Weil Pairings and the MOV Algorithm

Transforming the ECDLP over $\mathbb{F}_p$ to the DLP over $\mathbb{F}_{p^k}$

T. Ian Martiny

Department of Mathematics
University of Pittsburgh
Pittsburgh, PA 15260
tim24@pitt.edu

April 12, 2014

Rational functions

Definition

A rational function in one variable is any quotient of polynomials i.e.,

$$f(x) = \frac{a_0 + a_1x + \cdots + a_nx^n}{b_0 + b_1x + \cdots + b_kx^k} = \frac{(x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\cdots(x-\alpha_r)^{e_r}}{(x-\beta_1)^{d_1}(x-\beta_2)^{d_2}\cdots(x-\beta_s)^{d_s}}$$

We call the α_i's roots and the β_j's poles of the rational function $f(x)$.

Divisors

Definition

The divisor of a rational function is the formal sum:

$$\operatorname{div}(f(x)) = e_1[\alpha_1] + e_2[\alpha_2] + \cdots e_r[\alpha_r] - d_1[\beta_1] - d_2[\beta_2] - \cdots - d_s[\beta_2]$$

Definition

The group of divisors on an elliptic curve $E: \; y^2 = x^3 + ax + b$ is all formal sums:

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

Where $n_p \in \mathbb{Z}$ and only finitely many are non-zero.

This is the Free Abelian group on the elements of E

Degree and Sum

Definition

The degree of a divisor D is:

$$\deg(D) = \sum_{P \in E} n_P$$

Definition

The Sum of a divisor D is:

$$\mathrm{Sum}(D) = \sum_{P \in E} n_P P$$

Relationship between divisors of rational functions and divisors of Elliptic curves

Theorem

Let E be an elliptic curve. 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 iff

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

Recall that for $m \in \mathbb{N}$ $E[m] = \{P \in E : mP = \mathcal{O}\}$ or over a field $E(k)[m] = \{P \in E(k) : mP = \mathcal{O}\}$

Example

Suppose $P \in E[m]$ examine the divisor $D = m[P] - m[\mathcal{O}]$
Then $\deg(D) = m - m = 0$ and $\text{Sum}(D) = mP - m\mathcal{O} = \mathcal{O} - \mathcal{O} = \mathcal{O}$
Thus D satisifies our Theorem, so there is some rational function $f_p(x, y)$ on E with $\text{div}(f_p) = m[P] - m[\mathcal{O}]$

Bilinear pairings

Definition

A bilinear pairing on an elliptic curve E will be a homomorphism $B : E \times E \to \mathbb{F}^*$ such that:

$$B(v_1 + v_2, w) = B(v_1, w) \cdot B(v_2, w)$$
$$B(v, w_1 + w_2) = B(v, w_1) \cdot B(v, w_2)$$

Ideas of Weil Pairing

The Weil Pairing will take a pair of points $P, Q \in E[m]$ and will return as output $e_m(P, Q)$, an mth root of unity, in the base field. With the given properties:

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

Weil Pairing

Definition

Let $P, Q \in E[m]$ and let f_P, f_Q be rational functions on E satisfying $\mathrm{div}(f_P) = m[P] - m[\mathcal{O}]$ and $\mathrm{div}(f_Q) = m[Q] - m[\mathcal{O}]$. Then the Weil Pairing of P and Q is:

$$e_m(P, Q) = \frac{f_P(Q+S)}{f_P(S)} \Bigg/ \frac{f_Q(P-S)}{f_Q(-S)}$$

Where S is any point on E, $S \notin \{\mathcal{O}, P, -Q, P-Q\}$

Well-definedness of Weil pairing with respect to functions

Suppose f_P and $\tilde{f}_P$ are both rational functions with divisor $m[P] - m[\mathcal{O}]$. Then $f_P = c\tilde{f}_P$ so:

$$\frac{\tilde{f}_P(Q+S)}{\tilde{f}_P(S)} = \frac{cf_P(Q+S)}{cf_P(S)} = \frac{f_P(Q+S)}{f_P(S)}$$

Similarly for f_Q and $\tilde{f}_Q$

Well-definedness of Weil pairing with respect to point S

Let $F : E \backslash \{\mathcal{O}, P, -Q, P-Q\} \to \mathbb{F}^*$

$$F(S) = \frac{f_P(Q+S)}{f_P(S)} \Big/ \frac{f_Q(P-S)}{f_Q(-S)} = \frac{f_P(Q+S) f_Q(-S)}{f_P(S) f_Q(P-S)}$$

$$\begin{aligned} \mathrm{div}(F) = & m[P-Q] + m[-Q] + m[\mathcal{O}] + m[P] \\ & - m[P-Q] - m[-Q] - m[\mathcal{O}] - m[P] \end{aligned}$$

Facts about the Weil Pairing

Facts

Fact 1: The Weil Pairing is bilinear.
Fact 2: $e_m(P, Q)^m = 1$.
Fact 3: The Weil Pairing is alternating i.e.,

$$e_m(P, P) = 1 \implies e_m(P, Q) = e_m(Q, P)^{-1}$$

Fact 4: The Weil Pairing is non-degenerate i.e,

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

Unhelpful example - computing a Weil Pairing

Let $m = 2$ and $E : y^2 = x^3 + ax + b = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Note that $\alpha_1 + \alpha_2 + \alpha_3 = 0$.
Let $P_1 = (\alpha_1, 0)$, $P_2 = (\alpha_2, 0)$, $P_3 = (\alpha_3, 0)$ these are points of order 2. And let $f_{P_i} = x - \alpha_i$ then $\mathrm{div}(f_{P_i}) = 2[P_i] - 2[\mathcal{O}]$. Let $S = (x, y)$ be any allowable point on E, then to compute $e_2(P_1, P_2)$ we will need $x(P_1 - S)$ and $x(P_2 + S)$.

$$\begin{aligned} x(P_1 - S) &= \left(\frac{-y}{x - \alpha_1}\right)^2 - x - \alpha_1 \\ &= \frac{y^2 - (x - \alpha_1)^2 (x + \alpha_1)}{(x - \alpha_1)^2} \\ &= \frac{(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) - (x - \alpha_1)^2 (x + \alpha_1)}{(x - \alpha_1)^2} \end{aligned}$$

since $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$

Example cont'd

$$\begin{aligned}
&= \frac{(x-\alpha_2)(x-\alpha_3)-(x-\alpha_1)(x+\alpha_1)}{x-\alpha_1} \\
&= \frac{(-\alpha_2-\alpha_3)x+\alpha_2\alpha_3+\alpha_1^2}{x-\alpha_1} \\
&= \frac{\alpha_1 x+\alpha_2\alpha_3+\alpha_1^2}{x-\alpha_1}
\end{aligned}$$

since $\alpha_1+\alpha_2+\alpha_3=0$

Similarly,

$$X(P_2+S) = \frac{\alpha_2 x+\alpha_1\alpha_3+\alpha_2^2}{x-\alpha_2}$$

Example cont'd

Recall $f_{P_i} = x - \alpha_i$, and with the assumption P_1, P_2 are distinct non-zero points in $E[2]$ we directly compute $e_2(P_1, P_2)$

$$
\begin{aligned}
e_2(P_1, P_2) =& \frac{f_{P_1}(P_2 + S)}{f_{P_1}(S)} \Big/ \frac{f_{P_2}(P_1 - S)}{f_{P_2}(-S)} \\
=& \frac{x(P_2 + S) - \alpha_1}{x(S) - \alpha_1} \Big/ \frac{x(P_1 - S) - \alpha_2}{x(-S) - \alpha_2} \\
=& \frac{\frac{\alpha_2 x + \alpha_1\alpha_3 + \alpha_2^2}{x - \alpha_2} - \alpha_1}{x - \alpha_1} \Big/ \frac{\frac{\alpha_1 x + \alpha_2\alpha_3 + \alpha_1^2}{x - \alpha_1} - \alpha_2}{x - \alpha_2} \\
=& \frac{(\alpha_2 - \alpha_1)x + \alpha_1\alpha_3 + \alpha_2^2 + \alpha_1\alpha_2}{(\alpha_1 - \alpha_2)x + \alpha_2\alpha_3 + \alpha_1^2 + \alpha_1\alpha_2} \\
=& \frac{(\alpha_2 - \alpha_1)x + \alpha_2^2 - \alpha_1^2}{(\alpha_1 - \alpha_2)x + \alpha_1^2 - \alpha_2^2} \\
=& -1
\end{aligned}
$$

A Theorem to help compute the Weil Pairing

Theorem

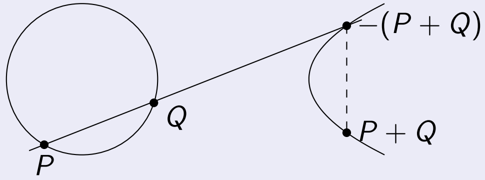
Given P, Q on E, let λ be the slope of the line connecting P, Q, or $\lambda = \infty$, or the slope of the tangent line, if necessary. Then define

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

Then $div(g_{P,Q}) = [P] + [Q] - [P + Q] - [\mathcal{O}]$

Proof.

If $\lambda \neq \infty$ let $y = \lambda x + \nu$ be the line through P and Q, this will intersect E at P,Q, and $-(P+Q)$. Thus
$\operatorname{div}(y - \lambda x - \nu) = [P] + [Q] + [-P-Q] - 3[\mathcal{O}]$



Notice by our addition formula: $x_{P+Q} = \lambda^2 - x_P - x_Q$. So
$\operatorname{div}(x - x_{P+Q}) = [P+Q] + [-P-Q] - 2[\mathcal{O}]$.
Finally, $g_{P,Q} = \frac{y - \lambda x - \nu}{x -_{P+Q}}$ and thus
$\operatorname{div}(g_{P,Q}) = [P] + [Q] - [P+Q] - [\mathcal{O}]$ $\square$

Miller's Algorithm

Goal: construct f_P with $\operatorname{div}(f_P) = m[P] - [mP] - (m-1)[\mathcal{O}]$. Thus when $P \in E[m]$ $\operatorname{div}(f_P) = m[P] - m[\mathcal{O}]$.

First for $m \in \mathbb{N}$ write $m = m_0 + m_1 \cdot 2 + \cdots + m_{n-1} \cdot 2^{n-1}$ with $m_{n-1} \neq 0$.

$T \leftarrow P$
$f \leftarrow 1$
for $i = n-2$ **to** 0 *by -1*
do
  $f \leftarrow f^2 \cdot g_{T,T}$
  $T \leftarrow 2T$
  if $m_i = 1$ **then**
    $f \leftarrow f \cdot g_{T,P}$
    $T \leftarrow T + P$
  end
end
return f

This algorithm is simply the double-and-add algorithm for adding points on elliptic curves. Using that

$$\operatorname{div}(g_{T,T}) = 2[T] - [2T] - [\mathcal{O}]$$

$$\operatorname{div}(g_{T,P}) = [T] - [P] - [T+P] - [\mathcal{O}]$$

Example following divisor of f

Example

Let $m = 5 = 1 + 1 \cdot 2^2$. Thus $n - 1 = 2$. Let $P \in E[5]$
Initialization: $T = P$, $f = 1$, $\mathrm{div}(f) = 0$.
$i = 1$: $f = 1^2 \cdot g_{P,P}$, $T = 2P$,

$$\mathrm{div}(f) = 2[P] - [2P] - [\mathcal{O}]$$

$m_1 = 0$ so skip the if step.
$i = 0$: $f = f^2 \cdot g_{2P,2P}$, $T = 4P$,

$$\begin{aligned}\mathrm{div}(f) =& 2[P] - [2P] - [\mathcal{O}] + 2[P] - [2P] - [\mathcal{O}] + 2[2P] - [4P] - [\mathcal{O}] \\ =& 4[P] + -[4P] - 3[\mathcal{O}]\end{aligned}$$

Example cont'd

Example

$m_0 = 1$ so compute:
$f = f \cdot g_{4P,P}$, $T = 5P = \mathcal{O}$.

$$\begin{aligned}\mathrm{div}(f) =& 4[P] + -[4P] - 3[\mathcal{O}] + [4P] + [P] - [5P] - [\mathcal{O}] \\ =& 5[P] - 5[\mathcal{O}]\end{aligned}$$

Example computation

Example

Let $E: y^2 = x^3 + 30x + 34$ over $\mathbb{F}_{631}$. $P = (36, 60)$, $Q = (121, 387)$ are both points of order 5 on $E(\mathbb{F}_{631})$. Choose the $S = (0, 36)$. Then Miller's Algorithm gives:

$$\frac{f_P(Q+S)}{f_P(S)} = \frac{103}{219} = 473 \in \mathbb{F}_{631}$$

$$\frac{f_Q(P-S)}{f_Q(-S)} = \frac{284}{204} = 88 \in \mathbb{F}_{631}$$

So,

$$e_5(P, Q) = \frac{473}{88} = 242 \in \mathbb{F}_{631}$$

Embedding degree

A result from Algebraic Geometry gives that if E is an elliptic curve over $\mathbb{F}_p$ and $m \in \mathbb{N}$ with $p \nmid m$ then there is some $k \in \mathbb{N}$ such that

$$E(\mathbb{F}_{p^k}) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Definition

The embedding degree $k \in \mathbb{N}$ of E with respect to m is the smallest k such that:

$$E(\mathbb{F}_{p^k}) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

MOV algorithm

Let E be an elliptic curve over $\mathbb{F}_p$ and $P \in E(\mathbb{F}_P)[m]$ (generally m is a prime $m \neq p$, and usually $m > \sqrt{p} + 1$). Let k be the embedding degree with respect to m; suppose we know how to solve the DLP in $\mathbb{F}_{p^k}$. Let $Q \in E(\mathbb{F}_P)$ with $Q = nP$, we wish to find this n.

1. Compute $N = \#E(\mathbb{F}_{p^k})$

   [Note: $m|N$ since by assumption $E(\mathbb{F}_p)$ has a point of order m]
2. Choose any $T \in E(\mathbb{F}_{p^k})$; $T \notin E(\mathbb{F}_p)$
3. Compute $T' = (N/m)T$

   [If $T' = \mathcal{O}$ go back to step 2]
4. Compute the Weil Pairing values:

$$\alpha = e_m(P, T') \qquad \beta = e_m(Q, T')$$

   [If $\alpha = 1$ go back to step 2]
5. Solve the DLP for $\beta = \alpha^n$
6. Then $Q = nP$.

Wait, what?

The Weil Pairing is a non-degenerate, bilinear pairing, that creates an mth root of unity, thus $e_m(P, T')^r = 1$ iff $m|r$.
So if $Q = jP$ our goal is to find j, or to find $n \equiv j (\bmod\ m)$ $[mP = \mathcal{O}]$.
The MOV algorithm returns an n such that $e_m(Q, T') = e_m(P, T')^n$, thus by bilinearity:

$$\begin{aligned} e_m(P, T')^n =& e_m(Q, T') \\ =& e_m(jP, T') \\ =& e_m(P, T')^j \end{aligned}$$

Thus $e_m(P, T')^{n-j} = 1 \implies n \equiv j (\bmod\ m)$

Consequences of MOV algorithm

The algorithm is essentially unusable if our embedding degree $k > (\ln p)^2$, and in general, a random elliptic curve over $\mathbb{F}_p$ will have embedding degree much larger than $(\ln p)^2$.
However a certain group of elliptic curves, namely *super-singular curves*, with $\#E(\mathbb{F}_p) = p + 1$ have embedding degrees $k \leq 6$.
This algorithm should be seen more as a cautionary tale, if your elliptic curve has low embedding degree, your cryptosystem is NOT based off of the difficulty of the ECDLP, but rather the difficulty of the DLP.

Distortion maps

A main property of the Weil Pairing is that $e_m(P, P) = 1$ for all P, which can cause issues in some cryptographic settings where $Q = nP$. Then $e_m(P, Q) = 1$.

Definition

Let $m \geq 3$ be a prime and E be an elliptic curve and $P \in E[m]$. Then $\phi : E \to E$ is an *m-distortion map for P* if:

(i) $\phi(nP) = n\phi(P)$, $\forall\, n \geq 1$

(ii) $e_m(P, \phi(P))^r = 1$ iff $m|r$

(iii) ϕ can be "efficiently" computed.

Modified Weil Pairings

Definition

Let E be an elliptic curve, $P \in E[m]$ and ϕ be an $m-$distortion map for P. Then the modified Weil Pairing $\hat{e}_m$ on $E[m]$ (relative to ϕ) is:

$$\hat{e}_m(Q, Q') = e_m(Q, \phi(Q'))$$

Then $\hat{e}_m(Q, Q\prime) = 1$ iff $Q = \mathcal{O}$ or $Q' = \mathcal{O}$

Tripartite Diffie-Hellman key exchange

Alice, Bob, and Carl want to all have a shared secret (key) with as few passes of information as possible:

Public Parameter Creation		
Alice, Bob, and Carl all decide and publish a finite field $\mathbb{F}_q$, an elliptic curve $E/\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ of prime order m and an m-distortion map ϕ for P.		
Private Computations		
Alice	**Bob**	**Carl**
Choose secret n_A Compute $Q_A = n_A P$	Choose secret n_B Compute $Q_B = n_B P$	Choose secret n_C Compute $Q_C = n_C P$
Publication of Values		
Alice, Bob, and Carl publish their points Q_A, Q_B, Q_C		
Further Private Computations		
Alice	**Bob**	**Carl**
Compute $\hat{e}_m(Q_B, Q_C)^{n_A}$	Compute $\hat{e}_m(Q_A, Q_C)^{n_B}$	Compute $\hat{e}_m(Q_A, Q_B)^{n_C}$
The shared secret value is $\hat{e}_m(P, P)^{n_A n_B n_C}$		

Cryptanalysis of Tripartite Diffie-Hellman

Clearly if an attacker can solve the ECDLP then the attacker has access to the key.
However, notice that the attacker has access to Q_A and P and can compute $\hat{e}_m$. Thus if the attacker can solve the DLP over $\mathbb{F}_q$ they can find n_A since:

$$\hat{e}_m(Q_A, P) = \hat{e}_m(P, P)^{n_A}$$

So our security is based off the security of the ECDLP as well as the DLP. Thus in practice the Tripartite Diffie-Hellman requires a much larger base field.

References

"An Introduction to Mathematical Cryptography" - Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

"The Arithemetic of Elliptic Curves" - Joseph H. Silverman

Thanks for listening!