Pairings I

Michael Naehrig

Eindhoven Institute for the Protection of Systems and Information
Technische Universiteit Eindhoven
michael@cryptojedi.org

ECC Summer School 2008, Eindhoven
18 September 2008
What is a pairing?

A pairing is a non-degenerate, bilinear map

\[ e : G_1 \times G_2 \rightarrow G_3, \]

where \( G_1, G_2 \) are abelian groups written additively and \( G_3 \) is a multiplicative abelian group.

- **Non-degenerate:**
  for all \( 0 \neq P \in G_1 \) there is a \( Q \in G_2 \) s.t. \( e(P, Q) \neq 1 \),
  for all \( 0 \neq Q \in G_2 \) there is a \( P \in G_1 \) s.t. \( e(P, Q) \neq 1 \).

- **Bilinear:** for \( P_1, P_2 \in G_1; Q_1, Q_2 \in G_2 \) we have

\[
\begin{align*}
e(P_1 + P_2, Q_1) &= e(P_1, Q_1)e(P_2, Q_1), \\
e(P_1, Q_1 + Q_2) &= e(P_1, Q_1)e(P_1, Q_2).
\end{align*}
\]

It follows: \( e([a]P, [b]Q) = e(P, Q)^{ab} = e([b]P, [a]Q) \).
What can be done with pairings?

Pairings on elliptic curves can be used,

- as a means to attack DL-based cryptography on groups of points on elliptic curves,
- or to construct crypto systems with certain special properties:
  - One-round tripartite key agreement,
  - Identity-based key agreement,
  - Identity-based encryption (IBE),
  - Hierarchical IBE (HIDE),
  - Short signatures (BLS).
  - much more ...
Elliptic curves

Let $p > 3$ be a prime, $\mathbb{F}_p$ the finite field with $p$ elements and

$$E : Y^2 = X^3 + AX + B$$

an elliptic curve over $\mathbb{F}_p$.

- For a field extension $\overline{\mathbb{F}_p} \supseteq L \supseteq \mathbb{F}_p$ let

$$E(L) = \{(x, y) \in L^2 : y^2 = x^3 + Ax + B\} \cup \{P_\infty\}$$

the group of $L$-rational points on $E$.

- Let $n = \#E(\mathbb{F}_p)$ be the number of $\mathbb{F}_p$-rational points. We have

$$n = p + 1 - t, \quad |t| \leq 2\sqrt{p},$$

where $t$ is the trace of Frobenius.
Torsion points

Let $m$ be a non-negative integer. The set of $m$-torsion points

$$E[m] = \{ P \in E = E(\overline{\mathbb{F}_p}) \mid [m]P = P_{\infty} \}$$

is a subgroup of $E$.

- We denote by

$$E[m](L) = \{ P \in E(L) \mid [m]P = P_{\infty} \}$$

the group of $L$-rational $m$-torsion points.

- If $p \nmid m$ we have

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$
The embedding degree

Let \( r \neq p \) be a large prime dividing \( n = \#E(\mathbb{F}_p) \).
The embedding degree of \( E \) with respect to \( r \) is the smallest integer \( k \) s.t.

\[ r \mid p^k - 1. \]

\[ X^k - 1 = \prod_{d \mid k} \Phi_d(X) = \Phi_k(X) \cdot \prod_{d \mid k, d \neq k} \Phi_d(X). \]

This is equivalent to \( r \mid \Phi_k(p) \), where \( \Phi_k \) is the \( k \)-th cyclotomic polynomial. This follows from
The embedding degree

- The embedding degree \( k \) is the order of \( p \) modulo \( r \). Therefore
  \[
  k \mid r - 1.
  \]

- For \( k > 1 \) the field \( \mathbb{F}_{p^k} \) is the smallest extension of \( \mathbb{F}_p \) which contains the group \( \mu_r \) of \( r \)-th roots of unity,
  and for which \( E(\mathbb{F}_{p^k}) \) contains all \( r \)-torsion points, i.e.
  \[
  E[r] \subseteq E(\mathbb{F}_{p^k}).
  \]

For crypto-sized curve \( E \) and prime divisor \( r \) the embedding degree is usually very large.
The Weil pairing

The Weil pairing is a map

\[ e_r : E[r] \times E[r] \to \mu_r \subseteq \mathbb{F}_p^*, \]

\[ (P, Q) \mapsto f_{r,P}(D_Q)/f_{r,Q}(D_P), \]

- where \( D_P \sim (P) - (P_\infty) \) and \( D_Q \sim (Q) - (P_\infty) \) are divisors with disjoint support,
- \( f_{r,P} \) and \( f_{r,Q} \) are functions on the curve with divisors

\[
(f_{r,P}) = rD_P = r(P) - r(P_\infty),
\]

\[
(f_{r,Q}) = rD_Q = r(Q) - r(P_\infty).
\]
The Weil pairing

The Weil pairing is a map

\[ e_r : E[r] \times E[r] \rightarrow \mu_r \subseteq \mathbb{F}_{p^k}, \]
\[ (P, Q) \mapsto f_{r, P}(D_Q)/f_{r, Q}(D_P), \]

For a divisor \( D = \sum_{P \in E} n_P(P) \) and a function \( f \in \overline{\mathbb{F}_p}(E) \), we can evaluate \( f \) at \( D \) by

\[ f(D) = \prod_{P \in E} f(P)^{n_P}. \]

The Weil pairing is bilinear, non-degenerate and alternating (i.e. \( e_r(P, P) = 1 \)).
The MOV-FR attack

**Theorem:** Let $P \in E[r](\mathbb{F}_p)$. Then there exists a point $Q \in E[r]$ s.t. $e_r(P, Q)$ is a primitive $r$-th root of unity, i.e. a generator of $\mu_r$.

- Let $P, Q$ be the points from the theorem. Then the map
  
  $$f : \langle P \rangle \to \mu_r, \ R \mapsto e_r(R, Q)$$

  is a group isomorphism.

- The map $f$ ’reduces’ the DLP on $E(\mathbb{F}_p)[r]$ to the DLP in $\mu_r \subseteq \mathbb{F}_p^*$: If $R = [m]P$ then
  
  $$e_r(R, Q) = e_r([m]P, Q) = e_r(P, Q)^m.$$
The MOV-FR attack

\[ R = \left[ m \right] P \]

\[ \uparrow \]

\[ e_r(R, Q) = e_r\left(\left[ m \right] P, Q\right) = e_r(P, Q)^m. \]

- One can find \( m \) by solving the DLP in \( \mathbb{F}_{p^k}^* \).
- This attack is only useful, if we can compute the Weil pairing efficiently,
- and if the DLP in \( \mathbb{F}_{p^k}^* \) is easier than the DLP in \( E(\mathbb{F}_p) \).
The Tate pairing

The Tate pairing is a map

$$\langle \cdot, \cdot \rangle_r : E[r](\mathbb{F}_{p^k}) \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \rightarrow \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r,$$

$$(P, Q) \mapsto f_{r,P}(D_Q).$$

- The divisor $D_Q$ is equivalent to the divisor $(Q) - (P_\infty)$ and its support is disjoint from the support of $(f_{r,P}) = r(P) - r(P_\infty)$.
- The result must be interpreted as representing a class in $\mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r$.
- $Q$ is a representative of a class in $E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$. 
The reduced Tate pairing

The reduced Tate pairing is a map

\[ t_r : E[r](\mathbb{F}_p) \times E[r](\mathbb{F}_{p^k}) \rightarrow \mu_r \subset \mathbb{F}_{p^k}^*, \]

\[ (P, Q) \mapsto f_{r,P}(Q) \frac{p^k - 1}{r}. \]

- For the first group we restrict to \( E[r](\mathbb{F}_p) \).
- If \( r^2 \nmid n \) we may represent \( E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \) by \( E[r](\mathbb{F}_{p^k}) \).
- For \( k > 1 \) we may replace \( D_Q \) by \( Q \) itself.
- Note that for \( k > 1 \) and \( P \in E[r](\mathbb{F}_p) \) we have \( t_r(P, P) = 1 \).
The reduced Tate pairing

The reduced Tate pairing is a map

\[ t_r : E[r](\mathbb{F}_p) \times E[r](\mathbb{F}_{p^k}) \to \mu_r \subset \mathbb{F}_{p^k}^*, \]

\[ (P, Q) \mapsto f_{r, P}(Q)^{\frac{p^k - 1}{r}}. \]

- We obtain a unique pairing value in \( \mu_r \) by raising \( f_{r, P}(Q) \) to the power of \( \frac{p^k - 1}{r} \).
- This so called final exponentiation is an isomorphism

\[ \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r \to \mu_r. \]
Miller functions

To compute pairings we need to know the functions $f_{r,P}$ with divisor $r(P) - r(P_{\infty})$.

- Let $f_{i,P}$, $i \in \mathbb{Z}$ be a function on $E$ which has a divisor

$$ (f_{i,P}) = i(P) - ([i]P) - (i - 1)(P_{\infty}). $$

$f_{i,P}$ is called a Miller function.

- The special case $i = r$ leads to

$$ (f_{r,P}) = r(P) - ([r]P) - (r - 1)(P_{\infty}) = r(P) - r(P_{\infty}), $$

since $[r]P = P_{\infty}$. 
Miller’s formula

Can we compute $f_{i+j,P}$ from $f_{i,P}$ and $f_{j,P}$?

- Compute the divisor of the product

\[
(f_{i,P}f_{j,P}) = i(P) - ([i]P) - (i - 1)(P_{\infty}) + j(P) - ([j]P) - (j - 1)(P_{\infty})
= (i + j)(P) - ([i]P) - ([j]P) - (i + j - 2)(P_{\infty})
= (i + j)(P) - ([i + j]P) - (i + j - 1)(P_{\infty}) + ([i + j]P) - ([i]P) - ([j]P) + (P_{\infty})
= (f_{i+j,P}) + ([i + j]P) - ([i]P) - ([j]P) + (P_{\infty})
\]

- The sum of the divisors is ’almost’ the divisor of $f_{i+j,P}$. 
Miller’s formula

Now have a look at the lines occuring in the addition

\[ [i]P + [j]P = [i + j]P. \]

- The first line \( l \) goes through \([i]P\), \([j]P\) and \(-[i + j]P\), it has the divisor

\[
(l) = ([i]P) + ([j]P) + (-[i + j]P) - 3(P_\infty).
\]

- The second line \( v \) is a vertical line through \([i + j]P\) and \(-[i + j]P\) with

\[
(v) = ([i + j]P) + (-[i + j]P) - 2(P_\infty).
\]

- Compute

\[
(l) - (v) = ([i]P) + ([j]P) - ([i + j]P) - (P_\infty).
\]
Miller’s formula

▶ Remember

\[(f_i, P f_j, P) = (f_{i+j}, P) + ([i + j] P) - ([i] P) - ([j] P) + (P_\infty)\]

▶ and

\[(l) - (v) = ([i] P) + ([j] P) - ([i + j] P) - (P_\infty).\]

We get an equation of divisors

\[(f_{i+j}, P) = (f_i, P f_j, P) + (l) - (v).\]

▶ For the functions we get **Miller’s formula**

\[f_{i+j}, P = f_i, P f_j, P \cdot l/v.\]

We can choose normalized functions, i.e. \(f_{1, P} = 1.\)
Computing pairings (Miller’s algorithm)

We can use the special cases \( i = j \) and \( j = 1 \) to compute the function \( f_{r,P} \) in a square-\&-multiply-like manner.

- **Square step:**
  
  \[
  f_{2i,P} = f_{i,P}^2 \cdot l_{[i]P,[i]P} \cdot v_{[2i]P}.
  \]

- **Multiply step:**
  
  \[
  f_{i+1,P} = f_{i,P} f_{1,P} \cdot l_{[i]P,P} \cdot v_{[i+1]P}.
  \]

- \( l_{R,S} \): line through \( R \) and \( S \), tangent if \( R = S \),

- \( v_R \): vertical line through \( R \).
Computing pairings (Miller’s algorithm)

**Input:** \( P \in E[r](\mathbb{F}_p), Q \in E[r](\mathbb{F}_{p^k}), r = (r_m, \ldots, r_0) \)

**Output:** \( f_{r,P}(Q) \)

\[
R \leftarrow P, \quad f \leftarrow 1
\]

for \((i \leftarrow m - 1; \ i \geq 0; \ i \leftarrow \)
\[
\begin{align*}
f & \leftarrow f^2 \frac{l_{R,R}(Q)}{v_{[2]} R(Q)} \\
R & \leftarrow [2] R \\
\text{if } (r_i = 1) \text{ then} \\
\quad f & \leftarrow f \frac{l_{R,P}(Q)}{v_{R+P}(Q)} \\
\quad R & \leftarrow R + P
\end{align*}
\]
end if
end for

return \( f \)
Computing pairings (Miller’s algorithm)

For Miller’s algorithm we need arithmetic in $E(\mathbb{F}_p)$ and $\mathbb{F}_{p^k}$.

- If $k$ is too large, we can’t compute pairings this way.
- We need special curves with small $k$ to be able to compute in $\mathbb{F}_{p^k}$.
- See tomorrow’s talk for methods how to find such curves.
Tripartite key agreement

Tanja, Dan and Nigel would like to share a common secret key.

- They each choose a secret \( a, b, c \in \mathbb{Z}_r \) resp.
- They compute \( aP, bP, cP \) resp. and send it to the other two.
Using a pairing $e$ the three can compute a common secret key using their secrets:

$$e(aP, bP)^c = e(bP, cP)^a = e(aP, cP)^b = e(P, P)^{abc}.$$ 

Only one round of communication is needed.
Symmetric Pairings

If $k > 1$ we can use the reduced Tate pairing on supersingular curves to construct a symmetric pairing

$$e : E[r](\mathbb{F}_p) \times E[r](\mathbb{F}_p) \rightarrow \mu_r \subseteq \mathbb{F}_{p^k}^*,$$

s.t. $e(P, P) \neq 1$.

- Supersingular elliptic curves have $k \leq 6$.
- Supersingular elliptic curves have distortion maps.
- A distortion map is an endomorphism $\phi$ of $E$ for which $\phi(P) \not\in E(\mathbb{F}_p)$. If $E(\mathbb{F}_{p^k})$ has no points of order $r^2$ then

$$e(P, P) := t_r(P, \phi(P)) \neq 1.$$
BLS signatures

Using pairings it is possible to define a signature scheme with very short signatures.

- System parameters are the pairing

\[ e : \langle P \rangle \times \langle Q \rangle \rightarrow \mu_r \subseteq \mathbb{F}_{p^k}^* , \]

points \( P \in E[r](\mathbb{F}_p) \), \( Q \in E[r](\mathbb{F}_{p^k}) \) s.t. \( e(P, Q) \neq 1 \) and a hash function

\[ H : \{0, 1\}^* \rightarrow E[r](\mathbb{F}_p). \]
BLS signatures

- To sign messages, Tanja chooses a private key $x_T \in \mathbb{Z}_r$ and publishes her public key $Q_T = [x_T]Q$.
- She signs the message $M \in \{0, 1\}^*$ by computing $H(M) \in E[r](\mathbb{F}_p)$ and the signature

$$\sigma = [x_T]H(M).$$

- To verify, anyone may take $Q_T$ and check if

$$e(\sigma, Q) = e(H(M), Q_T).$$

$$e(\sigma, Q) = e([x_T]H(M), Q) = e(H(M), [x_T]Q) = e(H(M), Q_T).$$
The signature $\sigma$ is just one point in $E[r](\mathbb{F}_p)$, so can be represented by 2 $\mathbb{F}_p$-elements.

Compare this to the signatures from Tanja's 1st talk. There the signature was $(R, S)$, where

$$R = [k]P, \quad S = s_\text{sym} + kH([k]P) \mod r.$$ 

This is 1 element of size $r$ larger.

If we represent points in $E(\mathbb{F}_p)$ by their $x$-coordinate only, this might be about half the size of the whole signature.
The Tate pairing is a bit slow...
Reducing the loop length - variants of the Tate pairing

It is possible to reduce the loop length in Miller’s algorithm significantly and still get a pairing.

- **Ate pairing:**

\[
\text{ate} : E[r](\mathbb{F}_{p^k}) \times E[r](\mathbb{F}_p) \rightarrow \mu_r \subset \mathbb{F}_{p^k}^*,
\]

\[
(Q, P) \mapsto f_{T,Q}(P) \frac{p^{k-1}}{r}.
\]

Here \( T = t - 1 \) where \( t \) is the trace of Frobenius, i.e. the number of bits in \( T \) is about half that of \( r \).
Reducing the loop length - variants of the Tate pairing

- Twisted ate pairing: If $E$ has a twist $E'$ of degree $d$, we get a pairing

$$\eta: E[r](\mathbb{F}_p) \times E'[r](\mathbb{F}_{p^{k/d}}) \rightarrow \mu_r \subset \mathbb{F}_{p^k}^*,$$

$$(P, Q') \mapsto f_{T^e, P}(\phi(Q'))^{p^k - 1 \over r}.$$

We have $T = t - 1$ and $T^e \equiv \zeta_m \mod r$, $e = k/m$, $m = \gcd(k, d)$. $\phi: E'[r](\mathbb{F}_{p^{k/d}}) \rightarrow E[r](\mathbb{F}_{p^k})$. 
Reducing the loop length - variants of the Tate pairing

- There are other choices for the loop variable which even give shorter loops depending on the type of curves one is using.
- Shortest loops right now are of length $1/\varphi(k)$ times the length of $r$. Corresponding pairings are called optimal pairings.
For more information we refer to