L'Enseignement Mathématique (2) 61 (2015), 211–243 DOI 10.4171/LEM/61-1/2-9

Bilinear pairings on elliptic curves

Andreas Enge

Abstract. We give an elementary and self-contained introduction to pairings on elliptic curves over finite fields. The three different definitions of the Weil pairing that can be found in the literature are stated and proved to be equivalent using Weil reciprocity. Pairings with shorter loops, such as the ate, ate_i, R-ate and optimal pairings, together with their twisted variants, are presented with proofs of their bilinearity and non-degeneracy. Finally, we review different types of pairings in a cryptographic context. This article can be seen as an update chapter to A. Enge, *Elliptic Curves and Their Applications to Cryptography – An Introduction*, Kluwer Academic Publishers 1999.

Mathematics Subject Classification (2010). Primary: 14, 14-02, 14H52, 14Q05; Secondary: 11, 11-02, 11Y40.

Keywords. Elliptic curves, Weil pairing, Tate pairing.

1. Introduction

Consider three abelian groups G_1, G_2 (written additively) and G_3 (written multiplicatively), which can equivalently be seen as $\mathbb{Z}$-modules. A *pairing* on G_1 and G_2 with values in G_3 is a $\mathbb{Z}$-bilinear map

$$e : G_1 \times G_2 \to G_3,$$

so that

$$e(aP, bQ) = e(P, Q)^{ab}$$

for all elements $P \in G_1$, $Q \in G_2$ and integers a and b. In the following, G_1 and G_2 will be groups related to an elliptic curve E defined over some field K: They will be subgroups of the elliptic curve group (in the case of the Weil pairing of §3) or subgroups and quotient groups (in the case of the Tate pairing of §4 and related pairings presented in §7). The group G_3 will be a subgroup or a quotient of the multiplicative group K^*.

Elliptic curve cryptosystems are currently among the most efficient public-key systems. Their security relies on the difficulty of computing discrete logarithms in suitable instances of elliptic curves over finite fields, that is, on the difficulty of computing x given two points P and $R = xP$ on the curve. Pairings then transport the discrete logarithm problem from the curve into the multiplicative group of a finite field, where it is potentially easier to solve [Odl]: As $e(R, Q) = e(P, Q)^x$, the discrete logarithm of $e(R, Q)$ with respect to the basis $e(P, Q)$ yields x. Consequently, pairings have first been suggested as a means of attacking elliptic curve cryptosystems [MOV, FR]. First constructive cryptographic applications have been described in [Jou, SOK, BF], and since then, the number of publications introducing pairing-based cryptographic primitives has exploded. A new conference series, *Pairing*, is devoted to the topic [TOOO, GP, SW, JMO, AL, CZ].

This document provides a self-contained introduction to pairings and aims at summarising the state of the art as far as the definitions of different pairings and their cryptographic use are concerned. While being as accessible as possible, we do not sacrifice mathematical rigour, in the style of [Eng1], of which the current article can be seen as an update chapter. While most of the following holds over arbitrary perfect or even more general fields, we limit the presentation to the only case of interest in the cryptographic context, namely K being a finite field $\mathbb{F}_q$ with q elements. Pairings can be defined in Jacobians of arbitrary curves or, more generally, in abelian varieties. However, due to recent progress in solving the discrete logarithm problem (see the survey [Eng2]), only elliptic curves and genus 2 hyperelliptic curves appear to be suited for cryptography. For the latter, the problem of finding efficiently implementable instances has not yet been solved satisfactorily: We need the pairing to have values in a sufficiently small finite field to be efficiently computed and represented (see the definition of the embedding degree at the beginning of §3), and we need the size of the subgroup to be reasonably close to that of the full group to allow for bandwidth-efficient protocols. So in the following we consider only elliptic curves.

An excellent survey is given by Galbraith in [Gal]. We complement his presentation by concentrating on the Weil pairing instead of the Tate pairing and by reporting on progress made after the publication of [Gal] concerning pairings with shorter evaluation loops.

2. Elliptic curves and Weil reciprocity

2.1. Divisors and group law. We assume the reader to be familiar with basic algebra, in particular with finite fields. For proofs of the following facts on elliptic curves, see [Sil1, Engl]. Other sources for the use of elliptic curves in cryptography are [CFA, BSS]. From now on, we assume that $K = \mathbb{F}_q = \mathbb{F}_{p^m}$ is the finite field of characteristic p with q elements. (This is motivated by the cryptologic applications and meant to ease the exposition. All statements concerning the Weil pairing hold in fact over arbitrary fields. The definition given of the Tate pairing in §4, however, is not valid for all fields; over finite fields, it yields a non-degenerate pairing.)

In several places, we will consider the algebraic closure $\overline{K}$ for convenience; this could be replaced by a sufficiently large extension field to contain the coordinates of all points under consideration. An *elliptic curve* over K is given by a non-singular, absolutely irreducible *long Weierstraß equation*

$$E : Y^2 + (a_1 X + a_3)Y = X^3 + a_2 X^2 + a_4 X + a_6$$

with $a_i \in K$. If $p \geq 5$, the equation can be transformed into short Weierstraß form in which all but a_4 and a_6 vanish. The points on E are given by the *affine* points $(x, y) \in K^2$ satisfying the equation, together with a *projective point at infinity* $\mathcal{O}$. The *coordinate ring* of E is the ring $K[E] = K[X, Y]/(E)$ of polynomial functions, its *function field* $K(E) = K(X)[Y]/(E) = \{a(X)+b(X)Y : a, b \in K(X)\}$ is the set of *rational functions* from E to $K \cup \{\infty\}$; the value ∞ is reached when the function has a pole in a point. It turns out that the points on E are in a one-to-one correspondence with the discrete valuation rings of $K(E)$, given by the rings $\mathcal{O}_P$ of functions that do not have a pole in P.

The set $E(K)$ of points on E with coordinates in K (including $\mathcal{O}$) can be turned into a finite abelian group via the tangent-and-chord law: $\mathcal{O}$ is the neutral element of the group law, and three points on a line sum to $\mathcal{O}$. The only delicate point in proving the group law is associativity; the simplest proof, which also generalises to other curves, is sketched in the following. It uses divisors, which are needed anyway to define pairings. So let

$$\mathrm{Div}(E) = \left\{ \sum_P n_P[P] : P \in E(K), n_P \in \mathbb{Z}, \text{only finitely many } n_P \text{ are non-zero} \right\}$$

be the free abelian group over the points on E, define the degree of a divisor as the sum $\sum n_P$ of its coefficients, and let $\mathrm{Div}^0(E)$ be the subgroup of $\mathrm{Div}(E)$ consisting of divisors of degree 0. To a rational function $f \in K(E)$, associate its divisor $\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f)[P]$, where $\mathrm{ord}_P(f)$ is the valuation of f with respect to $\mathcal{O}_P$: If P is a zero of f, then $\mathrm{ord}_P(f) > 0$ gives its multiplicity; if P is a pole of f, then $\mathrm{ord}_P(f) < 0$ gives its (negative) multiplicity; if P is neither a zero nor a pole of f, then $\mathrm{ord}_P(f) = 0$. Let $\mathrm{Prin}(E) = \{\mathrm{div}(f) : f \in K(E)\} \subseteq \mathrm{Div}^0(E)$ be the set of *principal divisors*. Then the quotient $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E)$ is evidently a group, and it can be identified with $E(K)$ via $P \mapsto [P]-[\mathcal{O}]$, which maps $\mathcal{O}$ to the neutral element O.

Let $\sim$ denote equivalence modulo $\mathrm{Prin}(E)$. The geometric tangent-and-chord law is recovered as follows. For a point $R=(x_R, y_R)$, let

$$v_R = X - x_R \tag{1}$$

be the vertical line through R. Then $\mathrm{div}(v_R) = [R]+[\overline{R}]-2[\mathcal{O}] \sim 0$ with $\overline{R} = (x_R, -y_R - a_1 x_R - a_3)$, so that $-R = \overline{R}$. For two points $P=(x_P, y_P)$ and $Q=(x_Q, y_Q)$ with $Q \neq -P$ let $\ell_{P,Q}$ be the chord through P and Q if $P \neq Q$ or the tangent at P if $P = Q$:

$$\begin{aligned} \lambda_{P,Q} &= \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & \text{if } P \neq Q \\ \frac{3x_P^2 + 2a_2 x_P + a_4}{2y_P + a_1 x_P + a_3} & \text{if } P = Q \end{cases} \\ \ell_{P,Q} &= (Y - y_P) - \lambda_{P,Q}(X - x_P) \end{aligned} \tag{2}$$

Then $\ell_{P,Q}$ intersects E in a third point $R=(x_R,y_R) \neq \mathcal{O}$, and $\mathrm{div}\left(\frac{\ell_{P,Q}}{v_R}\right) = \mathrm{div}(\ell_{P,Q}) - \mathrm{div}(v_R) = \big([P]+[Q]+[R]-3[\mathcal{O}]\big) - \big([R]+[\overline{R}]-2[\mathcal{O}]\big) = [P]+[Q]-[\overline{R}]-[\mathcal{O}] \sim 0$ implies that $P+Q=\overline{R}$.

By induction, this proves the following characterisation of principal divisors, which is a special case of Abel's theorem:

Theorem 1. *A divisor $D=\sum_P n_P[P]$ is principal if and only if* $\deg D = 0$ *and $\sum_P n_P P = \mathcal{O}$ on E. The function associated to a principal divisor is unique up to multiplication by constants in K^*.*

It is often useful to assume the following normalisation.

Definition 2. *The leading coefficient of a function f at $\mathcal{O}$ is*

$$\mathrm{lc}(f) = \left(\left(\frac{X}{Y}\right)^{-\mathrm{ord}_{\mathcal{O}}(f)} f\right)(\mathcal{O}).$$

A function f is monic at $\mathcal{O}$ if $\mathrm{lc}(f)=1$.

In particular, the lines v_R and $\ell_{P,Q}$ given above for the tangent-and-chord law are monic at $\mathcal{O}$, and this implies that the functions computed in Algorithm 12 will also be monic at $\mathcal{O}$.

2.2. Rational maps, isogenies and star equations. Let E, E' be two elliptic curves over the same field K. A *rational map* $\alpha : E \to E'$ is an element of $E'(K(E))$. Explicitly, α is given by rational functions in X and Y that satisfy the Weierstraß equation for E'. Unless α is constant, it is surjective. If $\alpha(\mathcal{O}) = \mathcal{O}'$, then α is in fact a group homomorphism, and it is called an *isogeny*. If furthermore $E = E'$, then α is called an *endomorphism*. The endomorphisms that are most important in the following are multiplications by an integer n, denoted by $[n]$.

A non-constant rational map $\alpha : E \to E'$ induces an injective homomorphism of function fields $\alpha^* : K(E') \to K(E)$, $f' \mapsto f' \circ \alpha$; the *degree* of α is the degree of the function field extension $[K(E) : \alpha^*(K(E'))]$. For instance, $\deg([n]) = n^2$. If α is an isogeny, there is another isogeny $\hat{\alpha}$ of the same degree, called its *dual*, such that $\hat{\alpha} \circ \alpha = [\deg \alpha]$.

For a point $P \in E$ and $P' = \alpha(P)$, there is an integer $e_\alpha(P)$, called *ramification* index, such that $\mathrm{ord}_P(\alpha^*(f')) = e_\alpha(P)\,\mathrm{ord}_{P'}(f')$ for any $f' \in K(E')$. When α is an isogeny, $e_\alpha(P)$ is independent of P. In this case, we have $\deg \alpha = e_\alpha \cdot \#(\ker \alpha)$, and two extreme cases can occur: If $e_\alpha = 1$, then α is called *separable*; in particular, $[n]$ is separable if $p \nmid n$. If $\#(\ker \alpha) = 1$, then α is (up to isomorphisms) a power of the *purely inseparable Frobenius endomorphism* $(x, y) \mapsto (x^q, y^q)$ of degree and ramification index q. An arbitrary isogeny can be decomposed into a separable one and a power of Frobenius, which is often convenient for proving theorems.

The ramification index allows to define a homomorphism $\alpha^* : \mathrm{Div}(E') \to \mathrm{Div}(E)$ on divisors by

$$\alpha^*([P']) = \sum_{P \in \alpha^{-1}(P')} e_\alpha(P)[P]$$

in such a way that the maps α^* on functions and divisors are compatible; the proof follows immediately from the definition of e_α.

Theorem 3 (Upper star equation). *If $\alpha : E \to E'$ is a non-constant rational map and $f' \in K(E')$, then*

$$\alpha^*\big(\mathrm{div}(f')\big) = \mathrm{div}\,\big(\alpha^*(f')\big).$$

The following result is concerned with the composition of rational maps; it can be proved by a direct computation as in the proof of [Engl, Proposition 3.15].

Lemma 4. *If $\alpha : E \to E'$ and $\beta : E' \to E''$ are non-constant rational maps between elliptic curves, then $\beta \circ \alpha : E \to E''$ is non-constant, and*

$$(\beta \circ \alpha)^* = \alpha^* \circ \beta^*$$

as maps on functions or divisors.

On the other hand, the map $\alpha_* : \mathrm{Div}(E) \to \mathrm{Div}(E')$ is defined by $\alpha_*([P]) = [\alpha(P)]$. A corresponding map on function fields $K(E) \to K(E')$ can be defined by

$$\alpha_*(f) = (\alpha^*)^{-1} \left(\mathrm{N}_{K(E)/\alpha^*(K(E'))}(f)\right),$$

where N denotes the norm with respect to the function field extension. The map α_* is well-defined: Since the norm is an element of $\alpha^*(K(E'))$, a preimage exists; since α^* is injective, this preimage is unique.

It is shown in [CC, (18)] that

$$\mathrm{N}_{K(E)/\alpha^*(K(E'))}(f) = \Big(\prod_{R \in \ker \alpha} (f \circ \tau_R)\Big)^{e_\alpha}, \tag{3}$$

where τ_R is the translation by R; the product accounts for the separable, the exponent for the inseparable part of the isogeny. This can be used to show the following result:

Theorem 5 (Lower star equation). *If $\alpha : E \to E'$ is a non-constant isogeny and $f \in K(E)$, then*

$$\alpha_*\big(\mathrm{div}(f)\big) = \mathrm{div}\,\big(\alpha_*(f)\big).$$

2.3. Weil reciprocity. The key to the definition of pairings is the evaluation of rational functions in divisors. For $D = \sum_P n_P[P]$ let its *support* be $\mathrm{supp}(D) = \{P : n_P \neq 0\}$. The evaluation of a rational function f in points is extended to a group homomorphism from divisors (with support disjoint from $\mathrm{supp}(\mathrm{div}\, f)$) to K^* via

$$f\Big(\sum_P n_P[P]\Big) = \prod_P f(P)^{n_P}.$$

In order to handle common points in the supports, let the *tame symbol* of two functions f and $g \in K(E)$ be defined as

$$\langle f, g\rangle_P = (-1)^{\mathrm{ord}_P(f)\,\mathrm{ord}_P(g)} \Big(\frac{f^{\mathrm{ord}_P(g)}}{g^{\mathrm{ord}_P(f)}}\Big)(P).$$

Theorem 6 (Generalised Weil reciprocity). *If f, $g \in K(E)$, then*

$$\prod_{P \in E(\overline{K})} \langle f, g\rangle_P = 1.$$

In particular, if $\mathrm{supp}(f) \cap \mathrm{supp}(g) = \varnothing$, *then*

$$f(\mathrm{div}\, g) = g(\mathrm{div}\, f). \tag{4}$$

For a proof, see [CC, §7].

3. Weil pairing

Let $E[n] = \{P \in E(\overline{K}) : nP = \mathcal{O}\} = \ker([n])$ be the set of n-torsion points of E, which are in general not defined over K itself. For future reference, we denote by $E(K)[n] = E[n] \cap E(K)$ the set of points of $E[n]$ defined over K, which contains at least $\mathcal{O}$. From now on, we will assume that $\gcd(n, p) = 1$; then the group $E[n]$ is finite and isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The field L obtained by adjoining to $K = \mathbb{F}_q$ all coordinates of n-torsion points is thus a finite field extension $\mathbb{F}_{q^k}$, and k is called the *embedding degree* of the n-torsion and $\mathbb{F}_{q^k}$ its *embedding field*. We have $L \supseteq K(\zeta_n)$, where ζ_n is a primitive n-th root of unity, and equality holds in the case of main cryptographic interest, namely that n is a prime and $n \nmid q - 1$ by [BK, Th. 1]. Then k is the smallest integer such that $n \mid q^k - 1$.

Theorem 7. *The Weil pairing is a map*

$$e_n : E[n] \times E[n] \to \mu \subset L^*,$$

where μ is the set of n-th roots of unity in L, satisfying the following properties:

(a) *Bilinearity:*

$$\begin{aligned} &e_n(P_1 + P_2, Q) = e_n(P_1, Q)e_n(P_2, Q), \\ &e_n(P, Q_1 + Q_2) = e_n(P, Q_1)e_n(P, Q_2) \quad \forall P, P_1, P_2, Q, Q_1, Q_2 \in E[n]; \end{aligned}$$

(b) *Identity:*

$$e_n(P, P) = 1 \quad \forall P \in E[n];$$

(c) *Alternation:*

$$e_n(P, Q) = e_n(Q, P)^{-1} \quad \forall P, Q \in E[n];$$

(d) *Non-degeneracy: For any $P \in E[n]\backslash\{\mathcal{O}\}$, there is a $Q \in E[n]$, and for any $Q \in E[n]\backslash\{\mathcal{O}\}$, there is a $P \in E[n]$ such that $e_n(P, Q) \neq 1$;*

(e) *Compatibility with isogenies:*

$$e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{\deg \alpha}, \tag{5}$$

$$e_n(P', \alpha(Q)) = e_n(\hat{\alpha}(P'), Q) \tag{6}$$

for P, $Q \in E[n]$, $P' \in E'[n]$, $\alpha : E \to E'$ a non-zero isogeny defined over L and $\hat{\alpha}$ its dual isogeny. In particular, α may be the Frobenius endomorphism on E of degree q. (Here and in the following, we use the same notation e_n for the Weil pairing independently of the curve, E or E', over which it is defined.)

In the literature, there are in fact three equivalent definitions of the Weil pairing, and depending on which one is chosen, the different properties are more or less easy to prove, the most intricate one being non-degeneracy. In the following, we show equivalence of these definitions, which is also non-trivial and makes intensive use of Weil reciprocity, and we prove the five properties of the Weil pairing using for each the definition that yields the easiest proof.

First definition of the Weil pairing ([Sil1, §III.8], [Engl, §3.7]). For $P \in E[n]$, consider $D = [n]^*([P] - [\mathcal{O}]) = \sum_{R \in E[n]}([P_0 + R] - [R])$, where P_0 is any point such that $nP_0 = P$. By Theorem 1, D is principal; let g_P be such that $\operatorname{div} g_P = D$. Let again $\tau_Q : R \mapsto R + Q$ denote the translation by $Q \in E[n]$. Then

$$e_n(P, Q) = \frac{g_P \circ \tau_Q}{g_P}. \tag{7}$$

While g_P is defined only up to multiplication by non-zero constants, the quotient is a well-defined rational function. Since $\operatorname{div}(g_P \circ \tau_Q) = \operatorname{div}(\tau_Q^*(g_P)) = \tau_Q^*(\operatorname{div} g_P)$ by Theorem 3 and the latter divisor equals

$$\sum_{R \in E[n]} \big([P_0 + R - Q] - [R - Q]\big) = \operatorname{div} g_P$$

for $Q \in E[n]$, the Weil pairing yields indeed a constant in $\overline{K}$. That it yields an n-th root of unity follows from bilinearity.

Proof of Theorem 7(a): Using (c), proved below, it is sufficient to show linearity in the second argument, which follows from the definition:

$$\begin{aligned} e_n(P, Q_1 + Q_2) &= \frac{g_P \circ \tau_{Q_1+Q_2}}{g_P} = \left(\frac{g_P \circ \tau_{Q_1}}{g_P} \circ \tau_{Q_2}\right) \frac{g_P \circ \tau_{Q_2}}{g_P} \\ &= e_n(P, Q_1) e_n(P, Q_2) \text{ since the constant } e_n(P, Q_1) \\ &\qquad\qquad \text{is invariant under } \tau_{Q_2}. \end{aligned}$$

□

Proof of Theorem 7(d): We sketch the approach of [Engl, Prop. 3.60]. Using (c), it is sufficient to show non-degeneracy with respect to the first argument. For $P \in E[n]$, suppose that $e_n(P, Q) = 1$ for all $Q \in E[n]$. This means that g_P is invariant under translations by all $Q \in E[n] = \ker([n])$, so that all conjugates of g_P with respect to the field extension $K(E)/[n]^*(K(E))$ are g_P itself, see (3). Hence, there is a function f_P such that $g_P = [n]^*(f_P)$. By Theorem 3, this implies that $\operatorname{div} f_P = [P] - [\mathcal{O}]$, which by Theorem 1 implies $P = \mathcal{O}$. □

Proof of Theorem 7(e): We prove (5) as in [Engl, Prop. 3.60] with a slight simplification. Consider the function $h = \frac{g_{\alpha(P)} \circ \alpha}{g_P^{\deg \alpha}}$ and its divisor, which satisfies

$$\begin{aligned}
\operatorname{div}(h) &= \operatorname{div}(\alpha^*(g_{\alpha(P)})) - \deg(\alpha)\operatorname{div}(g_P)\\
&= \alpha^*(\operatorname{div}(g_{\alpha(P)}) - \deg(\alpha)\operatorname{div}(g_P) \text{ by Theorem 3}\\
&= \alpha^*\big([n]^*([\alpha P]-[\mathcal{O}])\big) - \deg(\alpha)[n]^*([P]-[\mathcal{O}])\\
&\quad \text{by the definitions of } g_P \text{ and } g_{\alpha(P)}\\
&= [n]^*\big(\alpha^*([\alpha P]-[\mathcal{O}]) - \deg\alpha([P]-[\mathcal{O}])\big)\\
&\quad \text{by Lemma 4 and the fact that } \alpha \text{ commutes with } [n]\\
&= [n]^*\Big(e_\alpha \sum_{R\in\ker(\alpha)}([P+R]-[R]) - \deg(\alpha)[P] + \deg(\alpha)[\mathcal{O}]\Big)\\
&= [n]^*(\operatorname{div}(h')) \text{ for some function } h' \text{ by Theorem 1, using}\\
&\qquad\qquad\qquad\qquad \deg(\alpha) = e_\alpha\cdot\#\ker(\alpha)\\
&= \operatorname{div}(h'\circ[n]) \text{ by Theorem 3.}
\end{aligned}$$

Thus $h = h'\circ[n]$ after multiplying h' by a suitable constant. Now we obtain

$$\begin{aligned}
e_n\big(\alpha(P),\alpha(Q)\big) &= e_n(\alpha(P),\alpha(Q))\circ\alpha \text{ since the Weil pairing is a constant}\\
&= \frac{g_{\alpha(P)}\circ\tau_{\alpha(Q)}\circ\alpha}{g_{\alpha(P)}\circ\alpha}\\
&= \frac{g_{\alpha(P)}\circ\alpha\circ\tau_Q}{g_P^{\deg(\alpha)}\circ\tau_Q}\cdot\frac{g_P^{\deg(\alpha)}}{g_{\alpha(P)}\circ\alpha}\cdot\left(\frac{g_P\circ\tau_Q}{g_P}\right)^{\deg(\alpha)}\\
&= \frac{h\circ\tau_Q}{h}\cdot e_n(P,Q)^{\deg(\alpha)}\\
&= e_n(P,Q)^{\deg(\alpha)},
\end{aligned}$$

since $h = h'\circ[n]$ is invariant under translation by the n-torsion point Q.

Concerning (6), let P be such that $\alpha(P) = P'$; then $\hat\alpha(P') = (\hat\alpha\circ\alpha)(P) = (\deg\alpha)P$, and

$$e_n(\hat\alpha(P'),Q) = e_n(P,Q)^{\deg\alpha} = e_n\big(\alpha(P),\alpha(Q)\big) = e_n\big(P',\alpha(Q)\big).$$

□

Second definition of the Weil pairing. For $P,Q\in E[n]\backslash\{\mathcal{O}\}$, $P\neq Q$, let f_P and f_Q be such that $\operatorname{div} f_P = n[P]-n[\mathcal{O}]$ and $\operatorname{div} f_Q = n[Q]-n[\mathcal{O}]$, which is possible by Theorem 1. Then

$$e_n(P,Q) = (-1)^n\cdot\frac{f_P(Q)}{f_Q(P)}\cdot\frac{f_Q}{f_P}(\mathcal{O}); \tag{8}$$

if f_P and f_Q are chosen monic at $\mathcal{O}$ as in Definition 2, then

$$e_n(P,Q) = (-1)^n\cdot\frac{f_P(Q)}{f_Q(P)}.$$

For $P = Q$ or one or both of P and Q being $\mathcal{O}$, the definition needs to be completed by $e_n(P, Q) = 1$.

Remark 8. *This definition is the most suited one for computations, see Algorithm 12. The factor $(-1)^n$ is often missing in the literature.*

Proof of equivalence of the two definitions: We essentially follow [CC, §10]. Assume that e_n is defined as in (7).

Let P_0 and Q_0 be such that $nP_0 = P$ and $nQ_0 = Q$. Let g_P be the function, monic at $\mathcal{O}$, such that

$$\operatorname{div}(g_P) = \sum_{R \in E[n]} \big([P_0 + R] - [R]\big),$$

and similarly for g_Q.

If $P = \mathcal{O}$, we may take $P_0 = \mathcal{O}$, which shows that $g_{\mathcal{O}} = 1$ and $e_n(\mathcal{O}, Q) = 1$. If $Q = \mathcal{O}$, then $\tau_Q = \mathrm{id}$, and $e_n(P, \mathcal{O}) = 1$. So from now on, P, $Q \neq \mathcal{O}$.

Let h_Q be the function, monic at $\mathcal{O}$, such that

$$\operatorname{div} h_Q = (n-1)[Q_0] + [Q_0 - Q] - n[\mathcal{O}],$$

which exists by Theorem 1, and let $H_Q = \prod_{R \in E[n]} (h_Q \circ \tau_R)$. By comparing divisors and leading coefficients, $H_Q = \mathrm{lc}(H_Q) \cdot g_Q^n$.

By generalised Weil reciprocity of Theorem 6, we have

$$\prod_{S \in \operatorname{supp}(\operatorname{div} g_P) \cup \operatorname{supp}(\operatorname{div} h_Q)} \langle g_P, h_Q \rangle_S = 1.$$

If $P \neq Q$, then $\operatorname{supp}(\operatorname{div} g_P) \cap \operatorname{supp}(\operatorname{div} h_Q) = \{\mathcal{O}\}$, and we easily compute the different contributions of tame symbols:

$$\begin{aligned}
\langle g_P, h_Q \rangle_{Q_0} &= g_P^{n-1}(Q_0) \\
\langle g_P, h_Q \rangle_{Q_0 - Q} &= g_P(Q_0 - Q) \\
\langle g_P, h_Q \rangle_{P_0 + R} &= h_Q^{-1}(P_0 + R) \text{ for } R \in E[n] \\
\langle g_P, h_Q \rangle_R &= h_Q(R) \text{ for } R \in E[n] \backslash \{\mathcal{O}\} \\
\langle g_P, h_Q \rangle_{\mathcal{O}} &= (-1)^n \frac{h_Q}{g_P^n}(\mathcal{O}) = (-1)^n \text{ since } g_P \text{ and } h_Q \text{ are monic at } \mathcal{O}.
\end{aligned}$$

Multiplying them together, we find that

$$\begin{aligned}
1 &= g_P^n(Q_0) \underbrace{\frac{g_P(Q_0 - Q)}{g_P(Q_0)}}_{\frac{g_P}{g_P \circ \tau_Q}(Q_0 - Q) = e_n(P,Q)^{-1}} \underbrace{\frac{1}{H_Q(P_0)}}_{\mathrm{lc}(H_Q)^{-1} g_Q(P_0)^{-n}} \underbrace{\frac{H_Q}{h_Q}}_{\mathrm{lc}(H_Q)}(\mathcal{O})(-1)^n \\
&= (-1)^n \frac{g_P^n(Q_0)}{g_Q^n(P_0)} \cdot \frac{1}{e_n(P, Q)}.
\end{aligned}$$

Since $\operatorname{div}(g_P^n) = n[n]^*([P]-[\mathcal{O}]) = [n]^* \operatorname{div}(f_P)$, Theorem 3 implies that

$$g_P^n = c^{-1} \cdot [n]^*(f_P)$$

with $c = \operatorname{lc}([n]^*(f_P)) = \left((f_P \circ [n])\frac{X^n}{Y^n}\right)(\mathcal{O})$. An analogous equation holds for g_Q^n, so that

$$\frac{g_P^n(Q_0)}{g_Q^n(P_0)} = \frac{f_P(Q)}{f_Q(P)} \cdot \frac{f_Q}{f_P}(\mathcal{O}).$$

If $P = Q$, then $\operatorname{supp}(\operatorname{div}(h_Q)) \subseteq \operatorname{supp}(\operatorname{div}(g_Q))$, and a similar computation shows that $e_n(P,P) = 1$. □

Proof of Theorem 7(b): This is part of the second definition. (The only statement needing proof is that this also holds for the first definition, as shown above.) □

Proof of Theorem 7(c): This is immediate from (8). □

Third definition of the Weil pairing. For any degree zero divisor D such that $nD \sim 0$ in $\operatorname{Pic}^0(E)$, we denote by f_D the function, monic at $\mathcal{O}$, such that $\operatorname{div}(f_D) = nD$; thus $f_{[P]-[\mathcal{O}]} = f_P$. Choose $D_P \sim [P]-[\mathcal{O}]$ and $D_Q \sim [Q]-[\mathcal{O}]$ with disjoint supports. Then

$$e_n(P,Q) = \frac{f_{D_P}(D_Q)}{f_{D_Q}(D_P)}. \tag{9}$$

Note the similarity with (8), but also the missing factor $(-1)^n$, due to the common pole $\mathcal{O}$ of f_P and f_Q.

Remark 9. *The third definition corresponds to Weil's original one in* [Wei]. *The first definition is given in* [Sil1, Engl] *with the roles of P and Q exchanged, which by the alternation property yields the inverse of the Weil pairing. The definition with P and Q in the order of this paper is used in the Notes on Exercises, p. 462 of the second edition of* [Sil1], *as well as in* [Sil3].

One needs to check that (9) is well-defined. Let $D_Q' \sim [Q]-[\mathcal{O}]$ be another possible choice instead of D_Q. Then $D_Q' = D_Q + \operatorname{div}(h)$ for some function h with support disjoint from D_P, and $f_{D_Q'} = f_{D_Q} h^n$, which implies

$$\frac{f_{D_P}(D_Q')}{f_{D_Q'}(D_P)} = \frac{f_{D_P}(D_Q) f_{D_P}(\operatorname{div} h)}{f_{D_Q}(D_P) h(D_P)^n} = \frac{f_{D_P}(D_Q) f_{D_P}(\operatorname{div} h)}{f_{D_Q}(D_P) h(\operatorname{div} f_{D_P})} = \frac{f_{D_P}(D_Q)}{f_{D_Q}(D_P)}$$

by Weil reciprocity (4). By symmetry, the same argument holds when D_P is chosen differently.

Proof of equivalence between the second and third definitions: A proof is given in [Mil, Prop. 8]. The basic idea is to choose $D_P = [P-R]-[-R]$ and $D_Q = [Q+R]-[R]$ for some point R. Then (9) becomes

$$\frac{f_{D_P}(Q+R)}{f_{D_Q}(P-R)} \cdot \frac{f_{D_Q}(-R)}{f_{D_P}(R)}.$$

Informally, letting $R \to \mathcal{O}$, the first factor tends to $e_n(P,Q)$ as defined in (8), the second factor tends to $(-1)^n$. This can be made rigorous using formal groups or the Deuring lift of E to the field of complex numbers.

Alternatively, one may again use generalised Weil reciprocity. Let $D_P = [P]-[\mathcal{O}]$, so that $f_{D_P} = f_P$. Let R be such that $D_Q = [Q+R]-[R]$ and D_P have disjoint supports; then $D_Q = [Q]-[\mathcal{O}]+\operatorname{div}(h)$ with h monic at $\mathcal{O}$ such that $\operatorname{div} h = [Q+R]-[Q]-[R]+[\mathcal{O}]$, and $f_{D_Q} = f_Q h^n$.

Assume first that $P \neq Q$. Then by Theorem 6,

$$1 = \prod_{S \in E(\overline{K})} \langle f_P, h \rangle_S = \frac{f_P(Q+R)}{f_P(R) f_P(Q) h^n(P)} \cdot (-1)^n \underbrace{(f_P h^n)(\mathcal{O})}_{=\operatorname{lc}(f_P)}.$$

So

$$\begin{aligned} \frac{f_{D_P}(D_Q)}{f_{D_Q}(D_P)} &= \frac{(f_Q h^n)(\mathcal{O})}{(f_Q h^n)(P)} \cdot \frac{f_P(Q+R)}{f_P(R)} = \frac{\operatorname{lc}(f_Q) f_P(Q)}{f_Q(P)} \cdot \frac{f_P(Q+R)}{f_P(Q) h^n(P) f_P(R)} \\ &= (-1)^n \frac{f_P(Q)}{f_Q(P)} \cdot \frac{\operatorname{lc}(f_Q)}{\operatorname{lc}(f_P)} \end{aligned}$$

by the previous equation.

If $P = Q$, a similar computation shows that (9) evaluates to 1. □

4. Tate pairing

The Tate pairing has been used in cryptology at first as a means of transporting the discrete logarithm problem from curves to the multiplicative groups of finite fields [FR]. It goes back to Tate, who in [Tat] considers abelian varieties defined over local fields and defines a non-degenerate pairing involving Galois cohomology groups of the variety and the dual abelian variety. Lichtenbaum defines in [Lic] a pairing in terms of Picard groups of curves defined over local fields and their Galois cohomology. This pairing turns out to be a special case of the Tate pairing and as such is non-degenerate. Its advantage is that it can easily be computed in terms of divisors and functions on the curve as stated in (10). See also [Sil2, §§5–8] for an accessible presentation of these Galois cohomology related pairings. By considering torsion elements in the groups and reducing modulo the discrete valuation of the local field, Frey and Rück obtain a non-degenerate pairing for curves defined over finite fields. It is often called the Tate–Lichtenbaum pairing [Frey, §3.3],[CFA, §6.4.1], although the name Frey–Rück–Tate–Lichtenbaum pairing might be more appropriate. In the cryptologic literature, the shorter term Tate pairing has imposed itself, and we will stick to this tradition.

Computationally, the Tate pairing can be seen as "half a Weil pairing"; the idea is to define it directly as $f_P(Q)$ instead of the quotient (8). Its precise definition depends on a field extension L of K such that $E[n]$ is contained in $E(L)$; usually, but not necessarily, L is chosen minimal with this property.

First definition of the Tate pairing. Let $P \in E[n]$, let D_P be a degree zero divisor, defined over L, with $D_P \sim [P] - [\mathcal{O}]$, and let f_{D_P}, defined over L, be such that $\operatorname{div} f_{D_P} = nD_P$. Let Q be another point on $E(L)$ (not necessarily of n-torsion) and let $D_Q \sim [Q] - [\mathcal{O}]$ be defined over L of support disjoint from D_P. Then the Tate pairing of P and Q is given by

$$e_n^{\mathrm{T}}(P, Q) = f_{D_P}(D_Q). \tag{10}$$

Algorithm 12 shows that f_{D_P} may indeed be defined over L, so that the pairing takes values in L. Notice that f_{D_P} is defined only up to a multiplicative constant, but that this does not change the pairing value since D_Q is of degree 0. Weil reciprocity (4) shows that if D_Q is replaced by $D'_Q = D_Q + \operatorname{div} h \sim D_Q$, then (10) is multiplied by $h(D_P)^n$. Replacing D_P by $D'_P = D_P + \operatorname{div} h$ changes f_{D_P} to $f_{D'_P} = f_{D_P} h^n$ and thus multiplies the pairing value by an n-th power. So the pairing value is well defined up to n-th powers in L.

Finally, if Q is replaced by $Q + nR$ with $R \in E(L)$, the value changes again by an n-th power. This leads to adapting the range and domain of e_n^{T} as follows.

Theorem 10. *For $E[n] \subseteq E(L)$, the Tate pairing is a map*

$$e_n^{\mathrm{T}} : E[n] \times E(L)/nE(L) \to L^*/(L^*)^n$$

satisfying the following properties as defined in Theorem 7:

(a) *Bilinearity,*

(b) *Non-degeneracy,*

(c) *Compatibility with isogenies.*

Proof. Bilinearity is immediate from the definition using $[Q_1 + Q_2] - [\mathcal{O}] \sim [Q_1] + [Q_2] - 2[\mathcal{O}]$ by Theorem 1, so that $D_{Q_1+Q_2} = D_{Q_1} + D_{Q_2}$ and $f_{P_1+P_2} = f_{P_1} f_{P_2}$.

Non-degeneracy does not hold over arbitrary fields. In particular, the pairing becomes completely trivial if every element of L is an n-th power, for instance if $L = \overline{K}$. So the proofs of non-degeneracy use the structure of the groups over a finite field, see [FR, Hes2, Sch, Bru].

In the following, we will use that for a rational map $\beta : E \to E'$, a function f on E' and a divisor D on E, we have by definition that

$$f\big(\beta_*(D)\big) = (f \circ \beta)(D) = \beta^*(f)(D). \tag{11}$$

Let α be an isogeny. By Theorem 5 we may choose $D_{\alpha(P)} = \alpha_*(D_P)$ and $D_{\alpha(Q)} = \alpha_*(D_Q)$, and $f_{D_{\alpha(P)}} = \alpha_*(f_{D_P})$. We may furthermore assume that D_P and D_Q are chosen so that all function values encountered during the proof are defined and non-zero. Then

$$\begin{aligned} e_n^{\mathrm{T}}(\alpha(P), \alpha(Q)) = f_{D_{\alpha(P)}}(D_{\alpha(Q)}) &= (\alpha_*(f_{D_P}))\big(\alpha_*(D_Q)\big) \\ &= \Big(\alpha^*\big(\alpha_*(f_{D_P})\big)\Big)(D_Q) \text{ by (11)} \\ &= \Big(\prod_{R \in \ker(\alpha)} (f_{D_P} \circ \tau_R)(D_Q)\Big)^{e_\alpha} \text{ by (3)} \\ &= \Big(\prod_{R \in \ker \alpha} f_{D_P}\big((\tau_R)_*(D_Q)\big)\Big)^{e_\alpha} \text{ by (11).} \end{aligned}$$

Now Theorem 1 shows that $(\tau_R)_*(D_Q) \sim D_Q$, so that each factor equals $e_n^{\mathrm{T}}(P, Q)$, which finishes the proof. □

Again, an alternative definition yields a computationally advantageous form of the pairing.

Second definition of the Tate pairing. For $P \in E[n]$ and $Q \in E(L)$ (representing a class modulo $nE(L)$), P, $Q \neq \mathcal{O}$ and $P \neq Q$, let f_P be monic at $\mathcal{O}$ such that $\mathrm{div}(f_P) = n[P] - n[\mathcal{O}]$. Then

$$e_n^{\mathrm{T}}(P, Q) = \frac{f_P(Q)}{\mathrm{lc}(f_P)}; \tag{12}$$

if f_P is chosen monic as in Definition 2,

$$e_n^{\mathrm{T}}(P, Q) = f_P(Q).$$

For one or both of P and Q equal to $\mathcal{O}$, one has $e_n^{\mathrm{T}}(P, Q) = 1$. If $P = Q$, one may choose some point $R \in E(L)$ such that $nR \notin \{\mathcal{O}, -Q\}$, if it exists, and replace Q by $Q + nR$.

Proof of equivalence of the two definitions: Letting $D_Q = [Q] - [\mathcal{O}]$, so that $f_{D_Q} = f_Q$, and $D_P = [P + R] - [R]$ so that D_P and D_Q have disjoint supports and $f_{D_P} = f_P h^n$ for the function h, monic at $\mathcal{O}$, with $\operatorname{div}(h) = [P+R] - [P] - [R] + [\mathcal{O}]$, we immediately obtain

$$f_{D_P}(D_Q) = \frac{(f_P h^n)(Q)}{(f_P h^n)(\mathcal{O})} = \frac{f_P(Q) h^n(Q)}{\operatorname{lc}(f_P)} = \frac{f_P(Q)}{\operatorname{lc}(f_P)}$$

up to n-th powers. □

Unlike the Weil pairing, the Tate pairing is neither alternating nor identically 1 on the diagonal (which is hardly surprising given that its two arguments live in different sets). On single n-torsion points P, it may or may not hold that $e_n^{\mathrm{T}}(P,P) = 1$.

The definition of the domain of the Tate pairing as a quotient group is unwieldy in cryptographic applications, where unique representatives of pairing results are desired. It can be remedied by observing that L^* is a cyclic group of order $\#L - 1 = q^k - 1$, which is divisible by n; so the map

$$L^*/(L^*)^n \to \mu, \quad x \mapsto x^{\frac{q^k-1}{n}}$$

is an isomorphism with the n-th roots of unity μ, and the *reduced Tate pairing*

$$(13) \quad e_n^{\mathrm{T}'} : E[n] \times E(L)/nE(L) \to \mu, \quad (P,Q) \mapsto e_n^{\mathrm{T}}(P,Q)^{\frac{q^k-1}{n}} = f_P(Q)^{\frac{q^k-1}{n}}$$

(for P, $Q \neq \mathcal{O}$, $P \neq Q$) is an equivalent pairing with the same properties as the Tate pairing itself.

It is not generically possible to similarly replace the set $E(L)/nE(L)$ from which the second argument is taken by $E[n]$. As an abelian group, $E(L)$ is isomorphic to $\mathbb{Z}/r_1\mathbb{Z} \times \mathbb{Z}/r_2\mathbb{Z}$ with $n \mid r_1 \mid r_2$, and $E(L)/nE(L) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Consider the homomorphism

$$\psi : E(L)/nE(L) \to E[n], \quad Q \mapsto \frac{r_2}{n} Q.$$

This homomorphism is injective (and thus an isomorphism by cardinality considerations) if and only if $\gcd\left(\frac{r_2}{r_1}, n\right) = 1$. A sufficient (but not necessary) condition is that $\gcd\left(\frac{r_2}{n}, n\right) = 1$, or equivalently $\gcd\left(\frac{\#E(L)}{n^2}, n\right) = 1$; this is often satisfied in cryptography, where n is a large prime. Then the function

$$e : E[n] \times E[n] \to \mu, \quad (P,Q) = f_P(Q)^{\frac{q^k-1}{n}}$$

satisfies $e(P,Q) = e_n^{\mathrm{T}'}(P, \psi^{-1}(Q))^{\frac{r_2}{n}}$, and since powering by $\frac{r_2}{n}$ induces a permutation on μ, it inherits the properties of the reduced Tate pairing.

5. Computation

The main ingredients of the Weil and the Tate pairings are functions with given divisors; an algorithm computing them is published in [Mil] and has become known as Miller's algorithm. The basic idea is to have the tangent-and-chord law of §2.1 not only reduce a sum of two points to only one point, but at the same time output the lines that have served for the reduction. Applied iteratively, it thus reduces a principal divisor to 0 and returns the function having this divisor as a quotient of products of lines. The algorithm is applicable to any principal divisor, but we only present it for the case of $n[P]-n[\mathcal{O}]$ where P is an n-torsion point, which can be used for computing the Weil pairing via (8) and the (reduced) Tate pairing via (10) or (12) and (13).

Definition 11. *For $i \in \mathbb{Z}$, let $f_{i,P}$ be the function (monic at $\mathcal{O}$) with divisor $i[P]-[iP]-(i-1)[\mathcal{O}]$.*

The function $f_{i,P}$ exists by Theorem 1. Notice that $f_{1,P}=1$ and $f_{n,P}=f_P$. The tangent-and-chord law, applied to iP and jP, shows that

$$f_{i+j,P} = f_{i,P}\, f_{j,P}\, \frac{\ell_{iP,jP}}{v_{(i+j)P}} \tag{14}$$

with ℓ, v defined as in (2), (1) for $i \not\equiv -j \pmod{n}$, $\ell_{iP,(n-i)P} = v_{iP}$ and $v_{\mathcal{O}} = 1$. Moreover,

$$f_{-i,P} = \frac{1}{f_{i,P}\, v_{iP}}.$$

These observations yield the following algorithm:

Algorithm 12. *Input: An integer n and an n-torsion point P*
Output: ℓ and v, products of lines, such that $f_P = \frac{\ell}{v}$

(a) *Compute an addition-negation chain $r_1, \ldots, r_s$ for n, that is, a sequence of integers such that $r_1 = 1$, $r_s = n$ and each element r_i is either*

- *the negative of a previously encountered one: There is $1 \leq j(i) < i$ such that $r_i = -r_{j(i)}$; or*
- *the sum of two previously encountered ones: There are $1 \leq j(i) \leq k(i) < i$ such that $r_i = r_{j(i)} + r_{k(i)}$.*

(b) $P_1 \leftarrow P$, $L_1 \leftarrow 1$, $V_1 \leftarrow 1$

(c) ***for*** $i = 2, \ldots, s$

$\quad j \leftarrow j(i), k \leftarrow k(i)$

$\quad$ ***if*** $r_i = -r_j$

$\quad\quad P_i \leftarrow -P_j$

$\quad\quad L_i \leftarrow V_j$

$\quad\quad V_i \leftarrow L_j v_{P_i}$

$\quad$ ***else***

$\quad\quad P_i \leftarrow P_j + P_k$

$\quad\quad L_i \leftarrow L_j L_k \ell_{P_{j(i)}, P_{k(i)}}$

$\quad\quad V_i \leftarrow V_j V_k v_{P_i}$

(d) ***return*** $\ell = L_s, \ v = V_s$

Throughout the loop, we have $P_i = r(i)P$ and $\frac{L_i}{V_i} = f_{r(i),P}$, which proves the correctness of the algorithm. The numerator ℓ and the denominator v are computed separately to avoid costly divisions in a direct computation of f_P. Memory handling of the algorithm is simplified if the standard double-and-add addition chain is used, in which $r_i = 2r_{i-1}$ or $r_i = r_{i-1} + 1$, so that the result can be accumulated in two variables ℓ and v, see [Gal, Alg. IX.1].

For a reasonable addition-negation-chain of length $s \in O(\log n)$, the algorithm carries out $O(\log n)$ steps. Unfortunately, the degrees of L_i and V_i grow exponentially to reach $O(n)$. This problem can be solved in two ways: Instead of storing L_i and V_i as dense polynomials, store them in factored form as a product of lines. This may make sense if several pairings with the same P are computed.

Otherwise, if $f_P(E)$ is sought for a divisor E, one may compute directly $L_i(E)$ and $V_i(E)$ during the loop, thus manipulating only elements of the finite field L; one should then separate again according to the points with positive or negative multiplicity in E to avoid divisions. This approach fails when E contains any of the points $P_i = r(i)P$ encountered during the algorithm, which will then be zeroes of some of the lines. The solution given in [Mil] is to work with the leading coefficients of the lines with respect to their Laurent series in local parameters associated to the points in the support of E (analogously to Definition 2). Alternatively, one might regroup quotients of consecutive lines having P_i as zeroes and replace them (by working modulo the curve equation) by a rational function that is defined and non-zero at P_i. Both approaches are not very practical, since they replace simple arithmetic in a finite field by more complicated symbolic algebra. A simpler technique is to replace the divisor E by an equivalent divisor not containing any of the P_i in its support, and using (9) and (10); the price to pay is that E then contains at least two points instead of only one in (8) and (12). Concerning the Tate pairing, since the second argument Q

is defined only up to n-th multiples, one may replace it by $Q+nR$ for some point R. Finally, one may simply use an addition-negation chain avoiding the support of E. Since any addition chain necessarily passes through 2, it may be necessary to use negation if E contains $2P$ in its support.

The reduced Tate pairing (13) is usually faster to compute than the Weil pairing (8): It requires only one instead of two applications of Algorithm 12. On the other hand, the advantage is partially lost through the final exponentiation in the reduced Tate pairing.

6. Pairings on cyclic subgroups

All supposedly hard problems on which pairing-based cryptographic primitives rely can be broken by computing discrete logarithms arbitrarily in $E[n]$ or the group μ of n-th roots of unity in the embedding field L. So algorithms using Chinese remaindering for discrete logarithms imply that n being prime is the best choice. We then follow a convention often found in the literature on pairings and use the letter r in the place of n. Then $E[r]$ is a group of order r^2 isomorphic to $\mathbb{Z}/r\mathbb{Z}\times\mathbb{Z}/r\mathbb{Z}$. For the sake of security proofs, it may be desirable to restrict the Weil and reduced Tate pairings to subgroups, yielding pairings

$$e : G_1 \times G_2 \to \mu \subseteq L$$

on cyclic groups $G_i \subset E[r]$ of prime order r. In practice, there is no definite need for such a restriction: The choice of points when executing the protocol (for instance, by hashing into $E[r]$) implicitly defines cyclic subgroups G_i generated by these points; but the subgroups change with each execution of the algorithm. Notice, however, that some optimised pairings (see §7) can only be defined on specific subgroups, which are reviewed in the following. An exhaustive description of the cryptographic properties of different subgroups is given by Galbraith, Paterson and Smart in [GPS]. We retain their classification into type 1, 2 and 3 subgroups and pairings and concentrate on the main characteristics of the different choices.

For the sake of computational efficiency in Algorithm 12, it is desirable that G_1 and G_2 be defined over fields that are as small as possible. So the curve $E(K)$ is chosen such that $r \mid \#E(K)$, and G_1 is generated by a point of order r defined over K. As usual in cryptography, we assume that $k \geq 2$. Then G_1 is defined uniquely as $E(K)[r]$, and the pairing types differ in their selection of G_2. An important cryptographic property that may or may not be given is hashing into the different groups, or the (essentially equivalent) possibility of random sampling from the groups. It is a trivial observation that if

$H:\{0,1\}^* \to \{0,\dots,r-1\}$ is a collision-resistant hash-function and $G_i = \langle P_i \rangle$, then $H_i : \{0,1\}^* \to G_i$, $m \mapsto H(m)P_i$, is also collision-resistant. But H_i reveals discrete logarithms, which breaks most pairing-based cryptographic primitives. A comparatively expensive way of hashing into G_1 is to first hash into a point on $E(K)$ (by hashing to its X- or Y-coordinate and solving the resulting equation for the other coordinate; if no solution exists, one needs to hash the message concatenated with a counter that is increased upon each unsuccessful trial). One may then multiply by the cofactor $h = \frac{\#E(K)}{r}$, which yields a point in G_1. A similar procedure hashes to arbitrary r-torsion points in $E(L)$, but these need not lie in a fixed subgroup G_2.

6.1. Type 1: $G_1 = G_2$. Most of the early papers on pairing-based cryptography are formulated only for the case of a *symmetric pairing*, in which $G_2 = G_1$. However, it is in fact not possible to simply choose the arguments of the pairings of §§3 and 4 from $G_2 = G_1$, since then the pairing becomes trivial. This is clear for the Weil pairing from Theorem 7(b), but also holds for the reduced Tate pairing: Algorithm 12 implies that the result lies in the field K over which both arguments are defined, but $K \cap \mu = \{1\}$. A symmetric pairing may be obtained for supersingular curves with a so-called *distortion map*, an explicit monomorphism $\psi : E(K)[r] \to E[r]\backslash G_1$. The non-degeneracy of the Weil pairing then implies that

$$e : G_1 \times G_1 \to \mu, \quad (P, Q) \mapsto e_r(P, \psi(Q))$$

is also a non-degenerate pairing; the same usually holds for the reduced Tate pairing.

Algebraic distortion maps cannot exist for ordinary elliptic curves, whose endomorphism rings are abelian. Then ψ would be an endomorphism and it would commute with the Frobenius, so the image of $G_1 \subseteq E(K)[r]$ would again lie in $E(K)$ and thus be equal to G_1.

Conversely, supersingular elliptic curves have a non-abelian endomorphism ring, and it has been shown by Galbraith and Rotger in [GR, Th. 5.2] that they always admit an algebraic distortion map coming from the theory of complex multiplication (cf. [Deu]) as long as $r \geq 5$; the same article describes an algorithm for explicitly determining such a map. It is well-known that supersingular curves with $k = 2$ admit particularly simple distortion maps, namely,

$$\psi(x, y) = (-x, iy) \tag{15}$$

for $E : Y^2 = X^3 + X$ over $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$ and

$$\psi(x, y) = (\zeta_3 x, y) \tag{16}$$

for $E : Y^2 = X^3 + 1$ over $\mathbb{F}_p$ with $p \geq 5$ and $p \equiv 2 \pmod 3$, where ζ_3 and i are primitive third and fourth roots of unity, respectively, in $\mathbb{F}_{p^2}$.

If the X-coordinate of ψ is defined over K (for instance, in (15), but not in (16)), it is observed in [BKLS] that the computation of the reduced Tate pairing

$$e(P, Q) = e_n^{\mathrm{T}'}\big(P, \psi(Q)\big) = f_P\big(\psi(Q)\big)^{\frac{q^k-1}{r}} \text{ by (13)}$$

can be simplified by omitting denominators. Indeed, notice that if a pure addition chain (without subtractions) is used, the denominator v returned by Algorithm 12 is a polynomial in $K[X]$ not involving Y; since $X(\psi(Q)) \in K$, the value $v(Q)$ disappears through the final exponentiation.

The main drawback of type 1 pairings is the lack of flexibility of the embedding degree k: Since it is limited to supersingular curves, we have $k \leq 2$ for curves over fields of characteristic at least 5, $k \leq 4$ over fields of characteristic 2 and $k \leq 6$ over fields of characteristic 3 by [Wat, Theorem 4.1].

6.2. Type 2: $G_2 \hookrightarrow G_1$. The pairing is of type 2 when there is an efficiently computable monomorphism ϕ from G_2 to G_1. In some sense, this is the converse of type 1, where there is a non-trivial monomorphism from G_1 into another r-torsion group. This case, however, is essentially the generic one and available in supersingular and ordinary curves alike. Let $\pi : (x, y) \mapsto (x^q, y^q)$ be the Frobenius endomorphism related to the field extension $L/K = \mathbb{F}_{q^k}/\mathbb{F}_q$. Then $K(E)$ is fixed by π or, otherwise said, G_1 are the r-torsion points that are eigenvectors under π with eigenvalue 1. Hasse's theorem then implies that the r-torsion of E is generated by one point P with eigenvalue 1 and another point Q with eigenvalue q. We now consider the *trace* defined as a map on points by

$$\mathrm{Tr} : E(L) \to E(K), \quad R \mapsto \sum_{i=0}^{k-1} R^{\pi^i}.$$

Since the trace of a point is invariant under π, it is indeed a point defined over K. We have $\mathrm{Tr}(P) = kP \neq \mathcal{O}$ in a cryptographic context, where r is much bigger than k, and $\mathrm{Tr}(Q) = Q + qQ + \cdots + q^{k-1}Q = \frac{q^k-1}{q-1}Q = \mathcal{O}$ since the order r of Q divides $q^k - 1$, but not $q - 1$. If R is any r-torsion point, then $R = aP + bQ$, $\mathrm{Tr}(R) = akP$ and $Q' := kR - \mathrm{Tr}(R) = kbQ \in \langle Q \rangle$. Unless $R \in \langle P \rangle$, in which case $Q' = \mathcal{O}$, the element Q' is thus a generator of $\langle Q \rangle$, which can be found efficiently by a randomised algorithm.

Let R be an arbitrary r-torsion point that is a pure multiple of neither P nor Q (which can be checked using the Weil pairing; in practice, a random r-torsion point satisfies this restriction with overwhelming probability). Let $G_2 = \langle R \rangle$, and $\phi = \mathrm{Tr}$.

The existence of ϕ reduces problems (for instance, the discrete logarithm problem or the decisional Diffie–Hellman problem) defined in terms of G_2 into problems defined in terms of G_1, which may be helpful for reductionist security proofs. But as usual, the existence of additional algebraic structures (here, the map ϕ) raises doubts as to the introduction of a security flaw. Furthermore, hashing or random sampling in G_2 appears to be impossible, except for the trivial approach revealing discrete logarithms. Recent work by Chatterjee and Menezes [CM] introduces a heuristic construction to transform a cryptographic primitive in the type 2 setting, together with its security argument, into an equivalent type 3 primitive. Thus, type 2 pairings should probably be avoided in practice.

6.3. Type 3. The remaining case where there is no apparent efficiently computable monomorphism $G_2 \to G_1$ is called type 3. In view of the discussion of §6.2, this implies that

$$\begin{aligned} G_2 &= \{R \in E[r] : R^{\pi} = qR\} \\ &= \{R \in E[r] : \mathrm{Tr}(R) = \mathcal{O}\}. \end{aligned}$$

The previous discussion has also shown how to find a generator of G_2. Hashing into G_2 may be accomplished in a similar manner: Hash to an arbitrary point $R \in E[r]$, and define $kR - \mathrm{Tr}(R)$ as the final hash value.

7. Loop-shortened pairings

Subsequent work has concentrated on devising pairings with a shorter loop in Algorithm 12, generally starting from the Tate pairing (12). It turns out that in certain special cases,

$$e(P, Q) = f_{\lambda,P}(Q) \qquad \text{or} \qquad e(P, Q) = f_{\lambda,Q}(P)$$

define non-degenerate, bilinear pairings for $\lambda \ll n$ with $f_{\lambda,P}$ as in Definition 11. The proof proceeds by showing that the pairing is the M-th power of the original Tate pairing for some M prime to n. Cryptographic applications may then directly use the new pairing, or, for the sake of interoperability, the Tate pairing may be retrieved by an additional exponentiation with $M^{-1} \bmod n$. The first such pairing, called η pairing, was described by Barreto, Galbraith, Ó'hÉigeartaigh and Scott in [BGOS]. It was limited to supersingular curves and thus yielded a type 1 pairing (see §6.1). The examples in [BGOS] show that $\lambda \approx \sqrt{n}$ is achievable in supersingular curves over fields of characteristic 2 and 3.

In the remainder of this section, we fix the same setting as in §6. In particular, $n = r$ is prime. All pairings will be defined on $G_1 \times G_2$, where $G_1 = E(K)[r]$

and G_2 is the set of r-torsion points defined over $L = \mathbb{F}_{q^k}$ with eigenvalue q under the Frobenius $\pi : (x, y) \mapsto (x^q, y^q)$. This is crucial for the proofs, and incidentally leads to type 3 pairings.

Lemma 13. *Let $P \in E[n]$. If N is such that $n \mid N \mid q^k - 1$, then*

$$f_{N,P} = f_{n,P}^{N/n}.$$

If N is such that $n \mid N$, then

$$f_{N+1,P} = f_{N,P}.$$

Both properties hold by definition; the first one was used in [GHS, §6] to speed up the computation by replacing r with a small multiple of low Hamming weight.

7.1. Ate pairing. The ate pairing (short for "loop-shortened Tate pairing") is defined in [HSV, Theorem 1] as

$$e_r^{\mathrm{A}} : G_1 \times G_2 \to L^*/(L^*)^r, \quad (P, Q) \mapsto f_{T,Q}(P) \tag{17}$$

with $T = t - 1$, where t is the trace of Frobenius satisfying $\#E(K) = q + 1 - t$.

Theorem 14. *e_r^{A} is bilinear, and if $r^2 \nmid T^k - 1$, it is non-degenerate. More precisely,*

$$\left(e_r^{\mathrm{A}}(P, Q)\right)^{kq^{k-1}} = e_r^{\mathrm{T}}(Q, P)^{\frac{T^k - 1}{r}}.$$

For the ate pairing and all other pairings presented in the following, a reduced variant with unique values in $\mu \subseteq L^*$ is obtained as in (13) by raising to the power $\frac{q^k-1}{r}$.

Proof of Theorem 14: The crucial step is the observation that for any λ,

$$\begin{aligned} f_{\lambda,T^i Q} \circ \pi^i &= f_{\lambda,q^i Q} \circ \pi^i \text{ since } T \equiv q \pmod r \\ &= f_{\lambda,\pi^i(Q)} \circ \pi^i \text{ since } Q \in G_2 \\ &= f_{\lambda,Q}^{q^i}, \end{aligned} \tag{18}$$

since the coefficients of the rational function $f_{\lambda,Q}$ can be expressed in the coefficients of Q and of the curve, and the latter lie in $\mathbb{F}_q$.

In particular for $P \in G_1$ and $\lambda = T$, $f_{T,T^i Q}(P) = f_{T,Q}^{q^i}(P)$.

Then

$$
\begin{aligned}
e_r^{\mathrm{T}}(Q,P)^{\frac{T^k-1}{r}} &= f_{r,Q}^{\frac{T^k-1}{r}}(P) = f_{T^k-1,Q}(P) \text{ by Lemma 13} \\
&= f_{T^k,Q}(P) \text{ by Lemma 13 since } T^k - 1 \equiv q^k - 1 \equiv 0 \pmod r \\
&= \prod_{i=0}^{k-1} f_{T,T^iQ}^{T^{k-1-i}}(P) \text{ by comparing divisors and collapsing} \\
&\qquad\qquad\qquad\qquad\qquad \text{the telescopic sum} \\
&= f_{T,Q}^{\sum_{i=0}^{k-1} T^{k-1-i} q^i}(P) \text{ by (18)} \\
&= e_r^{\mathrm{A}}(P,Q)^{kq^{k-1}} \text{ in } L^*/(L^*)^r, \text{ since } T \equiv q \pmod r.
\end{aligned}
$$

□

By Hasse's theorem, $T \in O(\sqrt{q})$, so that the number of operations in Algorithm 12 drops generically by a factor of about 2; the effect can, however, be much more noticeable for certain curves. For instance, [FST] describes a family of curves for $k = 24$ with $r \in \Theta(q^{4/5})$ and $T \in O(q^{1/10}) = O(r^{1/8})$. Notice that $8 = \phi(24)$, cf. §7.3. A price to pay is that the arguments P and Q are swapped: The elliptic curve operations need to be carried out over $\mathbb{F}_{q^k}$ instead of $\mathbb{F}_q$. (Algorithm 12 in this context is sometimes called "Miller full", while the more favourable situation is called "Miller light".)

7.2. Twisted ate pairing. The twisted variant of the ate pairing keeps the usual order of the arguments, but sacrifices on the loop length.

Assume $\operatorname{char} \mathbb{F}_q \geq 5$, and let $d = \gcd(k, \#\operatorname{Aut}(E))$ and $e = \frac{k}{d}$. Then there is a twist E' of degree d of E, that is, a curve E' defined over $\mathbb{F}_q$ with an isomorphism $\psi : E' \to E$, which is defined over $\mathbb{F}_{q^d}$. It can be given explicitly as follows for $E : Y^2 = X^3 + aX + b$ in short Weierstraß form, see [Sil1, §X.5.4]:

$$
\begin{aligned}
d = 2:& \quad E' : Y^2 = X^3 + D^2 aX + D^3, & \psi(x,y) &= \left(Dx, \sqrt{D^3}y\right); \\
d = 4:& \quad E' : Y^2 = X^3 + DaX, & \psi(x,y) &= \left(\sqrt{D}x, \sqrt[4]{D^3}y\right); \\
d \in \{3,6\}:& \quad E' : Y^2 = X^3 + Db, & \psi(x,y) &= \left(\sqrt[3]{D}x, \sqrt{D}y\right);
\end{aligned}
$$

where D is a non-square in $\mathbb{F}_q$ for $d \in \{2,4\}$, a non-cube and square for $d = 3$, and a non-cube and non-square for $d = 6$. The formulæ make sense since for $d = 4$, we have $b = 0$ and $q \equiv 1 \pmod 4$, while for $d \in \{3,6\}$, we have $a = 0$ and $q \equiv 1 \pmod 3$. Up to isomorphism over $\mathbb{F}_q$, the twist is unique for $d = 2$, and there are two different ones for $d \in \{3,6\}$ (such that gD or $g^2 D$, respectively, is a cube for g a generator of $\mathbb{F}_q^*$) and $d = 4$ (such that gD or $g^3 D$, respectively, is a fourth power). One can then show, see [HSV, §§4-5], that besides E itself there is a unique twist E' of E, defined over $\mathbb{F}_{q^e}$, such that $r \mid \#E'(\mathbb{F}_{q^e})$. (This uses that $r^2 \nmid \#E(\mathbb{F}_q)$.) If $G_2' = E'(\mathbb{F}_{q^e})[r]$, then

$G_2 = \psi(G_2')$. In particular, the X-coordinates of the points in G_2 lie in $\mathbb{F}_{q^{k/2}}$ for d even, and the Y-coordinates lie in $\mathbb{F}_{q^{k/3}}$ for $3 \mid d$.

The twisted ate pairing of [HSV, §VI] is defined by

$$e_r^{\tilde{\mathrm{A}}} : G_1 \times G_2 \to L^*/(L^*)^r, \quad (P, Q) \mapsto f_{T^e, P}(Q). \tag{19}$$

Let $\pi' : (x, y) \mapsto (x^q, y^q)$ be the Frobenius of E', and let the endomorphism α of E be defined as $\alpha = \psi \circ (\pi')^e \circ \psi^{-1}$. Then $\alpha|_{G_2} = \alpha|_{\psi(G_2')} = \mathrm{id}$, $\alpha^d|_{G_1} = \mathrm{id}$, and thus $\alpha(G_1) \subseteq G_1$. Since ψ is an isomorphism and $\deg((\pi')^e) = q^e$, this implies that $\alpha|_{G_1}$ is multiplication by q^e. So α behaves similarly to the Frobenius endomorphism, but with the roles of G_1 and G_2 reversed and of degree q^e instead of q: G_2 is the eigenspace of eigenvalue 1, and G_1 is the eigenspace of eigenvalue q^e. The same proof as for Theorem 14 thus carries through after replacing π by α, q by q^e, T by T^e and k by d.

Theorem 15. *$e_r^{\tilde{\mathrm{A}}}$ is bilinear, and if $r^2 \nmid T^k - 1$, it is non-degenerate. More precisely,*

$$\left(e_r^{\tilde{\mathrm{A}}}\right)^{dq^{e(d-1)}} = \left(e_r^{\mathrm{T}}\right)^{\frac{T^k-1}{r}}.$$

Generically, one has $T^e = T^{k/d} \in O\left(q^{k/(2d)}\right)$; as soon as $k > 2d$, so certainly for $k > 12$, the loop becomes larger than for the standard Tate pairing, which has the same order of arguments.

7.3. Optimal pairings. The discovery of the ate pairing based on a function $f_{\lambda,Q}$, where $\lambda = T$ is not a multiple of the order of Q, raised the question of further possible values for λ, and on the possibility of minimising the loop length $\log_2 \lambda$. (Strictly speaking, the loop length in Algorithm 12 depends on the addition-negation chain; $\lfloor \log_2 \lambda \rfloor$ measures the number of doublings in a standard double-and-add chain.)

For $i = 1, \ldots, k-1$, Zhao, Zhang and Huang define in [ZZH] the ate$_i$ pairing by

$$e_r^{\mathrm{A}_i} : G_1 \times G_2 \to L^*/(L^*)^r, \quad (P, Q) \mapsto f_{T^i \bmod r, Q}(P). \tag{20}$$

For a curve with an automorphism of order $d \mid k$ and $e = \frac{k}{d}$, a twisted version may be defined for $i = 1, \ldots, d-1$ as

$$e_r^{\tilde{\mathrm{A}}_i} : G_1 \times G_2 \to L^*/(L^*)^r, \quad (P, Q) \mapsto f_{T^{ei} \bmod r, P}(Q).$$

Their bilinearity and non-degeneracy (if $r^2 \nmid T^{ik'}$, where $k' = \frac{k}{\gcd(k,i)}$ is the order of T^i modulo r) is proved as in Theorems 14 and 15, after replacing π by π^i or π' by $(\pi')^i$, respectively.

In [LLP], for the first time two such pairings were combined: If $t_1 = t_0\lambda_1 + \lambda_0$ and $f_{t_0,Q}$ and $f_{t_1,Q}$ define powers of the Tate pairing $e_r^{\mathrm{T}}(Q,P)$, then so does

$$f_{\lambda_1,t_0Q}\, f_{\lambda_0,Q} \frac{\ell_{t_0\lambda_1 Q,\lambda_0 Q}}{v_{t_1 Q}}, \tag{21}$$

called the R-ate pairing. The proof relies on the equation

$$f_{t_0\lambda_1,Q} = f_{t_0,Q}^{\lambda_1} f_{\lambda_1,t_0Q}, \tag{22}$$

which is readily verified by comparing divisors, so that (21) equals the pairing-defining function $\frac{f_{t_1,Q}}{f_{t_0,Q}^{\lambda_1}}$ by (14). Non-degeneracy holds as soon as the exponent with respect to the Tate pairing, readily computed from the previous equation, is not divisible by r. The added loop length in the computation of (21) is $\log_2(\lambda_1) + \log_2(\lambda_0)$. Since the computation of f_{λ_1,t_0Q} and $f_{\lambda_0,Q}$ by Algorithm 12 finishes with $t_0\lambda_1 Q$ and $\lambda_0 Q$, the correction factor is obtained as the quotient of lines from adding these last two points. Additionally, $t_0 Q$ needs to be computed (which can be done in parallel with Algorithm 12 for $f_{\lambda_0,Q}$ if an addition-negation sequence passing through both λ_0 and t_0 is used), and an exponentiation with λ_1 is needed, which will usually be negligible compared to the final exponentiation for obtaining reduced pairings.

Several examples of curve families are given in [LLP] with t_0, t_1 a power of T and λ_0, $\lambda_1 \in O\left(r^{1/\phi(k)}\right)$. That this is no coincidence has been shown by Heß in [Hes1] and Vercauteren in [Ver], who defined more general pairing functions, leading to a notion of optimality that reaches this quantity $O\left(r^{1/\phi(k)}\right)$.

7.3.1. Heß pairings.

Theorem 16 ([Hes1], Theorem 1). *Let $t = \sum_{i=0}^{\deg t} t_i Y^i \in \mathbb{Z}[Y]$, and let y be a primitive k-th root of unity modulo r^2 such that $r \mid t(y)$. Let $f_{t,y,Q}$ be the function, monic at $\mathcal{O}$, such that*

$$\operatorname{div}(f_{t,y,Q}) = \sum_{i=0}^{\deg t} t_i \left([y^i Q] - [\mathcal{O}]\right). \tag{23}$$

Then the Heß pairing

$$e_r^{\mathrm{H}} : G_1 \times G_2 \to L^*/(L^*)^r, \quad (P,Q) \mapsto f_{t,y,Q}(P), \tag{24}$$

is bilinear and, if $r^2 \nmid t(y)$, non-degenerate.

Proof. Let $t(y) = rL$, and rewrite (23) as

$$\operatorname{div}(f_{t,y,Q}) = \sum_{i=0}^{\deg t} t_i y^i [Q] - \sum_{i=0}^{\deg t} t_i \left(y^i [Q] - [y^i Q] \right) - \Big(\sum_{i=0}^{\deg t} t_i + 1 \Big) [\mathcal{O}],$$

which implies that

$$f_{t,y,Q} = f_{r,Q}^L \prod_{i=0}^{\deg t} \left(f_{y^i,Q} \right)^{-t_i}.$$

Since q is a primitive k-th root of unity modulo r, we have $y \equiv q^j \pmod r$ for some j, and $y^i \equiv q^{ij} \pmod r$. The same proof as for the ate (or ate$_i$) pairing, with y^i in the place of T and π^{ij} in the place of π, shows that

$$f_{y^i,Q}^{kq^{k-1}}(P) = e_r^{\mathrm{T}}(Q,P)^{\frac{y^{ik}-1}{r}} = 1 \text{ since } r^2 \mid y^k - 1.$$

Since $r \nmid kq^{k-1}$, we have $f_{y^i,Q}(P) = 1$. So $e_r^{\mathrm{H}} = (e_r^{\mathrm{T}})^L$ is bilinear, and non-degenerate for $r \nmid L$. $\square$

Remark 17. *The condition that y be a primitive k-th root of unity modulo r^2 is clearly not necessary. If y is a root of unity modulo r, then the previous proof carries through, showing that e_r^{H} is bilinear. More precisely, $(e_r^{\mathrm{H}})^{kq^{k-1}} = (e_r^{\mathrm{T}})^N$ with*

$$N = kq^{k-1}\frac{t(y)}{r} - \sum_{i=0}^{\deg t} t_i \frac{y^{ik}-1}{r} = \frac{1}{r}\Big(kq^{k-1} t(y) - \big(t(y^k) - t(1) \big) \Big),$$

so that e_r^{H} is non-degenerate if and only if $r \nmid kq^{k-1}t(y) - \big(t(y^k) - t(1)\big)$. This should hold with overwhelming probability. For instance, one can usually choose $y = T = q \bmod r$.

Since y is a k-th root of unity modulo the order r of Q, any function as in (23) is realised by a polynomial t of degree at most $\phi(k) - 1$. Those with a root at y modulo r can be seen as elements of the $\mathbb{Z}$-lattice with basis $r, Y - y, Y^2 - (y^2 \bmod r), \ldots, Y^{\phi(k)-1} - (y^{\phi(k)-1} \bmod r)$ of dimension $\phi(k)$ and determinant r. For fixed dimension, the Lenstra–Lenstra–Lovász (LLL) lattice basis reduction algorithm [LLL] finds an element t of degree at most $\phi(k) - 1$ and with $|t_i| \in O\left(r^{1/\phi(k)}\right)$.

There is a twisted variant of the Heß pairing: If E has a twist of order $d \mid k$ and $e = \frac{k}{d}$, y is a d-th root of unity modulo r and $r \mid t(y)$, then

$$e_r^{\tilde{\mathrm{H}}} : G_1 \times G_2 \to L^*/(L^*)^r, \quad (P,Q) \mapsto f_{t,y,P}(Q)$$

defines a bilinear pairing that is non-degenerate if y is a primitive d-th root of unity modulo r^2 or, more generally, if $r^2 \nmid dq^{e(d-1)}t(y) - \big(t(y^d) - t(1)\big)$.

Using LLL, one obtains a polynomial of degree less than $\phi(d)$ and with $|t_i| \in O\left(r^{1/\phi(d)}\right)$. The only cases of interest are $d \in \{3, 4, 6\}$, for which $\phi(d) = 2$. Even then, there is only a constant gain in the loop length that does not increase with k, so that asymptotically, the Heß pairing will be preferred to its twisted version. Finally, [Hes1] also contains an optimal version of the Weil pairing.

To see whether (24) can be computed efficiently, let $R_i = y^i Q$, $s_i = \sum_{j=0}^{i} t_j y^j$ and $S_i = s_i Q = \sum_{j=0}^{i} t_j R^j$ for $i \geq 0$ and $s_{-1} = 0$ and $S_{-1} = \mathcal{O}$. Then (24) can be rewritten as

$$\begin{aligned}
&\sum_{i=0}^{\deg t} t_i \big([R_i] - [\mathcal{O}]\big) \\
&\qquad = \sum_{i=0}^{\deg t} \operatorname{div}(f_{t_i,R_i}) + \sum_{i=0}^{\deg t} ([t_i R_i] - [\mathcal{O}]) \\
&\qquad = \sum_{i=0}^{\deg t} \operatorname{div}(f_{t_i,R_i}) + \sum_{i=0}^{\deg t} \left([S_i] - [S_{i-1}] + \operatorname{div}\left(\frac{\ell_{S_{i-1},t_i R_i}}{v_{S_i}}\right)\right)
\end{aligned}$$

and

$$f_{t,y,Q} = \prod_{i=0}^{\deg t} f_{t_i,R_i} \prod_{i=0}^{\deg t} \frac{\ell_{S_{i-1},t_i R_i}}{v_{S_i}}.$$

The precomputation of the R_i by $\deg t - 1$ scalar multiplications can already be rather costly. As $t_i R_i$ is a sideproduct of the computation of f_{t_i,R_i}, each quotient of two lines comes out of a point addition on $E(L)$. But by computing each f_{t_i,R_i} separately via Algorithm 12, the factor $\phi(k)$ gained in the loop length is lost again through the number of evaluations. So while it is shown in [Hes1, Lemma 1] that the Heß pairing uses a function of relatively low degree in $O\left(r^{1/\phi(k)}\right)$, it is unclear whether this function can always be evaluated in $\frac{\log_2(r)}{\phi(k)}$ steps or a very small multiple thereof.

7.3.2. Vercauteren pairings. If one removes the condition that y be a primitive k-th root of unity modulo r^2 in the Heß pairing, one may let $y = q$ under the conditions of Remark 17, a special case considered independently by Vercauteren in [Ver]. Then the R_i may be computed by successive applications of the Frobenius map, and moreover,

$$f_{t_i,R_i}(P) = f_{t_i,q^i Q}(P) = f_{t_i,Q}^{q^i}(P) \qquad \text{by (18).}$$

These functions have the advantage of being computed by Algorithm 12 with respect to the same base point Q. By choosing an addition-negation sequence that passes through all the t_i, they may thus be obtained at the same time. Currently known algorithms compute such sequences with $\log_2 N + \phi(k) O\left(\frac{\log N}{\log\log N}\right)$ steps, where $N = \max |t_i|$, for instance by [Yao]. This shows that, up to the minor factor $\log \log N$, again the gain of $\phi(k)$ in the loop lengths is offset by the number of functions. One should notice, however, that better addition sequences can often be found in practice. Moreover, coefficients occurring in a pairing context are far from random, but exhibit arithmetic peculiarities, as illustrated in the next paragraph.

7.3.3. Optimal pairings on curve families. Elliptic curves suitable for pairing-based cryptography, that is, with a small embedding degree k, are extremely rare among all elliptic curves, see [Box]. An excellent survey article on the problem of finding good parameter combinations is [FST], so there is no need to give any details here. Starting with the article by Brezing and Weng [BW], work has concentrated on finding families of curves parameterised by polynomials. For fixed k, these are given by $p(X)$, $r(X)$ and $u(X) \in \mathbb{Z}[X]$ satisfying arithmetic properties so that if $x_0 \in \mathbb{Z}$ such that $p(x_0)$ is prime, then there is an elliptic curve over $\mathbb{F}_{p(x_0)}$ with trace of Frobenius $u(x_0)$ and a subgroup of order $r(x_0)$ of embedding degree k. Concrete instances are thus given whenever $p(X)$ and $r(X)$ simultaneously represent primes. In practice, one has $\deg(p(X)) = \phi(k)$ or $2\phi(k)$, and the polynomials tend to have small and arithmetically meaningful coefficients (for instance, they are often divisible by prime factors of k).

As an example, Freeman gives a family in [Fre, Theorem 3.1] for $k = 10$ with

$$\begin{aligned}
p(X) &= 25X^4 + 25X^3 + 25X^2 + 10X + 3, \\
u(X) &= 10X^2 + 5X + 3, \\
r(X) &= 25X^4 + 25X^3 + 15X^2 + 5X + 1.
\end{aligned}$$

To construct optimal pairings, one may now work directly with polynomials instead of integers, looking for short vectors in the $\mathbb{Z}[X]$-lattice with basis

$$r(X), Y - y(X), Y^2 - \big(y(X)^2 \bmod r(X)\big), \dots, Y^{\phi(k)} - \big(y(X)^{\phi(k)} \bmod r(X)\big).$$

In Heß's construction of §7.3.1, $y(X)$ is hereby a primitive k-th root of unity modulo $r(X)^2$; notice that $r(X)$ is necessarily irreducible since it represents primes.

For Vercauteren's specialisation of §7.3.2, one has $y(X) = p(X)$, and the above family leads to a short vector (see [Ver, §IV.B])

$$t(Y) = XY^3 + XY^2 - XY - (X + 1).$$

This means that whenever $p(x_0)$ and $r(x_0)$ are prime for some $x_0 \in \mathbb{Z}$, then we obtain a curve and an optimal pairing in which the computation of the $f_{t_i(x_0),Q}$ boils down to $f_{x_0,Q}$. Notice that $x_0 \approx r(x_0)^{1/\deg r(X)} = r(x_0)^{1/\phi(10)}$, and in this family, the gain of a factor of $\phi(k)$ in each invocation of Algorithm 12 leads indeed to a corresponding speed-up in the complete function evaluation.

Acknowledgements. I thank Ilaria Chillotti for pointing out a typo in one of the formulæ, Damien Robert for spotting an error in a previous version of the proof of Theorem 7(e) and Alexandre Gabard for his very thorough proofreading. This research was partially funded by ERC Starting Grant ANTICS 278537.

References

[AL] M. Abdalla and T. Lange, editors, *Pairing-Based Cryptography — Pairing 2012*, volume 7708 of *Lecture Notes in Computer Science*, Heidelberg, 2013. Springer-Verlag. Zbl 1258.94002

[BF] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229, Berlin, 2001. Springer-Verlag. Zbl 1002.94023 MR 1931424

[BGOS] P. S. L. M. Barreto, S. D. Galbraith, C. Ó'hÉigeartaigh and M. Scott, Efficient pairing computation on supersingular abelian varieties. *Designs, Codes and Cryptography* **42** (2007), 239–271. Zbl 1142.14307 MR 2298936

[BK] R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm. *Journal of Cryptology* **11** (1998), 141–145. Zbl 0978.94038 MR 1620936

[BKLS] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, Efficient algorithms for pairing-based cryptosystems. In M. Yung, editor, *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 354–369, Berlin, 2002. Springer-Verlag. Zbl 1026.94520 MR 2054831

[Box] J. Boxall, Heuristics on pairing-friendly elliptic curves. *Journal of Mathematical Cryptology* **6** (2012), 81–104. Zbl 1277.94014 MR 2988897

[Bru] P. Bruin, The Tate pairing for abelian varieties over finite fields. *Journal de Théorie des Nombres de Bordeaux* **23** (2011), 323–328. Zbl 1246.11123 MR 2817932

[BSS] I. Blake, G. Seroussi and N. Smart, *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1999. Zbl 0937.94008 MR 1771549

[BW] F. Brezing and A. Weng, Elliptic curves suitable for pairing based cryptography. *Designs, Codes and Cryptography* **37** (2005), 133–141. Zbl 1100.14517 MR 2165045

[CC] L. S. Charlap and R. Coley, An elementary introduction to elliptic curves II. CCR Expository Report 34, Institute for Defense Analyses, Princeton, July 1990. `http://www.idaccr.org/reports/er34.ps`.

[CFA] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete mathematics and its applications. Chapman & Hall/CRC, Boca Raton, 2006. Zbl 1082.94001

[CM] S. Chatterjee and A. Menezes, On cryptographic protocols employing asymmetric pairings – the role of ψ revisited. *Discrete Applied Mathematics* **159** (2011), 1311–1322. Zbl 1250.94031 MR 2812595

[CZ] Z. Cao and F. Zhang, editors, *Pairing-Based Cryptography – Pairing 2014*, volume 8365 of *Lecture Notes in Computer Science*, Cham, 2014. Springer-Verlag. Zbl 1280.94006

[Deu] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abhandlungen aus dem mathematischen Seminar der hamburgischen Universität* **14** (1941), 197–272. JFM 67.0107.01 MR 0005125

[Eng1] A. Enge, *Elliptic Curves and Their Applications to Cryptography – An Introduction*. Kluwer Academic Publishers, 1999.

[Eng2] —— Discrete logarithms in curves over finite fields. In G. L. Mullen, D. Panario, and I. E. Shparlinski, editors, *Finite Fields and Applications*, volume 461 of *Contemporary Mathematics*, pages 119–139. American Mathematical Society, 2008. Zbl 1236.11108 MR 2436330

[Frey] G. Frey, Applications of arithmetical geometry to cryptographic constructions. In Dieter Jungnickel and Harald Niederreiter, editors, *Finite Fields and Applications – Proceedings of The Fifth International Conference on Finite Fields and Applications F_{q^5}, held at the University of Augsburg, Germany, August 2–6, 1999*, pages 128–161, Berlin, 2001. Springer-Verlag. Zbl 1015.94545 MR 1849086

[FR] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation* **62** (1994), 865–874. Zbl 0813.14045 MR 1218343

[Fre] D. Freeman, Constructing pairing-friendly elliptic curves with embedding degree 10. In F. Hess, S. Pauli and M. Pohst, editors, *Algorithmic Number Theory — ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 452–465, Berlin, 2006. Springer-Verlag. Zbl 1143.14302 MR 2282942

[FST] D. Freemann, M. Scott and E. Teske, A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology* **23** (2010), 224–280. Zbl 1181.94094 MR 2578668

[Gal] S. Galbraith. Pairings. In I. F. Blake, G. Seroussi and N. P. Smart, editors, *Advances in Elliptic Curve Cryptography*, chapter 9, pages 183–213. Cambridge University Press, Cambridge, 2005.

[GHS] S. D. Galbraith, K. Harrison and D. Soldera, Implementing the Tate pairing. In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory — ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337, Berlin, 2002. Springer-Verlag. Zbl 1058.11072 MR 2041094

[GP] S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, Berlin, 2008. Springer-Verlag. Zbl 1155.94002 MR 2733918

[GPS] S. D. Galbraith, K. G. Paterson and N. P. Smart, Pairings for cryptographers. *Discrete Applied Mathematics* **156** (2008), 3113–3121. Zbl 1156.94347 MR 2462118

[GR] S. D. Galbraith and V. Rotger. Easy decision Diffie–Hellman groups. *LMS Journal of Computation and Mathematics*, 7:201–218, 2004. Zbl 1116.14014 MR 2085876

[Hes1] F. Hess, Pairing lattices. In S. D. Galbraith and K. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 18–38, Berlin, 2008. Springer-Verlag. Zbl 1186.94444 MR 2733902

[Hes2] —— A note on the Tate pairing of curves over finite fields. *Archiv der Mathematik* **82** (2004), 28–32. Zbl 1051.11030 MR 2034467

[HSV] F. Hess, N. P. Smart and F. Vercauteren, The eta pairing revisited. *IEEE Transactions on Information Theory* **52** (2006), 4595–4602. Zbl 1189.11057 MR 2300839

[JMO] M. Joye, A. Miyaji and A. Otsuka, editors, *Pairing-Based Cryptography – Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*, Berlin, 2010. Springer-Verlag. Zbl 1200.94008

[Jou] A. Joux, A one round protocol for tripartite Diffie–Hellman. In W. Bosma, editor, *Algorithmic Number Theory – ANTS-IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 385–393, Berlin, 2000. Springer-Verlag. Zbl 1029.94026 MR 1850619

[Lic] S. Lichtenbaum, Duality theorems for curves over p-adic fields. *Inventiones mathematicae* **7** (1969), 120–136. Zbl 0186.26402 MR 0242831

[LLL] A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovász, Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982. Zbl 0488.12001 MR 0682664

[LLP] E. Lee, H.-S. Lee and C.-M. Park, Efficient and generalized pairing computation on abelian varieties. *IEEE Transactions on Information Theory*, 55(4):1793–1803, 2009. MR 2582765

[Mil] V. S. Miller, The Weil pairing, and its efficient calculation. *Journal of Cryptology* **17** (2004), 235–261. Zbl 1078.14043 MR 2090556

[MOV] A. J. MENEZES, T. OKAMOTO and S. A. VANSTONE, Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, September 1993. Zbl 0801.94011 MR 1281712

[Odl] A. ODLYZKO, Discrete logarithms over finite fields. In Gary L. Mullen and Daniel Panario, editors, *Handbook of Finite Fields*, Discrete Mathematics and Its Applications, chapter 11.6, page 393–401. Chapman and Hall/CRC, Boca Raton, 2013.

[Sch] E. F. SCHAEFER, A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field. In T. SHASKA, editor, *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Series on Computing*, pages 1–12, Singapore, 2005. World Scientific Publishing Company. Zbl 1154.14320 MR 2181869

[Sil1] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer-Verlag, New York, 2nd 2009 edition, 1986. Zbl 1194.11005 MR 2514094

[Sil2] —— A survey of local and global pairings on elliptic curves and abelian varieties. In M. JOYE, A. MIYAJI and A. OTSUKA, editors, *Pairing-Based Cryptography – Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*, pages 377–396, Berlin, 2010. Springer-Verlag. Zbl 1291.14042 MR 2781836

[Sil3] J. H. SILVERMAN, Elliptic curves. In G. L. MULLEN and D. PANARIO, editors, *Handbook of Finite Fields*, Discrete Mathematics and Its Applications, chapter 12.2. Chapman and Hall/CRC, Boca Raton, 2013.

[SOK] R. SAKAI, K. OHGISHI and M. KASAHARA, Cryptosystems based on pairing, 2000. SCIS 2000, The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 26–28.

[SW] H. SHACHAM and B. WATERS, editors, *Pairing-Based Cryptography – Pairing 2009*, volume 5671 of *Lecture Notes in Computer Science*, Berlin, 2009. Springer-Verlag. Zbl 1169.94002

[Tat] J. TATE, WC-groups over p-adic fields. Exposé no. 156. In *Années 1956/57–1957/58, exposés 137–168*, volume 4 of *Séminaire Bourbaki*, pages 265–277. Société Mathématique de France, 1956–1958. Zbl 0091.33701 MR 1610926

[TOOO] T. TAKAGI, T. OKAMOTO, E. OKAMOTO and T. OKAMOTO, editors, *Paring-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, Berlin, 2007. Springer-Verlag.

[Ver] F. VERCAUTEREN, Optimal pairings. *IEEE Transactions on Information Theory* **56** (2010), 455–461. MR 2589457

[Wat] W. C. WATERHOUSE, Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure, 4^e Série* **2** (1969), 521–560. Zbl 0188.53001 MR 0265369

[Wei] A. WEIL, Sur les fonctions algébriques à corps de constantes fini. *Comptes rendus hebdomadaires des séances de l'Académie des sciences* **210** (1940), 592–594. Zbl 0023.29401 MR 0002863

[Yao] A. C.-C. YAO, On the evaluation of powers. *SIAM Journal on Computing* **5** (1976), 100–103. Zbl 0326.68025 MR 0395331

[ZZH] C.-A. ZHAO, F. ZHANG and J. HUANG, A note on the Ate pairing. *International Journal of Information Security* **7** (2008), 379–382.

(*Reçu le 23 février 2014*)

Andreas ENGE, INRIA, LFANT, Univ. Bordeaux, CNRS, IMB, UMR 5251, 33400 Talence, France

e-mail: andreas.enge@inria.fr