Pairings for Cryptography

Michael Naehrig

Technische Universiteit Eindhoven
michael@cryptojedi.org

Nijmegen, 11 December 2009
Pairings

A pairing is a bilinear, non-degenerate map

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

where \((G_1, +), (G_2, +), (G_3, \cdot)\) are abelian groups.

- **bilinear:**
  \[
  e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1),
  \]
  \[
  e(P_1, Q_1 + Q_2) = e(P_1, Q_1)e(P_1, Q_2),
  \]
  i.e. \(e(aP, Q) = e(P, Q)^a = e(P, aQ), a \in \mathbb{Z} \).

- **non-degenerate:** given \(0 \neq P \in G_1\) there is a \(Q \in G_2\) with \(e(P, Q) \neq 1\).

Cryptographic applications require \(e\) to be efficiently computable and the DLPs in \(G_1, G_2, G_3\) to be hard.
Applications of pairings in cryptography


- Construct crypto systems with certain special properties:
  - One-round tripartite key agreement (Joux-2000),
  - Identity-based, non-interactive key agreement (Ohgishi-Kasahara-2000),
  - Identity-based encryption (Boneh-Franklin-2001),
  - Hierarchical IBE (Gentry-Silverberg-2002),
  - Short signatures (Boneh-Lynn-Shacham-2001),
  - Searchable encryption (Boneh-Di Crescenzo-Ostrovsky-Persiano-2004),
  - Non-interactive proof systems (Groth-Sahai-2008),
  - much more...
Elliptic curves

Take an elliptic curve $E$ over $\mathbb{F}_q$ ($\text{char}(\mathbb{F}_q) = p > 3$) with

- Weierstrass equation

$$E : y^2 = x^3 + ax + b,$$

- $E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : y^2 = x^3 + ax + b\} \cup \{O\}$,
- $n = \#E(\mathbb{F}_q) = q + 1 - t$, $|t| \leq 2\sqrt{q}$,
- and $r \mid n$ a large prime divisor of $n$ ($r \neq p$).
- For $\mathbb{F} \supseteq \mathbb{F}_q$:

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F}^2 : y^2 = x^3 + ax + b\} \cup \{O\},$$

- $E = E(\overline{\mathbb{F}_q})$, $\overline{\mathbb{F}_q}$ an algebraic closure of $\mathbb{F}_q$.
- $E$ is an abelian group (written additively) with neutral element $O$. 
The set of $r$-torsion points on $E$ is

$$E[r] = \{ P \in E \mid [r]P = \mathcal{O} \} \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$  

Since $r \mid \#E(\mathbb{F}_q)$, we have $E(\mathbb{F}_q)[r] \neq \emptyset$. The embedding degree of $E$ w.r.t. $r$ is the smallest integer $k$ with

$$r \mid q^k - 1.$$  

For $k > 1$ we have

$$E[r] \subset E(\mathbb{F}_{q^k}),$$  

i.e. $E(\mathbb{F}_q)[r] \subseteq E(\mathbb{F}_{q^k})[r] = E[r]$.  

The reduced Tate pairing

Let $k > 1$. The reduced Tate pairing

$$t_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/[r] E(\mathbb{F}_{q^k}) \rightarrow \mu_r \subseteq \mathbb{F}_{q^k}^*,$$

$$(P, Q) \mapsto f_{r,P}(Q)^{\frac{q^k-1}{r}}$$

is a non-degenerate, bilinear map, where

- $f_{r,P}$ is a function with divisor $(f_{r,P}) = r(P) - r(O)$,
- $\mu_r$ is the subgroup of $r$-th roots of unity in $\mathbb{F}_{q^k}^*$.

The computation of the pairing has two stages:

- evaluation of the Miller function $f_{r,P}$ at $Q$,
- the final exponentiation to the power $(q^k - 1)/r$. 
Specific parameters for crypto

- $k$ should be small,
- DLPs in all groups must be hard,
- for efficiency reasons balance the security.

<table>
<thead>
<tr>
<th>Security level (bits)</th>
<th>Extension field size of $q^k$ (bits)</th>
<th>EC base point order $r$ (bits)</th>
<th>ratio $\rho \cdot k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>1248</td>
<td>160</td>
<td>7.8</td>
</tr>
<tr>
<td>112</td>
<td>2432</td>
<td>224</td>
<td>10.9</td>
</tr>
<tr>
<td>128</td>
<td>3248</td>
<td>256</td>
<td>12.7</td>
</tr>
<tr>
<td>192</td>
<td>7936</td>
<td>384</td>
<td>20.7</td>
</tr>
<tr>
<td>256</td>
<td>15424</td>
<td>512</td>
<td>30.1</td>
</tr>
</tbody>
</table>

ECRYPT II recommendations (2009), $\rho = \log(q) / \log(r)$. 
Small embedding degree

The embedding degree condition says

\[ r \mid q^k - 1, \ r \nmid q^m - 1, \ m < k \]

or

\[ q^k \equiv 1 \pmod{r}, \ q^m \not\equiv 1 \pmod{r}, \ m < k. \]

This means:

- \( k \) is the (multiplicative) order of \( q \) modulo \( r \),
- \( k \mid r - 1 \).

There are only \( \varphi(k) < k \) elements of order \( k \) mod \( r \). Given \( r \) and \( q \), it is very unlikely that \( q \) is one of them.

(Note: \( r \) has at least 160 bits.)
Pairing-friendly curves

Fix a suitable value for $k$ and find primes $r, p$ and a number $n$ with the following conditions:

- $n = p + 1 - t$, $|t| \leq 2\sqrt{p}$,
- $r \mid n$,
- $r \mid p^k - 1$,
- $t^2 - 4p = Dv^2 < 0$, $D, v \in \mathbb{Z}$, $D < 0$ squarefree, $|D|$ small enough to compute the Hilbert class polynomial in $\mathbb{Q}(\sqrt{D})$.

Given such parameters, a corresponding elliptic curve over $\mathbb{F}_p$ can be constructed by the CM method.

See Freeman, Scott, and Teske (A taxonomy of pairing-friendly elliptic curves) for an overview of construction methods and recommendations.
MNT curves and Freeman curves

- **MNT curves (2001):** $\rho \approx 1$ and $k \in \{3, 4, 6\}$.

  $$p(u) = 12u^2 - 1, \quad t(u) = -1 \pm 6u$$  
  $$p(u) = u^2 + u + 1, \quad t(u) = -u \text{ or } u + 1$$  
  $$p(u) = 4u^2 + 1, \quad t(u) = 1 \pm 2u$$

- **Freeman curves (2006):** $\rho \approx 1$ and $k = 10$.

  $$p(u) = 25u^4 + 25u^3 + 25u^2 + 10u + 3,$$
  $$t(u) = 10u^2 + 5u + 3.$$ 

- In both families, curves are very rare. Need to solve a Pell equation to find curves.

- $D$ is variable.
BN curves
(Barreto-N., 2005)

If \( u \in \mathbb{Z} \) such that
\[
\begin{align*}
p &= p(u) = 36u^4 + 36u^3 + 24u^2 + 6u + 1, \\
n &= n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1
\end{align*}
\]
are both prime, then there exists an ordinary elliptic curve

- with equation \( E : y^2 = x^3 + b, \ b \in \mathbb{F}_p \),
- \( r = n = \#E(\mathbb{F}_p) \) is prime, i.e. \( \rho \approx 1 \),
- the embedding degree is \( k = 12 \),
- \( t^2 - 4p(u) = -3(6u^2 + 4u + 1)^2 \).

BN curves are ideal for the 128-bit security level.
### Specific parameters

<table>
<thead>
<tr>
<th>Security level (bits)</th>
<th>Family</th>
<th>$r$ (bits)</th>
<th>$k$</th>
<th>$\rho$</th>
<th>$\rho \cdot k$</th>
<th>$\rho^k$ (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>MNT</td>
<td>208</td>
<td>6</td>
<td>1.00</td>
<td>6</td>
<td>1248</td>
</tr>
<tr>
<td>112</td>
<td>Fre</td>
<td>244</td>
<td>10</td>
<td>1.00</td>
<td>10</td>
<td>2440</td>
</tr>
<tr>
<td>128</td>
<td>BN</td>
<td>256</td>
<td>12</td>
<td>1.00</td>
<td>12</td>
<td>3072</td>
</tr>
<tr>
<td>192</td>
<td>KSS</td>
<td>384</td>
<td>16</td>
<td>1.25</td>
<td>20</td>
<td>7680</td>
</tr>
<tr>
<td>192</td>
<td>KSS</td>
<td>384</td>
<td>18</td>
<td>1.33</td>
<td>24</td>
<td>9216</td>
</tr>
<tr>
<td>256</td>
<td>Cyc</td>
<td>512</td>
<td>24</td>
<td>1.25</td>
<td>30</td>
<td>15360</td>
</tr>
</tbody>
</table>
Three groups

In practice, restrict the arguments of the Tate pairing to groups of prime order \( r \).

Assume \( r^2 \mid \# \mathbb{F}_{p^k} \), \( k > 1 \). Define:

- \( G_1 = \mathbb{F}_{p^k} [r] \cap \ker(\phi_p - [1]) = \mathbb{F}_p [r] \),
- \( G_2 = \mathbb{F}_{p^k} [r] \cap \ker(\phi_p - [p]) \),
- \( G_3 = \mu_r \subset \mathbb{F}_{p^k}^* \).

\( \phi_p \) is the \( p \)-power Frobenius on \( E \), i.e. \( \phi_p(x, y) = (x^p, y^p) \). It is \( \mathbb{F}_{p^k} [r] = G_1 \oplus G_2 \).

- If \( P \in \mathbb{F}_p [r] \), then \( t_r(P, P) = 1 \). Take \( Q \not\in \langle P \rangle = G_1 \).
- Can compute the Tate pairing on \( G_1 \times G_2 \) or on \( G_2 \times G_1 \).
Two choices

- **The reduced Tate pairing:**
  \[
  t_r : G_1 \times G_2 \rightarrow G_3, \\
  (P, Q) \mapsto f_{r,P}(Q) \frac{p^k - 1}{r}.
  \]

- **The ate pairing:** Let \( T = t - 1 \).
  \[
  a_T : G_2 \times G_1 \rightarrow G_3, \\
  (Q, P) \mapsto f_{T,Q}(P) \frac{p^k - 1}{r}.
  \]
Miller’s algorithm (Tate)

**Input:** \( P \in G_1, Q \in G_2, r = (r_m, \ldots, r_0)_2 \)

**Output:** \( t_r(P, Q) = f_{r,P}(Q)^{p^k-1}_r \)

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

\[
\text{for } (i \leftarrow m - 1; \ i \geq 0; \ i \rightarrow) \ \text{do}
\]

\[
f \leftarrow f^2 \frac{l_{R,R(Q)}}{v[2]_{R(Q)}}
\]

\[
R \leftarrow [2]R
\]

\[
\text{if } (r_i = 1) \ \text{then}
\]

\[
f \leftarrow f \frac{l_{R,P(Q)}}{v_{R+P(Q)}}
\]

\[
R \leftarrow R + P
\]

\[
\text{end if}
\]

\[
\text{end for}
\]

\[
f \leftarrow f^{p^k-1}_r
\]

**return** \( f \)
Miller’s algorithm (ate)

**Input:** \( P \in G_1, Q \in G_2, T = (t_m, \ldots, t_0)_2 \)

**Output:** \( a_T(P, Q) = f_{T,Q}(P)^{p^k-1}_r \)

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

\textbf{for} \ (i \leftarrow m - 1; \ i \geq 0; \ i \rightarrow -) \ 	extbf{do}

\[ f \leftarrow f^2 l_{R,R}(P) \]

\[ R \leftarrow [2] R \]

\textbf{if} \ (t_i = 1) \ 	extbf{then}

\[ f \leftarrow f \frac{l_{R,Q}(P)}{v_{[2]R}(P)} \]

\[ R \leftarrow R + Q \]

\textbf{end if}

\textbf{end for}

\[ f \leftarrow f^{p^k-1}_r \]

\textbf{return} \ f
Line functions

- Line functions correspond to the lines in the point doubling/addition,

- \( l_{P_1,P_2} \): line through \( P_1 \) and \( P_2 \), tangent if \( P_1 = P_2 \),

- \( v_{P_3} \): vertical line through \( P_3 = P_1 + P_2 \).

\[ E \]

(a) addition

(b) doubling
The final exponentiation

Let $\Phi_d$ be the $d$-th cyclotomic polynomial.

- We have
  \[ X^k - 1 = \prod_{d|k} \Phi_d(X). \]

- $r \mid p^k - 1$, $r \nmid p^d - 1$ for $d < k \iff r \mid \Phi_k(p)$.

- Write the final exponent as:
  \[ \frac{p^k - 1}{r} = \prod_{d|k, d \neq k} \Phi_d(p) \cdot \frac{\Phi_k(p)}{r}. \]

Let $e \mid k$, $e \neq k$, then $\alpha^{(p^k - 1)/r} = 1$ for all $\alpha \in \mathbb{F}_{p^e}$ since $(p^e - 1) \mid \prod_{d|k, d \neq k} \Phi_d(p)$.

Factors in proper subfields of $\mathbb{F}_{p^k}$ are mapped to 1 by the final exponentiation.
The final exponentiation ($k$ even)

$$
\frac{p^k - 1}{r} = \left(p^{k/2} - 1\right) \frac{p^{k/2} + 1}{\Phi_k(p)} \cdot \frac{\Phi_k(p)}{r}.
$$

- Use $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(\alpha)$, $\alpha^2 = \beta$, $\beta$ a non-square in $\mathbb{F}_{p^{k/2}}$.
  For $f = f_0 + f_1 \alpha \in \mathbb{F}_{p^k}$: $(f_0 + f_1 \alpha)^{p^{k/2}} = f_0 - f_1 \alpha$,
  and $(f_0 + f_1 \alpha)^{p^{k/2}-1} = (f_0 - f_1 \alpha)/(f_0 + f_1 \alpha)$.
- $(p^{k/2} + 1)/\Phi_k(p)$ is a sum of $p$-powers, use the $p$-power Frobenius automorphism.
  $k = 12$: $f(p^6 + 1)/r = f(p^2 + 1) \cdot \frac{p^4 - p^2 + 1}{r} = ((fp)^p . f)(p^4 - p^2 + 1)/r$.
- The last part is done with multi-exponentiation or by finding a good addition chain for $\Phi_k(p)/r$. 
Using a twist to represent $G_2$

Here: A twist $E'$ of $E$ is a curve isomorphic to $E$ over $\mathbb{F}_{p^k}$.

- A twist is given by
  $E' : y^2 = x^3 + (a/\omega^4)x + (b/\omega^6)$, $\omega \in \mathbb{F}_{p^k}$
  with isomorphism
  $$\psi : E' \rightarrow E, \ (x', y') \mapsto (\omega^2 x', \omega^3 y').$$

- If $E'$ is defined over $\mathbb{F}_{p^{k/d}}$ and $\psi$ is defined over $\mathbb{F}_{p^k}$
  and no smaller field, $d$ is called the degree of $E'$.

- Define $G'_2 := E'(\mathbb{F}_{p^{k/d}})[r]$, then $\psi : G'_2 \rightarrow G_2$ is a group
  isomorphism.

- Points in $G_2$ have a special form.
Maximal possible twist degrees

<table>
<thead>
<tr>
<th>$d$</th>
<th>$j(E)$, $a, b$</th>
<th>fields of definition for powers of $\omega$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$\not\in {0, 1728}$, $a \neq 0, b \neq 0$</td>
<td>$\omega^2 \in \mathbb{F}<em>{q^{k/2}}$ $\omega^3 \in \mathbb{F}</em>{q^k} \setminus \mathbb{F}_{q^{k/2}}$</td>
</tr>
<tr>
<td>4</td>
<td>1728, $a \neq 0, b = 0$</td>
<td>$\omega^4 \in \mathbb{F}<em>{q^{k/4}}, \omega^2 \in \mathbb{F}</em>{q^{k/2}}$ $\omega^3 \in \mathbb{F}<em>{q^k} \setminus \mathbb{F}</em>{q^{k/2}}$</td>
</tr>
<tr>
<td>6</td>
<td>0, $a = 0, b \neq 0$</td>
<td>$\omega^6 \in \mathbb{F}<em>{q^{k/6}}, \omega^3 \in \mathbb{F}</em>{q^{k/3}}$ $\omega^2 \in \mathbb{F}_{q^{k/2}}$</td>
</tr>
</tbody>
</table>

$E': y^2 = x^3 + \left(\frac{a}{\omega^4}\right)x + \left(\frac{b}{\omega^6}\right)$

$\psi: E' \rightarrow E, (x', y') \mapsto (\omega^2 x', \omega^3 y')$
Advantages of using twists

If $E$ has a twist of degree $d$ and $d \mid k$:

- Replace all curve arithmetic in $G_2$ (over $\mathbb{F}_{p^k}$) by curve arithmetic in $G'_2$ (over $\mathbb{F}_{p^{k/d}}$)
- For $d > 2$, curve arithmetic is faster since $a = 0$ or $b = 0$.
- For even $k$, the $x$-coordinates of points in $G_2$ lie in $\mathbb{F}_{p^{k/2}}$, i.e. the vertical line function values $v_{P_3}(Q) = x_Q - x_3$ lie in $\mathbb{F}_{p^{k/2}}$ and can be omitted.
- Can use the twisted ate pairing $(e = k/d$ and $T_e = (t - 1)^e \mod r)$:

$$\eta_{T_e} : G_1 \times G_2 \to G_3, \ (P, Q) \mapsto f_{T_e, P}(Q)^{(p^k - 1)/r}.$$ 

For $d > 2$, can have $\log(T_e) < \log(r)$. 
Loop shortening

There are several possibilities to reduce the number of iterations in Miller’s algorithm:

- Can take $T^j_e \mod r$ for $1 \leq j \leq d - 1$ instead of $T_e$ in the twisted ate pairing. Choose the shortest non-trivial power.

- For the ate pairing, can replace $T$ by $T^j \mod r$ for $1 \leq j \leq k - 1$ to possibly get a shorter loop.

- More combinations are possible, often leading to optimal pairings with a minimal loop length of $\log(r)/\varphi(k)$.

- For BN curves, the R-ate pairing is optimal:

$$R(Q, P) = \left( f_{c, Q}(P)(f_{c, Q}(P)l_{[c]Q, Q(P)})^p \cdot l_{\phi_p([c]Q+Q), [c]Q(P)} \right)^{(p^{12} - 1)/n},$$

where $c = 6u + 2$. 
Line functions for ate pairings

\[ f \leftarrow f \cdot l_{R,Q}(P), \quad R \leftarrow R + Q \]

Do curve arithmetic in Miller’s algorithm in \( G'_2 \). Replace points \( R, Q \in G_2 \) by corresponding points \( R', Q' \in G'_2 \).

- Using the slope on the twist:

\[
\lambda = \frac{y_R - y_Q}{x_R - x_Q} = \frac{\omega^3 y_{R'} - \omega^3 y_{Q'}}{\omega^2 x_{R'} - \omega^2 x_{Q'}} = \omega \frac{y_{R'} - y_{Q'}}{x_{R'} - x_{Q'}} = \omega \lambda'
\]

- Computing the line function on the twist:

\[
l_{R,Q}(P) = y_R - y_P - \lambda (x_R - x_P) \\
= \omega^3 y_{R'} - \omega^3 y_{P'} - \omega \lambda' (\omega^2 x_{R'} - \omega^2 x_{P'}) \\
= \omega^3 (y_{R'} - y_{P'} - \lambda (x_{R'} - x_{P'})) = \omega^3 \cdot l'_{R',Q'}(P')
\]
Choice of coordinates

For “real” implementations, one tries to avoid inversions by using projective coordinates.

- Can do pairing computation with only 1 finite field inversion (needed in the final exponentiation).
- Can avoid inversions completely when using compressed representation of pairing values.
- The best choice of coordinates is different for different classes of curves.
- For the fastest explicit formulas to compute the DBL and ADD steps in Miller’s algorithm on curves with twists of degree $d > 2$, see preprint *Faster Pairing Computations on Curves with High-Degree Twists* (joint work with Craig Costello and Tanja Lange, will be out soon).
Thanks for your attention

- Database and web interface to get and compute parameters of BN curves:
  http://www.ti.rwth-aachen.de/research/cryptography/bncurves.php

- C-Implementation of several pairings on BN curves:
  http://www.cryptojedi.org/crypto

michael@cryptojedi.org