The Weil Pairing and its Efficient Calculation

Victor S. Miller

IDA, Center for Communications Research
Princeton, NJ 08540 USA

30 Oct, 2006

Why Study the Weil-Pairing?

- The Weil pairing does for Elliptic Curve groups what the inner product does for real vector spaces.
- It relates the algebra of adding points on an elliptic curve to multiplying non-zero elements in a field.
- It can also be used to construct identity-based cryptosystems.

Outline

Algebraic Groups

- K – a field
- V/K – an affine variety – solutions to a finite system of polynomials with coefficients in K.
- If L/K is a field, $V(L)$ is the set of solutions with coordinates in L.
- V/K is projective if the equations are all homogeneous (exclude 0 and identify points which are scalar multiples).
- V is a *group variety* – group law given by polynomials in coordinates.
- $\mathbb{G}_m : \{(x, y)|xy = 1\}$, and $(x_1, y_1) \cdot (x_2, y_2) := (x_1x_2, y_1y_2)$.

Elliptic Curves

- Simplest example of a projective group variety.
- Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  where $a_i \in K$ $(\mathrm{wt}(x) = 2, \mathrm{wt}(y) = 3, \mathrm{wt}(a_j) = j)$.
- $L_{P_1,P_2} = 0$: equation of line passing through P_i.
- $P_1 * P_2 =$ third point of intersection of L_{P_1,P_2} with E.
- $P + Q := (P * Q) * 0$, where 0 is the "point at ∞" on E. $P * 0$ is reflection in the line $y + a_1x + a_3 = 0$.

Points of finite order

- G is a group variety, and n a positive integer, then $G[n]$ is the subvariety of points order dividing n: add the equation $P^n = 1$ to the equations of G.
- $\mu_n := \mathbb{G}_m[n]$, the n-th roots of unity.
- $E[n]$ where E is an elliptic curve.
- The Weil-pairing connects the two.
- If Ω/K is algebraically closed, then $E[n](\Omega) \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as a group, if $\mathrm{char}(K) \nmid n$.

The Weil Pairing

- E/K an elliptic curve, n relatively prime to $p := \mathrm{char}(K)$.
- $e_n : E[n] \times E[n] \to \mu_n$
- Bilinear: $P, Q, R \in E[n]$

$$e_n(P+R, Q) = e_n(P, Q)e_n(R, Q)$$
$$e_n(P, Q+R) = e_n(P, Q)e_n(P, R)$$

- Skew-Symmetric: $e_n(P, P) = 1 \Rightarrow e_n(P, Q) = e_n(Q, P)^{-1}$
- Non-degenerate: $e_n(P, Q) = 1, \forall Q \in E[n](\Omega) \Rightarrow P = 0$.
- Compatible: $P \in E[mn], Q \in E[n] \Rightarrow e_{mn}(P, Q) = e_n(mP, Q)$.
- Galois Action: $\sigma \in \mathrm{Gal}(\Omega/K) \Rightarrow e_n(P, Q)^\sigma = e_n(P^\sigma, Q^\sigma)$.

Divisors on a Curve

- C/K a curve.
- Divisor on C is a formal finite sum of points: $\mathcal{D} = \sum_{P \in C} a_P[P]$, where $a_P \in \mathbb{Z}$.
- $\deg(\mathcal{D}) := \sum_P a_P$.
- If $f : C \to \mathbb{P}^1$ is a function, then

$$\operatorname{div}(f) := \sum_{P \in C} v_P(f)[P],$$

  where $v_P(f)$ is the order of the zero or pole of f at P.
- Define $\mathcal{D} \sim \mathcal{D}' \Leftrightarrow \mathcal{D} - \mathcal{D}' = \operatorname{div}(f)$ for some function f.
- Abel-Jacobi: E an elliptic curve, $\mathcal{D} = \operatorname{div}(f)$ for some f if and only if, $\deg(\mathcal{D}) = 0$, and $\sum_P a_P P = 0$.

Weil's Definition

- $\mathrm{supp}(\sum_P a_P[P]) := \{P | a_P \neq 0\}$.
- f a function and $\mathcal{D} = \sum_P a_P[P]$, set $f(\mathcal{D}) := \prod_P f(P)^{a_P}$ when $\mathrm{supp}(\mathcal{D}) \cap \mathrm{supp}(\mathrm{div}(f)) = \emptyset$.
- $0 \neq P \in E(K)$, $f_{n,P}$: $\mathrm{div}(f_{n,P}) = n[P] - [nP] - (n-1)[0]$. Exists by Abel-Jacobi. Constructed explicitly below.
- $\mathcal{D} = \sum_P a_P[P]$, then $f_{n,\mathcal{D}} := \prod_{P \neq 0} f_{n,P}^{a_P}$
- $\mathcal{D}, \mathcal{D}'$ such that $n\mathcal{D}, n\mathcal{D}' \sim 0$, and $\mathrm{supp}(\mathcal{D}) \cap \mathrm{supp}(\mathcal{D}') = \emptyset$ then $e_n(\mathcal{D}, \mathcal{D}') := f_{n,\mathcal{D}}(\mathcal{D}')/f_{n,\mathcal{D}'}(\mathcal{D})$.
- $\mathcal{D}_1 \sim \mathcal{D}, \mathcal{D}_1' \sim \mathcal{D}_1$ then $e_n(\mathcal{D}_1, \mathcal{D}_1') = e_n(\mathcal{D}, \mathcal{D}')$, so function of $\sim$ class only.
- $P, Q \in E[n]$, $e_n(P, Q) := e_n([P] - [0], [Q + R] - [R])$, $R \neq 0, -Q, P, P - Q$.

Explicit formula for $f_{n,P}(Q)$

- $L_{P,Q} = y + \lambda x + \nu$, if $x(P) \neq x(Q)$, $x - x(P)$, otherwise.
- where $\lambda = \frac{y(P)-y(Q)}{x(P)-x(Q)}$, and $\nu = \frac{y(Q)x(P)-y(P)x(Q)}{x(P)-x(Q)}$.
- $g_{P,Q} = \frac{L_{P,Q}}{L_{P+Q,-(P+Q)}}$.
- $\mathrm{div}(g_{P,Q}) = [P] + [Q] - [P+Q] - [0]$.
- $f_{1,P} := 1$.
- $f_{n+1,P} := f_{n,P} g_{P,nP}$
- $f_{-n,P} := \frac{1}{f_{n,P} g_{nP,-nP}}$.

Laurent Series

- Formal power series with a finite number of negative powers.

$$f(t) = \sum_{j=m}^{\infty} a_j t^j, a_m \neq 0.$$

- Example: $t^{-2} + 3t^{-1} + 2 - 4t + \ldots$.
- Leading Coefficient: $\mathrm{lc}(f) := a_m$, $\mathrm{lc}(fg) = \mathrm{lc}(f)\,\mathrm{lc}(g)$.
- $\deg_t(f) := m$, $\deg_t(fg) = \deg_t(f) + \deg_t(g)$.
- $f(x, y) = 0$ a curve, and $D_x f(P)$ or $D_y f(P) \neq 0$ there is a rational function u_P of x, y which is a *uniformizer* at P.
- That is $u_P(P) = 0$ and x and y can be written as Laurent series in u_P. $v_P(f) := \deg_{u_P}(f)$.

Recursive formulas for $f_{n,P}$

- $\mathrm{div}(f_{n,P}) = n[P] - [nP] - (n-1)[P]$, by easy induction.

$$\mathrm{div}(f_{m+n,P}) = \mathrm{div}(f_{m,P} f_{n,P} g_{mP,nP}) \tag{1}$$

$$\mathrm{div}(f_{mn,P}) = \mathrm{div}(f_{m,P}^{n} f_{n,mP}) = \mathrm{div}(f_{n,P}^{m} f_{m,nP}) \tag{2}$$

- But all functions have leading coefficient of 1 at 0.
- More specifically, let $u_0 = y/x$, uniformizer at 0.
- $\mathrm{lc}_{u_0}(f_{n,P}), \mathrm{lc}_{u_0}(g_{P,Q}) = 1$.
- So previous formulas yield equality of the functions!

Addition-Subtraction Chains

- Addition subtraction chain: $\mathcal{A} : 1 = a_0, a_1, \ldots, a_t$, $0 \leq r_i, l_i < i$ $\epsilon_i = \pm 1$.
- $a_i = a_{r_i} + \epsilon_i a_{l_i}$.
- The value $v(\mathcal{A}) = a_t$. The length $\ell(\mathcal{A}) = t$.
- If all $\epsilon_i = 1$, it is an addition chain.
- Example: $1, 2, 3, 6, 12, 24, 21$
- Given $n > 0$ there is an addition chain whose value is n and whose length is $\leq 1 + 2 \log_2 n$. Can usually do much better.

Algorithm to evaluate $f_{n,P}(Q)$

1. Fix an addition-subtraction chain $\mathcal{A} : r_i, l_i, \epsilon_i$ of length t, whose value is n.
2. Set $w_1 = 1$, $L_1 = P$, $i = 1$.
3. Set $i := i + 1$
4. If $i > t$ return w_t.
5. Set $L_t = L_{l_i} + \epsilon_i L_{r_i}$, $w_t = w_{l_i} w_{r_i} \operatorname{lc}_Q(g_{L_{l_i}, \epsilon_i L_{r_i}})$ (here we use (1)).
6. Return to step 3.

Mumford's Theta Groups

- Algorithm for calculating $f_{n,P}$ is connected with Mumford's Theta Groups (Frey-Müller-Rück).
- $\mathcal{D}$ a divisor on E/K of degree 0.
- $L \subseteq K$ an extension field, $G = L^* \times E(L)$.
- Group law: $(a_1, P_1) \cdot (a_2, P_2) := (a_1 a_2 g_{P_1,P_2}(\mathcal{D}), P_1 + P_2)$.
- $(a, P)^{-1} := (a^{-1} g_{P,-P}(\mathcal{D})^{-1}, -P)$, unit $(1, 0)$.
- Then $(1, P)^m = (f_{m,P}(\mathcal{D}), mP)$

A simple formula for $e_n(P, Q)$

- If $P, Q \in E[n]$ and $P \neq Q$ then

$$e_n(P, Q) = (-1)^n \frac{f_{n,P}(Q)}{f_{n,Q}(P)}. \tag{3}$$

- Let z be a transcendental, and a point T be defined by

$$\begin{aligned} x(T) &:= \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z + O(z^2) \\ y(T) &:= -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + O(z). \end{aligned}$$

- We have

$$e_n(P, Q) = \frac{f_{n,P}(Q)}{f_{n,Q}(P)} \frac{f_{n,Q}(P)}{f_{n,Q}(P+T)} \frac{f_{n,P}(Q-T)}{f_{n,P}(Q)} \frac{f_{n,Q}(T)}{f_{n,P}(-T)}. \tag{4}$$

Complexity and calculation of e_n

- The number of point additions/subtractions in step 5 is t.
- To calculate $\mathrm{lc}_Q(g_{L_{l_i},\epsilon_i L_{r_i}})$ takes a fixed amount of arithmetic in K because the curve is cubic, and g is a ratio of linear functions.
- Total complexity is thus $O(t)$ operations in K.
- Since we can find $\mathcal{A}$ with $t \leq 1 + 2\log_2(n)$, we have complexity $O(\log n)$.
- By (3) we need two calculations like $f_{n,P}(Q)$ to calculate $e_n(P, Q)$.
- To calculate $e_n(P, Q)$ also takes $O(\log n)$ K-operations.

Elliptic DL and Multiplicative Group DL

- Suppose $P \in E[n](K)$ has order n.
- By non-degeneracy of e_n $\exists Q \in E[n](\Omega)$ such that $\mathrm{ord}(\zeta) = n$, where $\zeta := e_n(P, Q)$.
- Let $f : E[n](\Omega) \to \mu_n$ be given by $f(R) := e_n(R, Q)$.
- If $R = aP$, then $f(R) = \zeta^a$. Conversely, if $R \in \langle P \rangle$, and $f(R) = \zeta^a$, then $R = aP$.
- So Elliptic DL over K is reduced to the multiplicative group DL over $L := K(Q)$.
- However, $\deg_K L$ is almost always of order $q := |K|$.
- Notable exception: E is supersingular, then $\deg_K L \leq 2$ (except in characteristic 2 or 3, where it is ≤ 12).

The Group Structure of $E(K)$

- If K is a finite field, E/K elliptic curve, can calculate $|E(K)|$ quickly using Schoof's algorithm, or one of its variants.
- One knows that, as a group, $E(K) \cong Z_d \times Z_e$, where $d|e$.
- Problem: Given E/K, find d and e, the *elementary divisors* of $E(K)$.
- Can use the Weil pairing to solve the following: Given $P, Q \in E(K)$, do they generate $E(K)$?
- P, Q generate $E(K)$ if and only if $m\,\mathrm{ord}(e_m(P, Q)) = N$, where $m = \mathrm{lcm}(\mathrm{ord}(P), \mathrm{ord}(Q))$, and $N = |E(K)|$.
- In that case the elementary divisors of $E(K)$ are $N/m, m$.

Algorithm for Elementary Divisors of $E(K)$

1. Calculate $N = |E(K)|$.
2. Pick $P, Q \in_R E(K)$ (uniformly and independently).
3. Calculate $m := \operatorname{lcm}(\operatorname{ord}(P), \operatorname{ord}(Q))$.
4. Calculate $\zeta := e_m(P, Q)$.
5. Calculate $d := \operatorname{ord}(\zeta)$.
6. If $md = N$, return (d, m), and P, Q as generators, else go to step 2.

Analysis of the Algorithm

- Calculating $\mathrm{ord}(P)$ and $\mathrm{ord}(Q)$ requires factorization of N be known.
- Each iteration of the loop takes time $O(\log^2 q)$ operations in K, where $q = |K|$.
- Expected number of iterations is

$$\frac{1}{\Pr(P \text{ and } Q \text{ generate } E(K))}.$$

- But, there is an absolute constant $C > 0$ such that

$$\Pr(P \text{ and } Q \text{ generate } E(K)) \geq \frac{C}{\log \log N}.$$

A Modified Algorithm

1. Calculate $N = |E(K)|$.
2. Set $r \leftarrow \gcd(N, q-1)$.
3. Write $N = N_0 N_1$, where $\gcd(N_0, N_1) = 1$, and $\ell | r \Leftrightarrow \ell | N_0$.
4. Pick $P, Q \in_R E(K)$; $P' \leftarrow N_1 P$, $Q' \leftarrow N_1 Q$.
5. Calculate $m := \operatorname{lcm}(\operatorname{ord}(P'), \operatorname{ord}(Q'))$.
6. Calculate $\zeta := e_m(P', Q')$.
7. Calculate $d := \operatorname{ord}(\zeta)$.
8. If $md = r$, return $(d, N/d)$, else go to step 2.

Probability of Generating a finite abelian group

- Let A be a finite abelian group.
- $\phi_k(A) := |\{(a_1, \dots, a_k) \in A^k | (a_i) \text{ generates } A\}|$.
- $\phi_i(A)/|A|^k =$ probability that A is generated by a random k-tuple of elements of A.
- Multiplicativity:

$$\frac{\phi_k(A)}{|A|^k} = \prod_{p||A|} \frac{\phi_k(A/pA)}{|A/pA|^k}.$$

Lower Bounds for the Probability

- $P_1, \ldots, P_r \in A$ are independent if $m_1 P_1 + \cdots + m_r P_r = 0 \Rightarrow m_i P_i = 0$.
- Torsion Rank of A: the maximum number of independent torsion elements of A, $= \max_p \dim_{\mathbb{F}_p} A/pA$.
- V/k vector space of dimension r. Probability of being generated by a random $r+k$-tuple is $(1-q^{k+1})\ldots(1-q^{k+r})$.
- If $r =$ torsion rank of A, then

$$\frac{\phi_{r+k}(A)}{|A|^{r+k}} \geq \begin{cases} \frac{\phi(|A|)}{|A|} \prod_{j=2}^{r} \zeta(j)^{-1} & \text{if } k = 0 \\ \prod_{j=k+1}^{r} \zeta(j)^{-1} & \text{if } k > 0 \end{cases}$$

Conclusions

- The Weil pairing can be computed quickly.
- It can be used to reduced the ECDL to the ordinary DL, in an extension field, usually of very large degree.
- It can be used to give a fast random algorithm for finding the group structure of a group of rational points on an elliptic curve.
- The same construction given here (suitably generalized) also works for Jacobians of curves.