Chapter 5.8
Bilinear pairings on elliptic curves

For any vectors v_1, v_2, w_1, w_2 and for any real numbers a_1, a_2, b_1, b_2,
Ex. Bilinear pairing: $\beta(a_1\vec{v_1} + a_2\vec{v_2}, w) = a_1\beta(\vec{v_1}) + a_2\beta(\vec{v_2}, w)$ (5.14)
The determinant map on $\mathbb{R}$ is also a bilinear pairing, and it also has the alternating property, which means that if we switch the vectors, the value changes sign.

The bilinear pairings in this chapter are similar in that they take as input two points on an elliptic curve and give as output a number. However the bilinearity condition is slightly different, because the output value is a nonzero element of a finite field, so the sum on the right hand side of the equation above is replaced by a product (5.14).

Bilinear pairings on elliptic curves have quite a few important cryptographic applications. In order to implement these, it is necessary to work with finite fields $\mathbb{F}_{p^k}$.

5.8.1
Points of finite order on elliptic curves

Definition: Let $m \geq 1$ be an integer. A point $P \in E$ satisfying $mP = \mathcal{O}$ is called a point of order m in the group E. We denote the set of points of order m by

$$E[m] = \{P \in E : [m]P = \mathcal{O}\}$$

Such points are called points of finite order or torsion points
Proposition 5.33: Let $m \geq 1$ be an integer.

(a) Let E be an elliptic curve over $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$. Then
$E(\mathbb{C})[m] \cong \mathbb{Z}/m\mathbb{Z}$ x $\mathbb{Z}/m\mathbb{Z}$
is a product of two cyclic groups of order m.
(b) Let E be an elliptic curve over $\mathbb{F}_p$ and assume that p does not divide m.
Then there exists a value of k such that
$E(\mathbb{F}_{p^{jk}})[m] \cong \mathbb{Z}/m\mathbb{Z}$ x $\mathbb{Z}/m\mathbb{Z}$ for all $j \geq 1$.

From this, we can write that $P = E[m]$ can be written as a linear combination

$$P = aP_1 + bP_2$$

for a unique choice of coefficients of $a, b \in \mathbb{Z}/m\mathbb{Z}$. If m is large it may be very difficult to find a and b. If P is a multiple of P_1, then finding the value of a is the same as solving the ECDLP for P and P_1.

5.8.2

Rational functions and divisors on elliptic curves

If E is an elliptic curve

$$E : Y_2 = X_3 + AX + B,$$

and if f(X,Y) is a rational function of two variables, then there are points of E where the numerator of f goes away and there are points of E where the denominator of f goes away, so f has zeros and poles on E. Further, one can assign multiplicities to the zeros and poles, so f has an associated divisor

$$div(f) = \sum_{P \in E} n_p[P]$$

In this summation, the coefficients n_p are integers, and only finitely many of the n_p are nonzero, so div(f) is a finite sum.

Generally, we define a divisor on E to be any formal sum

$$D = \sum_{P \in E} n_p[P] \text{ with } n_p \in \mathbb{Z} \text{ and } n_p = 0 \text{ for all but finitely many P.}$$

The degree of a divisor is the sum of its coefficients,

$$deg(D) = deg(\sum_{P \in E} n_p[P]) = \sum_{P \in E} n_p$$

The sum of a divisor is given by

$$Sum(D) = Sum(\sum_{P \in E} n_p[P]) = \sum_{P \in E} n_p P$$

$n_p P$ means to add P to itself n_p times using the addition law on E. Which divisors are divisors of functions, and to what extent the divisor of a function determines the function?

Theorem 5.36: Let E be an elliptic curve

(a) Let f and f' be rational functions on E. If $div(f) = div(f')$, then there is a nonzero constant c such that $f = cf'$.

(b) Let D = $\sum_{P \in E} n_p[P]$ be a divisor on E.

Then D is the divisor of a rational function on E if and only if

$$deg(D) = 0 \text{ and } Sum(D) = \mathcal{O}$$

i.e., if a rational function on E has no zeros or no poles, then it is a constant.

5.8.3

The Weil Pairing

The Weil Pairing, which is denoted by e_m, takes as input a pair of points $P, Q \in E[m]$ and gives as output an m^th root of unity $e_m(P, Q)$. The bilinearity of the Weil pairing is expressed by the equations

$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q),$$
$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2)$$

This is similar to the bilinearity described in (5.14), but note that the bilinearity in the equations above is multiplicative, in the sense that the quantities on the right-hand side are multiplied, while the bilinearity in (5.14) is additive, in the sense that the quantities on the right-hand side are added.

Definition : Let $P, Q \in E[m]$, i.e., P and Q are points of order m in the group E. Let f_P and f_Q be rational functions on E satisfying

$$div(f_P) = m[P] - m[\mathcal{O}] \text{ and } div(f_Q) = m[Q] - m[\mathcal{O}]$$

The Weil pairing of P and Q is the quantity

$$e_m(P, Q) = f_P(Q + S) \div f_P(S) / f_Q(P - S) \div f_Q(-S)$$

Where $S \in E$ is any point satisfying $S \notin \{\mathcal{O}, P, -Q, P - Q\}$
The weil pairing e_m has many useful properties.

Theorem 5.38
(a) The values of the Weil pairing satisfy

$e_m(P, Q)^m = 1$ for all $P, Q \in E[m]$, i.e., $e_m(P, Q)$ is an m^{th} root of unity.

(b) The Weil pairing is bilinear, which means that

$$e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q) \text{ for all } P_1, P_2, Q \in E[m].$$
and
$$e_m(P, Q_1 + Q_2) = e_m(P, Q_1)e_m(P, Q_2) \text{ for all } P, Q_1, Q_2 \in E[m].$$

(c) The Weil pair is alternating, which means that

$$e_m(P, P) = 1 \text{ for all } P \in E[m]$$

This implies that $e_m(P, Q) = e_m(Q, P)^{-1}$ for all $P, Q \in E[m]$
(d) The Weil pairing is nondegenerate, which means that

$$\text{if } e_m(P, Q) = 1 \text{ for all } Q \in E[m], \text{ then } P = \mathcal{O}$$

5.8.4
An efficient algorithm to compute the Weil pairing
Theorem 5.41: Let E be an elliptic curve and let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be nonzero points on E.
(a) Let λ be the slope of the line connecting P and Q, or the slope of the tangent line to E at P if $P = Q$. Define a function $g_{P,Q}$ as follows:

$$g_{P,Q} = \begin{cases} \frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2}, & \text{if } \lambda \neq \infty \\ x - x_P, & \text{if } \lambda = \infty \end{cases}$$
$$\text{Then } div(g_P, Q) = [P] + [Q] - [P + Q] - [\mathcal{O}]$$

(b) (Miller's Algorithm) Let $m \geq 1$ and write the binary expansion of m as

$$m = m_0 + m_1 * 2 + M_2 * 2^2 + ... + m_n - 1 * 2^{n-1}$$
with $m_i \in 0, 1$ and $m_{n-1} \neq 0$.

The following algorithm returns a function f_P whose divisor satifies

$$div(f_P) = m[P] - [mP] - (m-1)[\mathcal{O}]$$

where the functions $g_{T,T}$ and $g_{T,P}$ used by the algorithm are defined in (a)
(1) Set $T = P$ and $f = 1$
(2) Loop $i = n - 2$ down to 0
    (3) Set $f = f^2 * g_{T,T}$
    (4) Set $T = 2T$
    (5) If $m_i = 1$
        (6) Set $f = f * g_{T,P}$
        (7) set $T = T + P$
    (8) End If
(9) End i Loop
(10) Return the value f
In particular, if $P \in E[m]$, then $div(f_P) = m[P] - m[\mathcal{O}$
5.85
The Tate pairing
The Weil pairing is a nondegenerate bilinear form on elliptic curves defined over any field. For elliptic curves over finite fields there is another pairing, called the Tate pairing, that is often used in cryptography because it is somewhat more efficient computationally than the Weil pairing.

Definition: Let E be an elliptic curve over $\mathbb{F}_q$, let l be a prime, let $P \in E(\mathbb{F}_q)[l]$, and let $Q \in E(\mathbb{F}_q)$. Choose a rational function f_P on E with

$$div(f_P) = l[P] - l[(O)]$$

The Tate pairing of P and Q is the quantity

$$\tau(P, Q) = \frac{f_P(Q+S)}{f_P(S)} \in \mathbb{F}_q^*,$$

where S is any point in $E(\mathbb{F}_q)$ such that $f_P(Q + S)$ and $f_P(S)$ are defined and nonzero. It turns out that the value of the Tate pairing is well-defined only up to multiplying it by the $l^t h$ power of an element of $\mathbb{F}_q^*$. If $q \equiv 1 \pmod{l}$, we define the (modified) Tate pairing of P and Q to be

$$\hat{\tau}(P, Q) = \tau(P, Q)^{(q-1)/l} = (\frac{f_P(Q+S)}{f_P(S)})^{(q-1)/l} \in \mathbb{F}_q^*$$

Theorem 5.44: Let E be an elliptic curve over $\mathbb{F}_q$ and let l be a prime with

$$q \equiv 1 \pmod{l} \text{ and } E(\mathbb{F}_q)[l] \cong \mathbb{Z}/l\mathbb{Z}$$

Then the modified Tate pairing gives a well-defined map

$$\hat{\tau} : E(\mathbb{F}_q)[l] \text{ x } E(\mathbb{F}_q)[l] \longrightarrow \mathbb{F}_q$$

having the following properties: (a) Bilinearity

(b) Nondegeneracy

5.9

The Weil pairing over fields of prime power order

- m-embedding degree
- MOV algorithm
- Distortion maps on E

Defintion: Let E be an elliptic curve over $\mathbb{F}_p$ and let $m \geq 1$ be an integer with $p \nmid m$. The embedding degree of an elliptic curve E with respect to m is the smallest value of k such that

$$E((F_{p^k})[m] \cong (Z)/m(Z) \text{ x } (Z)/m(Z)$$

In cryptographic applications, when m is a (large) prime, there are alternative characterizations of the embedding degree.

Proposition 5.45. Let E be an elliptic curve over Fp and let $l \neq p$ be a prime. Assume that $E(\mathbb{F}_p)$ contains a point of order l. Then the embedding degree of E with respect to l is given by one of the following cases:

(i) The embedding degree of E is 1. (This cannot happen if $l > \sqrt{p} + 1$)

(ii) $p \equiv 1 \pmod{l}$ and the embedding degree is l.

(iii) $p \not\equiv 1 \pmod{l}$ and the embedding degree is the smallest value of $k \geq 2$ such that

$$p^k \equiv 1 \pmod{l}.$$

The reason why the embedding degree k is important is because the Weil pairing embeds the ECDLP on the elliptic curve $E(\mathbb{F}_p)$ into the DLP in the field F_{p^k}

The MOV algorithm - Solves the ECDLP for points P and Q, where $Q \in E(\mathbb{F}_p)$ and is a multiple of P.

(1) Compute the number of points $N = \#E(\mathbb{F}_{p^k})$

(2) Choose a random point $T \in E(\mathbb{F}_{p^k})$ with $T \notin E(\mathbb{F}_p)$

(3) Let $T' = (N/l)T$. If $T' = \mathcal{O}$, go back to step 2. Otherwise T' is a point of order l, so go to step 4.

(4) Compute the Weil pairing values

$$\alpha = e_l(P, T') \in \mathbb{F}^*_{p^k} \text{ and } \beta = e_l(Q, T') \in \mathbb{F}^*_{p^k}$$

(5) Solve the DLP for α and β in $\mathbb{F}_{p^{k*}}$, i.e., find an exponent n such that $\beta = \alpha^n$

(6) Then also $Q = nP$, so the ECDLP has been solved

An elliptic curve E over a finite field $\mathbb{F}_{\text{ı}}$ is called anomalous if $\#E(\mathbb{F}_{\text{ı}}) = p$. A number of people observed that there is a very fast (linear time) algorithm to solve the ECDLP on anomalous elliptic curves, so such curves must be avoided in cryptographic applications.

5.9.2

Distortion Maps and a modified Weil Pairing

The Weil pairing is alertnating, which means that $e_m(P,P) = 1$ for all P. In order to use the Weil pairing in cryptographic applications, we want to find away around this since using them alone is not very helpful.

Definition: Let $l \geq 3$ be a prime, let E be an elliptic curve, let $P \in E[l]$ be a point of order l, and let $\phi : E \longrightarrow E$ be a map from E to itself. We say that ϕ is an l-distortion map for P if it has the following two properties:

(i) $\phi(nP) = n\phi(P)$ for all $n \geq 1$.

(ii) The number $e_l(P, \phi(P))$ is a primitive l^{th} root of unity. This means that

$$e_l(P,\phi(P))^r = 1 \text{ if and only if r is a multiple of } l.$$

Definition: Let E be an elliptic curve, let $P \in E[l]$, let ϕ be an l-distotion map for P and let $\hat{e}_l$ be the modified Weil pairing relative to ϕ. Let Q and Q' be multiples of P. Then

$$\hat{e}_l(Q,Q') = 1 \text{ iff } Q = \mathcal{O} \text{ or } Q' = \mathcal{O}$$

Elliptic curve with a distortion map

Ex. We take $E : y^2 = x^3 + x$ and the prime p = 547. Then

$$\#E(\mathbb{F}_{547}) = 548 = 2^2 * 137$$

By trial and error we find the point $P_0 = (2, 253) \in E(\mathbb{F}_{547})$, and then

$$\text{P} = (67,\ 481) = 4P_0 = 4(2,253) \in E(\mathbb{F}_{547})$$

is a point of order 137.

In order to find more points of order 137, we go to the larger field

$$\mathbb{F}_{547^2} = a + bi : a, b \in \mathbb{F}_{547}^2, \text{ where } i^2 = -1$$

The distortion map gives

$$\phi(P) = (-67, 481i) \in E(\mathbb{F}_{547^2})$$

In order to compute the Weil pairing of P and $\phi(P)$, we randomly choose a point

$S = (256 + 110i, 441 + 15i) \in E(\mathbb{F}_{547}^2)$

and use Miller's algorithm to compute : 510 + 96i, 451 + 37i

Then

$$\hat{e_{137}}(P,P) = e_{137}(P,\phi(P)) = \tfrac{510+96i}{451+37i} = 37 + 452i \in \mathbb{F}_{547^2}$$

Ex continued. Now we use the MOV algorithm to solve the ECDLP for the point $Q = (167, 405) \in E(\not\trianglelefteq\not\trianglerighteq\not\trianglerighteq)$

The distortion map gives $\phi(Q) = (380, 405i)$, and we use the randomly chosen point $S = (402 + 397i, 271 + 205i) \in E(\mathbb{F}_{547}^2)$ to compute

$$\hat{e}_{547}(P,Q) = e_{547}(P,\phi(Q)) = 530 + 455i \in \mathbb{F}_{547}^2$$

From previously we have $\hat{e}_{137}(P,P) = 37 + 453i$, so we need to solve the DLP

$$(37 + 452i)^n = 530 + 455i \in \mathbb{F}_{547^2}$$

The solution to this DLP is $n = 83$, and the MOV algorithm tells us that $n = 83$ is also a solution to the ECDLP. We can check by verifying $Q = 83P$

5.10 Applications of the Weil Pairing

Tripartite Diffie-Hellman key exchange

Using weil pairing, we can perfrom a Diffie-Hellman Key exchange using three people now!

This is done as follows:

We have three people: Alice, Bob, and Carl

Private Computatioins:

Alice chooses a secret n_A and computes $Q_A = n_A P$, Bob chooses a secret n_B and computes $Q_B = n_B P$, and Carl chooses a secret n_C and computes $Q_C = n_B P$

Publication of Values:

Alice, Bob, and Carl publish their points $Q_A, Q_B.Q_C$

Further Private Computations

Alice computes $\hat{e}_l(Q_B, Q_C)^{n_A}$

Bob computes $\hat{e}_l(Q_A, Q_C)^{n_B}$

Carl computes $\hat{e}_l(Q_A, Q_B)^{n_C}$

Their shared secret value is $\hat{e}_l(P,P)^{n_A n_B n_C}$

ID-based public key cryptosystems

ID-based cryptography's goal is as follows: One would like a public key cryptosystem in which the user's public key address can be chosen by the user.

Let's say that there is a trusted authority Tom who is able to perform computations and distribute information. Tom publishes a master public key Tom^{pub} and keeps secret an associated private key Tom^{pri}. When Bob wants to send Alice a message, he uses the master public key $Tom^{p}ub$ and Alice's ID-based public key $Alice^{pub}$ (which could simply be her email address) in some sort of cryptographic algorithm to encrypt his message. In the meantime, Alice tells Tom that she wants to use $Alice^{pub}$ as her ID-based public key. Tom uses the master private key Tom^{pri} and Alice's ID-based public key $Alice^{pub}$ to create a private key $Alice^{pri}$ for Alice. Alice then uses $Alice^{pri}$i to decrypt and read Bob's message.

The trusted authority Tom needs to keep track of which public keys he has assigned, since otherwise Eve could send Alice's public key to Tom and ask him to create and send her the associated private key, which would be the same as Alice's private key.

Another problem that could occur:

Eve is allowed to send Tom a large number of public keys of her choice (other than ones that have already been assigned to other people) and ask Tom to create the associated private keys. It is essential that knowledge of these additional private keys not allow Eve to recover Tom's master private key Tom^{pri}, since otherwise Eve would be able to reconstitute everyone's private keys. In addition, Eve's possession of a large number of public private key pairs should not allow her to create any additional public–private key pairs.

Identity-based encryption using pairings on elliptic curves

Public Parameter Creation

A trusted authority Tom publishes a finite field $\mathbb{F}_q$, an elliptic curve $E/\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ of prime order l, and an l-distortion map ϕ for P. Tom also chooses hash functions

$H_1 : \{IDs\} \longrightarrow E(\mathbb{F}_q)$ and $H_2 : \mathbb{F}_q \longrightarrow \{0,1\}^B$

Master Key Creation

Tom chooses a secret integer s modulo m

Tom publishes the point $P^{Tom} = sP \in E(\mathbb{F}_q)$

Private Key Extraction

Alice chooses an ID-based public key $Alice^{pub}$

Tom chooses the point $P^{Alice} = H_1(Alice^{Pub}) \in E(\mathbb{F}_q)$

Tom sends the point $Q^{Alice} = sP^{Alice} \in E(\mathbb{F}_q)$ to Alice

Encryption

Bob chooses a plaintext M and a random number r modulo $q - 1$

Bob computes the point $P^{Alice} = H_1(Alice^{Pub}) \in E(\mathbb{F}_q)$

Bob's ciphertext is the pair

$C = (rP, M \text{ xor } H_2(\hat{e}_l(P^{Alice}, P^{Tom})^r)$

Decryption

Alice decrypts the ciphertext (C_1, C_2) by computing

C_2 xor $\hat{e}_l(Q^{Alice}, C_1)$