Methods for Constructing Pairing-Friendly Elliptic Curves

David Freeman

University of California, Berkeley, USA

10th Workshop on Elliptic Curve Cryptography
Fields Institute, Toronto, Canada
19 September 2006
Outline

1. All about pairings
   - What is a pairing?
   - Pairings in cryptography
   - Pairings on elliptic curves

2. How to construct pairing-friendly ordinary elliptic curves
   - The MNT strategy
   - The Cocks-Pinch strategy
   - The Dupont-Enge-Morain strategy

3. The state of the art
All about pairings

- What is a pairing?
- Pairings in cryptography
- Pairings on elliptic curves

How to construct pairing-friendly ordinary elliptic curves

- The MNT strategy
- The Cocks-Pinch strategy
- The Dupont-Enge-Morain strategy

The state of the art
What is a pairing?

- Let $G_1, G_2, G_T$ be finite cyclic groups used in cryptography.
- A *cryptographic pairing* is a bilinear, nondegenerate map

$$e : G_1 \times G_2 \rightarrow G_T.$$  

- To be useful in applications, we need:
  1. the discrete logarithm problem (DLP) in $G_1, G_2,$ and $G_T$ to be computationally infeasible, and
  2. the pairing to be easy to compute.

- Most common situation:
  - $G_1, G_2$ are prime-order subgroups of an elliptic curve $E / \mathbb{F}_q$;
  - $G_T$ is a prime-order subgroup of $\mathbb{F}_q^\times$ (for some $k$).
  - $e$ is (a variant of) the *Weil pairing* or *Tate pairing* on $E$. 

Uses of pairings in cryptography

- Attack on ECDLP for supersingular elliptic curves (Menezes-Okamoto-Vanstone).
  - Map DLP on elliptic curve to (perhaps easier) DLP in finite field.
- One-round 3-way key exchange (Joux).
- Identity-based encryption (Sakai-Ohgishi-Kasahara; Boneh-Franklin).
- Short digital signatures (Boneh-Lynn-Shacham).
- Many other applications...
  - Group signatures, batch signatures, aggregate signatures, threshold cryptography, authenticated encryption, broadcast encryption, etc.
Pairings on elliptic curves

- Elliptic curve pairings used in cryptography are of the form

$$e : E[r] \times E[r] \rightarrow \mathbb{F}_p^\times,$$

where $E$ is an elliptic curve defined over a finite field $\mathbb{F}_p$.

- $k$ is the embedding degree of $E$ (with respect to $r$).
  - $k$ is the smallest integer such that $r \mid p^k - 1$.
  - $k$ is the order of $p$ in $(\mathbb{Z}/r\mathbb{Z})^\times$.
  - Want $k$ large enough so that DLP in $\mathbb{F}_p^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.

- $r$ is a large prime dividing $\#E(\mathbb{F}_p)$
  - Define $\rho = \log p / \log r$.
  - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want $\rho$ small to save bandwidth.
  - If curve has prime order, $\rho \approx 1$. 

David Freeman
Methods for Constructing Pairing-Friendly Elliptic Curves
Bal., Kob.: If $E/\mathbb{F}_p$ is a “random” elliptic curve with an order-$r$ subgroup, then $k \sim r$.

- Pairing computation on random curves is totally infeasible:
  - If $r \sim p \sim 2^{160}$, pairing is computed in field of size $2^{2^{160}}$.

A **pairing-friendly curve** is an elliptic curve with a large prime-order subgroup ($\rho \leq 2$) and small embedding degree ($k < 40$).

Problem: construct pairing-friendly elliptic curves for specified values of $k$ and number of bits in $r$.

- MOV: Supersingular elliptic curves always have $k \leq 6$ (and $k = 2$ if defined over a prime field).
- Pairing-friendly curves must be ordinary for $k > 6$ (and $k \neq 2$ if defined over a prime field).
Outline

1. All about pairings
   - What is a pairing?
   - Pairings in cryptography
   - Pairings on elliptic curves

2. How to construct pairing-friendly ordinary elliptic curves
   - The MNT strategy
   - The Cocks-Pinch strategy
   - The Dupont-Enge-Morain strategy

3. The state of the art
The CM Method of Curve Construction

- Main tool: Complex Multiplication method of curve construction (Atkin, Morain).
- For given square-free $D > 0$, CM method constructs elliptic curve with CM by $\mathbb{Q}(\sqrt{-D})$.
  - Used to construct curves with specified number of points.
- Running time depends on the class number $h_D$ of $\mathbb{Q}(\sqrt{-D})$.
  - Bottleneck is computing the Hilbert class polynomial, a polynomial of degree $h_D$.
  - Best known algorithms run in (roughly) $O(h_D^2) = O(D)$ (Enge).
- Can be efficiently implemented if $h_D$ not too large.
  - Current record is $h_D = 10^5$. 

David Freeman
Methods for Constructing Pairing-Friendly Elliptic Curves
Recall: The trace of $E/F_q$ satisfies $\#E(F_q) = q + 1 - t$.

To apply the CM method: Fix $D, k$. Look for $t, r, q$ (representing trace, order of subgroup, and size of field) satisfying

1. $q, r$ prime;
2. $r$ divides $q + 1 - t$ (formula for number of points);
3. $r$ divides $q^k - 1$ (embedding degree $k$);
4. $Dy^2 = 4q - t^2$ for some integer $y$.

For such $t, r, q$, if $h_D$ is not too large ($\sim 10^5$) we can construct an elliptic curve $E$ over $F_q$ with an order-$r$ subgroup and embedding degree $k$. 

Observations about the CM Method

- Barreto, Lynn, Scott: The embedding degree condition $r \mid q^k - 1$ can be replaced with $r \mid \Phi_k(t - 1)$, where $\Phi_k$ is the $k$-th cyclotomic polynomial. Why?
  - $k$ smallest such that $r \mid q^k - 1$ implies $r \mid \Phi_k(q)$.
  - $r$ divides $q + 1 - t$ implies $q \equiv t - 1 \pmod{r}$.

- To construct families of curves: Parametrize $t, r, q$ as polynomials: $t(x), r(x), q(x)$. Construct curves by finding integer solutions $(x, y)$ to the “CM equation”

$$Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - (t(x) - 2)^2.$$  

- $h(x)$ is a “cofactor” satisfying $\#E(\mathbb{F}_q) = h(x)r(x)$. 
3 different strategies

For fixed $D, k$, we look for polynomials $t(x), r(x), h(x)$ satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$$

for some $(x, y)$.

1. **Miyaji-Nakabayashi-Takano**: Choose $t(x), h(x)$, compute $r(x)$ satisfying divisibility conditions, solve CM equation in 2 variables $x, y$.

2. **Cocks-Pinch**: Choose $r(x)$, compute $t(x), h(x)$ satisfying divisibility conditions, compute $y(x)$ satisfying CM equation.

3. **Dupont-Enge-Morain**: Choose $D, y$, use resultants to find $t$ and $r$ simultaneously, compute $h$ such that CM equation is satisfied.
Outline

1. All about pairings
   - What is a pairing?
   - Pairings in cryptography
   - Pairings on elliptic curves

2. How to construct pairing-friendly ordinary elliptic curves
   - The MNT strategy
   - The Cocks-Pinch strategy
   - The Dupont-Enge-Morain strategy

3. The state of the art
Overview of the MNT strategy

- Recall: for fixed $D$, $k$, we are looking for polynomials $t(x), r(x), h(x)$ satisfying certain divisibility conditions and the CM equation

\[ Dy^2 = 4h(x)r(x) - (t(x) - 2)^2 \]

for some $(x, y)$.

- MNT strategy: Choose $t(x), h(x)$, compute $r(x)$ satisfying divisibility conditions, solve CM equation in 2 variables $x, y$.

- Good for constructing curves of prime order.
- Only 5 possible embedding degrees: $k = 3, 4, 6, 10, 12$.
- Curves are usually sparse.
The MNT strategy

- **Strategy 1:** First used by Miyaji-Nakabayashi-Takano; also used by Scott-Barreto, Barreto-Naehrig, F.
  1. Fix $D$, $k$, and choose polynomials $t(x)$, $h(x)$.
     - $h(x) = 1$ if searching for curves of prime order.
  2. Choose $r(x)$ an irreducible factor of $\Phi_k(t(x) - 1)$.
  3. Compute $q(x) = h(x)r(x) + t(x) - 1$.
  4. Find integer solutions $(x, y)$ to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
  5. If $q(x)$, $r(x)$ are both prime, use CM method to construct elliptic curve over $\mathbb{F}_{q(x)}$ with $h(x)r(x)$ points.

- For the rest of this section, we will assume $h(x)$ is a constant.
Obstacles to the MNT strategy

- Step 4 is the difficult part: finding integer solutions \((x, y)\) to
  \[ Dy^2 = 4hr(x) - (t(x) - 2)^2. \]
- If \(f(x) = 4hr(x) - (t(x) - 2)^2\) has degree \(\geq 3\) and no multiple roots, then \(Dy^2 = f(x)\) has only a finite number of integer solutions! (Siegel’s Theorem)
- Upshot: need to choose \(t(x), r(x)\) so that \(f(x)\) is quadratic or has multiple roots.
- This is hard to do for \(k > 6\), since \(\text{deg } r(x)\) must be a multiple of \(\text{deg } \Phi_k > 2\).
The MNT solution for $k = 3, 4, 6$

- Goal: Choose $t(x)$, find factor $r(x)$ of $\Phi_k(t(x) - 1)$, such that $f(x) = 4hr(x) - (t(x) - 2)^2$ is quadratic.

- Solution:
  1. Choose $t(x)$ linear; then $r(x)$ is quadratic, and so is $f(x)$.
  2. Use standard algorithms to find solutions $(x, y)$ to $Dy^2 = f(x)$.
  3. If no solutions of appropriate size, or $q(x)$ or $r(x)$ not prime, choose different $D$ and try again.

- Since construction depends on solving a Pell-like equation, MNT curves of prime order are sparse (Luca-Shparlinski).

- Scott-Barreto extend MNT idea by allowing “cofactor” $h(x) \neq 1$, so that $\#E(\mathbb{F}_q) = h(x)r(x)$.
  - Find many more suitable curves than original MNT construction.
Goal: Choose $t(x)$, find factor $r(x)$ of $\Phi_{12}(t(x) - 1)$, such that $f(x) = 4r(x) - (t(x) - 2)^2$ has a multiple root.
   - All irreducible factors of $\Phi_{12}(t(x) - 1)$ must have $4 \mid$ degree.
   - No obvious solutions if $t(x)$ linear.

Galbraith-McKee-Valença: Characterized quadratic $t(x)$ such that $\Phi_{12}(t(x) - 1)$ factors into two quartics.
One of these $t(x)$ gives the desired multiple root!
   - CM equation becomes $Dy^2 = 3(6x^2 + 4x + 1)^2$.

BN curves are not sparse; i.e. easy to specify bit size of $q$. 
Our solution for $k = 10$

- Goal: Choose $t(x)$, find factor $r(x)$ of $\Phi_{10}(t(x) - 1)$, such that $f(x) = 4r(x) - (t(x) - 2)^2$ is quadratic.
  - All irreducible factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid$ degree.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and $t^2$ cancel out.
  - Smallest possible case: $\text{deg } r = 4$, $\text{deg } t = 2$.
- Galbraith-McKee-Valença: Characterized quadratic $t(x)$ such that $\Phi_{10}(t(x) - 1)$ factors into two quartics.
  - One of these $t(x)$ gives the desired cancellation!
- Construct curves via Pell-like equation as in MNT solution.
  - Like MNT curves, $k = 10$ curves are expected to be sparse.
Outline

1. All about pairings
   - What is a pairing?
   - Pairings in cryptography
   - Pairings on elliptic curves

2. How to construct pairing-friendly ordinary elliptic curves
   - The MNT strategy
   - The Cocks-Pinch strategy
   - The Dupont-Enge-Morain strategy

3. The state of the art
Overview of the Cocks-Pinch strategy

- Recall: for fixed $D$, $k$, we are looking for polynomials $t(x)$, $r(x)$, $h(x)$ satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$$

for some $(x, y)$.

- CP strategy: Choose $r(x)$, compute $t(x)$, $h(x)$ satisfying divisibility conditions, compute $y(x)$ satisfying CM equation for any $x$.
  - Good for constructing curves with arbitrary $k$.
  - Can’t construct curves of prime order; usually $\rho \approx 2$.
  - Many curves possible, easy to specify bit sizes.
Strategy 2, as first suggested by Cocks-Pinch:

1. Fix $D$, $k$, and choose a prime $r$.
   - Require that $k$ divides $r - 1$ and $-D$ is a square mod $r$.
2. Compute $t = 1 + x^{(r-1)/k}$ for $x$ a generator of $(\mathbb{Z}/r\mathbb{Z})^\times$.
3. Compute $y = (t - 2)/\sqrt{-D}$ (mod $r$).
4. Compute $q = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
5. If $q$ is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_q$ with an order-$r$ subgroup.

$y$ is constructed so that CM equation $Dy^2 = 4hr - (t - 2)^2$ is automatically satisfied.

Since $t$, $y$ are essentially random integers in $[0, r)$, $q \approx r^2$, so $\rho \approx 2$. 
Extending the Cocks-Pinch strategy

- Idea of Barreto-Lynn-Scott, Brezing-Weng: do same construction with $r(x)$, $q(x)$, $t(x)$ polynomials.

1. Fix $D$, $k$, and choose an irreducible polynomial $r(x)$.
   - Let $K$ be the number field $\mathbb{Q}[x]/(r(x))$.
   - Require that $\zeta_k, \sqrt{-D} \in K$.
2. Choose $t(x)$ to be a polynomial representing $1 + \zeta_k \in K$.
3. Set $y(x)$ to be a polynomial representing $(t(x) - 2)/\sqrt{-D} \in K$.
4. Compute $q(x) = (t(x)^2 + Dy(x)^2)/4$ (in $\mathbb{Q}[x]$).
5. If $q(x)$ is an integer and $q(x)$, $r(x)$ are prime, use CM method to construct elliptic curve over $\mathbb{F}_{q(x)}$ with an order-$r(x)$ subgroup.
Advantages of the extended Cocks-Pinch method

- For large $x$, $\rho \approx \deg q / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg q \leq 2 \deg r - 2$.
  - Can always get $\rho < 2$, improving on basic method.
  - With clever choices of $r(x), t(x)$, $\rho$ can be decreased even further.
  - Best current results (F.): $\rho = \frac{k+1}{k-1}$ for $k$ prime $\equiv 3$ (mod 4).
- No restrictions on $k$, and many values of $x, D$ produce curves.
  - Compare with MNT strategy: $k \leq 12$, and curves are sparse.
1. All about pairings
   - What is a pairing?
   - Pairings in cryptography
   - Pairings on elliptic curves

2. How to construct pairing-friendly ordinary elliptic curves
   - The MNT strategy
   - The Cocks-Pinch strategy
   - The Dupont-Enge-Morain strategy

3. The state of the art
Overview of the Dupont-Enge-Morain strategy

- Recall: for fixed $D, k$, we are looking for polynomials $t(x), r(x), h(x)$ satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$$

for some $(x, y)$.

- DEM strategy: Choose $D, y$, use resultants to find $t$ and $r$ simultaneously, compute $h$ such that CM equation is satisfied.
  - Good for constructing curves with arbitrary $k$.
  - Can’t construct curves of prime order; usually $\rho \approx 2$.
  - Has not been generalized to produce families of curves.
Strategy 3, as proposed by Dupont-Enge-Morain:

1. Choose $D, y$, compute resultant

\[
\text{Res}_t(\Phi_k(t - 1), Dy^2 - (t - 2)^2).
\]

2. If resultant has a large prime factor $r$, then can compute $t$ such that $\Phi_k(t - 1) \equiv Dy^2 - (t - 2) \equiv 0 \pmod{r}$.

3. Compute $q = (t^2 + Dy^2)/4$.

4. If $q$ is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_q$ with an order-$r$ subgroup.

Since $t$ is essentially random in $[0, r)$, $q \approx r^2$, so $\rho \approx 2$.

Not yet generalized to find polynomials $t(x), r(x), q(x)$ producing families of curves.
Outline

1. All about pairings
   - What is a pairing?
   - Pairings in cryptography
   - Pairings on elliptic curves

2. How to construct pairing-friendly ordinary elliptic curves
   - The MNT strategy
   - The Cocks-Pinch strategy
   - The Dupont-Enge-Morain strategy

3. The state of the art
3 different strategies

1. **MNT strategy:**
   - Good for constructing curves of prime order.
   - Only 5 possible embedding degrees ($k = 3, 4, 6, 10, 12$).
   - Curves are usually sparse.

2. **CP strategy:**
   - Good for constructing curves with arbitrary $k$.
   - Can’t construct curves of prime order ($1 < \rho \leq 2$).
   - Many curves possible, easy to specify bit sizes.

3. **DEM strategy:**
   - Constructs same types of curves as CP strategy.
   - No generalization to produce curves with $\rho < 2$. 
## The state of the art for various $k$

Smallest known $\rho$ value for even embedding degrees $k$ (limit as $q, r \to \infty$):

<table>
<thead>
<tr>
<th>$k$</th>
<th>$\rho$</th>
<th>Strategy</th>
<th>$k$</th>
<th>$\rho$</th>
<th>Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
<td>MNT</td>
<td>22</td>
<td>13/10</td>
<td>CP</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>MNT</td>
<td>24</td>
<td>5/4</td>
<td>CP</td>
</tr>
<tr>
<td>8</td>
<td>5/4</td>
<td>CP</td>
<td>26</td>
<td>7/6*</td>
<td>CP</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>MNT</td>
<td>28</td>
<td>4/3*</td>
<td>CP</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>MNT</td>
<td>30</td>
<td>3/2</td>
<td>CP</td>
</tr>
<tr>
<td>14</td>
<td>4/3*</td>
<td>CP</td>
<td>32</td>
<td>17/16*</td>
<td>CP</td>
</tr>
<tr>
<td>16</td>
<td>11/8*</td>
<td>CP</td>
<td>34</td>
<td>9/8*</td>
<td>CP</td>
</tr>
<tr>
<td>18</td>
<td>19/12*</td>
<td>CP</td>
<td>36</td>
<td>17/12</td>
<td>CP</td>
</tr>
<tr>
<td>20</td>
<td>11/8</td>
<td>CP</td>
<td>38</td>
<td>7/6</td>
<td>CP</td>
</tr>
</tbody>
</table>

* Indicates improvement over best previously published results (work in progress, joint with Mike Scott).