Elliptic Curve VI

1) The Weil pairing:

$E/\mathbb{F}_q$, l (a prime)

$e_{W,l} : E[l] \times E[l] \to \mu_l \subset \overline{\mathbb{F}_q}$

↑ The l-th roots of unity

$$(P,Q) \longmapsto (-1)^l \frac{f_{l,P}(Q)}{f_{l,Q}(P)}$$

Recall that $f_{l,P}$ is the unique function with divisor $\operatorname{div}(f_{l,P}) = l(P) - l(O_E)$ which is normalized at O_E.

More generally, if P is any point, $f_{l,P}$ as $\operatorname{div} f_{l,P} = l(P) - (lP) - (l-1)(O_E)$

Miller's algorithm use a double and add algorithm to compute $f_{l,P}$: $f_{2m,P} = f_{m,P}^2 \, \mu_{mP,mP}$ (double)

$f_{m+1,P} = f_{m,P} \, \mu_{mP,P}$ (add)

And $\operatorname{div}(\mu_{P,Q}) = (P) + (Q) - (P+Q) - (O_E)$

In practice: evaluate at each step

Warning: To evaluate $f_{l,P}(Q)$, Miller's algorithm computes intermediate evaluations $f_{m,P}(Q)$. More precisely, if $l = b_0 \dots b_k$ in base 2 it computes for $m = b_0$, $m = b_0 b_1$, $m = b_0 b_1 b_2$, ...

But $f_{m,P}$ has divisor $m(P) - ((m-1)P) - (m-1)(O_E)$ so is not well defined on Q if $Q = (m-1)(P)$

2) Properties

Pairing = bilinear non degenerate

- Bilinear on the right: $e(P, Q_1+Q_2) = e(P,Q_1) \times e(P,Q_2)$
  on the left: $e(P_1+P_2, Q) = e(P_1,Q)\, e(P_2,Q)$

- Non degeneracy on the right: if $e(P,Q)=1$ for all $P \Rightarrow Q = O_E$
  i.e. $e(-,Q)$ is constant $\Leftrightarrow Q = O_E$
  on the left: $e(P,-) = 1 \Leftrightarrow P = O_E$

* Additional property:
Antisymetry: $e_w(P,Q) = e_w(Q,P)^{-1}$ (immediate from the definition)

Corollary: $e_w(P,P) = 1$ (if l is odd)
$e_w(\lambda P, \mu P) = 1$ (by bilinearity)

Corollary: Assume $l \neq 2$ prime.
Since $e_{w,l}$ is non degenerate, then $e_{w,l}(P,Q) \neq 1 \Leftrightarrow Q$ not a multiple of P
$\Leftrightarrow P, Q$ is a basis of $E[l]$.

Application: if during Miller's algo we encounter one of the extra pbs, then this means that $Q = mP$ for some $m = b_0 \dots b_\ell$ in binary.
$\Rightarrow e_{w,l}(P,Q) = 1$.

3) Embedding degree:

$\mu_\ell \subset \overline{\mathbb{F}}_q$

definition: Embedding degree k (or d) is the minimal integer such that $\mu_\ell \subset \mathbb{F}_{q^k}$

Let $\mu_\ell = \langle \xi \rangle$, ξ a primitive ℓ-th root of unity.
We have $\xi \in \mathbb{F}_{q^k} \Leftrightarrow \Pi_{q^k}(\xi) = \xi$
$\Leftrightarrow \xi^{q^k} = \xi \Leftrightarrow \xi^{q^k-1} = 1 \Leftrightarrow \ell \mid q^k - 1$
$\Leftrightarrow q^k \equiv 1 [\ell]$ since ξ is of exact order ℓ.

Corollary: k is the order of q in $(\mathbb{Z}/\ell\mathbb{Z})^*$

Remark: * for a "random" E with $\#E(\mathbb{F}_q) = \ell$, expect k to be "random" ie of magnitude $\sim \ell$.
$\Rightarrow$ can't use pairings since μ_ℓ lives in an extension too big

*' If E is supersingular and $p > 3$, then $k = 2$.
$\Rightarrow$ can use the DLP on $\mathbb{F}_{q^k}$ ($\leftarrow$ subexponential) to solve the DLP on E.

*' In practice: for 128 bits of security, we want $q \sim 2^{256}$, and $q^k \sim 2^{3096}$
so we want $k \geq 12$.

4) Structure of $E[\ell]$:

What is the smallest e such that $E[\ell] \subset E(\mathbb{F}_{q^e})$.
Remark: $k \mid e$ since $e_{\pi,\ell}$ is non-degenerate on $E[\ell] \subset E(\mathbb{F}_{q^e})$
$\Leftrightarrow \Pi^\ell = 1$ on $E[\ell]$

* General case: Recall that $\chi_\Pi(X) = X^2 - tX + q$
Π on $E[\ell]$ has 2 ~~eyes~~ forms

a) $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ $t = \lambda_1 + \lambda_2$ $\quad \lambda_1, \lambda_2 \in \mathbb{F}_\ell$
$q = \lambda_1 \lambda_2$ $\quad$ or $\lambda_1, \lambda_2 \in \mathbb{F}_{\ell^2}$

So e is the order of λ_1 $\vee$ the order of λ_2 = the order of $\lambda \vee \ell$
(since $\lambda_1 \lambda_2 = q$ and q is of order k in $\mathbb{F}_\ell^*$)

b) $\Pi \begin{pmatrix} \lambda & 1 \\ & \lambda \end{pmatrix}$, $\lambda \in \mathbb{F}_\ell$, $\Pi^m = \begin{pmatrix} \lambda^m & m \\ & \lambda^m \end{pmatrix}$ so e = order of $\lambda \vee \ell$
here $\lambda^2 = q[\ell]$

* Cryptographic case:
$E(\mathbb{F}_q)/E(\mathbb{F}_q)$ has a point P of order ℓ.
Question: e / $E[\ell] \subset E(\mathbb{F}_{q^k})$

a) $\Pi = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$: $\Pi^k = 1 \iff q^k = 1$ so $e = k$

b) $\Pi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ Here $q \equiv 1 [\ell]$, so $k = 1$ but $e = \ell$.

In summary, in the crypto setting:
* if $k > 1$, $\Pi = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$ is diagonalizable and $e = k$

* If $k = 1$: either $\Pi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $E[\ell] \subset E(\mathbb{F}_q)$ or
$\Pi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $E[\ell] \subset E(\mathbb{F}_{q^2})$

5) Restricting to cyclic subgroups.

* Assume we are in the crypto settings and $k > 1$. G_1 and G_2 the subgroups of $E[\ell]$ of eigenvectors for the eigenvalues 1 and q respectively
$G_1 = \{ P \in E[\ell] \,/\, \Pi P = P \} = E[\ell](\mathbb{F}_q)$
$G_2 = \{ P \in E[\ell] \,/\, \Pi P = qP \} \subset E(\mathbb{F}_{q^k})$

Property: $e_{w,\ell}$ is non degenerate on $G_1 \times G_2$ and on $G_2 \times G_1$

II) The Tate Pairing:

1) Definition:

* Assume we are in the cryptographic case:
  $E(\mathbb{F}_q)$ has a point of l-torsion.

Definition $E[l](\mathbb{F}_{q^k}) \times E(\mathbb{F}_{q^k})/lE(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*l}$

$$e_{T,l} : (P,Q) \mapsto f_{l,P}(Q)$$

Bilinear and nondegenerate

- If $E(\mathbb{F}_{q^k})$ has no points of l^2-torsion, then $E(\mathbb{F}_{q^k})/lE(\mathbb{F}_{q^k}) \simeq E[l](\mathbb{F}_{q^k})$ via if $\#E(\mathbb{F}_{q^k}) = ml$, $P \to mP$
- Likewise, $\mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*l} \simeq \mu_l$ always via $x \mapsto x^{\frac{q^k-1}{l}}$

So we have the reduced Tate pairing:

$$E[l](\mathbb{F}_{q^k}) \times E[l](\mathbb{F}_{q^k}) \to \mu_l$$
$$(P,Q) \mapsto f_{l,P}(Q)^{\frac{q^k-1}{l}}$$

$\frac{q^k-1}{l}$ is called the final exponentiation

If $k > 1$: one can prove that it stays nondegenerate on $G_1 \times G_2$ and on $G_2 \times G_1$.

Special case: $k=1$, $E[l] \subset E(\mathbb{F}_{q^l}) \not\subset E(\mathbb{F}_q)$
The Tate pairing is nondegenerate on $E[l](\mathbb{F}_q) \times E[l](\mathbb{F}_q)$
while the Weil pairing is degenerate.
Soit $P \in E[l](\mathbb{F}_q)$, $Q \neq O_E$

$$e_{W,l}(P,P) = 1$$
but $e_{T,l}(P,P) \neq 1$

2) Computing the Tate pairing ($k>1$):

* The final exponentiation kills any $x \in \mathbb{F}_{q^k}^*$ that lives in a subfield

Proof: If $x^{\frac{q^k-1}{l}} \neq 1$, and $x \in \mathbb{F}_{q^k}^*$, with $k'|k$ we would have $\mu_l \subset \mathbb{F}_{q^{k'}}^*$ contradicting the definition of k.

* If k is even, and $P \in G_2$. Then $P=(x_P, y_P)$ with $x_P \in \mathbb{F}_{q^{k/2}}^*$ lives in a subfield.

Proof: $\pi_{q^{k/2}}(P) = q^{k/2} P$ since $\pi_q P = qP$ but $q^k \equiv 1 [l]$, so $q^{k/2} \equiv 1 [l]$
so $\pi_{q^{k/2}}(P) = -P = (x_P, -y_P)$ so $\pi_{q^{k/2}}(x_P) = x_P$

* Miller's algorithm involve functions $\mu_{\lambda_1 P, \lambda_2 P}$ of the form $\frac{l_{\lambda_1 P, \lambda_2 P}}{v_{(\lambda_1+\lambda_2)P}}$

Evaluating these functions need division by $x_Q - x_{(\lambda_1+\lambda_2)P}$ in general.
But in the special case of Tate on $G_2 \times G_1$, and k even, $x_Q \in \mathbb{F}_{q^{k/2}}$ so $x_Q \in \mathbb{F}_q$ so the denominators are in a subfield of $\mathbb{F}_{q^k}$ so they are killed by the final exponentiation!
→ We only need the numerators during the algorithm.
Same on $G_1 \times G_2$

3) Link between Weil and (reduced) Tate pairing:

$P \in E[l](\mathbb{F}_{q^k})$, $Q \in E(\mathbb{F}_{q^k}) / lE(\mathbb{F}_{q^k})$
$t_{T,l}(P,Q) \in \mu_l$ the reduced Tate pairing.

Let Q_0 be such that $lQ_0 = Q$. Then $\pi^2 Q_0 - Q_0 \in E[l]$
Proof: If $T = \pi^k Q_0 - Q_0$, $lT = \pi^k Q - Q = 0$
we have $t_{T,l}(P,Q) = e_{W,l}(P, \pi^k Q_0 - Q_0)$

III) Full general definition of the Weil and Tate pairing:

* Let f be a function of divisor $\operatorname{div}(f)$ and D be a divisor of degree 0 with its support disjoint from $\operatorname{div}(f)$.

If $D = \sum n_P (P)$, define: $\boxed{f(D) = \prod f(P)^{n_P}}$

Remark: Since $\deg D = 0$, $f(D)$ only depends on $\operatorname{div} f$.

If D_1 is principal and D_2 of deg 0. We may define $D_1(D_2)$ has $f_{D_1}(D_2)$ for any f_{D_1} with divisor D_1

Theorem (Weil's reciprocity): If D_1 and D_2 are principal of disjoint support, $D_1(D_2) = D_2(D_1)$

Remark: this can be extended to non disjoint support.

* General definition of the Weil and Tate pairing: $P, Q \in E[l]$

Let D_P, D_Q be any divisors linearly equivalent to $(P)-(O)$, $(Q)-(O)$ then

$$\boxed{e_{W,l}(P,Q) = \pm \frac{f_{l D_P}(D_Q)}{f_{l D_Q}(D_P)}}$$

$$\boxed{e_{T,l}(P,Q) = f_{l D_P}(D_Q)}$$

Example 1: Take $D_P = (P)-(O)$ $\quad D_Q = (Q)-(O)$

$$e_{W,l}(P,Q) = f_{l D_P}\frac{((Q)-(O))}{f_{l D_Q}((P)-(O))}$$

And if we take $f_{l D_P} = f_{l,P}$ the fonction normalized at O_E)

that simplifies to $\boxed{\frac{f_{\ell,P}(Q)}{f_{\ell,Q}(P)}}$.

Example 2: Take $D_P = (P) - (O)$
$D_Q = (Q+R) - (R)$
$\sim (Q) - (O)$

$$r_{T,\ell}(P,Q) = f_{\ell D_P}(D_Q) = f_{\ell,P}(D_Q)$$
$$= \frac{f_{\ell,P}(Q+R)}{f_{\ell,P}(R)}$$