2 - t_1 \cdot Y_2 + t_1 \cdot y_Q \\ t_3 &= t_1^2, t_3 = c \cdot t_3, X_3 = t_3 \cdot X_1, t_3 = t_1 \cdot t_3, t_4 = t_2^2 \\ t_4 &= t_4 \cdot Z_1, t_4 = t_3 + t_4, t_4 = t_4 - X_3, X_3 = X_3 - t_4, t_2 = t_2 \cdot X_3, Y_3 = t_3 \cdot Y_1 \\ Y_3 &= t_2 - Y_3, X_3 = t_1 \cdot t_4, Z_3 = Z_1 \cdot t_3, \end{aligned}$$

where $c_1 = X_2 - x_Q$. The total cost is $(2k/d+9)\mathbf{m}+2\mathbf{s}$. In Table 3.1 we summarize all these results.

3.4 Appendix: the general form of the Weil and Tate pairing

The versions of the Tate and Weil pairing we gave required to evaluate a function on a point. In this section we will give a generalised definition which requires to evaluate a function on a divisor.

Furthermore, we have seen that during the execution of Miller's algorithm, some intermediate poles and zeroes are introduced. As we pointed out, this is not really a problem in practice, since this situation only happens when computing a pairing between P and Q with Q a multiple of P. As explained in Section 3.2.2, for the Tate pairing we can circumvent the problem by using a random point R.

Another way to circumvent the problem is to define the (extended) evaluation of a function on a point or a divisor even in the case when the supports are non disjoint. This allow us to generalize Miller's algorithm so that it always works and to give a more general definition of the Weil and Tate pairing. From this more general definition, we can prove their bilinearity and that they are non degenerate.

3.4.1 Evaluating functions on a divisor

If $D = \sum n_i[P_i]$ is a divisor on E, we define the *support* $\mathrm{supp}(D)$ as the set $\{P_i \mid n_i \neq 0\}$. By abuse of langage we define the support of f as the support of $\mathrm{div}\, f$, so the support of f is simply the union of the zeroes and poles of f.

If the support of f and the support of D are disjoint, then one can define the evaluation of f on $D = \sum n_i P_i$ as

$$f(D) = \prod_i f(P_i)^{n_i}. \tag{3.12}$$

It is easy to check that we have $(fg)(D) = f(D).g(D)$ and $f(D_1 + D_2) = f(D_1).f(D_2)$.

One can extend this definition even when the supports are non disjoint by *fixing once and for all* uniformisers t_P for every points $P \in E(K)$. Then one can define the *extended evaluation* of f at P as $(\frac{f}{t_P^{\mathrm{ord}_P(f)}}(P), \mathrm{ord}_P(f))$. We will often simply refer to $\frac{f}{t_P^{\mathrm{ord}_P(f)}}(P)$ as the *value* of f at P and to $\mathrm{ord}_P(f)$ as the *valuation* (or the *order*) of this value. If P is not in the support of f then the extended evaluation of f at P is simply $(f(P), 0)$. One can define a product on the extended values by taking the product of the values and adding the valuations: $(\alpha, n).(\beta, m) = (\alpha\beta, n+m)$. This definition of the product allows us to have the standard property:

$$(fg)(P) = f(P).g(P).$$

By using Equation (3.12) one can define the extended evaluation of f at a divisor $D = \sum n_i P_i$ as $f(D) = \prod_i f(P)^{n_i}$ where this time the product is on extended values. By the definition of $f(D)$ and the product on extended values we have $(fg)(D) = f(D).g(D)$ and $f(D_1 + D_2) = f(D_1).f(D_2)$.

When D and f do not have disjoint supports, one needs to be careful that the extended value $f(D)$ depends on choice of uniformisers and is not intrinsic to the curve. For example if P is a point in the support of f with order n, then changing the uniformiser t_P at P by $t'_P = \alpha t_P$ change the value by α^{-n} (but the order stays the same). So in the following we fix once and for all the following uniformisers for the elliptic curve:

- $t_{0_E} = x/y$;
- $t_P = x - x_P$, except when $H(x_P) = 0$;
- $t_P = y$, when $H(x_P) = 0$ (so $y_P = 0$).

A powerful tool used in computing evaluation of divisors is Weil's reciprocity theorem.

THEOREM 3.9 (Weil's reciprocity theorem) *Let $f, g \in K(E)$. Then*

$$f(\mathrm{div}(g)) = (-1)^{\sum_P \mathrm{ord}_P(f)\,\mathrm{ord}_P(g)} g(\mathrm{div}(f)).$$

Expressing the above equation in terms of divisors (see Definition 3.1, we get the following reformulation: Let D_1 and D_2 be two degree 0 divisors and define $\epsilon(D_1, D_2) = (-1)^{\sum_P \mathrm{ord}_P(D_1)\,\mathrm{ord}_P(D_2)}$. If D_1 and D_2 are principal, then

$$f_{D_1}(D_2) = \epsilon(D_1, D_2) f_{D_2}(D_1).$$

Proof. See [21, p. 44–46]. □

3.4.2 Miller's algorithm for pairing computation

Let $f \in k(E)$ be a rational function on E and D a divisor of degree 0. Then $f(D)$ depends only on $\mathrm{div}(f)$, not on f. Indeed, if g has the same divisor as f, there exists $\lambda \in K^*$ such that $g = \lambda f$ so that $g(D) = \lambda^{\deg D} f(D) = f(D)$. One can see the divisor $F = \mathrm{div}\, f$ as an efficient way to encode the rational function f. Recall that we note f_F the normalised function with divisor F.

As we have seen in Section 3.2, all pairing computations involve the following computation: given $P \neq 0_E$ a point of r-torsion on E, and $Q \neq P, 0_E$ a point of the elliptic curve, evaluate $f_{r,P}(Q)$. We recall that $f_{r,P}$ is the normalised function with divisor $r([P] - [0_E])$.

This computation is a particular case of the following more general framework: *Let $P \neq 0_E$ be a point of r-torsion on E, and $Q \neq 0_E$ a point of the elliptic curve. Let D_P and D_Q be two divisors linearly equivalent to $[P] - [0_E]$ and $[Q] - [0_E]$ respectively. Then evaluate the function f_{rD_P} on the divisor D_Q.*

The evaluation makes sense because $r[P] - r[0_E]$ is a principal divisor by Proposition 3.1, so rD_P is principal too. Taking $D_P = [P] - [0_E]$ and $D_Q = [Q] - [0_E]$, we recover the previous computation since by Definition 3.3, the evaluation of a function associated to $r[P] - r[0_E]$ on $[Q] - [0_E]$ is simply $f_{r,P}(Q)$. One has to take care here that the divisors $r[P] - r[0_E]$ and $[Q] - [0_E]$ do not have disjoint support, so the evaluations above are to be understood as extended evaluations: if $P \neq Q$ then the value $f_{r,P}(Q)$ has valuation $-r$, otherwise the value has valuation $r - r = 0$.

We have seen in Section 3.1 how to use Miller's algorithm to compute $f_{r,P}(Q)$. More generally, given F and D two degree zero divisors, we give a general version of Miller's algorithm which allows to compute the value $f_F(D)$. The key principle behind this extended Miller's algorithm is to use the functions $\mu_{P,Q}$ introduced in Definition 3.2.

Whenever we have two points P and Q different from 0_E in the support of F, we can decompose F as $F = [P] + [Q] + F'$ and then use the function $\mu_{P,Q}$ to get $F = [P] + [Q] - [P+Q] - [0_E] + [P+Q] + [0_E] + F' = \mathrm{div}(\mu_{P,Q}) + [P+Q] + [0_E] + F' = \mathrm{div}(\mu_{P,Q}) + F_1$ where $F_1 = [P+Q] + [0_E] + F'$. This decomposition of F means that we just need to evaluate $\mu_{P,Q}$ and F_1 on D and then take the product. Since $\mu_{P,Q}$ is an explicit function, evaluating it on D simply means evaluating it on each point in the support of D and then taking the product.

Now to evaluate F_1 on D we proceed as we did for F and decompose F_1 again. Each time we decompose the divisor, we decrease the number of non zero points in the support (counted with multiplicities). After a finite number of iterations, we find a divisor F_n of degree 0 which has at most one non zero point in its support (counted with multiplicity). So F_n is of the form $[P] - [0_E]$ and since F is principal, F_n is principal too and by Proposition 3.1 we have that $P + 0_E = 0_E$, or in other words $P = 0_E$ and $F_n = 0$. Of course $f_{F_n} = 1$ and $F_n(D) = 1$.

So evaluating F on D decomposes to the evaluation of the functions $\mu_{P,Q}$ appearing in the decomposition of F on the points in the support of D. We give explicit formulae in Lemma 3.4.

LEMMA 3.4 (Evaluating $\mu_{P,Q}$) *Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, and $R = (x_R, y_R)$ be points on E, with P, Q and $P+Q$ all different from 0_E. Then $\mu_{P,Q} = \frac{l_{P,Q}}{v_{P,Q}}$ where $l_{P,Q} = y - \alpha x - \beta$ with $\alpha = \frac{y_P - y_Q}{x_P - x_Q}$ when $P \neq Q$ and $\alpha = \frac{H'(x_P)}{2y_P}$ when $P = Q$, $\beta = y_P - \alpha x_P = y_Q - \alpha x_Q$ and $v_{P,Q} = x - x_{P+Q}$ with $x_{P+Q} = \alpha^2 - x_P - x_Q$.*

The extended value of $v_{P,Q}(R)$ is given by the following cases (taking into account that $\mathrm{div}(v_{P,Q}) = [P+Q] + [-P-Q] - 2[0_E]$):

- *If R is different from $P+Q$, $-P-Q$ or 0_E, then R is not in the support of $\mathrm{div}\, v_{P,Q}$ and we have a value with valuation 0: $v_{P,Q}(R) = x_R - x_{P+Q}$;*
- *If $R = 0_E$ then we have a value with valuation -2. By definition, since the uniformiser at 0_E is the function y/x:*

$$v_{P,Q}(0_E) = \frac{x - x_{P+Q}}{(y/x)^{-2}}(0_E) = \frac{x^2(x - x_{P+Q})}{y^2}(0_E) = 1$$

because $y^2 = x^3 + ax + b$;

- *If $R = P+Q$ or $R = -P-Q$ but $P+Q \neq -P-Q$ (or in other words $P+Q$ is not a point of two torsion), then we have a value with valuation 1. The uniformiser is $x - x_R$ because $H(x_R) \neq 0$ since R is not a point of 2-torsion, and the value is*

$$v_{P,Q}(R) = \frac{x - x_{P+Q}}{x - x_R}(x_R) = 1$$

because in this case $x_R = x_{P+Q}$;

- *If $R = P+Q$ and $P+Q$ is a point of 2-torsion, then this time we have a value with valuation 2. Since $H(x_R) = 0$ the uniformiser is y, so we have*

$$v_{P,Q}(R) = \frac{x - x_{P+Q}}{y^2}(x_R) = \frac{1}{f'(x_{P+Q})}.$$

Indeed if we write $H(x) = (x - x_{P+Q})g(x)$, then since $y^2 = H(x)$ we have $\frac{x - x_{P+Q}}{y^2}(x_R) = \frac{1}{g(x_{P+Q})}$, and we compute $H'(x) = (x - x_{P+Q})g'(x) + g(x)$ so that $H'(x_{P+Q}) = g(x_{P+Q})$.

The extended value of $l_{P,Q}(R)$ is given by the following cases (taking into account that $\mathrm{div}(l_{P,Q}) = [P] + [Q] + [-P-Q] - 3[0_E]$):

- *If R is different from P, Q, $-P-Q$ or 0_E, then R is not in the support of $\mathrm{div}\, l_{P,Q}$ and we have a simple value with valuation 0: $l_{P,Q}(R) = y_R - \alpha x_R - \beta$;*
- *If $R = 0_E$ then we have a value with valuation -3 and*

$$l_{P,Q}(0_E) = \frac{y - \alpha x - \beta}{(x/y)^{-3}}(0_E) = \frac{(y - \alpha x - \beta)x^3}{y^3}(0_E) = 1;$$

- *If $R = P$ or $R = Q$ or $R = -P-Q$ but $l_{P,Q}$ is not tangent to E at R, then we have a value with valuation 1. If R is not a point of two torsion then the uniformiser is $t_R = x - x_R$ and the value is*

$$l_{P,Q}(R) = \frac{y - \alpha x - \beta}{x - x_R}(R) = \frac{y - y_R - \alpha(x - x_R)}{x - x_R}(R) = \frac{y - y_R}{x - x_R}(R) - \alpha = \frac{f'(x_R)}{2y_R} - \alpha.$$

If R is a point of two torsion, then the uniformiser is $t_R = y$ and the value is

$$l_{P,Q}(R) = \frac{y - \alpha x - \beta}{y}(R) = 1 - \alpha\frac{x - x_R}{y}(R) = 1.$$

- *If $R = P$, $R = Q$ or $R = -P - Q$, and $l_{P,Q}$ is tangent to E at R but is not an inflection point, then we have a value of valuation 2. In this case R cannot be a point of two torsion so the uniformiser is $t_R = x - x_R$. To compute the value we must compute the formal series corresponding to y in the completion of $K[E]$ along $x - x_R$ up to order 2: $y = y_R + \alpha(x - x_R) + \alpha_2(x - x_R)^2 + O(x - x_R)^3$. We have $\alpha_2 = \frac{H''(x_R)/2 - \alpha^2}{2y_R}$, so the value is*

$$l_{P,Q}(R) = \frac{y - y_R - \alpha(x - x_R)}{(x - x_R)^2}(R) = \alpha_2.$$

- *Finally when R is an inflection point of H, so that $R = P = Q = -P - Q$ (and in particular is a point of 3-torsion), then we have a value with valuation 3. We compute the formal series corresponding to y in in the completion of $K[E]$ along $x - x_R$ up to order 3: $y = y_R + \alpha(x - x_R) + 0(x - x_R)^2 + \alpha_3(x - x_R)^3 + O((x - x_R)^4)$. We have $\alpha_3 = \frac{1}{2y_R}$ and*

$$l_{P,Q}(R) = \frac{y - y_R - \alpha(x - x_R)}{(x - x_R)^3}(R) = \alpha_3.$$

Combining these values we can now compute the extended value of $\mu_{P,Q}(R)$ (taking into account that $\mathrm{div}(\mu_{P,Q}) = [P] + [Q] - [P + Q] - [0_E]$):

- *When R is not equal to P, Q, $P + Q$, $-P - Q$ or 0_E then the valuation is 0 and we have a simple value:*

$$\mu_{P,Q}(R) = \frac{y_R - \alpha x_R - \beta}{x_R - x_{P+Q}}. \tag{3.13}$$

  (If $R = -P - Q$ and R is not in the support of $\mathrm{div}(\mu_{P,Q})$ then the valuation is also 0 but Equation (3.13) is not well defined so to compute the value we need to look at the particular cases above);
- *When $R = 0_E$ the valuation is -1 and we have*

$$\mu_{P,Q}(0_E) = 1. \tag{3.14}$$

  Since the value is 1 we see that the function $\mu_{P,Q}$ is indeed normalised at 0_E;
- *For all the other cases we refer to the study of the special cases done for $v_{P,Q}$ and $l_{P,Q}$ above.*

Finally, when $P = -Q$ (but $P \neq 0_E$) so that $P + Q = 0_E$, then $\mu_{P,Q} = x - x_P$ and the extended value of $\mu_{P,Q}$ at R is given by the same formulae as the study of $v_{P,Q}(R)$ above.

The second key insight into Miller's algorithm is to speed up the decomposition algorithm above by using a double-and-add algorithm. Indeed when P is a point on an elliptic curve, the scalar multiplication $P \mapsto r.P$ is computed a lot faster when doing a double and add algorithm than when doing a naive decomposition $rP = P + P + \cdots + P$: the complexity is $O(\log r)$ addition rather than $O(r)$. Proposition 3.2 and Algorithm 3.1 outline a similar strategy to evaluate the function f_F where F is the divisor $r[P] - r[0_E]$. More generally, by decomposing a divisor F as $F = F_1 + 2F_2 + 4F_3 + \cdots + 2^n F_n$, one can derive a general double and add algorithm for divisor evaluation.

3.4.3 The general definition of the Weil pairing

THEOREM 3.10 *Let E be an elliptic curve, r a prime number and P and Q two points of r-torsion on E. Let D_P be a divisor linearly equivalent to $[P] - [0_E]$ and D_Q be a divisor linearly*

equivalent to $[Q]-[0_E]$. *Then*

$$e_{W,r}(P,Q)=\epsilon(D_P,D_Q)^r\frac{f_{rD_P}(D_Q)}{f_{rD_Q}(D_P)} \tag{3.15}$$

is well defined, does not depend on the choice of uniformisers nor on the choice of D_P *and* D_Q *(*$\epsilon(D_P,D_Q)=\pm 1$ *is defined in Theorem 3.9 and has value* 1 *if* D_P *and* D_Q *have disjoint support). Furthermore the application* $E[r]\times E[r]\to\mu_r:(P,Q)\mapsto e_{W,r}(P,Q)$ *is a pairing, called the Weil pairing. The pairing* $e_{W,r}$ *is an alternate pairing, which means that* $e_{W,r}(P,Q)=e_{W,r}(Q,P)^{-1}$.

We recover Theorem 3.1 by taking $D_P=[P]-[0_E]$ and $D_Q=[Q]-[0_E]$. Indeed by Proposition 3.2, we get

$$e_{W,r}=(-1)^r\frac{f_{r,P}(Q)}{f_{r,Q}(P)}.$$

Proof. The fact that $e_{W,r}$ is alternate is immediate from Equation (3.15).

We have seen in Section 3.4.2 that the divisor $r[P]-r[0_E]$ is principal. We deduce that if D_P is linearly equivalent to $[P]-[0_E]$ then rD_P is also principal hence Equation (3.15) is well defined.

Let $D_{P,1}$ and $D_{P,2}$ be two divisors linearly equivalent to $[P]-[0_E]$. Then there exists a rational function $g\in k(E)$ such that $D_{P,1}=D_{P,2}+\operatorname{div} g$. Then

$$\epsilon(D_{P_1},D_Q)^r\frac{f_{rD_{P,1}}(D_Q)}{f_{rD_Q}(D_{P,1})}=\epsilon(D_{P_1},D_Q)^r\frac{f_{rD_{P,2}}(D_Q)\cdot g(D_q)^r}{f_{rD_Q}(D_{P,2})\cdot f_{rD_Q}(\operatorname{div} g)}. \tag{3.16}$$

But by Weil's reciprocity theorem (Theorem 3.9), we have

$$f_{rD_Q}(\operatorname{div} g)=\epsilon(\operatorname{div} g,rD_Q)g(rD_Q)=\epsilon(\operatorname{div} g,rD_Q)g(D_Q)^r.$$

Since $\epsilon(D_{P_1},D_Q)^r\epsilon(\operatorname{div} g,rD_Q)=\epsilon(D_{P_1},D_Q)^r$, the Equation (3.16) simplifies to

$$\epsilon(D_{P_1},D_Q)^r\frac{f_{rD_{P,1}}(D_Q)}{f_{rD_Q}(D_{P,1})}=\epsilon(D_{P_2},D_Q)^r\frac{f_{rD_{P,2}}(D_Q)}{f_{rD_Q}(D_{P,2})},$$

which shows that $e_{W,r}(P,Q)$ does not depend on the linear equivalence class of D_P. Likewise by (anti-)symmetry, it does not depend on the linear equivalence class of D_Q.

To show that it does not depend on the choice of uniformisers, we can as well take $D_P=[P]-[0_E]$ and $D_Q=[Q]-[0_E]$ (so that $\epsilon(D_P,D_Q)=-1$). Then a function associated to rD_P is the function $f_{rD_P}=f_{r,P}$ defined in Definition 3.4. If R is a point on the elliptic curve, the evaluation $f_{r,P}(R)$ does not depend on the choice of uniformisers, except when R is in the support of $\operatorname{div} f_{r,P}$ (i.e. if $R=P$ or $R=0_E$).

Going back to the definition of $e_{W,r}(P,Q)$ as

$$e_{W,r}(P,Q)=(-1)^r\frac{f_{r,P}([Q]-[0_E])}{f_{r,Q}([P]-[0_E])}=(-1)^r\frac{f_{r([P]-[0_E])}([Q]-[0_E])}{f_{r([Q]-[0_E])}([P]-[0_E])}$$

we see that the result does not depend on the uniformisers, except possibly when we change the uniformiser for 0_E, and (when $P=Q$) when we change the uniformiser for P. But if we replace the uniformiser x/y for 0_E by $\alpha x/y$, then both the numerator and denominator are multiplied by α^r, hence the result stays the same. Likewise when $P=Q$ and we change the uniformiser at P (actually from the definition it is obvious that $e_{W,r}(P,P)=1$ whatever the uniformiser at P).

We are left with showing bilinearity and non-degeneracy. For that it will be convenient to give yet another form of the Weil pairing, which is not convenient for computations but gives

easier proofs. If $D = [R]$ is a divisor, we define r^*D as $r^*D = \sum_{S \in E(\overline{K}), rS=R}[S]$. This extends by linearity to define a divisor r^*D for a general divisor D. If D is of degree 0 then r^*D is also of degree 0. Furthermore if $D = \operatorname{div} f$, then $r^*D = \operatorname{div} f \circ [r]$.

If $D_P = [P] - [0_E]$, then using Proposition 3.1 one can check that r^*D_P is a principal divisor. Let g_P be a function corresponding to r^*D_P. By definition of g_P, if P_0 is a point in E such that $P = rP_0$, then $\operatorname{div} g_P = \sum_{T \in E[r]}[P_0 + T] - [T]$. Now the function $x \mapsto g_P(x+Q)$ has for divisor $\operatorname{div} g_P(x+Q) = \sum_{T \in E[r]}[P_0 + T - Q] - [T - Q]$. But since $Q \in E[r]$, then $\operatorname{div} g_P(x+Q) = \operatorname{div} g_P$, hence both functions differ by a constant. We claim that this constant is $e_{W,r}(P, Q)$, hence:

$$e_{W,r}(P, Q) = g_P(x + Q)/g_P(x) \tag{3.17}$$

(whenever the right hand side is well defined).

Fix $D_Q = [Q] - [0_E]$, let Q_0 be such that $Q = rQ_0$, g_Q be a function with divisor r^*D_Q (and normalised at 0_E), and define h_Q to be the function normalised at 0_E with divisor $(r-1)[Q_0] + [Q_0 - Q] - r[0_E]$, which exists by Proposition 3.1. Let $H_Q = \prod_{T \in E[r]} h_Q(x + T)$. Then $H_Q = g_Q^r = f_Q \circ r$. Indeed they all have associated divisor $\sum_{T \in E[r]} r[Q_0 + T] - r[T]$ and are normalised. Now by Theorem 3.9, we have that $h_Q(\operatorname{div} g_P) = (-1)^r g_P(\operatorname{div} h_Q)$, which gives the equation

$$\frac{\prod_{T \in E[r]} h_Q(P_0 + T)}{\prod_{T \in E[r]} h_Q(T)} = (-1)^r g_P^r([Q_0] - [0_E]) \frac{g_P(Q_0 - Q)}{g_P(Q_0)}.$$

Combining with $g_Q^r = H_Q$ we find that

$$g_Q^r([P_0] - [0_E]) = H_Q([P_0] - [0_E]) = (-1)^r g_P^r([Q_0] - [0_E]) \frac{g_P(Q_0 - Q)}{g_P(Q_0)}.$$

Since $g_Q^r = f_Q \circ r$, we have that $f_{r,Q}(D_P) = g_Q^r([P_0] - [0_E])$, and similarly $f_{r,P}(D_Q) = g_P^r([Q_0] - [0_E])$. Putting everything together, we compute

$$e_{W,r}(P, Q) = (-1)^r \frac{f_{rD_P}(D_Q)}{f_{rD_Q}(D_P)} = (-1)^r \frac{f_{r,P}(D_Q)}{f_{r,Q}(D_P)} = (-1)^r \frac{g_P^r([Q_0] - [0_E])}{g_Q^r([P_0] - [0_E])} = \frac{g_P(Q_0)}{g_P(Q_0 - Q)}.$$

which proves Equation (3.17) (with $x = Q_0 - Q$).

Using this reformulation, we compute

$$e_{W,r}(P, Q_1 + Q_2) = \frac{g_P(x + Q_1 + Q_2)}{g_P(x)} = \frac{g_P(x + Q_1 + Q_2)}{g_P(x + Q_2)} \frac{g_P(x + Q_2)}{g_P(x)} = e_{W,r}(P, Q_1) e_{W,r}(P, Q_2)$$

so $e_{W,r}$ is bilinear on the right. Now by (anti-)symmetry, using Equation 3.15, $e_{W,r}$ is also bilinear on the left: $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$, so it is indeed bilinear. Furthermore using bilinearity $e_{W,r}(P, Q)^r = e_{W,r}(P, 0_E) = 1$ so $e_{W,r}(P, Q)$ is a r-root of unity.

We now show non-degeneracy, following [22, Proposition 8.1]. Once more by symmetry we just need non-degeneracy on the left, that is given $P \neq 0_E$ we need to show that there exits a Q such that $e_{W,r}(P, Q) \neq 1$. If this were not the case then by Equation 3.17 we would have $g_P(x+Q) = g_P(x)$ for all $Q \in E[r]$. So g_P would be a function invariant by translation by a point of r-torsion; this means that there would exists a rational function g on the curve E such that $g_P = g \circ [r]$ by [22, Theorem 4.10.b]. Then $\operatorname{div} g_P = [r]^* \operatorname{div} g$, but by definition $\operatorname{div} g_P = [r]^* D_P$. So $\operatorname{div} g = D_P = [P] - [0_E]$, but D_P is not principal by Proposition 3.1, so this is absurd. □

3.4.4 The general definition of the Tate pairing

THEOREM 3.11 *Let $E/\mathbb{F}_q$ be an elliptic curve, r a prime number dividing $\#E(\mathbb{F}_q)$, $P \in E[r](\mathbb{F}_{q^k})$ a point of r-torsion defined over $\mathbb{F}_{q^k}$ and $Q \in E(\mathbb{F}_{q^k})$ a point of the elliptic curve*

defined over $\mathbb{F}_{q^k}$. Let D_P be a divisor linearly equivalent to $[P]-[0_E]$ and D_Q be a divisor linearly equivalent to $[Q]-[0_E]$. Then

$$e_{T,r}(P,Q) = (f_{rD_P}(D_Q))^{\frac{q^k-1}{r}} \tag{3.18}$$

is well defined, does not depend on the choice of uniformisers nor on the choice of D_P and D_Q.

Furthermore the application $E[r](\mathbb{F}_{q^k}) \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r : (P,Q) \mapsto e_{T,r}(P,Q)$ is a pairing, called the Tate pairing.

Remark 3.2 There are two versions of the Tate pairing: the first one is to define the pairing as simply $f_{rD_P}(D_Q)$ and see the Tate pairing as a pairing with values in $\mathbb{F}^*_{q^k}/\mathbb{F}^{*,r}_{q^k}$, meaning that we identify two values differing by a r-power. The second one, which we have used in Equation 3.18 is to use the bijection $\mathbb{F}^*_{q^k}/\mathbb{F}^{*,r}_{q^k} \to \mu_r : \gamma \mapsto \gamma^{\frac{q^k-1}{r}}$. Indeed if $\gamma = \gamma'\alpha^r$, then $(\alpha^r)^{\frac{q^k-1}{r}} = \alpha^{q^k-1} = 1$ so $\gamma^{\frac{q^k-1}{r}} = (\gamma')^{\frac{q^k-1}{r}}$. We call the exponentiation by $\frac{q^k-1}{r}$ the *final exponentiation*, and the value $e_{T,r}(P,Q) = (f_{rD_P}(D_Q))^{\frac{q^k-1}{r}}$ the *reduced Tate pairing*.

There is an important difference to keep in mind between the Weil pairing and the Tate pairing. The Weil pairing is geometric: the value of $e_{W,r}(P,Q)$ does not depend on the field of definition we are working on. Whereas the Tate pairing is arithmetic. For instance if $P \in E[r](\mathbb{F}_{q^k})$ and $Q \in E(\mathbb{F}_{q^k})$, but we look at the Tate pairing over $\mathbb{F}_{q^{rk}}$ then the final exponentiation is to the power of $\frac{q^{rk}-1}{r}$ so that $e_{T,r,\mathbb{F}_{q^{rk}}}(P,Q) = 1$ (the Tate pairing stays non-degenerate over $\mathbb{F}_{q^{rk}}$ but one needs to take Q in $E(\mathbb{F}_{q^{rk}})$ to get a non trivial pairing with P for the Tate pairing over $\mathbb{F}_{q^{rk}}$).

Proof. We first show that the value does not depend on the linear equivalence class of D_P and D_Q. Unlike the Weil pairing where P and Q played symmetric roles, for the Tate pairing we have to handle the left argument and the right argument separately.

Let $D_{P,2} = D_{P,1} + \operatorname{div} g$ where g is a rational function. Let $f_{rD_{P,1}}$ be a function corresponding to the principal divisor $rD_{P,1}$, then a function corresponding to $rD_{P,2}$ is $f_{rD_{P,1}}g^r$. We compute

$$f_{rD_{P,2}}(D_Q)^{\frac{q^k-1}{r}} = f_{rD_{P,1}}(D_Q)^{\frac{q^k-1}{r}} \cdot g(D_Q)^{r\frac{q^k-1}{r}} = f_{rD_{P,1}}(D_Q)^{\frac{q^k-1}{r}}.$$

So we can as well take $D_P = r[P] - r[0_E]$.

Likewise, if $D_{Q,2} = D_{Q,1} + \operatorname{div} h$, then by Theorem 3.9, we have that $f_{rD_P}(\operatorname{div} h) = \epsilon h(\operatorname{div} f_{rD_P}) = \epsilon h(r[P] - r[0_E]) = \epsilon h([P] - [0_E])^r$ where $\epsilon = \epsilon(\operatorname{div} f, \operatorname{div} h)$. Since $\epsilon = \pm 1$, $\epsilon^{\frac{q^k-1}{r}} = 1$ so that we compute

$$\begin{aligned} f_{rD_P}(D_{Q,2})^{\frac{q^k-1}{r}} &= f_{rD_P}(D_{Q,1})^{\frac{q^k-1}{r}} \cdot f_{rD_P}(\operatorname{div} h)^{\frac{q^k-1}{r}} = f_{rD_P}(D_{Q,1})^{\frac{q^k-1}{r}} \cdot h([P]-[0_E])^{r\frac{q^k-1}{r}} \\ &= f_{rD_P}(D_{Q,1})^{\frac{q^k-1}{r}}. \end{aligned}$$

To show that $e_{T,r}$ does not depend on the choice of uniformisers, we can take $D_P = [P]-[0_E]$, $D_Q = [Q]-[0_E]$, and by Proposition 3.2 choose $f_{rD_P} = f_{r,P}$. Since $\operatorname{div} f_{r,P} = r[P] - r[0_E]$ changing uniformisers does not affect $f_{r,P}(D_Q)$ except at 0_E and P (when $P = Q$). But if we replace the uniformiser x/y at 0_E by $\gamma x/y$, then the value $f_{r,P}(D_Q)$ is multiplied by γ^r, which is then killed by the final exponentiation. Likewise for the uniformiser at P.

It remains to show that $e_{T,r}$ is a pairing. For simplicity here we assume that $E(\mathbb{F}_{q^k})$ contains all of $E[r]$. For the general case, we refer to [11, 20, 5].

For the bilinearity and the non-degeneracy, as for the Weil pairing it will be more convenient to give an alternative definition of the Tate pairing. Let P and Q be as in the theorem. Let $Q_0 \in E(\overline{\mathbb{F}_q})$ be a point such that $Q = rQ_0$. Let π be the Frobenius endomorphism of $\mathbb{F}_q$, which

acts on the points of E. Then π^k is the Frobenius endomorphism of $\mathbb{F}_{q^k}$. Let $Q_1 = \pi^k Q_0 - Q_0$. We compute $rQ_1 = \pi^k rQ_0 - rQ_0 = \pi^k Q - Q = 0_E$ (where we used the fact that scalar multiplication commutes with the Frobenius, and that Q is defined over $\mathbb{F}_{q^k}$, so that $\pi^k Q = Q$). So Q_1 is a point of r-torsion. Furthermore, it does not depend on Q_0: if we replace Q_0 by $Q_0 + T$ where $T \in E[r]$, then we compute $(\pi^k - 1)(Q_0 + T) = Q_1 + (\pi^k - 1)(T) = Q_1$ because $T \in E(\mathbb{F}_{q^k})$. So the application $\frac{\pi^k - 1}{r} : E(\mathbb{F}_{q^k}) \to E[r], Q \mapsto Q_1$ is well defined, and it is easy to check that it is an endomorphism of $E_{\mathbb{F}_{q^k}}$. We have

$$e_{T,r}(P,Q) = e_{W,r}(P, \frac{\pi^k - 1}{r} Q). \tag{3.19}$$

Equation (3.19) shows a strong link between the Weil and Tate pairing. To show Equation (3.19), we use Equation (3.17) to get $e_{W,r}(P, \pi^k Q_0 - Q_0) = \frac{g_P(\pi^k Q_0)}{g_P(Q_0)}$. Now since P is defined over $\mathbb{F}_{q^k}$, g_P is in $\mathbb{F}_{q^k}(E)$ so π^k commutes with g_P. We thus get

$$\frac{g_P(\pi^k Q_0)}{g_P(Q_0)} = g_P(Q_0)^{q^k - 1} = (g_P^r(Q_0))^{\frac{q^k - 1}{r}} = f_{r,P}(Q)^{\frac{q^k - 1}{r}},$$

where in the last equation we have used that $g_P^r = f_{r,P} \circ [r]$. This shows the equivalence between the two definitions of the Tate pairing.

Using Equation (3.19) we see that the Tate pairing is bilinear. For the non-degeneracy, we have to show that $\frac{\pi^k - 1}{r} : E(\mathbb{F}_{q^k}) \to E[r]$ is surjective. Indeed, because the Weil pairing is non-degenerate, Equation (3.19) will then show that the Tate pairing is non-degenerate too. The kernel of $\frac{\pi^k - 1}{r}$ restricted to $E(\mathbb{F}_{q^k})$ is $rE(\mathbb{F}_{q^k})$, so the image is isomorphic to $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$. Now $E(\mathbb{F}_{q^k})$ is a finite abelian group of the form $\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ with $a \mid b$, and since $E(\mathbb{F}_{q^k}) \supset E[r]$, we know that $r \mid a$ and $r \mid b$. We deduce that $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ is isomorphic to $\mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/r\mathbb{Z}$, in particular it has cardinal r^2 so the application is indeed surjective. □

Taking $D_P = [P] - [0_E]$ and $D_Q = [Q + R] - [R]$ where R is any point in $E(\mathbb{F}_{q^k})$ (this divisor is equivalent to $[Q] - [0_E]$ by Proposition 3.1), we recover the formula from Theorem 3.2:

$$e_{T,r}(P,Q) = \left(\frac{f_{r,P}(Q + R)}{f_{r,P}(R)} \right)^{\frac{q^k - 1}{r}}.$$

If we take $R = 0_E$, we find

$$e_{T,r}(P,Q) = f_{r,P}(Q)^{\frac{q^k - 1}{r}}.$$

Here Q may be a pole or zero of $f_{r,P}$, so we need to use the general Miller's algorithm to compute the extended evaluation.

Restriction of the Tate pairing to subgroups

We give a proof of Proposition 3.4 that the restriction of the Tate pairing to $\mathbb{G}_1 \times \mathbb{G}_2$ is non degenerate:

Proof. Recall that since $k > 1$ and the assumptions in Lemma 3.2 hold, $\mathbb{G}_1$ is the subgroup of $E[r]$ of eigenvectors for the eigenvalue 1 while $\mathbb{G}_2$ corresponds to eigenvectors for the eigenvalue $q \neq 1 \mod r$. We have already proved in Proposition 3.4 that the restriction of the Weil pairing to $\mathbb{G}_1 \times \mathbb{G}_2$ or to $\mathbb{G}_2 \times \mathbb{G}_1$ is non-degenerate.

Since the endomorphism $\frac{\pi^k - 1}{r}$ commutes with the Frobenius π, it stabilizes $\mathbb{G}_1$ and $\mathbb{G}_2$. The alternative definition of the Tate pairing given by Equation (3.19) shows that the Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_2$ or to $\mathbb{G}_2 \times \mathbb{G}_1$ is also non degenerate.

Likewise, the Tate pairing restricted to $\mathbb{G}_1 \times \mathbb{G}_1$ or to $\mathbb{G}_2 \times \mathbb{G}_2$ is degenerate, because the Weil pairing is degenerate. The same reasoning as in the proof for the Weil pairing shows that the Tate pairing on $\mathbb{G}_1 \times \mathbb{G}_3$ (and the other groups) is non degenerate. □

Remark 3.3 By the proof, $e_{T,r}(P,P) = 1$ when $P \in \mathbb{G}_1$ or $P \in \mathbb{G}_2$. However unlike the Weil pairing, we can have $e_{T,r}(P,P) \neq 1$ when $P \in E[r](\mathbb{F}_{q^k})$ but $P \notin \mathbb{G}_1$ and $P \notin \mathbb{G}_2$. See for instance [16] where the authors study the link between the Tate self pairing and the structure of the isogeny graph.

***The case of embedding degree* 1**

Let E be an elliptic curve defined over $\mathbb{F}_q$ such that $r \mid \#E(\mathbb{F}_q)$. By Lemma 3.2 if the embedding degree k is greater than 1, then $E[r] \subset E(\mathbb{F}_{q^k})$ and we can apply the proof of Theorem 3.11.

If $k = 1$, then $E(\mathbb{F}_q)$ may not contain the full r-torsion so we can't apply the elementary proof we have given. But even in this case one can still show using Galois cohomology that both Theorem 3.11 and the alternative definition of the Tate pairing given by Equation 3.19 stay true. In this case $\frac{\pi^k-1}{r}$ is not a well defined endomorphism, but represents a cocycle in a Galois cohomology class such that Equation 3.19 stays well defined over $\mathbb{F}_q$.

Moreover when $E(\mathbb{F}_q)$ does not contain points of r^2-torsion, then by a similar argument as in Proposition 3.4, we can show that $e_{T,r} : E[r](\mathbb{F}_q) \times E[r](\mathbb{F}_q) \to \mu_r \subset \mathbb{F}_q^*$ is still a pairing. In particular, when the rational r-torsion is cyclic, if $P \in E[r](\mathbb{F}_q)$ then $e_{T,r}(P,P) \neq 1$.

3.4.5 The optimal Ate and twisted optimal Ate pairing

In order to proof the formulae for the Ate and twisted Ate we need the following lemma.

LEMMA 3.5 *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$*

- *For any point P on the elliptic curve E*

$$f_{ab,P} = f_{a,P}^b \cdot f_{b,aP}. \tag{3.20}$$

- *Let ϕ an endomorphism of E of degree d, with trivial kernel. Then for any integer λ*

$$f_{\lambda,\phi(P)} = f_{\lambda,P}^d.$$

Proof. The first equation may be proved easily by writing down the divisors for the functions involved. For the second item, see [15]. □

We prove here Theorem 3.4.

Proof. Let $l = \phi(k)$. It is easy to see that:

$$f_{\lambda,Q}(P) = \prod_{i=0}^{l-1} f_{c_i q^i,Q}(P) \prod_{i=0}^{l-1} \frac{l_{s_{i+1}Q,c_i q^i Q}(P)}{v_{s_i Q}(P)}.$$

By Equation 3.20 and Lemma 3.5, we compute $f_{c_i q^i,Q}(P)$ as

$$f_{c_i q^i,Q}(P) = f_{q^i,Q}^{c_i} f_{c_i,q^i Q}(P) = f_{q^i,Q}^{c_i}(P) f_{c_i,Q}^{q^i}(P). \tag{3.21}$$

As a consequence, we obtain that

$$e_{T,r}(Q,P)^m = \prod_{i=0}^{l} \left(f_{q^i,Q}^{c_i}(P) \right)^{(q^k-1)/r} \cdot a_{[c_0,\ldots,c_l]}(Q,P).$$

Since the lefthand side and the factor in brackets are pairings, we conclude that $a_{[c_0,\ldots,c_l]}$ is a bilinear map. By Theorem 3.3, we have that the left hand side is

$$e_{T,r}(Q,P)^m = f_{q,Q}(P)^{mkq^{k-1}((q^k-1)/r)^{-1}}.$$

The product on the right hand side right writes as

$$\prod_{i=0}^{l}\left(f_{q^i,Q}^{c_i}(P)\right) = f_{q,Q}(P)^{\sum_{i=0}^{l} ic_iq^{i-1}}.$$

We conclude that if $mkq^{k-1}((q^k-1)/r)^{-1} \not\equiv \sum_{i=0}^{l} ic_iq^{i-1}$, then $a_{[c_0,\ldots,c_l]}$ is a non-degenerate map. This concludes the proof for the optimal ate pairing. □

For the twisted optimal Ate pairing, the proof of Theorem 3.8 is similar to the one above by inverting the role of P and Q. We give it below.

Proof. Note that by Theorem 3.5, we have that

$$\mathbb{G}_2 = \mathrm{Ker}(\xi_d \circ \pi_{q^e} - \mathrm{Id}).$$

It follows easily that

$$\mathbb{G}_1 = \mathrm{Ker}(\xi_d \circ \pi_{q^e} - q^e\,\mathrm{Id}).$$

As a consequence, in (3.21) we compute $f_{c_iq^{ie},P}(Q)$ by applying Lemma 3.5 for the endomorphism $\xi \circ \pi_{q^e}$. The rest of the computation follows naturally. □

References

[1] Christophe Arène, Tanja Lange, Michael Naehrig, and Christophe Ritzenthaler. Faster computation of the Tate pairing. *Journal of Number Theory*, 131(5):842–857, 2011.

[2] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In P. Q. Nguyen and E. Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pp. 1–16. Springer, Heidelberg, 2014.

[3] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[4] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004.

[5] Peter Bruin. The tate pairing for abelian varieties over finite fields. *J. de theorie des nombres de Bordeaux*, 23(2):323–328, 2011.

[6] Craig Costello, Tanja Lange, and Michael Naehrig. Faster pairing computations on curves with high-degree twists. In P. Q. Nguyen and D. Pointcheval, editors, *Public Key Cryptography – PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pp. 224–242. Springer, Heidelberg, 2010.

[7] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, 1994.

[8] Steven D. Galbraith and Victor Rotger. Easy decision Diffie-Hellman groups. *LMS Journal of Computation and Mathematics*, 7:201–218, 2004.

[9] Robert Granger, Dan Page, and Nigel P. Smart. High security pairing-based cryptography revisited. In F. Hess, S. Pauli, and M. E. Pohst, editors, *Algorithmic Number Theory (ANTS-VII)*, volume 4076 of *Lecture Notes in Computer Science*, pp. 480–494. Springer, 2006.

[10] F. Hess, N.P. Smart, and F. Vercauteren. The eta pairing revisited. Cryptology ePrint Archive, Report 2006/110, 2006. `http://eprint.iacr.org/2006/110`.

[11] Florian Hess. A note on the tate pairing of curves over finite fields. *Archiv der Mathematik*, 82(1):28–32, 2004.

[12] Florian Hess. Pairing lattices (invited talk). In S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pp. 18–38. Springer, Heidelberg, 2008.

[13] Florian Hess, Nigel P. Smart, and Frederik Vercauteren. The Eta pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.

[14] Sorina Ionica and Antoine Joux. Another approach to pairing computation in Edwards coordinates. In D. R. Chowdhury, V. Rijmen, and A. Das, editors, *Progress in Cryptology – INDOCRYPT 2008*, volume 5365 of *Lecture Notes in Computer Science*, pp. 400–413. Springer, Heidelberg, 2008.

[15] Sorina Ionica and Antoine Joux. Pairing computation on elliptic curves with efficiently computable endomorphism and small embedding degree. In M. Joye, A. Miyaji, and A. Otsuka, editors, *Pairing-Based Cryptography – Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*, pp. 435–449. Springer, Heidelberg, 2010.

[16] Sorina Ionica and Antoine Joux. Pairing the volcano. *Mathematics of Computation*, 82(281):581–603, 2013.

[17] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels (invited paper). In N. P. Smart, editor, *Cryptography and Coding*, volume 3796 of *Lecture Notes in Computer Science*, pp. 13–36. Springer, Heidelberg, 2005.

[18] Stephen Lichtenbaum. Duality theorems for curves over p-adic fields. *Inventiones mathematicae*, 7(2):120–136, 1969.

[19] Alfred Menezes, Scott A. Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *23rd Annual ACM Symposium on Theory of Computing*, pp. 80–89. ACM Press, 1991.

[20] Edward F Schaefer. A new proof for the non-degeneracy of the frey-rück pairing and a connection to isogenies over the base field. *Computational aspects of algebraic curves*, 13:1–12, 2005.

[21] Jean-Pierre Serre. *Groupes algébriques et corps de classes*, volume 7 of *Publications de l'Institut de mathématique de l'Université de Nancago*. Hermann, 2nd edition, 1975.

[22] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition, 2009.

[23] William Stein. *SAGE: Software for Algebra and Geometry Experimentation*. `http://www.sagemath.org/`.

[24] John Tate. WC-groups over p-adic fields. Exposé 156, Séminaire Bourbaki, 1957/58.

[25] F. Vercauteren. Optimal pairings. Cryptology ePrint Archive, Report 2008/096, 2008. `http://eprint.iacr.org/2008/096`.

[26] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Journal of Cryptology*, 17(4):277–296, 2004.

[27] Chang-An Zhao, Fangguo Zhang, and Jiwu Huang. A note on the Ate pairing. *International Journal of Information Security*, 7(6):379–382, 2008.