Chapter 26

Pairings on Elliptic Curves

This chapter is a very brief summary of the mathematics behind pairings on elliptic curves. Pairing-based cryptography was created by Sakai, Ohgishi and Kasahara [509] and Joux [316]. Some applications of pairings in elliptic curve cryptography have already been presented in the book (for example, the identity-based encryption scheme of Boneh and Franklin in Section 23.3.2 and the Boneh-Boyen signature scheme in Section 22.2.3). We present several other important applications of pairings, such as the Menezes-Okamoto-Vanstone/Frey-Rück reduction of the discrete logarithm problem from elliptic curves to finite fields.

Due to lack of space we do not give full details of the subject. Good general references for pairings and pairing-based cryptography are Chapters IX and X of [65], Chapters 6, 16 and 24 of [16] and [320].

26.1 Weil Reciprocity

The following theorem is an important tool for studying pairings. Recall that a divisor on a curve C over a field $\Bbbk$ is a finite sum $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$ (i.e., $n_P = 0$ for all but finitely many $P \in C(\overline{\Bbbk})$). The support of a divisor D is the set of points $\mathrm{Supp}(D) = \{P \in C(\overline{\Bbbk}) : n_P \neq 0\}$. To a function f on a curve one associates the divisor $\mathrm{div}(f)$ as in Definition 7.7.2. If f is a function on a curve and D is a divisor such that the support of D is distinct from the support of $\mathrm{div}(f)$ then $f(D)$ is defined to be $\prod_{P \in C(\overline{\Bbbk}), n_P \neq 0} f(P)^{n_P}$.

Exercise 26.1.1. Let D_1 and D_2 be divisors with disjoint support on a curve C. Suppose D_1 is principal. Show that $f(D_2)$ is well-defined, subject to $\mathrm{div}(f) = D_1$, if and only if D_2 has degree zero.

Theorem 26.1.2. *(**Weil reciprocity**) Let C be a curve over a field $\Bbbk$. Let $f, g \in \Bbbk(C)$*

be functions such that $\mathrm{Supp}(\mathrm{div}(f)) \cap \mathrm{Supp}(\mathrm{div}(g)) = \varnothing$. *Then*

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

Proof: (Sketch) One first shows that the result holds for functions on $C = \mathbb{P}^1$. Then take any covering $\phi : C \to \mathbb{P}^1$ and apply the pullback. We refer to the appendix of Chapter IX of [65] for details. A proof over $\mathbb{C}$ is given in the appendix to Section 18.1 of Lang [366]. □

Pages 24-26 of Charlap and Coley [126] present a generalised Weil reciprocity that does not require the divisors to have disjoint support.

26.2 The Weil Pairing

The Weil pairing plays an important role in the study of elliptic curves over number fields, but tends to be less important in cryptography. For completeness, we briefly sketch its definition.

Let E be an elliptic curve over $\Bbbk$ and let $n \in \mathbb{N}$ be coprime to $\mathrm{char}(\Bbbk)$. Let $P, Q \in E[n]$. Then there is a function $f \in \overline{\Bbbk}(E)$ such that $\mathrm{div}(f) = n(Q) - n(\mathcal{O}_E)$. Let $Q' \in E(\overline{\Bbbk})$ be any point such that $[n]Q' = Q$, and so $[n^2]Q' = \mathcal{O}_E$. Note that $[n]$ is unramified and the divisor $D = [n]^*((Q) - (\mathcal{O}_E))$ is equal to

$$\sum_{R \in E[n]} (Q' + R) - (R).$$

Since $\sum_{R \in E[n]} R = \mathcal{O}_E$ and $[n^2]Q' = \mathcal{O}_E$ it follows from Theorem 7.9.9 that D is a principal divisor. So there is a function $g \in \overline{\Bbbk}(E)$ such that $\mathrm{div}(g) = D = [n]^*((Q) - (\mathcal{O}_E))$. Now, consider the function $[n]^* f = f \circ [n]$. One has $\mathrm{div}([n]^* f) = [n]^*(\mathrm{div}(f)) = [n]^*(n(Q) - n(\mathcal{O}_E)) = nD$. Hence the functions $f \circ [n]$ and g^n have the same divisor. Multiplying f by a suitable constant gives $f \circ [n] = g^n$. Now, for any point $U \in E(\overline{\Bbbk})$ such that $[n]U \notin E[n^2]$ we have

$$g(U + P)^n = f([n]U + [n]P) = f([n]U) = g(U)^n.$$

In other words, $g(U + P)/g(U)$ is an n-th root of unity in $\overline{\Bbbk}$.

Lemma 26.2.1. *Let the notation be as above. Then* $g(U + P)/g(U)$ *is independent of the choice of the point* $U \in E(\overline{\Bbbk})$.

Proof: See Section 11.2 of Washington [626]. The proof is described as "slightly technical" and uses the Zariski topology. □

Definition 26.2.2. Let E be an elliptic curve over a field $\Bbbk$ and let $n \in \mathbb{N}$ be such that $\gcd(n, \mathrm{char}(\Bbbk)) = 1$. Define

$$\mu_n = \{z \in \overline{\Bbbk}^* : z^n = 1\}.$$

The **Weil pairing** is the function

$$e_n : E[n] \times E[n] \to \mu_n$$

defined (using the notation above) as $e_n(P, Q) = g(U + P)/g(U)$ for any point $U \in E(\overline{\Bbbk})$, $U \notin E[n^2]$ and where $\mathrm{div}(g) = [n]^*((Q) - (\mathcal{O}_E))$.

Theorem 26.2.3. *The Weil pairing satisfies the following properties.*

1. *(Bilinear) For $P_1, P_2, Q \in E[n]$, $e_n(P_1+P_2, Q) = e_n(P_1, Q)e_n(P_2, Q)$ and $e_n(Q, P_1+P_2) = e_n(Q, P_1)e_n(Q, P_2)$.*
2. *(Alternating) For $P \in E[n]$, $e_n(P, P) = 1$.*
3. *(Non-degenerate) If $e_n(P, Q) = 1$ for all $Q \in E[n]$ then $P = \mathcal{O}_E$.*
4. *(Galois invariant) If E is defined over $\Bbbk$ and $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$ then $e_n(\sigma(P), \sigma(Q)) = \sigma(e_n(P, Q))$.*
5. *(Compatible) If $P \in E[nm]$ and $Q \in E[n]$ then*

$$e_{nm}(P, Q) = e_n([m]P, Q).$$

Proof: See Theorem III.8.1 of Silverman [564] or Theorem 11.7 of Washington [626]. The non-degeneracy proof in [564] is very sketchy, but the treatment in [626] fills in the missing details. The non-degeneracy also needs the fact that the genus of E is not zero, so there is no function with divisor $(P) - (\mathcal{O}_E)$ (see Corollary 8.6.5). □

Exercise 26.2.4. Show that any function $e : E[n] \times E[n] \to \mu_n$ that has the properties of the Weil pairing as in Theorem 26.2.3 also has the following properties.

1. $e(\mathcal{O}_E, P) = e(P, \mathcal{O}_E) = 1$ for all $P \in E[n]$.
2. $e(-P, Q) = e(P, Q)^{-1}$ for all $P, Q \in E[n]$.
3. $e(P, Q) = e(Q, P)^{-1}$ for all $P, Q \in E[n]$.
4. If $\{P, Q\}$ generate $E[n]$ then the values of e on $E[n] \times E[n]$ are uniquely determined by the single value $e(P, Q)$.

Exercise 26.2.5. Let E be an elliptic curve over $\mathbb{F}_q$ and let $n \in \mathbb{N}$. Prove that $E[n] \subseteq E(\mathbb{F}_q)$ implies $n \mid (q - 1)$.

For elliptic curves over $\mathbb{C}$ the Weil pairing has a very simple interpretation. Recall that an elliptic curve over $\mathbb{C}$ is isomorphic (as a manifold) to $\mathbb{C}/L$, where L is a lattice of rank 2, and that this isomorphism also preserves the group structure. Fix a pair $\{z_1, z_2\}$ of generators for L as a $\mathbb{Z}$-module. The points of order n are $\frac{1}{n}L/L$, so are identified with $\{(az_1 + bz_2)/n : 0 \le a, b < n\}$. The function

$$e_n((az_1 + bz_2)/n, (cz_1 + dz_2)/n) = \exp(2\pi i(ad - bc)/n)$$

is easily checked to be bilinear, non-degenerate and alternating. Hence, it is (a power of) the Weil pairing. We refer to the appendix of Section 18.1 of Lang [366] for further details. Connections with the intersection pairing are discussed in Section 12.2 of Husemoller [302] and Edixhoven [189].

There is an alternative definition[1] of the Weil pairing that is more useful for implementation, but for which it is harder to prove non-degeneracy. For $P, Q \in E[n]$ let D_P and D_Q be degree zero divisors such that $D_P \equiv (P) - (\mathcal{O}_E)$, $D_Q \equiv (Q) - (\mathcal{O}_E)$ and $\mathrm{Supp}(D_P) \cap \mathrm{Supp}(D_Q) = \varnothing$. Let $f_P, f_Q \in \overline{\Bbbk}(E)$ be functions such that $\mathrm{div}(f_P) = nD_P$ and $\mathrm{div}(f_Q) = nD_Q$. Then

$$e_n(P, Q) = f_Q(D_P)/f_P(D_Q). \tag{26.1}$$

[1] The literature is inconsistent and some of the definitions (for example, Section 18.1 of Lang [366], Exercise 3.16 of Silverman [564] and Section 3 of Miller [427]) are actually for $e_n(Q, P) = e_n(P, Q)^{-1}$. For further discussion of this issue see Remark 11.3 and Section 11.6 of Washington [626]. Also see the "Warning" at the end of Section 4 of Miller [429].

The equivalence is shown in Theorem 4 of the extended and unpublished version of Hess [282], and in Section 11.6.1 of Washington [626].

The Weil pairing can be generalised from $E[n] \times E[n]$ to $\ker(\phi) \times \ker(\hat{\phi}) \subseteq E[n] \times \widetilde{E}[n]$ where $\phi : E \to \widetilde{E}$ is an isogeny. For details see Exercise 3.15 of Silverman [564] or Garefalakis [237]. For the Weil pairing on Jacobian varieties of curves of genus $g > 1$ we refer to Section 20 of Mumford [444].

26.3 The Tate-Lichtenbaum Pairing

Tate defined a pairing for Abelian varieties over local fields and Lichtenbaum showed how to compute it efficiently in the case of Jacobian varieties of curves. Frey and Rück [213] showed how to compute it for elliptic curves over finite fields, and emphasised its cryptographic relevance. This pairing is the basic building block of most pairing-based cryptography.

Exercise 26.3.1. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ and let $n \in \mathbb{N}$ be such that $\gcd(n, q) = 1$ and $n \mid \#E(\mathbb{F}_q)$. Define

$$nE(\mathbb{F}_q) = \{[n]Q : Q \in E(\mathbb{F}_q)\}.$$

Show that $nE(\mathbb{F}_q)$ is a group. Show that $E(\mathbb{F}_q)[n] = \{P \in E(\mathbb{F}_q) : [n]P = \mathcal{O}_E\}$, $E(\mathbb{F}_q)/nE(\mathbb{F}_q) = \{P + nE(\mathbb{F}_q) : P \in E(\mathbb{F}_q)\}$ and $\mathbb{F}_q^*/(\mathbb{F}_q^*)^n$ are finite groups of exponent n.

Let notation be as in Exercise 26.3.1. Let $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_q)$. Then $n(P) - n(\mathcal{O}_E)$ is principal, so there is a function $f \in \mathbb{F}_q(E)$ such that $\mathrm{div}(f) = n(P) - n(\mathcal{O}_E)$. Let D be a divisor on E with support disjoint from $\mathrm{Supp}(\mathrm{div}(f)) = \{\mathcal{O}_E, P\}$ but such that D is equivalent to $(Q) - (\mathcal{O}_E)$ (for example, $D = (Q + R) - (R)$ for some point[2] $R \in E(\overline{\mathbb{F}}_q)$, $R \notin \{\mathcal{O}_E, P, -Q, P - Q\}$). We define the **Tate-Lichtenbaum pairing** to be

$$t_n(P, Q) = f(D). \tag{26.2}$$

We will explain below that

$$t_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^n.$$

First we show that the pairing is well-defined. We sketch the proof, as it is a nice and simple application of Weil reciprocity.

Lemma 26.3.2. *Let the notation be as above. Let $P \in E(\mathbb{F}_q)[n]$ and let $f \in \mathbb{F}_q(E)$ be such that $\mathrm{div}(f) = n(P) - n(\mathcal{O}_E)$. Let D_1, D_2 be divisors on E defined over $\mathbb{F}_q$ with support disjoint from $\{\mathcal{O}_E, P\}$.*

1. *Suppose $D_1 \equiv D_2 \equiv (Q) - (\mathcal{O}_E)$ for some point $Q \in E(\mathbb{F}_q)$. Then $f(D_1)/f(D_2) \in (\mathbb{F}_q^*)^n$.*
2. *Suppose $D_1 \equiv (Q_1) - (\mathcal{O}_E)$ and $D_2 \equiv (Q_2) - (\mathcal{O}_E)$ where $Q_1, Q_2 \in E(\mathbb{F}_q)$ are such that $Q_1 \neq Q_2$ and and $Q_1 - Q_2 \in nE(\mathbb{F}_q)$. Then $f(D_1)/f(D_2) \in (\mathbb{F}_q^*)^n$.*

[2] One can usually take $R \in E(\mathbb{F}_q)$, but see page 187 of [65] for an example that shows that this is not always possible.

Proof: The first statement is a special case of the second, but it is a convenient stepping-stone for the proof. For the first statement, write $D_2 = D_1 + \mathrm{div}(h)$ where h is a function on E defined over $\mathbb{F}_q$. Note that $\mathrm{Supp}(\mathrm{div}(h)) \cap \{\mathcal{O}_E, P\} = \varnothing$. We have

$$f(D_2) = f(D_1 + \mathrm{div}(h)) = f(D_1)f(\mathrm{div}(h)).$$

Now, applying Weil reciprocity gives $f(\mathrm{div}(h)) = h(\mathrm{div}(f)) = h(n(P) - n(\mathcal{O}_E)) = (h(P)/h(\mathcal{O}_E))^n \in (\mathbb{F}_q^*)^n$.

For the second statement write $Q_1 - Q_2 = [n]R$ for some $R \in E(\mathbb{F}_q)$. We may assume that $R \neq \mathcal{O}_E$, since the first statement has already been proved. Then $(Q_1) - (Q_2) = n((R+S) - (S)) + \mathrm{div}(h_0)$ for some $h_0 \in \mathbb{F}_q(E)$ and some $S \in E(\mathbb{F}_q)$ with $S \notin \{\mathcal{O}_E, -R, P, P-R\}$.[3] We also have $D_1 = (Q_1) - (\mathcal{O}_E) + \mathrm{div}(h_1)$ and $D_2 = (Q_2) - (\mathcal{O}_E) + \mathrm{div}(h_2)$ for some $h_1, h_2 \in \mathbb{F}_q(E)$. Putting everything together

$$\begin{aligned} f(D_2) &= f(D_1 - n((R+S) - (S)) + \mathrm{div}(h_2) - \mathrm{div}(h_1) - \mathrm{div}(h_0)) \\ &= f(D_1)f((R+S) - (S))^n f(\mathrm{div}(h_2/(h_0h_1))). \end{aligned}$$

Since $\mathrm{Supp}(\mathrm{div}(h_2/(h_0h_1))) \subseteq \mathrm{Supp}(D_1) \cup \mathrm{Supp}(D_2) \cup \{R+S, S\}$ is disjoint from $\{\mathcal{O}_E, P\} = \varnothing$ the result follows from Weil reciprocity. □

Theorem 26.3.3. *The Tate-Lichtenbaum pairing satisfies the following properties.*

1. *(Bilinear) For $P_1, P_2 \in E(\mathbb{F}_q)[n]$, and $Q \in E(\mathbb{F}_q)$, $t_n(P_1+P_2, Q) = t_n(P_1, Q)t_n(P_2, Q)$. For $Q \in E(\mathbb{F}_q)[n]$ and $P_1, P_2 \in E(\mathbb{F}_q)$, $t_n(Q, P_1 + P_2) = t_n(Q, P_1)t_n(Q, P_2)$.*
2. *(Non-degenerate) Assume $\mathbb{F}_q^*$ contains a non-trivial n-th root of unity. Let $P \in E(\mathbb{F}_q)[n]$. If $t_n(P, Q) = 1$ for all $Q \in E(\mathbb{F}_q)$ then $P = \mathcal{O}_E$. Let $Q \in E(\mathbb{F}_q)$. If $t_n(P, Q) = 1$ for all $P \in E(\mathbb{F}_q)[n]$ then $Q \in nE(\mathbb{F}_q)$.*
3. *(Galois invariant) If E is defined over $\mathbb{F}_q$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ then $t_n(\sigma(P), \sigma(Q)) = \sigma(t_n(P, Q))$.*

Proof: Bilinearity can be proved using ideas similar to those used to prove Lemma 26.3.2 (for all the details see Theorem IX.7 of [65]). Non-degeneracy in the case of finite fields was shown by Frey and Rück [213], but simpler proofs can be found in Hess [282] and Section 11.7 of Washington [626]. Galois invariance is straightforward (see Theorem IX.7 of [65]). □

26.3.1 Miller's Algorithm

We now briefly explain how to compute the Tate-Lichtenbaum pairing (and hence the Weil pairing via equation (26.1)). The algorithm first appears in Miller [427].

Definition 26.3.4. Let $P \in E(\Bbbk)$ and $i \in \mathbb{N}$. A **Miller function** $f_{i,P} \in \Bbbk(E)$ is a function on E such that $\mathrm{div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O}_E)$. Furthermore, we assume that Miller functions are "normalised at infinity" in the sense that the power series expansion at infinity with respect to the canonical uniformizer $t_\infty = x/y$ is 1.

Exercise 26.3.5. Show that $f_{1,P} = 1$. Show that if $f_{i,P}$ and $f_{j,P}$ are Miller functions then one can take

$$f_{i+j,P} = f_{i,P}f_{j,P}l(x,y)/v(x,y)$$

where $l(x,y)$ and $v(x,y)$ are the lines arising in the elliptic curve addition of $[i]P$ to $[j]P$ (and so $\mathrm{div}(l(x,y)) = ([i]P) + ([j]P) + (-[i+j]P) - 3(\mathcal{O}_E)$ and $\mathrm{div}(v(x,y)) = ([i+j]P) + (-[i+j]P) - 2(\mathcal{O}_E)$).

[3] Some tedious calculations are required to show that one can choose $S \in E(\mathbb{F}_q)$ rather than $E(\overline{\mathbb{F}}_q)$ in all cases, but the claim is easy when n is large.

We can now give Miller's algorithm to compute $f_{n,P}(D)$ for any divisor D (see Algorithm 29). The basic idea is to compute the Miller function out of smaller Miller functions using a "square-and-multiply" strategy. As usual, we write an integer n in binary as $(1n_{m-1}\dots n_1 n_0)_2$ where $m = \lfloor \log_2(n) \rfloor$. Note that the lines l and v in lines 6 and/or 10 may be simplified if the operation is $[2]T = \mathcal{O}_E$ or $T + P = \mathcal{O}_E$.

Algorithm 29 Miller's Algorithm

```
INPUT: $n = (1n_{m-1}\dots n_1 n_0)_2 \in \mathbb{N}$, $P \in E(\Bbbk)$, such that $[n]P = \mathcal{O}_E$, $D \in \mathrm{Div}_{\overline{\Bbbk}}(E)$
OUTPUT: $f_{n,P}(D)$
 1: $f = 1$
 2: $T = P$
 3: $i = m - 1 = \lfloor \log_2(n) \rfloor - 1$
 4: while $i \geq 0$ do
 5:     Calculate lines $l$ and $v$ for doubling $T$
 6:     $f = f^2 \cdot l(D)/v(D)$
 7:     $T = [2]T$
 8:     if $n_i = 1$ then
 9:         Calculate lines $l$ and $v$ for addition of $T$ and $P$
10:         $f = f \cdot l(D)/v(D)$
11:         $T = T + P$
12:     end if
13:     $i = i - 1$
14: end while
15: return $f$
```

The main observation is that Miller's algorithm takes $O(\log_2(n))$ iterations, each of which comprises field operations in $\Bbbk$ if P and all points in the support of D lie in $E(\Bbbk)$. There are a number of important techniques to speed up Miller's algorithm in practice; we mention some of them in the following sections and refer to Chapter IX of [65], Chapter XII of [320] or Section 16.4 of [16] for further details.

Exercise 26.3.6. Give simplified versions of lines 6 and 10 of Algorithm 29 that apply when $[2]T = \mathcal{O}_E$ or $T + P = \mathcal{O}_E$.

26.3.2 The Reduced Tate-Lichtenbaum Pairing

Definition 26.3.7. Let $n, q \in \mathbb{N}$ be such that $\gcd(n, q) = 1$. Define the **embedding degree** $k(q, n) \in \mathbb{N}$ to be the smallest positive (non-zero) integer such that $n \mid (q^{k(q,n)} - 1)$.

Let E be an elliptic curve over $\mathbb{F}_q$ and suppose $n \mid \#E(\mathbb{F}_q)$ is such that $\gcd(n, q) = 1$. Let $k = k(q, n)$ be the embedding degree. Then $\mu_n \subseteq \mathbb{F}_{q^k}^*$ (in some cases μ_n can lie in a proper subfield of $\mathbb{F}_{q^k}$) and so the Tate-Lichtenbaum pairing maps into $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$. In practice it is inconvenient to have a pairing taking values in this quotient group, as cryptographic protocols require well-defined values. To have a canonical representative for each coset in $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$ it would be much more convenient to use μ_n. This is easily achieved using the facts that if $z \in \mathbb{F}_{q^k}^*$ then $z^{(q^k-1)/n} \in \mu_n$, and that the cosets $z_1(\mathbb{F}_{q^k}^*)^n$ and $z_2(\mathbb{F}_{q^k}^*)^n$ are equal if and only if $z_1^{(q^k-1)/n} = z_2^{(q^k-1)/n}$. Also, exponentiation is a group homomorphism from $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$ to μ_n.

For this reason, one usually considers the **reduced Tate-Lichtenbaum pairing**

$$\hat{t}_n(P, Q) = t_n(P, Q)^{(q^k-1)/n},$$

which maps $E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ to μ_n. The exponentiation to the power $(q^k - 1)/n$ is called the **final exponentiation**.

Exercise 26.3.8. Let $n \mid N \mid (q^k - 1)$. Show that

$$t_n(P, Q)^{(q^k-1)/n} = t_N(P, Q)^{(q^k-1)/N}.$$

Exercise 26.3.9. Explain why working in a group whose order has low Hamming weight leads to relatively fast pairings. Suppose $n = E(\mathbb{F}_q)$ has low Hamming weight but $r \mid n$ does not. Explain how to compute the reduced Tate-Lichtenbaum pairing $\hat{t}_r(P, Q)$ efficiently if n/r is small.

In the applications one usually chooses the elliptic curve E to satisfy the mild conditions in Exercise 26.3.10. In these cases it follows from the Exercise that we can identify $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ with $E(\mathbb{F}_{q^k})[r]$. Hence, if the conditions hold, we may interpret the reduced Tate-Lichtenbaum pairing as a map

$$\hat{t}_r : E[r] \times E[r] \to \mu_r,$$

just as the Weil pairing is.

Exercise 26.3.10. Let E be an elliptic curve over $\mathbb{F}_q$ and let r be a prime such that $r \| \#E(\mathbb{F}_q)$, $\gcd(r, q) = 1$, $E[r] \subseteq E(\mathbb{F}_{q^k})$ and $r^2 \| \#E(\mathbb{F}_{q^k})$, where $k = k(q, r)$ is the embedding degree. Show that $E[r]$ is set of representatives for $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$.

In most cryptographic situations one restricts to the case of points of prime order r. Further, one can often insist that $P \in E(\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_{q^k})$. An important observation is that if $k > 1$ and $z \in \mathbb{F}_q^*$ then $z^{(q^k-1)/r} = 1$. This allows us to omit some computations in Miller's algorithm. A further trick, due[4] to Barreto, Kim, Lynn and Scott [29], is given in Lemma 26.3.11 (a similar fact for the Weil pairing is given in Proposition 8 of Miller [429]).

Lemma 26.3.11. *Let E be an elliptic curve over $\mathbb{F}_q$, $P \in E(\mathbb{F}_q)$ a point of prime order r (where $r > 4$ and $\gcd(q, r) = 1$), and $Q \in E(\mathbb{F}_{q^k}) - E(\mathbb{F}_q)$ where $k > 1$ is the embedding degree. Then*

$$\hat{t}_r(P, Q) = f_{r,P}(Q)^{(q^k-1)/r}.$$

Proof: A proof for general curves (and without any restriction on r) is given in Lemma 1 of Granger, Hess, Oyono, Thériault and Vercauteren [265]. We give a similar argument.

We have $\hat{t}_r(P, Q) = f_{r,P}((Q+R)-(R))^{(q^k-1)/r}$ for any point $R \in E(\mathbb{F}_{q^k}) - \{\mathcal{O}_E, P, -Q, P-Q\}$. Choose $R \in E(\mathbb{F}_q) - \{\mathcal{O}_E, P\}$. Since $f_{r,P}(R) \in \mathbb{F}_q^*$ and $k > 1$ it follows that

$$\hat{t}_r(P, Q) = f_{r,P}(Q + R)^{(q^k-1)/r}.$$

Now, it is not possible to take $R = \mathcal{O}_E$ in the above argument. Instead we need to prove that $f_{r,P}(Q + R)^{(q^k-1)/r} = f_{r,P}(Q)^{(q^k-1)/r}$ directly. It suffices to prove that

$$f_{r,P}((Q + R) - (Q))^{(q^k-1)/r} = 1.$$

To do this, note that $(Q + R) - (Q) \equiv (R) - (\mathcal{O}_E) \equiv ([2]R) - (R)$. Set, for example, $R = [2]P$ so that $([2]R) - (R)$ has support disjoint from $\{\mathcal{O}_E, P\}$ (this is where the

[4] Though be warned that the "proof" in [29] is not rigorous.

condition $r > 4$ is used). Then there is a function $h \in \mathbb{F}_{q^k}(E)$ such that $(Q+R)-(Q) = ([2]R)-(R)+\operatorname{div}(h)$. We have

$$f_{r,P}((Q+R)-(Q)) = f_{r,p}(([2]R)-(R)+\operatorname{div}(h)) = f_{r,P}(([2]R)-(R))h(\operatorname{div}(f_{r,P})).$$

Finally, note that $f_{r,P}(([2]R)-(R)) \in \mathbb{F}_q^*$ and that $h(\operatorname{div}(f_{r,P})) = (h(P)/h(\mathcal{O}_E))^r \in (\mathbb{F}_{q^k}^*)^r$. The result follows. □

Exercise 26.3.12. Let the embedding degree k be even, $r \nmid (q^{k/2}-1)$, $P \in E(\mathbb{F}_q)$ and $Q = (x_Q, y_Q) \in E(\mathbb{F}_{q^k})$ points of order r. Suppose $x_Q \in \mathbb{F}_{q^{k/2}}$ (this is usually the case for points of cryptographic interest). Show that all vertical line functions can be omitted when computing the reduced Tate-Lichtenbam pairing.

26.3.3 Ate Pairing

Computing pairings on elliptic curves usually requires significantly more effort than exponentiation on an elliptic curve. There has been a concerted research effort to make pairing computation more efficient, and a large number of techniques are known. Due to lack of space we focus on one particular method known as "loop shortening". This idea originates in the work of Duursma and Lee [187] (for hyperelliptic curves) and was further developed by Barreto, Galbraith, Ó hÉigeartaigh and Scott [28]. We present the idea in the ate pairing formulation of Hess, Smart and Vercauteren [284]. Note that the ate pairing is not a "new" pairing. Rather, it is a way to efficiently compute a power, of a restriction to certain subgroups, of the Tate-Lichtenbaum pairing.

Let E be an elliptic curve over $\mathbb{F}_q$ and let r be a large prime such that $r \mid \#E(\mathbb{F}_q) = q+1-t$ and $r \mid (q^k-1)$ for some relatively small integer k, but $r \nmid (q-1)$. It follows that $\#(E[r] \cap E(\mathbb{F}_q)) = r$. Since the Frobenius map is linear on the $\mathbb{F}_r$-vector space $E[r]$, and its characteristic polynomial satisfies

$$x^2 - tx + q \equiv (x-1)(x-q) \pmod{r},$$

it follows that π_q has distinct eigenvalues 1 and $q \pmod{r}$ and corresponding eigenspaces (i.e., subgroups)

$$G_1 = E[r] \cap \ker(\pi_q - [1]) \ , \quad G_2 = E[r] \cap \ker(\pi_q - [q]). \tag{26.3}$$

Since, $r \mid (q^k-1)$ and $q \equiv (t-1) \pmod{r}$ it follows that $r \mid ((t-1)^k-1)$. Let $T = t-1$ and $N = \gcd(T^k-1, q^k-1)$. Note that $r \mid N$. Define the **ate pairing** $a_T : G_2 \times G_1 \to \mu_r$ by

$$a_T(Q,P) = f_{T,Q}(P)^{(q^k-1)/N}.$$

The point is that $|t| \le 2\sqrt{q}$ and, typically, $r \approx q$. Hence, computing the Miller function $f_{T,Q}$ typically requires at most half the number of steps as required to compute $f_{r,P}$. On the downside, the coefficients of the function $f_{T,Q}$ lie in $\mathbb{F}_{q^k}$, rather than $\mathbb{F}_q$ as before. Nevertheless, the ate pairing often leads to faster pairings if carefully implemented (especially when twists are exploited).

Theorem 26.3.13. *Let the notation be as above (in particular, $T = t-1$ and $N = \gcd(T^k-1, q^k-1)$). Let $L = (T^k-1)/N$ and $c = \sum_{i=0}^{k-1} q^i T^{k-1-i} \pmod{r}$. Then*

$$a_T(Q,P)^c = t_r(Q,P)^{L(q^k-1)/r}.$$

Hence, a_T is bilinear, and a_T is non-degenerate if and only if $r \nmid L$.

Proof: (Sketch) Consider $t_r(Q,P)^{(q^k-1)/r} = f_{r,Q}(P)^{(q^k-1)/r}$. Since $r \mid N$, Exercise 26.3.8 implies that this is equal to

$$f_{N,Q}(P)^{(q^k-1)/N}.$$

Indeed,

$$t_r(Q,P)^{L(q^k-1)/r} = f_{LN,Q}(P)^{(q^k-1)/N} = f_{T^k-1,Q}(P)^{(q^k-1)/N}.$$

Now, $[T^k-1]Q = \mathcal{O}_E$ so one can take $f_{T^k,Q} = f_{T^k-1,Q}$. (To prove this note that $\operatorname{div}(f_{T^k,Q}) = T^k(Q) - ([T^k]Q) - (T^k-1)(\mathcal{O}_E) = T^k(Q) - (Q) - (T^k-1)(\mathcal{O}_E) = (T^k - 1)(Q) - (T^k-1)(\mathcal{O}_E)$.) Hence, the L-th power of the reduced Tate-Lichtenbaum pairing is $f_{T^k,Q}(P)^{(q^k-1)/N}$. Now,

$$f_{T^k,Q}(P) = f_{T,Q}(P)^{T^{k-1}} f_{T,[T]Q}(P)^{T^{k-2}} \cdots f_{T,[T^{k-1}]Q}(P), \tag{26.4}$$

which follows by considering the divisors of the left- and right-hand sides. The final step, and the only place we use $\pi_q(Q) = [q]Q = [T]Q$, is to note that

$$f_{T,[T]Q}(P) = f_{T,\pi_q(Q)}(P) = f^q_{T,Q}(P). \tag{26.5}$$

where f^q denotes raising all coefficients of the rational function f to the power q. This follows because E and P are defined over $\mathbb{F}_q$, so $\sigma(f_{T,Q}(P)) = f_{T,\sigma(Q)}(P)$ for all $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)$. One therefore computes $f_{T^k,Q}(P) = f_{T,Q}(P)^c$, which completes the proof. □

Exercise 26.3.14. Generalise Theorem 26.3.13 to the case where $T \equiv q^m \pmod{r}$ for some $m \in \mathbb{N}$. What is the corresponding value of c?

26.3.4 Optimal Pairings

Lee, Lee and Park [369], Hess [283] and Vercauteren [618] have used combinations of pairings that have the potential for further loop shortening over that provided by the ate pairing.

Ideally, one wants to compute a pairing as $f_{M,Q}(P)$, with some final exponentation, where M is as small as possible. Hess and Vercauteren conjecture that the smallest possible value for $\log_2(M)$, for points of prime order r in an elliptic curve E over $\mathbb{F}_q$ with embedding degree $k(q,r)$, is $\log_2(r)/\varphi(k(q,r))$. For such a pairing, Miller's algorithm would be sped up by a factor of approximately $\varphi(k(q,r))$ compared with the time required when not using loop shortening. The method of Vercauteren actually gives a pairing as a product of $\prod_{i=0}^{l} f_{M_i,Q}(P)^{q^i}$ (together with some other terms) where all the integers M_i are of the desired size; such a pairing is not automatically computed faster than the naive method, but if the integers M_i all have a large common prefix in their binary expansions then such a saving can be obtained. If a pairing can be computed with approximately $\log_2(r)/\varphi(k(q,r))$ iterations in Miller's algorithm then it is called an **optimal pairing**.

The basic principle of Vercauteren's construction is to find a multiple ur, for some $u \in \mathbb{N}$, of the group order that can be written in the form

$$ur = \sum_{i=0}^{l} M_i q^i \tag{26.6}$$

where the $M_i \in \mathbb{Z}$ are "small". One can then show, just like with the ate pairing, that a certain power of the Tate-Lichtenbaum pairing is

$$\left(\prod_{i=0}^{l} f_{M_i,Q}(P)^{q^i} \prod_{i=1}^{l} g_i(P) \right)^{(q^k-1)/r}, \tag{26.7}$$

where the functions g_i take into account additions of certain elliptic curve points. Vercauteren proves that if

$$ukq^{k-1} \not\equiv \tfrac{(q^k-1)}{r}\left(\sum_{i=0}^{l} iM_i q^{i-1}\right) \pmod{r}$$

then the pairing is non-degenerate. The value of equation (26.7) can be computed efficiently only if all $f_{M_i,Q}(P)$ can, in some sense, be computed simultaneously. This is easiest when all but one of the M_i are small (i.e., in $\{-1,0,1\}$) or when the M_i have a large common prefix of most significant bits (possibly in signed binary expansion).

Vercauteren [618] suggests finding solutions to equation (26.6) using lattices. More precisely, given r and q one considers the lattice spanned by the rows of the following matrix

$$B = \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -q & 1 & 0 & \cdots & 0 \\ -q^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -q^l & 0 & 0 & \cdots & 1 \end{pmatrix}. \tag{26.8}$$

One sees that $(u, M_1, M_2, \dots, M_l)B = (M_0, M_1, \dots, M_l)$ and so candidate values for $u, M_0, \dots, M_l$ can be found by finding short vectors in the lattice. A demonstration of this method is given in Example 26.6.3.

Note that loop shortening methods should not be confused with the methods, starting with Scott [534], that use an endomorphism on the curve to "recycle" some computations in Miller's algorithm. Such methods do not reduce the number of squarings in Miller's algorithm and, while valuable, do not give the same potential performance improvements as methods that use loop shortening.

26.3.5 Pairing Lattices

Hess [283] developed a framework for analysing pairings that is closely related to the framework in the previous section. We briefly sketch the ideas.

Definition 26.3.15. Let notation be as in Section 26.3.3, in particular q is a prime power, r is a prime, q is a primitive k-th root of unity modulo r, and the groups G_1 and G_2 are as in equation (26.3). Let $s \equiv q^m \pmod{r}$ for some $m \in \mathbb{N}$. For any $h(x) \in \mathbb{Z}[x]$ write $h(x) = \sum_{i=0}^{d} h_i x^i$. Let $P \in G_1$, $Q \in G_2$ and define $f_{s,h(x),Q}$ to be a function normalised at infinity (in the sense of Definition 26.3.4) such that

$$\mathrm{div}(f_{s,h(x),Q}) = \sum_{i=0}^{d} h_i(([s^i]Q) - (\mathcal{O}_E)).$$

Define

$$a_{s,h(x)}(Q,P) = f_{s,h(x),Q}(P)^{(q^k-1)/r}.$$

We stress here that h is a polynomial, not a rational function (as it was in previous sections).

Since $[s]Q = [q^m]Q = \pi_q^m(Q)$, a generalisation of equation (26.5) shows that $f_{h_i,[s^i]Q}(P) = f_{h_i,Q}(P)^{q^{mi}}$. It follows that one can compute $f_{s,h(x),Q}(P)$ efficiently using Miller's algorithm in a similar way to computing the pairings in the previous section. The running time of Miller's algorithm is proportional to $\sum_{i=0}^{d} \log_2(\max\{1, |h_i|\})$ in the worse case (it performs better when the h_i have a large common prefix in their binary expansion).

Hess [283] shows that, for certain choices of $h(x)$, $a_{s,h(x)}$ is a non-degenerate and bilinear pairing. The goal is also to obtain good choices for $h(x)$ so that the pairing can be computed using a short loop. One of the major contributions of Hess [283] is to prove lower bounds on the size of the coefficients of any polynomial $h(x)$ that leads to a non-degenerate, bilinear pairing. This supports the optimality conjecture mentioned in the previous section.

Lemma 26.3.16. *Let notation be as in Definition 26.3.15.*

1. *$a_{s,r}(Q,P)$ is the Tate pairing.*
2. *$a_{s,x-s}(Q,P)$ is a power of the ate pairing.*
3. *$a_{s,h(x)x}(Q,P) = a_{s,h(x)}(Q,P)^s$.*
4. *Let $h(x), g(x) \in \mathbb{Z}[x]$. Then*

$$a_{s,h(x)+g(x)}(Q,P) = a_{s,h(x)}(Q,P)a_{s,g(x)}(Q,P) \quad \text{and} \quad a_{s,h(x)g(x)}(Q,P) = a_{s,h(x)}(Q,P)^{g(s)}.$$

Exercise 26.3.17.★ Prove Lemma 26.3.16.

Theorem 26.3.18. *Let notation be as above. Let $s \in \mathbb{N}$ be such that s is a primitive k-th root of unity modulo r^2. Let $h(x) \in \mathbb{Z}[x]$ be such that $h(s) \equiv 0 \pmod{r}$ but $r^2 \nmid h(s)$. Then $a_{s,h(x)}$ is a non-degenerate, bilinear pairing on $G_2 \times G_1$.*

Proof: Since $s^k \equiv 1 \pmod{r}$ it follows that $s \equiv q^m \pmod{r}$ for some $m \in \mathbb{N}$. Since $h(s) \equiv 0 \pmod{r}$ we can write

$$h(x) = g_1(x)(x-s) + g_2(x)r$$

for some $g_1(x), g_2(x) \in \mathbb{Z}[x]$. It follows from Lemma 26.3.16 that, for some $c \in \mathbb{N}$,

$$a_{s,h(x)}(Q,P) = a_T(Q,P)^{cg_1(s)}\hat{t}_r(Q,P)^{g_2(s)}$$

and so $a_{s,h(x)}$ is a bilinear pairing on $G_2 \times G_1$.

Finally, we need to prove non-degeneracy. By assumption, $r^2 \mid (s^k - 1)$ and so, in the version of Theorem 26.3.13 of Exercise 26.3.14, $r \mid L$. It follows that $a_T(Q,P) = 1$. Hence, $a_{s,h(x)}(Q,P) = \hat{t}_r(Q,P)^{g_2(s)}$. To complete the proof, note that $g_2(s) = h(s)/r$, and so $a_{s,h(x)}$ is non-degenerate if and only if $r^2 \nmid h(s)$. □

Hess [283] explains that this construction is "complete" in the sense that every bilinear map coming from functions in a natural class must correspond to some polynomial $h(x)$. Hess also proves that any polynomial $h(x) = \sum_{i=0}^{d} h_i x^i \in \mathbb{Z}[x]$ satisfying the required conditions is such that $\sum_{i=0}^{d} |h_i| \ge r^{1/\varphi(k)}$. Polynomials $h(x)$ that have one coefficient of size $r^{1/\varphi(k)}$ and all other coefficients small satisfy the optimality conjecture. Good choices for the polynomial $h(x)$ are found by considering exactly the same lattice as in equation (26.8) (though in [283] it is written with q replaced by s).

26.4 Reduction of ECDLP to Finite Fields

An early application of pairings in elliptic curve cryptography was to reduce the discrete logarithm problem in $E(\mathbb{F}_q)[n]$, when $\gcd(n,q) = 1$, to the discrete logarithm problem in the multiplicative group of a finite extension of $\mathbb{F}_q$. Menezes, Okamoto and Vanstone [417] used the Weil pairing to achieve this, while Frey and Rück [213] used the reduced Tate-Lichtenbaum pairing. The case $\gcd(n, q) \neq 1$ will be handled in Section 26.4.1.

The basic idea is as follows: Given an instance P, $Q = [a]P$ of the discrete logarithm problem in $E(\mathbb{F}_q)[n]$ and a non-degenerate bilinear pairing e, one finds a point $R \in E(\overline{\mathbb{F}}_q)$ such that $z = e(P, R) \neq 1$. It follows that $e(Q, R) = z^a$ in $\mu_n \subseteq \mathbb{F}_{q^k}^*$ where $k = k(q, n)$ is the embedding degree. When q is a prime power that is not prime then there is the possibility that μ_r lies in a proper subfield of $\mathbb{F}_{q^k}$, in which case re-define k to be the smallest positive rational number such that $\mathbb{F}_{q^k}$ is the smallest field of characteristic $\mathrm{char}(\mathbb{F}_q)$ containing μ_n.

The point is that if k is sufficiently small then index calculus algorithms in $\mathbb{F}_{q^k}^*$ could be faster than the baby-step-giant-step or Pollard rho algorithms in $E(\mathbb{F}_q)[n]$. Hence, one has reduced the discrete logarithm problem to a potentially easier problem. The reduction of the DLP from $E(\mathbb{F}_q)$ to a subgroup of $\mathbb{F}_{q^k}^*$ is called the **MOV/FR attack**.

Menezes, Okamoto and Vanstone [417] suggested to use the Weil pairing for the above idea. In this case, the point R can, in principle, be defined over a large extension of $\mathbb{F}_q$. Frey and Rück explained that the Tate-Lichtenbaum pairing is a more natural choice, since it is sufficient to take a suitable point $R \in E(\mathbb{F}_{q^k})$ where $k = k(q, n)$ is the embedding degree. Balasubramanian and Koblitz [26] showed that, in most cases, it is also sufficient to work in $E(\mathbb{F}_{q^k})$ when using the Weil pairing.

Theorem 26.4.1. *Let E be an elliptic curve over $\mathbb{F}_q$ and let r be a prime dividing $\#E(\mathbb{F}_q)$. Suppose that $r \nmid (q-1)$ and that $\gcd(r, q) = 1$. Then $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if r divides $(q^k - 1)$.*

Proof: See [26]. □

Balasubramanian and Koblitz also show that a "random" curve is expected to have very large embedding degree. Hence, the MOV/FR attack is not a serious threat to the ECDLP on randomly chosen elliptic curves. However, as noted by Menezes, Okamoto and Vanstone, supersingular elliptic curves are always potentially vulnerable to the attack.

Theorem 26.4.2. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$ and suppose $r \mid \#E(\mathbb{F}_q)$. Then the embedding degree $k(q, r)$ is such that $k(q, r) \leq 6$.*

Proof: See Corollary 9.11.9. □

26.4.1 Anomalous Curves

The discrete logarithm problem on elliptic curves over $\mathbb{F}_p$ with p points (such curves are called **anomalous elliptic curves**) can be efficiently solved. This was first noticed by Semaev [537] and generalised to higher genus curves by Rück [506]. We present their method in this section. An alternative way to view the attack (using p-adic lifting rather than differentials) was given by Satoh and Araki [512] and Smart [570].

The theoretical tool is an observation of Serre [541].

Lemma 26.4.3. *Let $P \in E(\mathbb{F}_p)$ have order p. Let f_P be a function in $\mathbb{F}_p(E)$ with $\mathrm{div}(f_P) = p(P) - p(\mathcal{O}_E)$. Then the map*

$$P \mapsto \frac{df_P}{f_P}$$

is a well-defined group homomorphism from $E(\mathbb{F}_p)[p]$ to $\Omega_{\mathbb{F}_p}(E)$.

Proof: First note that f_P is defined up to a constant, and that $d(cf_P)/(cf_P) = df_P/f_P$. Hence, the map is well-defined.

Now let $Q = [a]P$ and let f_P be as in the statement of the lemma. Then there is a function g such that

$$\operatorname{div}(g) = (Q) - a(P) + (a-1)(\mathcal{O}_E).$$

One has

$$\begin{aligned}\operatorname{div}(g^p f_P^a) &= p\operatorname{div}(g) + a\operatorname{div}(f_P)\\ &= p(Q) - ap(P) + p(a-1)(\mathcal{O}_E) + ap(P) - ap(\mathcal{O}_E)\\ &= p(Q) - p(\mathcal{O}_E).\end{aligned}$$

Hence, one can let $f_Q = g^p f_P^a$. Now, using part 4 of Lemma 8.5.17,

$$\frac{df_Q}{f_Q} = \frac{d(g^p f_P^a)}{g^p f_P^a} = \frac{g^p df_P^a + f_P^a dg^p}{g^p f_P^a}.$$

Part 6 of Lemma 8.5.17 gives $dg^p = pg^{p-1}dg = 0$ (since we are working in $\mathbb{F}_p$) and $df_P^a = af_P^{a-1}df_P$. Hence,

$$\frac{df_Q}{f_Q} = a\,\frac{df_P}{f_P},$$

which proves the result. □

Exercise 26.4.4. Generalise Lemma 26.4.3 to arbitrary curves.

Lemma 26.4.3 therefore maps the DLP in $E(\mathbb{F}_p)[p]$ to a DLP in $\Omega_{\mathbb{F}_p}(E)$. It remains to solve the DLP there.

Lemma 26.4.5. *Let the notation be as in Lemma 26.4.3. Let t be a uniformizer at $\mathcal{O}_E$. Write $f_P = t^{-p} + f_1 t^{-(p-1)} + f_2 t^{-(p-2)} + \cdots$. Then*

$$\frac{df_P}{f_P} = (f_1 + \cdots)dt.$$

Proof: Clearly, $f_P^{-1} = t^p - f_1 t^{p+1} + \cdots$. From part 8 of Lemma 8.5.17 we have

$$df_P = \left(\frac{\partial f_P}{\partial t}\right) dt = (-pt^{-p-1} - (p-1)f_1 t^{-p} + \cdots)dt.$$

Since we are working in $\mathbb{F}_p$, we have $df_P = (f_1 t^{-p} + \cdots)dt$. The result follows. □

Putting together Lemma 26.4.3 and Lemma 26.4.5: if $Q = [a]P$ then $df_P/f_P = (f_1 + \cdots)dt$ and $df_Q/f_Q = (af_1 + \cdots)dt$. Hence, as long as one can compute the expansion of df_P/f_P with respect to t, then one can solve the DLP. Indeed, this is easy: use Miller's algorithm with power series expansions to compute the power series expansion of f_P and follow the above calculations. Rück [506] gives an elegant formulation (for general curves) that computes only the desired coefficient f_1; he calls it the "additive version of the Tate-Lichtenbaum pairing".

26.5 Computational Problems

26.5.1 Pairing Inversion

We briefly discuss a computational problem that is required to be hard for many cryptographic applications of pairings.

Definition 26.5.1. Let G_1, G_2, G_T be groups of prime order r and let $e : G_1 \times G_2 \to G_T$ be a non-degenerate bilinear pairing. The **pairing inversion problem** is: Given $Q \in G_2, z \in G_T$ to compute $P \in G_1$ such that $e(P, Q) = z$.

The bilinear Diffie-Hellman problem was introduced in Definition 23.3.9. In additive notation it is: Given $P, Q, [a]Q, [b]Q$ to compute $e(P, Q)^{ab}$.

Lemma 26.5.2. *If one has an oracle for pairing inversion then one can solve BDH.*

Proof: Given the BDH instance $P, Q, [a]Q, [b]Q$ compute $z_1 = e(P, [a]Q)$ and call the pairing inversion oracle on (Q, z_1) to get P' such that $e(P', Q) = z_1$. It follows that $P' = [a]P$. One then computes $e(P', [b]Q) = e(P, Q)^{ab}$ as required. □

Further discussion of pairing inversion is given by Galbraith, Hess and Vercauteren [222].

Exercise 26.5.3. Show that if one can solve pairing inversion then one can solve the Diffie-Hellman problem in G_1.

Exercise 26.5.4. Show that if one has an oracle for pairing inversion then one can perform passive selective forgery of signatures in the Boneh-Boyen scheme presented in Figure 23.3.9.

Exercise 26.5.5. Show that if one has an oracle for pairing inversion then one can solve the q-SDH problem of Definition 22.2.17.

26.5.2 Solving DDH using Pairings

Pairings can be used to solve the decision Diffie-Hellman (DDH) problem in some cases. First, we consider a variant of DDH that can sometimes be solved using pairings.

Definition 26.5.6. Let $E(\mathbb{F}_q)$ be an elliptic curve and let $P, Q \in E(\mathbb{F}_q)$ have prime order r. The **co-DDH problem** is: Given $(P, [a]P, Q, [b]Q)$ to determine whether or not $a \equiv b \pmod{r}$.

Exercise 26.5.7. Show that co-DDH is equivalent to DDH if $Q \in \langle P \rangle$.

Suppose now that $E[r] \subseteq E(\mathbb{F}_q)$, $P \neq \mathcal{O}_E$, and that $Q \notin \langle P \rangle$. Then $\{P, Q\}$ generates $E[r]$ as a group. By non-degeneracy of the Weil pairing, we have $e_r(P, Q) \neq 1$. It follows that

$$e_r([a]P, Q) = e_r(P, Q)^a \quad \text{and} \quad e_r(P, [b]Q) = e_r(P, Q)^b.$$

Hence, the co-DDH problem can be efficiently solved using the Weil pairing.

The above approach cannot be used to solve DDH, since $e_r(P, P) = 1$ by the alternating property of the Weil pairing. In some special cases, the reduced Tate-Lichtenbaum pairing satisfies $\hat{t}_r(P, P) \neq 1$ and so can be used to solve DDH in $\langle P \rangle$. In general, however, DDH cannot be solved by such simple methods.

When E is a supersingular elliptic curve and $P \neq \mathcal{O}_E$ then, even if $\hat{t}_r(P, P) = 1$, there always exists an endomorphism $\psi : E \to E$ such that $\hat{t}_r(P, \psi(P)) \neq 1$. Such an endomorphism is called a **distortion map**; see Section 26.6.1. It follows that DDH is easy on supersingular elliptic curves.

26.6 Pairing-Friendly Elliptic Curves

The cryptographic protocols given in Sections 22.2.3 and 23.3.2 relied on "pairing groups". We now mention the properties needed to have a practical system, and give some popular examples.

For pairing-based cryptography it is desired to have elliptic curves E over $\mathbb{F}_q$ such that:

1. there is a large prime r dividing $\#E(\mathbb{F}_q)$, with $\gcd(r, q) = 1$;
2. the DLP in $E(\mathbb{F}_q)[r]$ is hard;
3. the DLP in $\mathbb{F}_{q^k}^*$ is hard, where $k = k(q, r)$ is the embedding degree;
4. computation in $E(\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^*$ is efficient;
5. elements of $E(\mathbb{F}_q)$ and $\mathbb{F}_{q^k}^*$ can be represented compactly.

Elliptic curves with these properties are called **pairing-friendly curves**. Note that the conditions are incompatible: for the DLP in $\mathbb{F}_{q^k}^*$ to be hard it is necessary that q^k be large (say, at least 3000 bits) to resist index calculus attacks like those in Chapter 15, whereas to represent elements of $\mathbb{F}_{q^k}^*$ compactly we would like q^k to be small. Luckily, we can use techniques such as those in Chapter 6 to represent field elements relatively compactly.

There is a large literature on pairing-friendly elliptic curves, culminating in the "taxonomy" by Freeman, Scott and Teske [210]. We give two examples below.

Example 26.6.1. For $a = 0, 1$ define

$$E_a : y^2 + y = x^3 + x + a$$

over $\mathbb{F}_2$. Then E_a is supersingular and $\#E_a(\mathbb{F}_{2^l}) = 2^l \pm 2^{(l+1)/2} + 1$ when l is odd. Some of these integers have large prime divisors, for example $2^{241} - 2^{121} + 1$ is prime. The embedding degree can be shown to be 4 in general; this follows since

$$(2^l + 2^{(l+1)/2} + 1)(2^l - 2^{(l+1)/2} + 1) = 2^{2l} + 1 \mid (2^{4l} - 1).$$

Example 26.6.2. (Barreto-Naehrig curves [30]) Consider the polynomials

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1 \qquad \text{and} \qquad t(x) = 6x^2 + 1 \tag{26.9}$$

in $\mathbb{Z}[x]$. Note that $t(x)^2 - 4p(x) = -3(6x^2 + 4x + 1)^2$, that $r(x) = p(x) + 1 - t(x)$ is irreducible over $\mathbb{Q}$, and that $r(x) \mid (p(x)^{12} - 1)$. Suppose $x_0 \in \mathbb{Z}$ is such that $p = p(x_0)$ is prime and $r = r(x_0)$ is prime (or is the product of a small integer with a large prime). Then the embedding degree $k(p, r)$ is a divisor of 12 (and is typically equal to 12). Furthermore, one can easily construct an elliptic curve $E/\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = r$; one of the 6 twists of $y^2 = x^3 + 1$ will suffice. Note that $p \equiv 1 \pmod 3$ and E is an ordinary elliptic curve.

Example 26.6.3. The family of curve parameters in Example 26.6.2 has $t \approx \sqrt{p}$ and so the ate pairing is computed in about half the time of the reduced Tate-Lichtenbaum pairing, as usual. We now demonstrate an optimal pairing with these parameters.

Substituting the polynomials $r(x)$ and $p(x)$ for the values r and q in the matrix of equation (26.8) gives a lattice. Lattice reduction over $\mathbb{Z}[x]$ yields the short vector $(M_0, M_1, M_2, M_3) = (6x+2, 1, -1, 1)$. It is easy to verify that $6x+2+p(x)-p(x)^2+p(x)^3 \equiv 0 \pmod{r(x)}$.

Now $f_{1,Q} = 1$ and $f_{-1,Q} = v_Q$ (and so both can be omitted in pairing computation, by Exercise 26.3.12). The ate pairing can be computed as $f_{6x+2,Q}(P)$ multiplied with three straight line functions, and followed by the final exponentiation; see Section IV of [618]. The point is that Miller's algorithm now runs for approximately one quarter of the iterations as when computing the Tate-Lichtenbaum pairing.

26.6.1 Distortion Maps

As noted, when $\hat{t}_r(P,P) = 1$ one can try to find an endomorphism $\psi : E \to E$ such that $\hat{t}_r(P, \psi(P)) \neq 1$.

Definition 26.6.4. Let E be an elliptic curve over $\mathbb{F}_q$, let $r \mid \#E(\mathbb{F}_q)$ be prime, let $e : E[r] \times E[r] \to \mu_r$ be a non-degenerate and bilinear pairing, and let $P \in E(\mathbb{F}_q)[r]$. A **distortion map** with respect to E, r, e and P is an endomorphism ψ such that $e(P, \psi(P)) \neq 1$.

Verheul (Theorem 5 of [620]) shows that if E is a supersingular elliptic curve then, for any point $P \in E(\mathbb{F}_{q^k}) - \{\mathcal{O}_E\}$, a distortion map exists. In particular, when $P \in E(\mathbb{F}_q)[r] - \{\mathcal{O}_E\}$ and $k > 1$ then there is an endomorphism ψ (necessarily not defined over $\mathbb{F}_q$) such that $\hat{t}(P, \psi(P)) \neq 1$. Since P is defined over the small field, we have a compact representation for all elliptic curve points in the cryptosystem, as well as efficiency gains in Miller's algorithm. For this reason, pairings on supersingular curves are often the fastest choice for certain applications.

Example 26.6.5. Consider again the elliptic curves from Example 26.6.1. An automorphism on E_a is $\psi(x, y) = (x + s^2, y + sx + t)$ where $s \in \mathbb{F}_{2^2}$ and $t \in \mathbb{F}_{2^4}$ satisfy $s^2 = s + 1$ and $t^2 = t + s$. One can represent $\mathbb{F}_{2^{4m}}$ using the basis $\{1, s, t, st\}$. It is clear that if $P \in E_a(\mathbb{F}_{2^l})$ where l is odd then $\psi(P) \in E_a(\mathbb{F}_{2^{4l}})$ and $\psi(P) \notin E_a(\mathbb{F}_{2^{2l}})$, and so ψ is a distortion map for P.

Exercise 26.6.6. Let E be an elliptic curve over $\mathbb{F}_q$ and let $r \mid \#E(\mathbb{F}_q)$ be prime. Let $k = k(q, r) > 1$ be the embedding degree. For any point $P \in E(\mathbb{F}_{q^k})$ define the trace map

$$\mathrm{Tr}(P) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q)} \sigma(P).$$

Show that $\mathrm{Tr}(P) \in E(\mathbb{F}_q)$. Now, suppose $P \in E[r]$, $P \notin E(\mathbb{F}_q)$ and $\mathrm{Tr}(P) \neq \mathcal{O}_E$. Show that $\{P, \mathrm{Tr}(P)\}$ generates $E[r]$. Deduce that the trace map is a distortion map with respect to E, r, e_r and P.

Exercise 26.6.7. Let notation be as in Exercise 26.6.6. Show that if $Q \in E[r] \cap \ker(\pi_q - [1])$ then $\mathrm{Tr}(Q) = [k]Q$. Show that if $Q \in E[r] \cap \ker(\pi_q - [q])$ then $\mathrm{Tr}(Q) = \mathcal{O}_E$. Hence, deduce that the trace map is not a distortion map for the groups G_1 or G_2 of equation (26.3).

26.6.2 Using Twists to Improve Pairing-Based Cryptography

There are significant advantages from using twists in pairing-based cryptography when using ordinary elliptic curves. Suppose we are using the ate pairing or some other optimal pairing and are working with the subgroups $G_1, G_2 \subset E(\mathbb{F}_{q^k})$, which are Frobenius eigenspaces. Then $G_1 \subset E(\mathbb{F}_q)$ and it can be shown that $G_2 \subset E'(\mathbb{F}_q^{k/d})$ where E' is a twist of E and $d = \#\mathrm{Aut}(E)$. For the elliptic curve in Example 26.6.2 one can represent the p-eigenspace of Frobenius in $E(\mathbb{F}_{p^{12}})$ as a subgroup of $E'(\mathbb{F}_{p^2})$ for a suitable twist of E (this is because $\#\mathrm{Aut}(E) = 6$). For details we refer to [30, 284].

There are at least two advantages to this method. First, elements in the group G_2 of the pairing have a compressed representation. Second, the ate pairing computation is made much more efficient by working with Miller functions on the twisted curve E'. We do not present any further details.