Cryptographic Applications of the Weil Pairing

Travis Scholl

January 11, 2019

Abstract

In this talk we will introduce the Weil pairing on an elliptic curve and give several cryptographic applications. We will review the argument of Boneh and Silverberg which suggests that this kind of pairing does not exist naturally on higher dimensional varieties. We will also look at some constructions of pairing-friendly elliptic curves.

Contents

1 Introduction

Last time we introduced the notion of a *cryptographic multilinear map*. This is a k-linear map of the form

$$e : G_1 \times \cdots \times G_1 \to G_2,$$

where G_1 and G_2 are cyclic groups of prime order ℓ. We require that:

1. Products and inverses in G_i are easy to compute.

2. The map e is easy to compute.

3. The DLP in G_1 is hard to compute.

Remark 1. If the DLP in G_1 is hard, then the DLP is G_2 must also be hard. This is because, using e, we can transfer any instance of the DLP from G_1 to an instance of the DLP for G_2 as $e(g, \cdots, g^a) = e(g, \ldots, g)^a$.

Last time we also showed that multilinear maps have many applications: multiparty key exchange, short signatures, and broadcast encryption.

The main open problem about cryptographic multilinear maps is to find one with $k \geq 3$. The only known example of a cryptographic multilinear map is the Weil pairing on an elliptic curve, which has $k = 2$. The main goal of this talk is to introduce the Weil pairing and argue that it does not generalize. We will also give examples of constructing "pairing-friendly" elliptic curves.

2 Background

2.1 Divisors

Let C be a smooth curve over a field F. Recall that $\operatorname{div}(C)$ is the free abelian group on the set of points $C(\overline{F})$. So $D \in \operatorname{div}(C)$ looks like $D = \sum n_P[P]$ where the sum is over all points $P \in C(\overline{F})$. The *degree* of D is $\deg D = \sum n_P$. The set of degree 0 divisors is $\operatorname{div}^0(E)$. For a function $f \in \overline{F}(C)$, we let $\operatorname{div} f = \sum_P \operatorname{Ord}_P(f)[P]$. A divisor D is *principle* if $D = \operatorname{div} f$ for some f.

Example 2. Let $C : y = 0$. Then $f = x$ is a function on C. Note that $\operatorname{div} f = [(0,0)] - [\infty]$, where ∞ is the point at infinity, or in projective coordinates it is $(1 : 0 : 0)$.

Example 3. Let $E : y^2 = x^3 - x$. Then $f = x$ is a function on E. One can show[1] that $\operatorname{div} f = 2[(0,0)] - 2[0]$, where 0 is the point at infinity, i.e. the zero element on the elliptic curve E. In projective coordinates, 0 corresponds to $(0 : 1 : 0)$. This is the same for any short Weirstrass equation.

The *Picard group* $\operatorname{Pic}^0(C)$ is defined by the exact (this needs to be proved) sequence:

$$1 \to \overline{F}^\times \to \overline{F}(C)^\times \to \operatorname{div}^0(C) \to \operatorname{Pic}^0(C) \to 0.$$

This is similar to the ideal class group for number fields $K/\mathbb{Q}$,

$$1 \to \mathcal{O}_K^\times \to K^\times \to \{\text{fraction ideals}\} \to \{classgroup\} \to 0.$$

2.2 Elliptic Curves

Let E be an elliptic curve over a field F.

[1] See the exercises in chapter 6 of [HPS14].

Theorem 4 ([Sil09, Prop. III.3.4])**.** *The map sending $P \in E(\overline{F})$ to the divisor $[P] - [0] \in \operatorname{div}^0(E)$ induces an isomorphism $E(\overline{F}) \cong \operatorname{Pic}^0(E)$.*

Corollary 5. *A divisor $D \in \operatorname{div}(E)$ is principle if and only if $\deg D = 0$ and $\sum n_P P = 0$ where the sum is taken in the group $E(\overline{F})$.*

Definition 6. The *sum* of a divisor $D = \sum n_P[P]$ is $\operatorname{Sum}(D) = \sum n_P P$.

2.3 Torsion Points

Let $m \in \mathbb{Z}$ be coprime to the characteristic of F. Recall that $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, where $E[m] = \{P \in E(\overline{F}) \colon mP = 0\}$.

Our goal is to come up with a bilinear pairing on $E[m]$. Since $E[m]$ has rank 2, there is a "natural" pairing coming from the determinate. Fix a basis $\{R, S\}$ of $E[m]$ and define $\det : E[m] \times E[m] \to \mathbb{Z}/m\mathbb{Z}$ by

$$\det(P, Q) = \det(aR + bS, cR + dS) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

This has two issues:

1. It is not independent of the basis.
2. It may not be Galois invariant, i.e. $\det(\sigma(P), \sigma(Q))$ may not be $\sigma(\det(P, Q))$ (where σ acts on $\mathbb{Z}/m\mathbb{Z}$ trivially).

Both of these issues suggest that this value may not admit a nice formula. In fact, the only way we now how to find a, b, c, d is by computing discrete logs.

To fix these issues, we will modify the pairing to be a map from $E[m] \times E[m] \to \mu_m(\overline{F})$. Essentially, we choose $e_m(P, Q) = \zeta^{ad-bc}$ for some $\zeta \in \mu_m(\overline{F})$.

3 Weil Pairing

Let $D = \sum n_P[P] \in \operatorname{div}^0(E)$ and $f \in \overline{F}(E)$. If the supports of D and $\operatorname{div} f$ are disjoint, then we define $f(D) = \prod f(P)^{n_P}$.

Lemma 7. *$f(D)$ depends only on $\operatorname{div} f$.*

Proof. If $\operatorname{div} g = \operatorname{div} f$, then $g = af$ for some $a \in \overline{F}^\times$. Note that $\prod a^{n_P} = a^{\deg D} = 1$ because $D \in \operatorname{div}^0(E)$. □

Let $P \in E[m]$ and $D_P \in \operatorname{div}^0(E)$ such that $\operatorname{Sum}(D_P) = P$. Because $mP = 0$, it follows that mD_P is principal. Choose f_P such that $\operatorname{div} f_P = mD_P$.

Now let $Q \in E[m]$ and choose D_Q and f_Q similarly. We may assume that D_P is disjoint from D_Q. For example, we can choose $X, Y \in E(\overline{F})$ at random and use

$$D_P = [P + X] - [X], \text{ and } D_Q = [Q + Y] - [Y].$$

These divisors are likely to be disjoint.

Definition 8. The *Weil pairing* is

$$e_m(P,Q) = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

To show that e_m is well defined, we have to show that it is independent of the choice of f_P, f_Q, D_P, and D_Q. The former two follows from the fact that the value of $f(D)$ depends only on $\operatorname{div} f$.

Suppose D'_P (and f'_P) is an alternate choice for D_P (and f_P). Then $D_P - D'_P$ is principle, say $D'_P = D_P + \operatorname{div} g$. Since we have already shown $e_m(P,Q)$ is independent of the choice of f_P, we may assume $f'_P = f_P g^m$ because $\operatorname{div} f'_P = mD'_P = mD_P + m \operatorname{div} g = \operatorname{div} f_P + \operatorname{div} g^m = \operatorname{div} f_P g^m$. Now by Weil reciprocity, $f_Q(\operatorname{div} g) = g(\operatorname{div} f_Q) = g^m(D_Q)$. So

$$\frac{f_P(D_Q)}{f_Q(D_P)} \cdot 1 = \frac{f_P(D_Q)}{f_Q(D_P)} \cdot \frac{g^m(D_Q)}{f_Q(\operatorname{div} g)} = \frac{f'_P(D_Q)}{f_Q(D'_P)}.$$

Theorem 9 ([Sil09, Prop. III.8.1])**.** *The Weil pairing satisfies the following properties.*

1. *It is in $\mu_m(\overline{F})$, ($e_m(P,Q)^m = 1$).*
2. *It is bilinear, ($e_m(P_1 + P_2, Q) = e_m(P_1, Q)e_m(P_2, Q)$).*
3. *It is alternating, ($e_m(P,Q) = e_m(Q,P)^{-1}$).*
4. *It is non-degenerate, (if $e_m(P,Q) = 1$ for all Q, then $P = 0$).*
5. *It is Galois invariant, ($e_m(\sigma(P), \sigma(Q)) = \sigma(e_m(P,Q))$).*
6. *It is compatible, ($e_{mm'}(P,Q) = e_m(m'P, Q)$ for $P \in E[mm']$, $Q \in E[m]$).*

Remark 10. Because e_m is alternating, $e_m(P,P) = 1$. For cryptographic bilinear maps $e : G_1 \times G_1 \to G_2$, if g is a generator for G_1, then $e(g,g)$ should be a generator for G_2. The Weil pairing does not satisfy this. However, we can fix this by using a twist. That is, we define $\tilde{e}_m(P,Q) = e_m(P, \phi(Q))$ for a certain endomorphism ϕ called a *distortion map*. As long as $\{P, \phi(P)\}$ is linearly independent, $\tilde{e}_m$ will have the desired properties.

4 Computing the Weil Pairing

Our goal is to compute $e_m(P,Q)$ given P and Q.

Let f_P, f_Q be functions with $\operatorname{div} f_P = m[P] - m[0]$ and $\operatorname{div} f_Q = m[Q] - m[0]$. Then for almost any choice of $X, Y \in E$, we have

$$e_m(P,Q) = \frac{f_P(Q-Y) f_Q(-X)}{f_P(-Y) f_Q(P-X)}.$$

To see why, note that $\operatorname{div}\{R \mapsto f_P(R-Y)\} = m[P+Y] - m[Y]$, which is m times a divisor $[P+Y] - [Y]$ that sums to P.

Remark 11. Formally what is happening is that we are using $f_p \circ \tau_{-Y}$ where τ_{-Y} is the translation by $-Y$ function. This is useful because τ_{-Y} is easy to compute.

So to calculate $e_m(P, Q)$ we need to solve the following problems:

1. Given $P \in E[m]$, find f_P such that $\operatorname{div} f_P = m[P] - m[0]$.
2. Evaluate f_P on several points.

Remark 12. Note that computing f_P completely is too expensive because it involves polynomials of degree $\approx m$. Instead, we will only compute the evaluations $f_P(S)$ for whichever points $S \in E$ we need.

Theorem 13 ([Sil09, Thm XI.8.1])**.** *Let E be an elliptic curve given by a Weirstrass equation $y^2 = x^3 + Ax + B$. Let $S = (x_S, y_S)$ and $T = (x_T, y_T)$ be point on E. Let λ denote the slope*[2] *of the line from S to T. If*

$$h_{S,T} = \begin{cases} \frac{y - y_S - \lambda(x - x_S)}{x + x_S + x_T - \lambda^2} & \text{if } \lambda \neq \infty, \\ x - x_S & \text{if } \lambda = \infty, \end{cases}$$

then

$$\operatorname{div} h_{S,T} = [S] + [T] - [S + T] - [0].$$

Theorem 14 ([Mil04], [Sil09, Thm. XI.8.1])**.** *Given $P \in E[m]$, Algorithm 1 returns a function f_P such that*

$$\operatorname{div} f_P = m[P] - m[0].$$

Algorithm 1 Miller's algorithm

```
Input: P ∈ E[m] where m = ε_0 + ··· ε_{t-1} 2^{t-1} + 2^t        ▷ ε_i ∈ {0, 1}
T ← P, f ← 1
for i = t − 1, ..., 0 do
    f ← f^2 · h_{T,T}
    T ← 2T
    if ε_i = 1 then
        f ← f · h_{T,P}
        T ← T + P
return f
```

Corollary 15. *Using Miller's algorithm, we can compute $e_m(P, Q)$ with $O(\log m)$ point additions and $O(\log m)$ field operations.*

Proof. Run Miller's algorithm with P and m, but instead of keeping track of f, we instead keep track of $f(S)$ for the necessary points $S \in E(\overline{F})$. This works because f is constructed as a product of $\log_2 m$ functions with bounded degree numerator and denominator. □

[2] If $S = T$ or the line is vertical λ can still be defined.

5 Obstructions To Generalizations

In this section we list several obstructions stopping us from generalizing the Weil pairing into a k-linear map for $k > 3$. These arguments are summarized from [BS03].

5.1 Tensor Products

One way to build a multilinear map out of a bilinear map is to take tensor powers.

Recall that $\mathbb{Z}/a\mathbb{Z} \otimes \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/\gcd(a,b)\mathbb{Z}$, and an isomorphism is given by $m \otimes n \mapsto mn$. Therefore $G_2^{\otimes \ell} \cong G_2$.

If $e : G_1 \times G_1 \to G_2$ is a bilinear map, then it induces a map

$$\tilde{e} : (G_1 \times G_1)^k \to G_2^{\otimes k} \cong G_2$$

sending

$$\tilde{e}(g_1, h_1, \ldots, g_k, h_k) = e(g_1, h_1) \otimes \cdots \otimes e(g_k, h_k).$$

This may seem great, but look at what the isomorphism $G_2^{\otimes k} \cong G_2$ is in multiplicative notation:

$$(g^{a_1}, \ldots, g^{a_n}) \mapsto g^{a_1 \cdots a_n}.$$

This is the multilinear Diffie-Hellman problem. We need this to be computationaly difficult for security. So $\tilde{e}$ can not be efficiently computable.

5.2 Galois Equivariance

Most natural multilinear maps coming from geometry are Galois equivariant. Any map that can be computed by polynomials with coefficients in the base field will have this property.

Let $A/\mathbb{F}_q$ be an abelian variety of dimension g. Then $A[\ell]$ is an $\mathbb{Z}/\ell\mathbb{Z}$-vector space of dimension $2g$. There is a unique (up to a constant) non-degenerate alternating multilinear form f on $A[\ell]$. It is given by the determinant. Assume that, like the Weil pairing, f takes values in $\mu_\ell(\overline{\mathbb{F}}_q)$. Fix a basis $P_1, \ldots, P_{2g}$ for $A[\ell]$ and let $\zeta = f(P_1, \ldots, P_{2g})$. If $Q_i = \sum a_{i,j} P_j$ then

$$f(Q_1, \ldots, Q_{2g}) = \zeta^{\det(a_{i,j})}.$$

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ denote the qth power Frobenius. Then f is Galois equivariant if and only if

$$f(\sigma(P_1), \ldots, \sigma(P_{2g})) = \sigma(\zeta),$$

Recall that the characteristic polynomial of the Frobenius acting on the ℓ-adic Tate module (we can just think of $A[\ell]$) has constant term q^g (this is a Corollary of the Weil conjectures, proven by Deligne). So the left hand side is $f(\sigma(P_1), \ldots, \sigma(P_{2g})) = f(P_1, \ldots, P_{2g})^{\det \sigma} = \zeta^{(q^g)}$. The right hand side is $\sigma(\zeta) = \zeta^q$.

Assuming $\ell \nmid q$, this shows that f is Galois equivariant if and only if

$$\zeta^{(q^g)} = \zeta^q \Leftrightarrow \ell \mid q^{g-1} - 1.$$

Notice that the bound on the right hand side is independent of ℓ. Moreover, if $g > 1$ then there is only finitely many such ℓ. This shows that if $g > 1$, then there is no "compatible system" of f that is Galois equivariant. That is, there is no f which works for all ℓ.

6 Pairing Friendly Curves

In this section, we summarize a construction of elliptic curves for which the Weil pairing is a cryptographic bilinear map.

Definition 16. If q is a prime power and ℓ is a prime with $\ell \nmid q$, then the *embedding degree* of ℓ with respect to q is the smallest positive integer k such that $\ell \mid q^k - 1$.

Remark 17. Note that k is also the multiplicative order of q in $\mathbb{Z}/\ell\mathbb{Z}$.

Let E be an elliptic curve over $\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ has a subgroup of large prime order ℓ. Note that the Weil pairing is a map

$$e_\ell : E[\ell] \times E[\ell] \to (\mathbb{F}_{q^k})^\times.$$

where k is the embedding degree of ℓ. If k is too large, then arithmetic in $\mathbb{F}_{q^k}$ is too hard. If k is too small, then the DLP in $\mathbb{F}_{q^k}$ is too easy. In practice, the optimal value is $k \approx 12$. Curves which achieve a good value of k are often called *pairing friendly*.

Remark 18. We expect that $k \approx q$ for most curves. To see why, note that most elements in $\mathbb{Z}/\ell\mathbb{Z}$ have large multiplicative order. Curves with small embedding degree are rare, and the chance of finding one randomly is negligible [BK98].

In [MNT01], Miyaji, Nakabayashi, and Takano show how to construct elliptic curves $E/\mathbb{F}_q$ such that $E(\mathbb{F}_q)$ has prime order and embedding degree[3] 3, 4, or 6. Curves constructed this way are commonly referred to as MNT curves. There has been many further generalizations of pairing friendly curves. Algorithm 2 gives a simple construction of pairing friendly curves and is due to Barreto and Naehrig [BN06].

Remark 19. The fact that step 6 in the algorithm works (i.e. there a twist of $y^2 = x^3 + 1$ with N points) is called the complex multiplication (CM) method. The CM method is a common strategy to construct elliptic curves over finite fields with special properties. See [CFA+06] for more on the CM method.

Theorem 20. *If Algorithm 2 returns E, then E has embedding degree* 12.

[3] When $E(\mathbb{F}_q)$ has prime order, we use $\ell = \#E(\mathbb{F}_q)$.

Algorithm 2 Barreto-Naehrig Curves

```
repeat
    x ← random integer of predetermined size
    p ← 36x^4 + 36x^3 + 24x^2 + 6x + 1
    t ← 6x^2 + 1
until p and N = p + 1 − t are prime
E ← twist of y^2 = x^3 + 1 over F_p with N points
return E
```

Proof. Recall that the embedding degree is the multiplicative order of p modulo N. Equivalently, we can use $t-1$. because $t-1 = p - N \equiv p \mod N$ By construction, there is a value x such that

$$\begin{aligned} p(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1 \\ t(x) &= 6x^2 + 1 \\ N(x) &= p(x) + 1 - t(x). \end{aligned}$$

A straightforward calculation shows that

$$\Phi_{12}(t(x) - 1) = N(x)N(-x),$$

where Φ_{12} is the usual cyclotomic polynomial. Therefore $t(x) - 1$ is a primitive 12th root of unity modulo N. □

References

[BK98] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. Cryptology*, 11(2):141–145, 1998.

[BN06] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected areas in cryptography*, volume 3897 of *LNCS*, pages 319–331. Springer, Berlin, 2006.

[BS03] Dan Boneh and Alice Silverberg. Applications of multilinear forms to cryptography. In *Topics in algebraic and noncommutative geometry (Luminy/Annapolis, MD, 2001)*, volume 324 of *Contemp. Math.*, pages 71–90. Amer. Math. Soc., Providence, RI, 2003.

[CFA+06] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[HPS14] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2014.

[Mil04] Victor S. Miller. The Weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.

[MNT01] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 84(5):1234–1243, 2001.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.