How to Construct Pairing-Friendly Curves

Michael Naehrig

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

LARC, USP
São Paulo, 28.09.2007

Motivation

Pairings on elliptic curves are used in cryptology,

Motivation

Pairings on elliptic curves are used in cryptology,

- as a means to attack cryptography based on elliptic curves, to analyse the discrete logarithm problem on elliptic curves,

Motivation

Pairings on elliptic curves are used in cryptology,

- as a means to attack cryptography based on elliptic curves, to analyse the discrete logarithm problem on elliptic curves,
- or to construct crypto systems with certain special properties:
  - One-round tripartite key agreement,
  - Identity Based Encryption (IBE),
  - Hierarchical IBE (HIDE),
  - Short signatures (BLS).

What is a Pairing?

A *pairing* is a non-degenerate, bilinear map

$$e : G_1 \times G_2 \to G_3,$$

where G_1, G_2 are additive groups and G_3 is written multiplicatively.

What is a Pairing?

A *pairing* is a non-degenerate, bilinear map

$$e : G_1 \times G_2 \to G_3,$$

where G_1, G_2 are additive groups and G_3 is written multiplicatively.

- Non-degenerate: for every $\mathcal{O} \neq P \in G_1$ there exists a $Q \in G_2$ 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

$$\begin{aligned} e(P_1 + P_2, Q_1) &= e(P_1, Q_1)e(P_2, Q_1), \\ e(P_1, Q_1 + Q_2) &= e(P_1, Q_1)e(P_1, Q_2). \end{aligned}$$

It follows: $e(aP, bQ) = e(P, Q)^{ab} = e(bP, aQ)$.

Mathematical Background: Elliptic Curves

- An *elliptic curve* E over a field K ($\mathrm{char}(K) \neq 2, 3$) is the set of solutions in $\overline{K}^2$ of an equation

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

where $a, b \in K$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$, together with some point $\mathcal{O}$ at infinity.

Mathematical Background: Elliptic Curves

- An *elliptic curve* E over a field K ($\mathrm{char}(K) \neq 2, 3$) is the set of solutions in $\overline{K}^2$ of an equation

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

  where $a, b \in K$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$, together with some point $\mathcal{O}$ at infinity.
- Here: $K = \mathbb{F}_p$ for a prime $p > 3$. For a field extension $\mathbb{F}_{p^f}$ the set

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

  is called the set of $\mathbb{F}_{p^f}$*-rational points* on E.

Mathematical Background: Elliptic Curves

- An *elliptic curve* E over a field K ($\mathrm{char}(K) \neq 2, 3$) is the set of solutions in $\overline{K}^2$ of an equation

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

where $a, b \in K$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$, together with some point $\mathcal{O}$ at infinity.

- Here: $K = \mathbb{F}_p$ for a prime $p > 3$. For a field extension $\mathbb{F}_{p^f}$ the set

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

is called the set of $\mathbb{F}_{p^f}$*-rational points* on E.

- The set $E(\mathbb{F}_{p^f})$ is an abelian group. We write $+$ for the group law. The neutral element is the point $\mathcal{O}$.

Mathematical Background: Elliptic Curves

- The group $E(\mathbb{F}_p)$ is finite. The number of points in the group is
$$\#E(\mathbb{F}_p) = n = p + 1 - t,$$
where $|t| \leq 2\sqrt{p}$. The number t is called the *trace of Frobenius*.

Mathematical Background: Elliptic Curves

- The group $E(\mathbb{F}_p)$ is finite. The number of points in the group is
$$\#E(\mathbb{F}_p) = n = p + 1 - t,$$
where $|t| \leq 2\sqrt{p}$. The number t is called the *trace of Frobenius*.
- For an integer m the points of order dividing m are called m*-torsion points*. The set of m-torsion points in $E(\mathbb{F}_{p^f})$ is denoted by
$$E(\mathbb{F}_{p^f})[m] = \{P \in E(\mathbb{F}_{p^f}) \mid [m]P = \mathcal{O}\}.$$

Mathematical Background: The Tate Pairing

- For a large prime divisor r of n we define the *embedding degree* to be the smallest integer k s.t. $r \mid p^k - 1$.

Mathematical Background: The Tate Pairing

- For a large prime divisor r of n we define the *embedding degree* to be the smallest integer k s.t. $r \mid p^k - 1$.
- All r-torsion points of the curve are contained in $E(\mathbb{F}_{p^k})$.

Mathematical Background: The Tate Pairing

- For a large prime divisor r of n we define the *embedding degree* to be the smallest integer k s.t. $r \mid p^k - 1$.
- All r-torsion points of the curve are contained in $E(\mathbb{F}_{p^k})$.
- The *Tate Pairing* is a map

$$\tau : E(\mathbb{F}_{p^k})[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \to \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r.$$

Mathematical Background: The Tate Pairing

- For a large prime divisor r of n we define the *embedding degree* to be the smallest integer k s.t. $r \mid p^k - 1$.
- All r-torsion points of the curve are contained in $E(\mathbb{F}_{p^k})$.
- The *Tate Pairing* is a map

$$\tau : E(\mathbb{F}_{p^k})[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \to \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r.$$

- In practice one uses the *reduced* Tate Pairing:

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

where $\mu_r \subset \mathbb{F}_{p^k}^*$ is the group of r-th roots of unity.

Mathematical Background: The Tate Pairing

- For a large prime divisor r of n we define the *embedding degree* to be the smallest integer k s.t. $r \mid p^k - 1$.
- All r-torsion points of the curve are contained in $E(\mathbb{F}_{p^k})$.
- The *Tate Pairing* is a map

$$\tau : E(\mathbb{F}_{p^k})[r] \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) \to \mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r.$$

- In practice one uses the *reduced* Tate Pairing:

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

  where $\mu_r \subset \mathbb{F}^*_{p^k}$ is the group of r-th roots of unity.
- We obtain a unique pairing value in μ_r by computing $\tau(P, Q)^{\frac{p^k-1}{r}}$. This is called the *final exponentiation*.

Requirements

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

We are looking for

Requirements

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

We are looking for

- a prime p

Requirements

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

We are looking for

- a prime p
- and an elliptic curve $E/\mathbb{F}_p$,
- whose group order n has a large prime divisor r (optimal: $n = r$),

Requirements

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

We are looking for

- a prime p
- and an elliptic curve $E/\mathbb{F}_p$,
- whose group order n has a large prime divisor r (optimal: $n = r$),
- s. t. the embedding degree k is small.

Requirements

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

We are looking for

- a prime p
- and an elliptic curve $E/\mathbb{F}_p$,
- whose group order n has a large prime divisor r (optimal: $n = r$),
- s. t. the embedding degree k is small.

Problem: For a random curve, k is enormous.

How can we find pairing-friendly elliptic curves?

Supersingular Curves

- An elliptic curve is called *supersingular*, iff $t \equiv 0 \pmod{p}$. Otherwise it is called *ordinary*.

Supersingular Curves

- An elliptic curve is called *supersingular*, iff $t \equiv 0 \pmod{p}$. Otherwise it is called *ordinary*.
- Supersingular elliptic curves have an embedding degree $k \leq 6$.

Supersingular Curves

- An elliptic curve is called *supersingular*, iff $t \equiv 0 \pmod{p}$. Otherwise it is called *ordinary*.
- Supersingular elliptic curves have an embedding degree $k \leq 6$.
- For $p \geq 5$ it even holds: $k \leq 2$.
  (Since $|t| \leq 2\sqrt{p}$, we have $t = 0$ and thus $n = p + 1$, so $n \mid p^2 - 1$.)

Supersingular Curves

- An elliptic curve is called *supersingular*, iff $t \equiv 0 \pmod{p}$. Otherwise it is called *ordinary*.
- Supersingular elliptic curves have an embedding degree $k \leq 6$.
- For $p \geq 5$ it even holds: $k \leq 2$.
(Since $|t| \leq 2\sqrt{p}$, we have $t = 0$ and thus $n = p + 1$, so $n \mid p^2 - 1$.)
- But, $k = 6$ or even $k = 2$ might be too small and some people don't like supersingular curves.

Supersingular Curves

- An elliptic curve is called *supersingular*, iff $t \equiv 0 \pmod{p}$. Otherwise it is called *ordinary*.
- Supersingular elliptic curves have an embedding degree $k \leq 6$.
- For $p \geq 5$ it even holds: $k \leq 2$.
(Since $|t| \leq 2\sqrt{p}$, we have $t = 0$ and thus $n = p + 1$, so $n \mid p^2 - 1$.)
- But, $k = 6$ or even $k = 2$ might be too small and some people don't like supersingular curves.
- We focus on the construction of ordinary curves
- whose group order n is prime, i.e. $r = n$.

Conditions

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

Conditions

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

- $n = \#E(\mathbb{F}_p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$,
- $r \mid n$,
- $r \mid p^k - 1$,

Conditions

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

- $n = \#E(\mathbb{F}_p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$,
- $r \mid n$,
- $r \mid p^k - 1$,
- $t^2 - 4p = DV^2$, $D, V \in \mathbb{Z}$, D squarefree, $|D|$ small enough.

The last condition ensures that the curve can be constructed using the CM method. Today we will treat CM as a black box.

Conditions

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

- $n = \#E(\mathbb{F}_p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$,
- $r \mid n$,
- $r \mid p^k - 1$,
- $t^2 - 4p = DV^2$, $D, V \in \mathbb{Z}$, D squarefree, $|D|$ small enough.

The last condition ensures that the curve can be constructed using the CM method. Today we will treat CM as a black box.

- $r \mid p^k - 1$ can be replaced by $r \mid \Phi_k(p)$, where $\Phi_k(X)$ is the k-th cyclotomic polynomial, since

$$X^k - 1 = \prod_{d|k} \Phi_d(X).$$

Φ_k has degree $\varphi(k) < k$.

MNT curves

Miyaji, Nakabayashi and Takano (MNT, 2001) give parametrisations of p and t as polynomials in $\mathbb{Z}[u]$ s.t.

$$n(u) \mid \Phi_k(p(u)).$$

The method yields ordinary elliptic curves of prime order ($r = n$) with embedding degree $k = 3, 4, 6$.

MNT curves

Miyaji, Nakabayashi and Takano (MNT, 2001) give parametrisations of p and t as polynomials in $\mathbb{Z}[u]$ s.t.

$$n(u) \mid \Phi_k(p(u)).$$

The method yields ordinary elliptic curves of prime order ($r = n$) with embedding degree $k = 3, 4, 6$.

k	$p(u)$	$t(u)$
3	$12u^2 - 1$	$-1 \pm 6u$
4	$u^2 + u + 1$	$-u$ or $u + 1$
6	$4u^2 + 1$	$1 \pm 2u$

MNT curves

Let's compute an MNT curve. Take $k = 6$, i.e. we parameterise

$$p(u) = 4u^2 + 1,\ t(u) = 2u + 1.$$

MNT curves

Let's compute an MNT curve. Take $k = 6$, i.e. we parameterise

$$p(u) = 4u^2 + 1,\ t(u) = 2u + 1.$$

- Then we have

$$n(u) = p(u) + 1 - t(u) = 4u^2 - 2u + 1.$$

MNT curves

Let's compute an MNT curve. Take $k = 6$, i.e. we parameterise

$$p(u) = 4u^2 + 1,\ t(u) = 2u + 1.$$

- Then we have

$$n(u) = p(u) + 1 - t(u) = 4u^2 - 2u + 1.$$

- We may now plug in integer values for u until we find u_0 s.t. $p(u_0)$ and $n(u_0)$ are both prime.
- Example: $u_0 = 2$ yields $p(u_0) = 17$ and $n(u_0) = 13$.

MNT curves

Let's compute an MNT curve. Take $k = 6$, i.e. we parameterise

$$p(u) = 4u^2 + 1, \; t(u) = 2u + 1.$$

- Then we have

$$n(u) = p(u) + 1 - t(u) = 4u^2 - 2u + 1.$$

- We may now plug in integer values for u until we find u_0 s.t. $p(u_0)$ and $n(u_0)$ are both prime.
- Example: $u_0 = 2$ yields $p(u_0) = 17$ and $n(u_0) = 13$.
- But we only have parameters, we do not have the curve.

MNT curves

In order to construct the curve via the CM method we need to find solutions to the norm equation

$$t^2 - 4p = DV^2,$$

and $|D|$ needs to be small.

MNT curves

In order to construct the curve via the CM method we need to find solutions to the norm equation

$$t^2 - 4p = DV^2,$$

and $|D|$ needs to be small.

- Let's get back to the example $k = 6$. We compute

$$t(u)^2 - 4p(u) = (2u+1)^2 - 4(4u^2+1) = -12u^2 + 4u - 3.$$

MNT curves

In order to construct the curve via the CM method we need to find solutions to the norm equation

$$t^2 - 4p = DV^2,$$

and $|D|$ needs to be small.

- Let's get back to the example $k = 6$. We compute

$$t(u)^2 - 4p(u) = (2u+1)^2 - 4(4u^2+1) = -12u^2 + 4u - 3.$$

- Therefore the norm equation becomes

$$-12u^2 + 4u - 3 = DV^2.$$

MNT curves

In order to construct the curve via the CM method we need to find solutions to the norm equation

$$t^2 - 4p = DV^2,$$

and $|D|$ needs to be small.

- Let's get back to the example $k = 6$. We compute

$$t(u)^2 - 4p(u) = (2u+1)^2 - 4(4u^2+1) = -12u^2 + 4u - 3.$$

- Therefore the norm equation becomes

$$-12u^2 + 4u - 3 = DV^2.$$

- For $u_0 = 2$ we obtain $DV^2 = -43$, here $|D|$ is too large.

MNT curves

Maybe we first should find solutions to the norm equation. Let's transform the equation:

MNT curves

Maybe we first should find solutions to the norm equation. Let's transform the equation:

- Start with
$$-12u^2 + 4u - 3 = DV^2.$$

MNT curves

Maybe we first should find solutions to the norm equation. Let's transform the equation:

- Start with
$$-12u^2 + 4u - 3 = DV^2.$$
- Multiply by -3 to get
$$36u^2 - 12u + 9 = -3DV^2.$$

MNT curves

Maybe we first should find solutions to the norm equation. Let's transform the equation:

- Start with
$$-12u^2 + 4u - 3 = DV^2.$$
- Multiply by -3 to get
$$36u^2 - 12u + 9 = -3DV^2.$$
- Complete the square:
$$(6u - 1)^2 + 8 = -3DV^2.$$

MNT curves

Maybe we first should find solutions to the norm equation. Let's transform the equation:

- Start with
$$-12u^2 + 4u - 3 = DV^2.$$
- Multiply by -3 to get
$$36u^2 - 12u + 9 = -3DV^2.$$
- Complete the square:
$$(6u-1)^2 + 8 = -3DV^2.$$
- Actually we need to solve (replace $6u-1$ by x, V by y)
$$x^2 + 3Dy^2 = -8.$$

MNT curves

How can we solve the equation $x^2 + 3Dy^2 = -8$?

MNT curves

How can we solve the equation $x^2 + 3Dy^2 = -8$?

- Theorem: If d is a positive squarefree integer then the equation
$$x^2 - dy^2 = 1$$
has infinitely many solutions. There is a solution (x_1, y_1) such that every solution has the form $\pm(x_m, y_m)$ where
$$x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m, \ m \in \mathbb{Z}.$$

MNT curves

How can we solve the equation $x^2 + 3Dy^2 = -8$?

- Theorem: If d is a positive squarefree integer then the equation
$$x^2 - dy^2 = 1$$
has infinitely many solutions. There is a solution (x_1, y_1) such that every solution has the form $\pm(x_m, y_m)$ where
$$x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m,\ m \in \mathbb{Z}.$$
- So if $d = -3D$ is positive and squarefree, we can compute infinitely many solutions to our equation if we find a solution (x_1, y_1).

MNT curves

How can we solve the equation $x^2 + 3Dy^2 = -8$?

- Theorem: If d is a positive squarefree integer then the equation
$$x^2 - dy^2 = 1$$
has infinitely many solutions. There is a solution (x_1, y_1) such that every solution has the form $\pm(x_m, y_m)$ where
$$x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m, \ m \in \mathbb{Z}.$$
- So if $d = -3D$ is positive and squarefree, we can compute infinitely many solutions to our equation if we find a solution (x_1, y_1).
- Use Cornacchia's algorithm to find a single solution.

MNT curves

Consider the field $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

MNT curves

Consider the field $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

- The norm of $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is defined to be

$$N(\alpha) = \alpha\overline{\alpha} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$$

so $x^2 - dy^2$ is the norm of the element $x + y\sqrt{d}$.

MNT curves

Consider the field $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

- The norm of $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is defined to be

$$N(\alpha) = \alpha\overline{\alpha} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$$

  so $x^2 - dy^2$ is the norm of the element $x + y\sqrt{d}$.
- We are actually looking for an element of norm -8.

MNT curves

Consider the field $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

- The norm of $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is defined to be

$$N(\alpha) = \alpha\overline{\alpha} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$$

  so $x^2 - dy^2$ is the norm of the element $x + y\sqrt{d}$.
- We are actually looking for an element of norm -8.
- The norm is multiplicative:

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

MNT curves

Consider the field $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

- The norm of $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is defined to be

$$N(\alpha) = \alpha\overline{\alpha} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$$

  so $x^2 - dy^2$ is the norm of the element $x + y\sqrt{d}$.
- We are actually looking for an element of norm -8.
- The norm is multiplicative:

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

- We need to find only one element α of norm -8, then the infinitely many elements $\beta_m = x_m + y_m\sqrt{d}$ of norm 1 will help us to find infinitely many elements of norm -8:

$$N(\alpha\beta_m) = N(\alpha)N(\beta_m) = -8 \cdot 1 = -8.$$

MNT curves

Back to the example: Choose $D = -11$, so $d = 33$.

- The equation becomes

$$x^2 - 33y^2 = -8.$$

MNT curves

Back to the example: Choose $D = -11$, so $d = 33$.

- The equation becomes

$$x^2 - 33y^2 = -8.$$

- A solution is $(5, 1)$. The corresponding element of $\mathbb{Q}(\sqrt{33})$ is $5 + \sqrt{33}$.

MNT curves

Back to the example: Choose $D = -11$, so $d = 33$.

- The equation becomes

$$x^2 - 33y^2 = -8.$$

- A solution is $(5, 1)$. The corresponding element of $\mathbb{Q}(\sqrt{33})$ is $5 + \sqrt{33}$.
- A solution to

$$x^2 - 33y^2 = 1$$

  is $(23, 4)$ with corresponding element $23 + 4\sqrt{33}$.

MNT curves

Back to the example: Choose $D = -11$, so $d = 33$.

- The equation becomes
$$x^2 - 33y^2 = -8.$$
- A solution is $(5, 1)$. The corresponding element of $\mathbb{Q}(\sqrt{33})$ is $5 + \sqrt{33}$.
- A solution to
$$x^2 - 33y^2 = 1$$
is $(23, 4)$ with corresponding element $23 + 4\sqrt{33}$.
- The elements
$$(5 + \sqrt{33})(23 + \sqrt{33})^m$$
all have norm -8, thus yield solutions to the original norm equation.

MNT curves

We now can compute many solutions to the equation
$x^2 - 33y^2 = -8$.

MNT curves

We now can compute many solutions to the equation $x^2 - 33y^2 = -8$.

$$
\begin{aligned}
(5+\sqrt{33})(23+\sqrt{33})^{-5} &= -76495073 + 13316083\sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{-4} &= -1663723 + 289617\sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{-3} &= -36185 + 6299\sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{-2} &= -787 + 137\sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{-1} &= -17 + 3\sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{0} &= 5 + \sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{1} &= 247 + 43\sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{2} &= 11357 + 1977\sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{3} &= 522175 + 90899\sqrt{33} \\
(5+\sqrt{33})(23+\sqrt{33})^{4} &= 24008693 + 4179377\sqrt{33}
\end{aligned}
$$

MNT curves

And compute back to find solutions for the original equation $-12u^2 + 4u - 3 = DV^2$. Remember $x = 6u - 1$

MNT curves

And compute back to find solutions for the original equation $-12u^2 + 4u - 3 = DV^2$. Remember $x = 6u - 1$

$\alpha\beta^i$	u	V
$-76495073 + 13316083\sqrt{33}$	12749179	13316083
$-1663723 + 289617\sqrt{33}$	-2124863	289617
$-36185 + 6299\sqrt{33}$	6031	6299
$-787 + 137\sqrt{33}$	-131	137
$-17 + 3\sqrt{33}$	3	3
$5 + \sqrt{33}$	1	1
$247 + 43\sqrt{33}$	-41	43
$11357 + 1977\sqrt{33}$	1893	1977
$522175 + 90899\sqrt{33}$	-87029	90899
$24008693 + 4179377\sqrt{33}$	4001449	4179377

MNT curves

We hope that some of the values for u give $p(u)$ and $n(u)$ prime.

MNT curves

We hope that some of the values for u give $p(u)$ and $n(u)$ prime.

- We are lucky. The value $u = 3$ gives

$$p(u) = 37,\ n(u) = 31,\ t(u) = 7.$$

MNT curves

We hope that some of the values for u give $p(u)$ and $n(u)$ prime.

- We are lucky. The value $u = 3$ gives

$$p(u) = 37,\ n(u) = 31,\ t(u) = 7.$$

- Giving the parameters $p = 37,\ n = 31,\ D = -11$ to the CM black box, we obtain the curve

$$E : y^2 = x^3 + 13x + 11$$

over the field $\mathbb{F}_{37}$ with 37 elements.

MNT curves

We hope that some of the values for u give $p(u)$ and $n(u)$ prime.

- We are lucky. The value $u = 3$ gives

$$p(u) = 37, \ n(u) = 31, \ t(u) = 7.$$

- Giving the parameters $p = 37, \ n = 31, \ D = -11$ to the CM black box, we obtain the curve

$$E : y^2 = x^3 + 13x + 11$$

  over the field $\mathbb{F}_{37}$ with 37 elements.
- The curve has 31 points and embedding degree $k = 6$.

MNT curves

We hope that some of the values for u give $p(u)$ and $n(u)$ prime.

- We are lucky. The value $u = 3$ gives

$$p(u) = 37,\ n(u) = 31,\ t(u) = 7.$$

- Giving the parameters $p = 37,\ n = 31,\ D = -11$ to the CM black box, we obtain the curve

$$E : y^2 = x^3 + 13x + 11$$

  over the field $\mathbb{F}_{37}$ with 37 elements.
- The curve has 31 points and embedding degree $k = 6$.
- Every point on the curve is a generator, since the order of the group is prime. The point $(1, 5)$ for example lies on the curve.

Generalisation of the MNT approach

We need to find parametrisations for p and n such that

$$n(u) \mid \Phi_k(p(u)).$$

Generalisation of the MNT approach

We need to find parametrisations for p and n such that

$$n(u) \mid \Phi_k(p(u)).$$

A result by Galbraith, McKee and Valença (2004) helps when p is parametrised as a quadratic polynomial.

Generalisation of the MNT approach

We need to find parametrisations for p and n such that

$$n(u) \mid \Phi_k(p(u)).$$

A result by Galbraith, McKee and Valença (2004) helps when p is parametrised as a quadratic polynomial.

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

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

  for irreducible polynomials $n_1(u), n_2(u) \in \mathbb{Q}[u]$ of degree $\varphi(k)$, if and only if the equation

  $$p(z) = \zeta_k$$

  has a solution in $\mathbb{Q}(\zeta_k)$.

Larger embedding degree

The MNT results can be obtained by applying this lemma. But we get more:

Larger embedding degree

The MNT results can be obtained by applying this lemma. But we get more:

- For $k = 12$ we get the following

$$\Phi_{12}(6u^2) = n(u)n(-u),$$

where $n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$.

Larger embedding degree

The MNT results can be obtained by applying this lemma. But we get more:

- For $k = 12$ we get the following

$$\Phi_{12}(6u^2) = n(u)n(-u),$$

  where $n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$.
- This does not help, since $6u^2$ can never be a prime.

Larger embedding degree

The MNT results can be obtained by applying this lemma. But we get more:

- For $k = 12$ we get the following

$$\Phi_{12}(6u^2) = n(u)n(-u),$$

  where $n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$.

- This does not help, since $6u^2$ can never be a prime.
- But since $n = p + 1 - t$ we have $p \equiv t - 1 \pmod{n}$, which means that

$$n \mid \Phi_k(p) \iff n \mid \Phi_k(t-1).$$

  We might as well parametrise $t(u) - 1 = 6u^2$.

BN curves

BN curves (Barreto, N., 2005) have embedding degree $k = 12$. Choose

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

We then have $t(u) = 6u^2 + 1$,

$$n(u) \mid \Phi_{12}(p(u))$$

and

$$t(u)^2 - 4p(u) = -3(6u^2 + 4u + 1)^2,$$

i. e. the conditions are satisfied in $\mathbb{Z}[u]$ (as polynomials).

BN curves

- Since the norm equation is of the required form with $D = -3$ already as polynomials, there is no need to solve an equation as in the MNT case.
- Only try different values for u until $p(u)$ and $n(u)$ are prime.

BN curves

- Since the norm equation is of the required form with $D = -3$ already as polynomials, there is no need to solve an equation as in the MNT case.
- Only try different values for u until $p(u)$ and $n(u)$ are prime.
- Since $D = -3$ always, there is no need to use the CM method, since such curves always have the form

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

- We only need to try different values for b until the curve has the right order.

BN curves

- Since the norm equation is of the required form with $D = -3$ already as polynomials, there is no need to solve an equation as in the MNT case.
- Only try different values for u until $p(u)$ and $n(u)$ are prime.
- Since $D = -3$ always, there is no need to use the CM method, since such curves always have the form

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

- We only need to try different values for b until the curve has the right order.
- It is very easy to find BN curves of a certain bitsize.
- And they have many advantages for efficient implementation of pairings.

A BN curve with 256 bits

The curve

$$E : y^2 = x^3 + 3$$

over $\mathbb{F}_p$ with

$$\begin{aligned} p &= 1157920892367772791549216121554858107 87\\ &\ 7511215206851142406435252036193317 50863 \end{aligned}$$

has

$$\begin{aligned} n &= 115792089236777279154921612155485810787\\ &\ 410839153764967643444263417404280302329 \end{aligned}$$

points and embedding degree $k = 12$. The group $E(\mathbb{F}_p)$ is generated by $(1, 2)$.
($u = -7530851732707558283$,
$t = 340282366920146597199261786215051448535$)

Freeman curves

Freeman curves (2006) have embedding degree $k = 10$. Choose

$$\begin{aligned} n(u) &= 25u^4 + 25u^3 + 15u^2 + 5u + 1, \\ p(u) &= 25u^4 + 25u^3 + 25u^2 + 10u + 3. \end{aligned}$$

We then have $t(u) = 10u^2 + 5u + 3$,

$$n(u) \mid \Phi_{10}(p(u))$$

and

$$t(u)^2 - 4p(u) = -(15u^2 + 10u + 3).$$

To solve the norm equation we also need to solve a Pell equation as in the classical MNT case.

Pairing-friendly elliptic curves

There are methods for constructing pairing-friendly elliptic curves with a prime order group of rational points in the following cases:

$k \in \{3, 4, 6\}$:	Miyaji, Nakabayashi, Takano (2001),
$k = 10$:	Freeman (2006),
$k = 12$:	Barreto, N. (2005).

Pairing-friendly elliptic curves

There are methods for constructing pairing-friendly elliptic curves with a prime order group of rational points in the following cases:

$k \in \{3, 4, 6\}$:	Miyaji, Nakabayashi, Takano (2001),
$k = 10$:	Freeman (2006),
$k = 12$:	Barreto, N. (2005).

For all other embedding degrees there are methods to construct pairing-friendly elliptic curves, but the groups of rational points are no longer of prime order.

For an overview see the ”Taxonomy of pairing-friendly elliptic curves” (Freeman, Scott, Teske, 2006).
`http://eprint.iacr.org/2006/372`

Outlook: Hyperelliptic curves

A *hyperelliptic curve* C of genus g over $\mathbb{F}_p$ is given by an equation

$$C : y^2 + h(x)y = f(x),$$

where $h(x),\ f(x) \in \mathbb{F}_p[x]$ s. t. $\deg(f) = 2g + 1$ and $\deg(h) \leq g$.

Outlook: Hyperelliptic curves

A *hyperelliptic curve* C of genus g over $\mathbb{F}_p$ is given by an equation

$$C : y^2 + h(x)y = f(x),$$

where $h(x),\ f(x) \in \mathbb{F}_p[x]$ s. t. $\deg(f) = 2g + 1$ and $\deg(h) \leq g$.

For cryptographic applications we are interested in the group $J_C(\mathbb{F}_p)$ (Jacobian variety). Algorithms for pairing computation are similar to those for elliptic curves.

Outlook: Hyperelliptic curves

A *hyperelliptic curve* C of genus g over $\mathbb{F}_p$ is given by an equation

$$C : y^2 + h(x)y = f(x),$$

where $h(x),\ f(x) \in \mathbb{F}_p[x]$ s. t. $\deg(f) = 2g + 1$ and $\deg(h) \leq g$.

For cryptographic applications we are interested in the group $J_C(\mathbb{F}_p)$ (Jacobian variety). Algorithms for pairing computation are similar to those for elliptic curves.

Why hyperelliptic curves?

Outlook: Hyperelliptic curves

Frey, Lange: ”Fast Bilinear Maps from the Tate-Lichtenbaum Pairing on Hyperelliptic Curves” (2006).

Outlook: Hyperelliptic curves

Frey, Lange: ”Fast Bilinear Maps from the Tate-Lichtenbaum Pairing on Hyperelliptic Curves” (2006).

”Our method speeds up the pairing computation by a factor of about g ... Thus there is no gain for elliptic curves but for hyperelliptic curves ...”

Outlook: Hyperelliptic curves

Frey, Lange: ”Fast Bilinear Maps from the Tate-Lichtenbaum Pairing on Hyperelliptic Curves” (2006).

”Our method speeds up the pairing computation by a factor of about g ... Thus there is no gain for elliptic curves but for hyperelliptic curves ...”

”Our paper is a purely theoretical one due to the lack of satisfying non-supersingular curves ...”

Requirements

We look for

Requirements

We look for

- a prime p

Requirements

We look for

- a prime p
- and a hyperelliptic curve $C/\mathbb{F}_p$,
- s. t. the group order of $J_C(\mathbb{F}_p)$ has a large prime divisor r

Requirements

We look for

- a prime p
- and a hyperelliptic curve $C/\mathbb{F}_p$,
- s. t. the group order of $J_C(\mathbb{F}_p)$ has a large prime divisor r
- and the embedding degree k is small.

Requirements

We look for

- a prime p
- and a hyperelliptic curve $C/\mathbb{F}_p$,
- s. t. the group order of $J_C(\mathbb{F}_p)$ has a large prime divisor r
- and the embedding degree k is small.

Embedding degree is defined as for elliptic curves.

Group order

The group order of $J_C(\mathbb{F}_p)$ is

$$n = \#J_C(\mathbb{F}_p) = P(1),$$

where

$$
\begin{aligned}
P(X) &= X^4 + a_1X^3 + a_2X^2 + pa_1X + p^2, \\
P(X) &= X^6 + a_1X^5 + a_2X^4 + a_3X^3 + pa_2X^2 + p^2a_1X + p^3,
\end{aligned}
$$

for $g = 2$ and $g = 3$ respectively. We have $a_i \in \mathbb{Z}$.

Group order

The group order of $J_C(\mathbb{F}_p)$ is

$$n = \#J_C(\mathbb{F}_p) = P(1),$$

where

$$\begin{aligned}
P(X) &= X^4 + a_1X^3 + a_2X^2 + pa_1X + p^2, \\
n &= 1 + a_1 + a_2 + pa_1 + p^2, \\
P(X) &= X^6 + a_1X^5 + a_2X^4 + a_3X^3 + pa_2X^2 + p^2a_1X + p^3, \\
n &= 1 + a_1 + a_2 + a_3 + pa_2 + p^2a_1 + p^3
\end{aligned}$$

for $g = 2$ and $g = 3$ respectively. We have $a_i \in \mathbb{Z}$.

Conditions

As in the case for elliptic curves we fix k and try to find primes p and r and a potential group order n, s. t.

Conditions

As in the case for elliptic curves we fix k and try to find primes p and r and a potential group order n, s. t.

- $n = P(1)$,
- $r \mid n$,
- $r \mid \Phi_k(p)$.

Conditions

As in the case for elliptic curves we fix k and try to find primes p and r and a potential group order n, s. t.

- $n = P(1)$,
- $r \mid n$,
- $r \mid \Phi_k(p)$.

How can we construct a hyperelliptic curve with given group order? Is there also a CM method?

Conditions

As in the case for elliptic curves we fix k and try to find primes p and r and a potential group order n, s. t.

- $n = P(1)$,
- $r \mid n$,
- $r \mid \Phi_k(p)$.

How can we construct a hyperelliptic curve with given group order? Is there also a CM method?

There is a CM method, but everything is much more complicated. To go into the details would take at least one more hour...

”Pairing-friendly” curves for $g = 2$

Freeman (2007) proposes an algorithm to construct hyperelliptic curves of genus $g = 2$ which have arbitrary embedding degree.

”Pairing-friendly” curves for $g = 2$

Freeman (2007) proposes an algorithm to construct hyperelliptic curves of genus $g = 2$ which have arbitrary embedding degree.

Unfortunately $\log(n)/\log(r) \approx 8$, which is very disadvantageous.

"Pairing-friendly" curves for $g = 2$

Freeman (2007) proposes an algorithm to construct hyperelliptic curves of genus $g = 2$ which have arbitrary embedding degree.

Unfortunately $\log(n)/\log(r) \approx 8$, which is very disadvantageous.

Open Problem 1: Find a construction for pairing-friendly genus 2 curves with smaller $\log(n)/\log(r)$.

”Pairing-friendly” curves for $g = 2$

Freeman (2007) proposes an algorithm to construct hyperelliptic curves of genus $g = 2$ which have arbitrary embedding degree.

Unfortunately $\log(n)/\log(r) \approx 8$, which is very disadvantageous.

Open Problem 1: Find a construction for pairing-friendly genus 2 curves with smaller $\log(n)/\log(r)$.

Open Problem 2: Find pairing-friendly curves of genus 3 and 4.

Questions?

Thank you for your attention!