Elliptic Curves 6

Damien Robert[1,2]

[1]Inria Bordeaux Sud Ouest [2]Univesité de Bordeaux

13 November 2020

The Weil pairing

- Let $E/\mathbb{F}_q$ be an elliptic curve, and $\ell \nmid p$;
- The Weil pairing is a non degenerate bilinear pairing

$$e_{W,\ell} : E[\ell] \times E[\ell] \to \mu_\ell$$

- $e_{W,\ell}(P,Q) = (-1)^\ell \frac{f_{\ell,P}((Q)-(0_E))}{f_{\ell,Q}((P)-(0_E))}$ where $div f_{\ell,P} = \ell(P) - \ell(0_E)$.
- $e_{W,\ell}(P,Q) = \frac{f_{\ell,P}(Q)}{f_{\ell,Q}(P)}$ if the functions $f_{\ell,P}$ and $f_{\ell,Q}$ are normalised at 0_E.

Properties

- Bilinearity on the right: $e_{W,\ell}(P, Q+R) = e_{W,\ell}(P,Q)e_{W,\ell}(P,R)$;
- Bilinearity on the left $e_{W,\ell}(P+Q, R) = e_{W,\ell}(P,R)e_{W,\ell}(Q,R)$;
- Non degeneracy on the right: if $e_{W,\ell}(P,Q) = 1$ for all $P \in E[\ell](\overline{\mathbb{F}}_q)$, $Q = 0_E$;
- Non degeneracy on the left if $e_{W,\ell}(P,Q) = 1$ for all $Q \in E[\ell](\overline{\mathbb{F}}_q)$, $P = 0_E$.
- Antisymmetry: $e_{W,\ell}(P,Q) = e_{W,\ell}(Q,P)^{-1}$. (Exercice!)
- Corollary: $e_{W,\ell}(P,P) = 1$ (in caracteristic $\neq 2$)

Computing the Weil pairing

- We recall that $f_{\ell,P}$ can be computed via a double and add algorithm;
- This uses the (normalised) $\mu_{P,Q}$ function, $div\, \mu_{P,Q} = (P) + (Q) - (P+Q) - (0_E)$.
- This computation introduces intermediate zeroes and poles.
- This is because Miller's algorithm evaluate intermediate functions $f_{\lambda,P}(Q)$;
- The zeroes and poles of these functions are multiple of P;
- So if there is a problem during the computation, $f_{\lambda,P}(Q)$ is not well defined, then $Q = mP$;
- We know then that $e_{W,\ell}(P,Q) = e_{W,\ell}(P,P)^m = 1$!

The embedding degree

- $e_{W,\ell}$ has value in μ_ℓ, the group of ℓ-roots of unity of $\overline{\mathbb{F}}_q$;
- What is the smallest extension $\mathbb{F}_{q^k}$ such that $\mu_\ell \subset \mathbb{F}_{q^k}$?
- Let ζ be a primitive ℓ-root of unity. Then $\zeta \in \mathbb{F}_{q^k}$ if and only if $\pi_{q^k}(\zeta) = \zeta$, ie $\zeta^{q^k} = \zeta$, ie $q^k = 1 \mod \ell$.
- The embedding degree k is thus the order of q in $\mathbb{Z}/\ell\mathbb{Z}$.
- If ℓ is prime, we have $k \mid \ell - 1$.
- Recall that $E(\mathbb{F}_q) = q + 1 - t$, t the trace of the Frobenius.
- If $E(\mathbb{F}_q)$ has a point of ℓ-torsion, $\ell \mid \#E(\mathbb{F}_q)$ so $q \equiv t - 1 \mod \ell$.
- The embedding degree is then also the order of $t - 1$ in $\mathbb{Z}/\ell\mathbb{Z}$.

The embedding degree

- If $E[\ell] \subset E(\mathbb{F}_q)$, the embedding degree k is 1.
- In particular, $\ell \mid q-1$.
- If $E(\mathbb{F}_q) = \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ with $a \mid b$, then $E[a] \subset E(\mathbb{F}_q)$ so $a \mid q-1$.

General definition of the Weil pairing

- Let D_P be any divisor linearly equivalent to $(P) - (0_E)$;
- Then ℓD_P is principal, let $f_{\ell D_P}$ be any function with this divisor;
- $e_{W,\ell}(P, Q) = \frac{f_{\ell D_P}(D_Q)}{f_{\ell D_Q}(D_P)}$;
- Exemple: $D_P = (P + R) - (R)$.

An alternative definition of the Weil pairing

- Let $D_P = (P) - (0_E)$, and $[\ell]^* D_P = \sum_{T' \mid \ell T' = P} (T') - \sum_{T \mid \ell T = 0_E} (T)$;
- If P_0 is such that $P = \ell P_0$, $[\ell]^* D_P = \sum_{T \mid \ell T = 0_E} \left((P_0 + T) - (T) \right)$;
- Exercice: if $P \in E[\ell]$, $[\ell]^* D_P$ is principal;
- Let $g_{\ell,P}$ be the corresponding normalised function;
- Then $e_{\ell,W}(P,Q) = \frac{g_{\ell,P}(x+Q)}{g_{\ell,P}(x)}$.
- The proof uses Weil's reciprocity theorem.
- Note: in general, $div f \circ [\ell] = [\ell]^* \, div f$;
- Application: $g_{\ell,P}^{\ell} = f_{\ell,P} \circ [\ell]$;
- Indeed both are normalised functions with divisor $[\ell]^* (\ell(P) - \ell(0_E))$.

Bilinearity

$$e_{W,\ell}(P, Q+R) = \frac{g_{\ell,P}(x+Q+R)}{g_{\ell,P}(x)} \tag{1}$$

$$= \frac{g_{\ell,P}(x+Q+R)}{g_{\ell,P}(x+R)} \frac{g_{\ell,P}(x+R)}{g_{\ell,P}(x)} \tag{2}$$

$$e_{W,\ell}(P, Q)e_{W,\ell}(P, R) \tag{3}$$

Corollary

$e_{W,\ell}(P, Q)^r = e_{W,\ell}(rP, Q) = e_{W,\ell}(0_E, P) = 1.$

Non degeneracy

- If $e_{W,\ell}(P,Q) = 1$ for all $Q \in E[\ell](\overline{\mathbb{F}}_q)$, then $g_{\ell,P}(x+Q) = g_{\ell,P}(x)$ for all $Q \in E[\ell](\overline{\mathbb{F}}_q)$.
- Then $g_{\ell,P} = h \circ [\ell]$.
- So $div\, g_{\ell,P} = [\ell]^* \, div\, h$ and $div\, h = (P) - (0_E)$.
- This implies $P = 0_E$.

Corollary

Fix ζ a primitive ℓ-root of unity. If $P \in E[\ell]$ is primitive (if ℓ is prime this means $P \neq 0$), there is a Q such that $e_{W,\ell}(P,Q) = \zeta$. We say that (P,Q) is a symplectic basis of $E[\ell]$.

Corollary

Every group morphism $E[\ell] \to \mu_\ell$ ("a character") is of the form $Q \mapsto e_{W,\ell}(P,Q)$.

Case ℓ not prime

- If $\ell = mn$, $P \in E[nm]$, $Q \in E[n]$, then $e_{W,mn}(P,Q) = e_{W,n} mP, Q$.
- Exemple: if $P, Q \in E[\ell]$, $e_{W,\ell^2}(P,Q) = 1$.
- Exemple: if $P, Q \in E[\ell]$, $P = \ell P_0$, $e_{W,\ell^2}(P_0,Q) = e_{W,\ell}(P,Q)$.

Applications

- Cryptography: discrete logarithm problem in the group $\langle P \rangle$, P a point of ℓ-torsion of an elliptic curve;
- ℓ is a large prime, around 2^{256} for 128 bits of security
- The Weil pairing allows to reduce the DLP from $E(\mathbb{F}_{q^k})$ to the DLP in $\mu_\ell \subset \mathbb{F}_{q^k}^*$
- We have subexponential algorithms for the DLP in $\mathbb{F}_{q^k}^*$.
- So if k is small: subexponential attack on E!
- Expected: $q \mod \ell$ is "random", so has order $\approx \ell$. Very large embedding degree.
- Exemple: a supersingular curve over $\mathbb{F}_p$ ($p > 3$) has $t = 0$.
- The embedding degree is $k = 2$.
- Reduction of the DLP to $\mathbb{F}_{p^2}$.

$\Rightarrow$ We need larger extensions to work securely with supersingular curves (at least $q > 2^{1024}$)!

Constructive applications

- Tripartite Diffie-Helman;
- Lot of cryptographic applications;
- Provide instance where Diffie-Helman is hard but decisional Diffie-Helman is easy;
- Problem: find curves suitable for crypto $\ell \mid \#E(\mathbb{F}_q)$ with suitable embedding degree.
- Ideally, $q \approx 2^{256}$ and $k \approx 12, 20$.

Field of definition of $E[\ell]$, ℓ prime

- Characteristic polynomial of the Frobenius: $\chi_\pi(X) = X^2 - tX + q$;
- This is the characteristic polynomial of π acting on $E[\ell]$;
- $E[\ell] \subset E(\mathbb{F}_{q^k})$ iff $\pi^k = \mathrm{Id}$;
- Three possibilities: $\pi = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, with $\lambda_1 \lambda_2 \equiv q \mod \ell$.
- The order of π is then the order of λ_1 (or λ_2) in $\mathbb{F}_q$.
- $\pi = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, with $\lambda^2 \equiv q \mod \ell$.
- The order of π is the order of λ.
- $\pi = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, with $\lambda^2 \equiv q \mod \ell$.
- $\pi^r = \begin{pmatrix} \lambda^r & r \\ 0 & \lambda^r \end{pmatrix}$;
- The order of π is then $ord(\lambda) \vee \ell$.

Field of definition of $E[\ell]$, ℓ prime

- In the crypto setting, there is one point of ℓ-torsion in $E[\ell](\mathbb{F}_q)$.
- Three possibilities: $\pi = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$.
- If k is the embedding degree, $E[\ell] \subset E(\mathbb{F}_{q^k})$
- $\pi = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- $E[\ell] \subset E(\mathbb{F}_q)$.
- $\pi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
- $E[\ell] \subset E(\mathbb{F}_{q^\ell})$.

Field of definition of $E[\ell]$, ℓ prime

- Assume that $\pi = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$, with $q \neq 1 \mod \ell$, ie $k \neq 1$.
- This is the usual cryptographic situation.
- Let $G_1 \subset E[\ell]$ correspond to the eigenvalue 1.
  $G_1 = \{P \in E[\ell], \pi(P) = P\}$.
- Let $G_2 \subset E[\ell]$ correspond to the eigenvalue q.
  $G_2 = \{P \in E[\ell], \pi(P) = qP\}$.
- $G_1 = E[\ell](\mathbb{F}_q)$, $G_2 \subset E[\ell](\mathbb{F}_{q^k})$, $E[\ell] = G_1 \oplus G_2$.

Corollary

The Weil pairing is non degenerate when restricted to $G_1 \times G_2$ or to $G_2 \times G_1$.

The Tate pairing

- Let $E/\mathbb{F}_q$ be an elliptic curve, and $\ell \nmid p$ such that $E(\mathbb{F}_q)$ contains a point of r-torsion;
- The Tate pairing is a non degenerate bilinear pairing $e_{T,\ell} : E[\ell](\mathbb{F}_{q^k}) \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}^*_{q^k}/\mathbb{F}^{*,\ell}_{q^k}$
- $e_{T,\ell}(P,Q) = f_{\ell,P}((Q) - (0_E))$ where $div f_{\ell,P} = \ell(P) - \ell(0_E)$.
- $e_{T,\ell}(P,Q) = f_{\ell,P}(Q)$ if the function $f_{\ell,P}$ is normalised at 0_E.

General definition of the Tate pairing

- Let D_P be any divisor linearly equivalent to $(P)-(0_E)$;
- Then ℓD_P is principal, let $f_{\ell D_P}$ be any function with this divisor;
- $e_{T,\ell}(P,Q) = f_{\ell D_P}(D_Q)$;
- Exemple: $e_{T,\ell}(P,Q) = \frac{f_{\ell,P}(Q+R)}{f_{\ell,P}(R)}$.
- This allows to circumvent the problem of intermediate poles and zeroes introduced by Miller's algorithm.
- Warning: unlike for the Weil pairing, we may have $e_{T,\ell}(P,P) \neq 1$.

Normalisation of the Tate pairing

- $\mathbb{F}_{q^k}^* / \mathbb{F}_{q^k}^{*,\ell} \simeq \mu_\ell$ via $x \mapsto x^{\frac{q^k-1}{\ell}}$.
- The (normalised or reduced) Tate pairing is a non degenerate bilinear pairing $e_{T,\ell} : E[\ell](\mathbb{F}_{q^k}) \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mu_\ell$,
- $e_{T,\ell}(P,Q) = f_{\ell,P}(Q)^{\frac{q^k-1}{\ell}}$
- This power to $\frac{q^k-1}{\ell}$ is called the final exponentiation;
- If ℓ is prime and $E(\mathbb{F}_{q^k})$ does not contain a point of ℓ^2-torsion, $E[\ell](\mathbb{F}_{q^k}) \simeq E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$ since the inclusion is injective and they have the same cardinal.
- The (normalised) Tate pairing is then a non degenerate bilinear pairing $e_{T,\ell} : E[\ell](\mathbb{F}_{q^k}) \times E[\ell](\mathbb{F}_{q^k}) \to \mu_\ell$.

Alternative definition of the reduced Tate pairing

- Let $P \in E[\ell](\mathbb{F}_{q^k})$, $Q \in E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k})$;
- Let Q_0 such that $Q = \ell Q_0$;
- Then $e_{T,\ell}(P,Q) = e_{W,\ell}(P, \pi^k Q_0 - Q_0)$;
- This does not depend on the choice of Q_0 (if $E[\ell] \subset E(\mathbb{F}_{q^k})$ this is because another choice $Q_1 = Q_0 + T$, $T \in E[\ell] \subset E(\mathbb{F}_{q^k})$ so $\pi^k T - T = 0$).
- If $Q \in \ell E(\mathbb{F}_{q^k})$, we may take $Q_0 \in E(\mathbb{F}_{q^k})$, so $\pi^k Q_0 = Q_0$, $e_{T,\ell}(P,Q) = 1$.
- This allows to prove bilinearity and non degeneracy.

Proof.

$e_{W,\ell}(P, \pi^k Q_0 - Q_0) = \frac{g_{\ell,P}(\pi^k Q_0)}{g_{\ell,P}(Q_0)} = g_{\ell,p}(Q_0)^{q^k-1} = g_{\ell,p}^{\ell}(Q_0)^{\frac{q^k-1}{\ell}} = f_{\ell,P}(Q)^{\frac{q^k-1}{\ell}} = eT,\ell(P,Q)$ using that $g_P^{\ell} = f_{\ell,P} \circ [\ell]$. □

Restricting the Tate pairing to subgroups (ℓ prime)

- The Tate pairing stays non degenerate when restricted to $G_2 \times E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) \to \mathbb{F}_{q^k}^* / \mathbb{F}_{q^k}^{*,\ell}$
- If $E(\mathbb{F}_q)$ does not contain a point of ℓ^2-torsion, $E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) \simeq G_1 = E[\ell](\mathbb{F}_q)$ so the Tate pairing is non degenerate on $G_2 \times G_1$.
- In particular, if the embedding degree $k = 1$ but $E[\ell] \not\subset E(\mathbb{F}_q)$, the Tate pairing is non degenerate on $E[\ell](\mathbb{F}_q) \times E[\ell](\mathbb{F}_q)$ (while the Weil pairing degenerates).
- In this situation, if $P \in E[\ell](\mathbb{F}_q)$, $e_{T,\ell}(P,P) \neq 1$.
- If $k > 1$, and $E(\mathbb{F}_{q^k})$ does not contain a point of ℓ^2-torsion, the Tate pairing is non degenerate on $G_1 \times G_2$.

Algorithmic computation of the Tate pairing (ℓ prime)

- If $P \in G_1$ and $Q \in G_2$, all the computations of $f_{\ell,P}$ are done over $\mathbb{F}_q$, its only the evaluation at the end which is done over $\mathbb{F}_{q^k}$;
- Since $\mathbb{F}_{q^k}$ is the smallest extension of $\mathbb{F}_q$ containing μ_ℓ, if $z \in \mathbb{F}_{q^d}$ is in a strict subfield ($d \mid k$, $d \neq k$), then it is killed by the final exponentiation: $z^{\frac{q^k-1}{\ell}} \in \mu_\ell \cap \mathbb{F}_{q^d} = \{1\}$.
- If $k = 2d$ is even, and $Q \in G_2$, then $x_Q \in \mathbb{F}_{q^d}$.
- Indeed $\pi(Q) = qQ$. But since $q^k \equiv 1 \mod \ell$, $q^d \equiv -1 \mod \ell$ (since k is the embedding degree).
- So $\pi^d(Q) = -Q$, $\pi^d(x_Q) = x_Q$, $x_Q \in \mathbb{F}_{q^d}$.
- Since the denominators durinr Miller's algorithm for the evaluation of $f_{\ell,P}$ only involve x_Q (and the coordinates of P which are in $\mathbb{F}_q$), the denominator is in $\mathbb{F}_{q^d}$.
- It is killed by the final exponentiation!