Pairing-Friendly Elliptic Curves of Prime Order

Michael Naehrig

Lehrstuhl für Theoretische Informationstechnik
RWTH Aachen University
mnaehrig@ti.rwth-aachen.de

Oberseminar Computer Security, b-it
Bonn, 12.01.2006

- This is joint work with

Paulo S. L. M. Barreto

pbarreto@larc.usp.br
(University of São Paulo, Brazil).

Outline

- What are pairing-friendly curves?
- Constructing pairing-friendly curves (review)
- Curves of prime order and embedding degree $k = 12$
- Notes on efficient implementation
- Open problems

Elliptic Curves

- Let $\mathbb{F}_q$ be a finite field, $q = p^f$, $p > 3$,
  $\overline{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$.
- For $a, b \in \mathbb{F}_q$ consider solutions (x, y) in $\overline{\mathbb{F}}_q^2$ of

$$y^2 = x^3 + ax + b.$$

Elliptic Curves

- Let $\mathbb{F}_q$ be a finite field, $q = p^f$, $p > 3$, $\overline{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$.
- For $a, b \in \mathbb{F}_q$ consider solutions (x, y) in $\overline{\mathbb{F}}_q^2$ of

$$y^2 = x^3 + ax + b.$$

- An *elliptic curve* over $\mathbb{F}_q$ is a set

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

where $a, b \in \mathbb{F}_q$ and the *discriminant* $\Delta \neq 0$, $\Delta = -16(4a^3 + 27b^2)$.

Elliptic Curves

- Let $\mathbb{F}_q$ be a finite field, $q = p^f$, $p > 3$,
  $\overline{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$.
- For $a, b \in \mathbb{F}_q$ consider solutions (x, y) in $\overline{\mathbb{F}}_q^2$ of

$$y^2 = x^3 + ax + b.$$

- An *elliptic curve* over $\mathbb{F}_q$ is a set

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

  where $a, b \in \mathbb{F}_q$ and the *discriminant* $\Delta \neq 0$,
  $\Delta = -16(4a^3 + 27b^2)$.
- $j = -1728(4a)^3/\Delta$ is the j*-invariant* of E.

Rational Points on Elliptic Curves

- For an extension $L \supseteq \mathbb{F}_q$

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

is called the set of L-*rational points* on E.

Rational Points on Elliptic Curves

- For an extension $L \supseteq \mathbb{F}_q$

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

  is called the set of L-*rational points* on E.
- Let $n = \#E(\mathbb{F}_q)$ be the number of $\mathbb{F}_q$-rational points.

Rational Points on Elliptic Curves

- For an extension $L \supseteq \mathbb{F}_q$

$$E(L) = \{(x,y) \in L^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

  is called the set of L-*rational points* on E.
- Let $n = \#E(\mathbb{F}_q)$ be the number of $\mathbb{F}_q$-rational points.
- Hasse's inequality states that

$$n = q + 1 - t, \ |t| \leq 2\sqrt{q}.$$

Rational Points on Elliptic Curves

- For an extension $L \supseteq \mathbb{F}_q$

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

  is called the set of L-*rational points* on E.
- Let $n = \#E(\mathbb{F}_q)$ be the number of $\mathbb{F}_q$-rational points.
- Hasse's inequality states that

$$n = q + 1 - t, \ |t| \leq 2\sqrt{q}.$$

- t is the trace of the *Frobenius endomorphism* ϕ_q ($\phi_q : (x, y) \mapsto (x^q, y^q)$).

The Group Law

- $E(L)$ is an abelian group.
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points in $E(L)$. Point addition is defined as follows.

The Group Law

- $E(L)$ is an abelian group.
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points in $E(L)$. Point addition is defined as follows.
  - $P + \mathcal{O} = \mathcal{O} + P = P$,

The Group Law

- $E(L)$ is an abelian group.
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points in $E(L)$. Point addition is defined as follows.
  - $P + \mathcal{O} = \mathcal{O} + P = P$,
  - $-P = (x_1, -y_1)$,

The Group Law

- $E(L)$ is an abelian group.
- Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points in $E(L)$. Point addition is defined as follows.
  - $P + \mathcal{O} = \mathcal{O} + P = P$,
  - $-P = (x_1, -y_1)$,
  - if $P \neq -Q$ let $P + Q = (x_3, y_3)$, then

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= (x_1 - x_3)\lambda - y_1, \end{aligned}$$

where

$$\lambda = \begin{cases} (y_1 - y_2)/(x_1 - x_2), & \text{if } P \neq Q, \\ (3x_1^2 + a)/2y_1, & \text{if } P = Q. \end{cases}$$

Elliptic Curve Cryptography

- Find a cyclic subgroup

$$\langle G \rangle \leq E(\mathbb{F}_q)$$

  with large prime order $r = \mathrm{ord}(G)$ and use it for DL-based crypto.

Elliptic Curve Cryptography

- Find a cyclic subgroup

$$\langle G \rangle \leq E(\mathbb{F}_q)$$

  with large prime order $r = \mathrm{ord}(G)$ and use it for DL-based crypto.

- The size of r should be at least 160 bits s.t. the ECDLP is considered to be hard.

Elliptic Curve Cryptography

- Find a cyclic subgroup

$$\langle G \rangle \leq E(\mathbb{F}_q)$$

  with large prime order $r = \mathrm{ord}(G)$ and use it for DL-based crypto.

- The size of r should be at least 160 bits s.t. the ECDLP is considered to be hard.

- The most efficient case occurs when $n = \#E(\mathbb{F}_q)$ is prime itself or is almost prime, i. e. $\rho = \log(q)/\log(r) \approx 1$.

Torsion Points

- Let $m \in \mathbb{Z}$, $P \in E$.
  - If $m > 0$ let $[m]P = P + P + \cdots + P$ (m times).
  - If $m < 0$ let $[m]P = [-m](-P)$.
  - $[0]P = \mathcal{O}$.

Torsion Points

- Let $m \in \mathbb{Z}$, $P \in E$.
  - If $m > 0$ let $[m]P = P + P + \cdots + P$ (m times).
  - If $m < 0$ let $[m]P = [-m](-P)$.
  - $[0]P = \mathcal{O}$.
- $E(L)[m] = \{P \in E(L) \mid [m]P = \mathcal{O}\}$ is the set of m-*torsion points* in $E(L)$.

Torsion Points

- Let $m \in \mathbb{Z}$, $P \in E$.
  - If $m > 0$ let $[m]P = P + P + \cdots + P$ (m times).
  - If $m < 0$ let $[m]P = [-m](-P)$.
  - $[0]P = \mathcal{O}$.
- $E(L)[m] = \{P \in E(L) \mid [m]P = \mathcal{O}\}$ is the set of m-*torsion points* in $E(L)$.
- If $p \nmid m$ we have $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Torsion Points

- Let $m \in \mathbb{Z}$, $P \in E$.
  - If $m > 0$ let $[m]P = P + P + \cdots + P$ (m times).
  - If $m < 0$ let $[m]P = [-m](-P)$.
  - $[0]P = \mathcal{O}$.
- $E(L)[m] = \{P \in E(L) \mid [m]P = \mathcal{O}\}$ is the set of m-*torsion points* in $E(L)$.
- If $p \nmid m$ we have $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Lemma: (Balasubramanian-Koblitz, 1998)

Let r be prime, $r \mid n$, $r \nmid q - 1$, $p \neq r$. Then:

$$E[r] \subseteq E(\mathbb{F}_{q^k}) \iff r \mid q^k - 1.$$

The Embedding Degree

- The smallest such k is called *embedding degree*.

The Embedding Degree

- The smallest such k is called *embedding degree*.
- Let $G \in E(\mathbb{F}_q)$ s.t. $r = \mathrm{ord}(G)$ is a large prime. Then $\langle G \rangle$ has embedding degree k, if
  - $r \mid q^k - 1$,
  - $r \nmid q^i - 1$ for $0 < i < k$.

The Embedding Degree

- The smallest such k is called *embedding degree*.
- Let $G \in E(\mathbb{F}_q)$ s.t. $r = \mathrm{ord}(G)$ is a large prime. Then $\langle G \rangle$ has embedding degree k, if
  - $r \mid q^k - 1$,
  - $r \nmid q^i - 1$ for $0 < i < k$.
- k is usually very large.
  (Balasubramanian-Koblitz, 1998)

The Embedding Degree

- The smallest such k is called *embedding degree*.
- Let $G \in E(\mathbb{F}_q)$ s.t. $r = \mathrm{ord}(G)$ is a large prime. Then $\langle G \rangle$ has embedding degree k, if
  - $r \mid q^k - 1$,
  - $r \nmid q^i - 1$ for $0 < i < k$.
- k is usually very large.
  (Balasubramanian-Koblitz, 1998)
- Note that the conditions mean that $\mathbb{F}_{q^k}^*$ contains the set μ_r of r-th roots of unity.

The Tate Pairing

- The *Tate pairing* is a map

$$\tau_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r,$$

  which is bilinear and nondegenerate.

The Tate Pairing

- The *Tate pairing* is a map

$$\tau_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r,$$

  which is bilinear and nondegenerate.
- To obtain a unique representative raise τ_r to the power $(q^k - 1)/r$.

The Tate Pairing

- The *Tate pairing* is a map

$$\tau_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r,$$

  which is bilinear and nondegenerate.
- To obtain a unique representative raise τ_r to the power $(q^k - 1)/r$.
- Under certain circumstances one may take $E(\mathbb{F}_{q^k})[r]$ as a set of representatives for the second argument.

The Tate Pairing

- The *Tate pairing* is a map

$$\tau_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r,$$

  which is bilinear and nondegenerate.
- To obtain a unique representative raise τ_r to the power $(q^k - 1)/r$.
- Under certain circumstances one may take $E(\mathbb{F}_{q^k})[r]$ as a set of representatives for the second argument.
- For applications the first argument is usually restricted to $E(\mathbb{F}_q)[r]$.

The Tate Pairing

- The *Tate pairing* is a map

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

  which is bilinear and nondegenerate.
- To obtain a unique representative raise τ_r to the power $(q^k - 1)/r$.
- Under certain circumstances one may take $E(\mathbb{F}_{q^k})[r]$ as a set of representatives for the second argument.
- For applications the first argument is usually restricted to $E(\mathbb{F}_q)[r]$.
- Obtain the *modified* Tate pairing

$$e_r : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] \rightarrow \mu_r \subseteq \mathbb{F}_{q^k}^*.$$

Pairing-Based Cryptography

- First cryptographic use of pairings were the MOV/FR attacks on the ECDLP (1993).

Pairing-Based Cryptography

- First cryptographic use of pairings were the MOV/FR attacks on the ECDLP (1993).
- But there are lots of constructive applications, e.g.
  - tripartite key agreement (Joux, 2000),
  - identity-based encryption (Boneh-Franklin, 2001),
  - short signatures (Boneh-Lynn-Shacham, 2001).

Pairing-Based Cryptography

- First cryptographic use of pairings were the MOV/FR attacks on the ECDLP (1993).
- But there are lots of constructive applications, e.g.
  - tripartite key agreement (Joux, 2000),
  - identity-based encryption (Boneh-Franklin, 2001),
  - short signatures (Boneh-Lynn-Shacham, 2001).
- Prerequisite: We need suitable elliptic curves to practically implement pairings.

Pairing-Friendly Curves

- An elliptic curve is *pairing-friendly* if it contains a subgroup $\langle G \rangle \subseteq E(\mathbb{F}_q)$ of (large) prime order r and embedding degree k where k is

Pairing-Friendly Curves

- An elliptic curve is *pairing-friendly* if it contains a subgroup $\langle G \rangle \subseteq E(\mathbb{F}_q)$ of (large) prime order r and embedding degree k where k is
  - small enough that arithmetic on $\mathbb{F}_{q^k}$ is feasible, i.e. we can efficiently compute the Tate pairing ($\rightarrow$ Miller's algorithm),

Pairing-Friendly Curves

- An elliptic curve is *pairing-friendly* if it contains a subgroup $\langle G \rangle \subseteq E(\mathbb{F}_q)$ of (large) prime order r and embedding degree k where k is
  - small enough that arithmetic on $\mathbb{F}_{q^k}$ is feasible, i.e. we can efficiently compute the Tate pairing ($\rightarrow$ Miller's algorithm),
  - large enough that the DLP on $\mathbb{F}_{q^k}^*$ is about as intractable as the ECDLP on $E(\mathbb{F}_q)[r]$, i.e. the MOV/FR attack is not feasible.

Pairing-Friendly Curves

- An elliptic curve is *pairing-friendly* if it contains a subgroup $\langle G \rangle \subseteq E(\mathbb{F}_q)$ of (large) prime order r and embedding degree k where k is
  - small enough that arithmetic on $\mathbb{F}_{q^k}$ is feasible, i.e. we can efficiently compute the Tate pairing ($\rightarrow$ Miller's algorithm),
  - large enough that the DLP on $\mathbb{F}^*_{q^k}$ is about as intractable as the ECDLP on $E(\mathbb{F}_q)[r]$, i.e. the MOV/FR attack is not feasible.
- What are good values for k?

Pairing-Friendly Curves

- An elliptic curve is *pairing-friendly* if it contains a subgroup $\langle G \rangle \subseteq E(\mathbb{F}_q)$ of (large) prime order r and embedding degree k where k is
  - small enough that arithmetic on $\mathbb{F}_{q^k}$ is feasible, i.e. we can efficiently compute the Tate pairing ($\rightarrow$ Miller's algorithm),
  - large enough that the DLP on $\mathbb{F}_{q^k}^*$ is about as intractable as the ECDLP on $E(\mathbb{F}_q)[r]$, i.e. the MOV/FR attack is not feasible.
- What are good values for k?
- How can we construct curves with good k?

The Problem

- The short signatures proposed by Boneh-Lynn-Shacham (2001) have length $\log(q)$.

The Problem

- The short signatures proposed by Boneh-Lynn-Shacham (2001) have length $\log(q)$.
- Compare this to DSA signatures (length 320 bits, security level 2048 e.g.).

The Problem

- The short signatures proposed by Boneh-Lynn-Shacham (2001) have length $\log(q)$.
- Compare this to DSA signatures (length 320 bits, security level 2048 e.g.).
- One gets signatures of length $2048/k$. To achieve short signatures we need $k > 6$.

The Problem

- The short signatures proposed by Boneh-Lynn-Shacham (2001) have length $\log(q)$.
- Compare this to DSA signatures (length 320 bits, security level 2048 e.g.).
- One gets signatures of length $2048/k$. To achieve short signatures we need $k > 6$.
- Boneh-Lynn-Shacham (2001)
  - Original challenge: how to build pairing-friendly curves with $k > 6$?
  - Modified challenge: how to build pairing-friendly curves of prime order with $k > 6$?

The Problem

- The short signatures proposed by Boneh-Lynn-Shacham (2001) have length $\log(q)$.
- Compare this to DSA signatures (length 320 bits, security level 2048 e.g.).
- One gets signatures of length $2048/k$. To achieve short signatures we need $k > 6$.
- Boneh-Lynn-Shacham (2001)
  - Original challenge: how to build pairing-friendly curves with $k > 6$?
  - Modified challenge: how to build pairing-friendly curves of prime order with $k > 6$?
- Suggested lower bound: $k = 10$.

Parameters

- Find parameters for suitable curves.
  Fix a value for k, e.g. $k = 10$ or $k = 12$.

Parameters

- Find parameters for suitable curves.
  Fix a value for k, e.g. $k = 10$ or $k = 12$.
- We need curves with
  1. n prime,
  2. $n = q + 1 - t$, $|t| \leq 2\sqrt{q}$,
  3. $n \mid q^k - 1$, but $n \nmid q^i - 1$ for $0 < i < k$.

Parameters

- Find parameters for suitable curves.
  Fix a value for k, e.g. $k = 10$ or $k = 12$.
- We need curves with
  1. n prime,
  2. $n = q + 1 - t$, $|t| \leq 2\sqrt{q}$,
  3. $n \mid q^k - 1$, but $n \nmid q^i - 1$ for $0 < i < k$.
- Since $X^k - 1 = \prod_{d|k} \Phi_d(X)$ the last condition is equivalent to

$$n \mid \Phi_k(q), \text{ but } n \nmid \Phi_d(q) \text{ for } d < k.$$

Parameters

- Find parameters for suitable curves.
  Fix a value for k, e.g. $k = 10$ or $k = 12$.
- We need curves with
  1. n prime,
  2. $n = q + 1 - t$, $|t| \leq 2\sqrt{q}$,
  3. $n \mid q^k - 1$, but $n \nmid q^i - 1$ for $0 < i < k$.
- Since $X^k - 1 = \prod_{d|k} \Phi_d(X)$ the last condition is equivalent to

$$n \mid \Phi_k(q), \text{ but } n \nmid \Phi_d(q) \text{ for } d < k.$$

- Look for divisors of $\Phi_k(q)$.

Complex Multiplication (CM)

- If suitable parameters are found, try to construct a curve with those parameters.
  Use the CM method.

Complex Multiplication (CM)

- If suitable parameters are found, try to construct a curve with those parameters.
  Use the CM method.

- The goal:
  Given p, n ($p > 3$ prime) find $a, b \in \mathbb{F}_p$ s.t.
  the elliptic curve $E : y^2 = x^3 + ax + b$
  has order $\#E(\mathbb{F}_p) = n$
  (and trace of the Frobenius $t = p + 1 - n$).

Complex Multiplication (CM)

- If suitable parameters are found, try to construct a curve with those parameters.
  Use the CM method.

- The goal:
  Given p, n ($p > 3$ prime) find $a, b \in \mathbb{F}_p$ s.t.
  the elliptic curve $E : y^2 = x^3 + ax + b$
  has order $\#E(\mathbb{F}_p) = n$
  (and trace of the Frobenius $t = p + 1 - n$).

- Prerequisite:
  The CM norm equation $DV^2 = 4p - t^2$ must be satisfied with moderate CM discriminant D.

Complex Multiplication (Some Details)

- Compute square-free factorisation $DV^2 = 4p - t^2$, if $D > 3$ the constructed curve will have order $p + 1 \pm t$.

Complex Multiplication (Some Details)

- Compute square-free factorisation $DV^2 = 4p - t^2$, if $D > 3$ the constructed curve will have order $p + 1 \pm t$.
- compute the Hilbert class polynomial $H_D(z)$,

Complex Multiplication (Some Details)

- Compute square-free factorisation $DV^2 = 4p - t^2$, if $D > 3$ the constructed curve will have order $p + 1 \pm t$.
- compute the Hilbert class polynomial $H_D(z)$,
- find a root j of $H_D(z) \pmod p$.

Complex Multiplication (Some Details)

- Compute square-free factorisation $DV^2 = 4p - t^2$, if $D > 3$ the constructed curve will have order $p + 1 \pm t$.
- compute the Hilbert class polynomial $H_D(z)$,
- find a root j of $H_D(z) \pmod{p}$.
- The root j is the j-invariant of a curve where
  - if $j = 0$ then $a = 0$, if $j = 1728$ then $b = 0$,
  - otherwise $a = 3c$ and $b = 2c$ with $c = j/(1728 - j)$.

Complex Multiplication (Some Details)

- Compute square-free factorisation $DV^2 = 4p - t^2$, if $D > 3$ the constructed curve will have order $p + 1 \pm t$.
- compute the Hilbert class polynomial $H_D(z)$,
- find a root j of $H_D(z) \pmod{p}$.
- The root j is the j-invariant of a curve where
  - if $j = 0$ then $a = 0$, if $j = 1728$ then $b = 0$,
  - otherwise $a = 3c$ and $b = 2c$ with $c = j/(1728-j)$.
- Check the order. If wrong, select another curve (by choosing a different root j or a twist of the curve).

Conditions

Required conditions for constructing pairing-friendly curves of prime order:

1. n prime,
2. $n = p + 1 - t$, $|t| \leq 2\sqrt{p}$,
3. $n \mid \Phi_k(p)$, but $n \nmid \Phi_d(p)$ for $0 < d < k$,
4. $DV^2 = 4p - t^2$ for moderate D.

The MNT Construction

- Miyaji-Nakabayashi-Takano (2001)
  use the fact that $n \mid \Phi_k(p)$ to parametrise p, n and t.

The MNT Construction

- Miyaji-Nakabayashi-Takano (2001)
  use the fact that $n \mid \Phi_k(p)$ to parametrise p, n and t.
- For example $k = 6$:
  parametrise $p(u) = 4u^2 + 1$ and $t(u) = 1 \pm 2u$.
  Find $u \in \mathbb{Z}$ s.t. both $p(u)$ and $n(u) = p(u) + 1 - t(u)$ are prime.

The MNT Construction

- Miyaji-Nakabayashi-Takano (2001)
  use the fact that $n \mid \Phi_k(p)$ to parametrise p, n and t.
- For example $k = 6$:
  parametrise $p(u) = 4u^2 + 1$ and $t(u) = 1 \pm 2u$.
  Find $u \in \mathbb{Z}$ s.t. both $p(u)$ and $n(u) = p(u) + 1 - t(u)$ are prime.
- Use CM to construct the curve,
  for $k \in \{3, 4, 6\}$ the CM norm equation reduces to a Pell equation $DV^2 = 4n(u) - (t(u) - 2)^2$.

The MNT Construction

- Miyaji-Nakabayashi-Takano (2001) use the fact that $n \mid \Phi_k(p)$ to parametrise p, n and t.
- For example $k = 6$: parametrise $p(u) = 4u^2 + 1$ and $t(u) = 1 \pm 2u$. Find $u \in \mathbb{Z}$ s.t. both $p(u)$ and $n(u) = p(u) + 1 - t(u)$ are prime.
- Use CM to construct the curve, for $k \in \{3, 4, 6\}$ the CM norm equation reduces to a Pell equation $DV^2 = 4n(u) - (t(u) - 2)^2$.
- Restriction: unable to handle larger k (norm equation at least quartic).

Some Constructions

- Cocks-Pinch (2002)
  algorithm based on the property that $r \mid n = p + 1 - t$ and $r \mid p^k - 1$.
  $\Rightarrow t - 1$ is a primitive k-th root of unity mod r.
  Strategy: take even $t = 2a$ and solve the norm equation mod r:
  $DV^2 = 4n - (t-2)^2 \Rightarrow V \equiv \frac{2(a-1)}{\sqrt{-D}} \pmod{r}$.
  Compute $p = (DV^2 + t^2)/4$, $n = p + 1 - t$.

Some Constructions

- Cocks-Pinch (2002)
  algorithm based on the property that $r \mid n = p + 1 - t$ and $r \mid p^k - 1$.
  $\Rightarrow t - 1$ is a primitive k-th root of unity mod r.
  Strategy: take even $t = 2a$ and solve the norm equation mod r:
  $DV^2 = 4n - (t-2)^2 \Rightarrow V \equiv \frac{2(a-1)}{\sqrt{-D}} \pmod{r}$.
  Compute $p = (DV^2 + t^2)/4$, $n = p + 1 - t$.
- Restriction: usually $\rho = {}^{\log p}/_{\log r} \approx 2$.

Some Constructions

- Barreto-Lynn-Scott (2002), Brezing-Weng (2003)
- For certain values of k and D there exist closed-form parametrisations for families of curves with known equations.
  (e.g. $k = 2^i 3^j$ and $D = 3$, or $k = 2^i 7^j$ and $D = 7$)

Some Constructions

- Barreto-Lynn-Scott (2002), Brezing-Weng (2003)
- For certain values of k and D there exist closed-form parametrisations for families of curves with known equations.
  (e.g. $k = 2^i 3^j$ and $D = 3$, or $k = 2^i 7^j$ and $D = 7$)
- Advantages: ρ closer to 1.
  (best case: $\rho = \frac{5}{4}$ for $k = 8$ and $D = 3$)

Some Constructions

- Barreto-Lynn-Scott (2002), Brezing-Weng (2003)
- For certain values of k and D there exist closed-form parametrisations for families of curves with known equations.
  (e.g. $k = 2^i 3^j$ and $D = 3$, or $k = 2^i 7^j$ and $D = 7$)
- Advantages: ρ closer to 1.
  (best case: $\rho = \frac{5}{4}$ for $k = 8$ and $D = 3$)
- Limitations: solutions known only for small D and curve order always composite (ρ still 'large').

Extending the MNT Approach

- Galbraith-McKee-Valença (2004)
  start from the property $n \mid \Phi_k(p)$ and parametrise $p(u)$ such that
  $$\Phi_k(p(u)) = n_1(u)n_2(u).$$

Extending the MNT Approach

- Galbraith-McKee-Valença (2004)
  start from the property $n \mid \Phi_k(p)$ and parametrise $p(u)$ such that
  $$\Phi_k(p(u)) = n_1(u)n_2(u).$$

Lemma:

Let $k \in \mathbb{N}$, $\zeta_k \in \mathbb{C}$ a primitive k-th root of unity, $p(u) \in \mathbb{Q}[u]$ a quadratic polynomial. Then

$$\Phi_k(p(u)) = n_1(u)n_2(u)$$

for irreducible polynomials $n_1, n_2 \in \mathbb{Q}[u]$ of degree $\varphi(k)$, if and only if $p(z) = \zeta_k$ has a solution in $\mathbb{Q}(\zeta_k)$. Otherwise $\Phi_k(p(u))$ is irreducible.

Extending the MNT Approach

- Leads to conditions on quadratic $p(u)$ s.t. the factors of $\Phi_k(p(u))$ are quartic for $k \in \{5, 8, 10, 12\}$.
  For example $k = 10$: $p(u) = 10u^2 + 5u + 2$,
  $k = 12$: $p(u) = 2u^2$ or $p(u) = 6u^2$.

Extending the MNT Approach

- Leads to conditions on quadratic $p(u)$ s.t. the factors of $\Phi_k(p(u))$ are quartic for $k \in \{5, 8, 10, 12\}$.
  For example $k = 10$: $p(u) = 10u^2 + 5u + 2$,
  $k = 12$: $p(u) = 2u^2$ or $p(u) = 6u^2$.
- Result: families of genus 2 curves similar to MNT elliptic curves.

Extending the MNT Approach

- Leads to conditions on quadratic $p(u)$ s.t. the factors of $\Phi_k(p(u))$ are quartic for $k \in \{5, 8, 10, 12\}$.
  For example $k = 10$: $p(u) = 10u^2 + 5u + 2$,
  $k = 12$: $p(u) = 2u^2$ or $p(u) = 6u^2$.
- Result: families of genus 2 curves similar to MNT elliptic curves.
- NB: $p(u)$ must be a prime (or prime power).

Extending the MNT Approach

- Leads to conditions on quadratic $p(u)$ s.t. the factors of $\Phi_k(p(u))$ are quartic for $k \in \{5, 8, 10, 12\}$.
  For example $k = 10$: $p(u) = 10u^2 + 5u + 2$,
  $k = 12$: $p(u) = 2u^2$ or $p(u) = 6u^2$.
- Result: families of genus 2 curves similar to MNT elliptic curves.
- NB: $p(u)$ must be a prime (or prime power).
- Some conditions cannot lead to solutions:
  for $k = 12$ the parametrisation $p(u) = 6u^2$ will never produce a prime power.

Extending the MNT Approach

- Leads to conditions on quadratic $p(u)$ s.t. the factors of $\Phi_k(p(u))$ are quartic for $k \in \{5, 8, 10, 12\}$.
  For example $k = 10$: $p(u) = 10u^2 + 5u + 2$,
  $k = 12$: $p(u) = 2u^2$ or $p(u) = 6u^2$.
- Result: families of genus 2 curves similar to MNT elliptic curves.
- NB: $p(u)$ must be a prime (or prime power).
- Some conditions cannot lead to solutions:
  for $k = 12$ the parametrisation $p(u) = 6u^2$ will never produce a prime power.
- How about changing the strategy?

New Strategy

- Start from $n \mid \Phi_k(t(u) - 1)$ and parametrise $t(u)$ s.t. $\Phi_k(t(u) - 1)$ splits into quartic factors $n_1(u)n_2(u)$.
- The only restriction on $t(u)$ is the Hasse bound. Since $n(u)$ is quartic, $t(u)$ must be at most quadratic for $k \in \{5, 8, 10, 12\}$.

New Strategy

- Start from $n \mid \Phi_k(t(u) - 1)$ and parametrise $t(u)$ s.t. $\Phi_k(t(u) - 1)$ splits into quartic factors $n_1(u)n_2(u)$.
- The only restriction on $t(u)$ is the Hasse bound. Since $n(u)$ is quartic, $t(u)$ must be at most quadratic for $k \in \{5, 8, 10, 12\}$.
- Most conditions do not lead to a favourable factorisation of the norm equation

$$DV^2 = 4n(u) - (t(u) - 2)^2.$$

New Strategy

- Start from $n \mid \Phi_k(t(u)-1)$ and parametrise $t(u)$ s.t. $\Phi_k(t(u)-1)$ splits into quartic factors $n_1(u)n_2(u)$.
- The only restriction on $t(u)$ is the Hasse bound. Since $n(u)$ is quartic, $t(u)$ must be at most quadratic for $k \in \{5, 8, 10, 12\}$.

- Most conditions do not lead to a favourable factorisation of the norm equation

$$DV^2 = 4n(u) - (t(u)-2)^2.$$

- But …

New Curves

- The condition $t(u) = 6u^2 + 1$ does lead to a favourable factorisation for $k = 12$.

$$\Phi_k(t(u) - 1) = n(u)n(-u).$$

- Parameters:

$$\begin{aligned} n(u) &= 36u^4 + 36u^3 + 18u^2 + 6u + 1 \\ p(u) &= 36u^4 + 36u^3 + 24u^2 + 6u + 1 \\ DV^2 &= 4p - t^2 = 3(6u^2 + 4u + 1)^2 \end{aligned}$$

NB: $u \in \mathbb{Z} \setminus \{0\}$ (positive or negative values).

New Curves

- Since $D = 3$, the curve equation has the form

$$E(\mathbb{F}_p) : y^2 = x^3 + b,$$

  with $b > 0$ adjusted to attain the right order. (A simple sequential search quickly finds a suitable b.)

- NB: the method always produces $p \equiv 1 \pmod 3$ (no supersingular curves).

Twisted Pairings

- For ordinary curves there are no distortion maps.

Twisted Pairings

- For ordinary curves there are no distortion maps.
- There exists a sextic twist $E'(\mathbb{F}_{p^2})$ and an injective group homomorphism

$$\psi : E'(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^{12}}).$$

Twisted Pairings

- For ordinary curves there are no distortion maps.
- There exists a sextic twist $E'(\mathbb{F}_{p^2})$ and an injective group homomorphism

$$\psi : E'(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^{12}}).$$

- Define a twisted pairing

$$\hat{e} : E(\mathbb{F}_p) \times E'(\mathbb{F}_{p^2}) \longrightarrow \mathbb{F}_{p^{12}}^*, \quad \hat{e}(P, Q') = e(P, \psi(Q')).$$

Twisted Pairings

- For ordinary curves there are no distortion maps.
- There exists a sextic twist $E'(\mathbb{F}_{p^2})$ and an injective group homomorphism

$$\psi : E'(\mathbb{F}_{p^2}) \longrightarrow E(\mathbb{F}_{p^{12}}).$$

- Define a twisted pairing

$$\hat{e} : E(\mathbb{F}_p) \times E'(\mathbb{F}_{p^2}) \longrightarrow \mathbb{F}^*_{p^{12}}, \quad \hat{e}(P, Q') = e(P, \psi(Q')).$$

- The field arithmetic needed for non-pairing operations is restricted to $\mathbb{F}_{p^2}$.
- The homomorphism is only needed when actually computing pairings.

Twisted Pairings

- Let $X^6 - \xi$ be an irreducible polynomial in $\mathbb{F}_{p^2}[X]$.
  Represent $\mathbb{F}_{p^{12}}$ as $\mathbb{F}_{p^2}[X]/(X^6 - \xi)$.
  Any element in $\mathbb{F}_{p^{12}}$ has the form
  $a_5z^5 + a_4z^4 + a_3z^3 + a_2z^2 + a_1z + a_0$ for a root z of
  $X^6 - \xi$.

Twisted Pairings

- Let $X^6 - \xi$ be an irreducible polynomial in $\mathbb{F}_{p^2}[X]$. Represent $\mathbb{F}_{p^{12}}$ as $\mathbb{F}_{p^2}[X]/(X^6 - \xi)$. Any element in $\mathbb{F}_{p^{12}}$ has the form $a_5 z^5 + a_4 z^4 + a_3 z^3 + a_2 z^2 + a_1 z + a_0$ for a root z of $X^6 - \xi$.
- The twist is $E' : y'^2 = x'^3 + b/\xi$.

Twisted Pairings

- Let $X^6 - \xi$ be an irreducible polynomial in $\mathbb{F}_{p^2}[X]$.
  Represent $\mathbb{F}_{p^{12}}$ as $\mathbb{F}_{p^2}[X]/(X^6 - \xi)$.
  Any element in $\mathbb{F}_{p^{12}}$ has the form $a_5 z^5 + a_4 z^4 + a_3 z^3 + a_2 z^2 + a_1 z + a_0$ for a root z of $X^6 - \xi$.
- The twist is $E' : y'^2 = x'^3 + b/\xi$.
- Let $(x', y') \in E'(\mathbb{F}_{p^2})$. The mapping

$$\psi : (x', y') \mapsto (z^2 x', z^3 y')$$

  does not incur any multiplication overhead and produces sparse elements of $\mathbb{F}_{p^{12}}$.

Compressed Pairings

- Pairing compression is possible with ratio $\frac{1}{3}$ in a way that naturally integrates with point compression.
- Instead of reducing a point $(x', y') \in E'(\mathbb{F}_{p^2})$ to its x-coordinate, discard it and keep only the y-coordinate. Recovering (x', y') creates ambiguity between three possible values of x'.

Compressed Pairings

- Pairing compression is possible with ratio $\frac{1}{3}$ in a way that naturally integrates with point compression.
- Instead of reducing a point $(x', y') \in E'(\mathbb{F}_{p^2})$ to its x-coordinate, discard it and keep only the y-coordinate. Recovering (x', y') creates ambiguity between three possible values of x'.

- The three points that share the same y-coordinate are conjugates, as are the pairing values computed on them (provided the points are n-torsion points).
- The trace of all three pairing values is the same $\mathbb{F}_{p^4}$ value.

Point Compression

- Discard one more bit of y', i.e. do not distinguish between y' and $-y'$.
- Keep only the information to represent an equivalence class $\{(x', \pm y'), (\zeta_3 x', \pm y'), (\zeta_3^2 x', \pm y')\}$.

Point Compression

- Discard one more bit of y', i.e. do not distinguish between y' and $-y'$.
- Keep only the information to represent an equivalence class $\{(x', \pm y'), (\zeta_3 x', \pm y'), (\zeta_3^2 x', \pm y')\}$.

- The $\mathbb{F}_{p^2}$-traces of the pairing values of all six points in the class are equal.
- Obtain a unique compressed pairing value over $\mathbb{F}_{p^2}$.

Point Compression

- Discard one more bit of y', i.e. do not distinguish between y' and $-y'$.
- Keep only the information to represent an equivalence class $\{(x', \pm y'), (\zeta_3 x', \pm y'), (\zeta_3^2 x', \pm y')\}$.

- The $\mathbb{F}_{p^2}$-traces of the pairing values of all six points in the class are equal.
- Obtain a unique compressed pairing value over $\mathbb{F}_{p^2}$.

- Represent points in $E'(\mathbb{F}_{p^2})$ with less than $\log(p^2)$ bits.
- Pairing compression with ratio $\frac{1}{6}$ may be possible.

Open Problems

- How to build pairing-friendly curves of genus $g \in \{1, 2, 3, 4\}$ and prime order for $k/g < 32$ and $\varphi(k) > 4$ over a field $\mathbb{F}_{p^f}$?
- Are there any real security problems with small D? Can we handle really large D?
- How are the special primes distributed? Are there infinitely many?
- ...

If you are interested . . .

- Curve Database:
  `http://www.ti.rwth-aachen.de/~mnaehrig`
  Lots of examples of bitsizes 160, 192, 224,. . . , 512 and program to compute curve of chosen bitsize.

- Paulo Barreto's Pairing-Based Crypto Lounge:
  `http://paginas.terra.com.br/informatica/paulobarreto/pblounge.html`