

Constructing Pairing-Friendly Elliptic Curves for Cryptography

David Freeman

University of California, Berkeley, USA

2nd KIAS-KMS Summer Workshop on Cryptography

Seoul, Korea
30 June 2007

Outline

- 1 Pairings in Cryptography
 - Introduction to Pairings
 - Pairings on Elliptic Curves
- 2 How to Construct Pairing-Friendly Elliptic Curves
 - Ordinary vs. Supersingular
 - The Complex Multiplication Method
 - Classification of Pairing-Friendly Elliptic Curves
- 3 Construction Methods
 - Curves with Arbitrary Embedding Degree
 - Cocks-Pinch and Dupont-Engge-Morain Methods
 - Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
 - Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

Outline

- 1 **Pairings in Cryptography**
 - Introduction to Pairings
 - Pairings on Elliptic Curves
- 2 **How to Construct Pairing-Friendly Elliptic Curves**
 - Ordinary vs. Supersingular
 - The Complex Multiplication Method
 - Classification of Pairing-Friendly Elliptic Curves
- 3 **Construction Methods**
 - Curves with Arbitrary Embedding Degree
 - Cocks-Pinch and Dupont-Engge-Morain Methods
 - Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
 - Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

What is a pairing?

- Many public-key cryptographic protocols are based on the *discrete logarithm problem* (DLP) in a finite cyclic group $\mathbb{G}$:
 - Given x, y in $\mathbb{G}$, find integer a such that $y = x^a$.
 - For systems involving $\mathbb{G}$ to be secure, the DLP must be computationally infeasible.
- A *cryptographic pairing* is map

$$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$$

that is

- Bilinear: $e(x^a, y^b) = e(x, y)^{ab}$ in $\mathbb{G}_T$.
- Nondegenerate: for any $x \in \mathbb{G}$, $x \neq 1$, there is a $y \in \mathbb{G}$ such that $e(x, y) \neq 1$ in $\mathbb{G}_T$.

What is a pairing?

- Many public-key cryptographic protocols are based on the *discrete logarithm problem* (DLP) in a finite cyclic group $\mathbb{G}$:
 - Given x, y in $\mathbb{G}$, find integer a such that $y = x^a$.
 - For systems involving $\mathbb{G}$ to be secure, the DLP must be computationally infeasible.
- A *cryptographic pairing* is map

$$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$$

that is

- Bilinear: $e(x^a, y^b) = e(x, y)^{ab}$ in $\mathbb{G}_T$.
- Nondegenerate: for any $x \in \mathbb{G}$, $x \neq 1$, there is a $y \in \mathbb{G}$ such that $e(x, y) \neq 1$ in $\mathbb{G}_T$.

What is a pairing?

- Many public-key cryptographic protocols are based on the *discrete logarithm problem* (DLP) in a finite cyclic group $\mathbb{G}$:
 - Given x, y in $\mathbb{G}$, find integer a such that $y = x^a$.
 - For systems involving $\mathbb{G}$ to be secure, the DLP must be computationally infeasible.
- A *cryptographic pairing* is map

$$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$$

that is

- Bilinear: $e(x^a, y^b) = e(x, y)^{ab}$ in $\mathbb{G}_T$.
- Nondegenerate: for any $x \in \mathbb{G}$, $x \neq 1$, there is a $y \in \mathbb{G}$ such that $e(x, y) \neq 1$ in $\mathbb{G}_T$.

What is a pairing?

- Many public-key cryptographic protocols are based on the *discrete logarithm problem* (DLP) in a finite cyclic group $\mathbb{G}$:
 - Given x, y in $\mathbb{G}$, find integer a such that $y = x^a$.
 - For systems involving $\mathbb{G}$ to be secure, the DLP must be computationally infeasible.
- A *cryptographic pairing* is map

$$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$$

that is

- 1 Bilinear: $e(x^a, y^b) = e(x, y)^{ab}$ in $\mathbb{G}_T$.
- 2 Nondegenerate: for any $x \in \mathbb{G}$, $x \neq 1$, there is a $y \in \mathbb{G}$ such that $e(x, y) \neq 1$ in $\mathbb{G}_T$.

What is a pairing?

- Many public-key cryptographic protocols are based on the *discrete logarithm problem* (DLP) in a finite cyclic group $\mathbb{G}$:
 - Given x, y in $\mathbb{G}$, find integer a such that $y = x^a$.
 - For systems involving $\mathbb{G}$ to be secure, the DLP must be computationally infeasible.
- A *cryptographic pairing* is map

$$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$$

that is

- 1 Bilinear: $e(x^a, y^b) = e(x, y)^{ab}$ in $\mathbb{G}_T$.
- 2 Nondegenerate: for any $x \in \mathbb{G}$, $x \neq 1$, there is a $y \in \mathbb{G}$ such that $e(x, y) \neq 1$ in $\mathbb{G}_T$.

What is a pairing?

- Many public-key cryptographic protocols are based on the *discrete logarithm problem* (DLP) in a finite cyclic group $\mathbb{G}$:
 - Given x, y in $\mathbb{G}$, find integer a such that $y = x^a$.
 - For systems involving $\mathbb{G}$ to be secure, the DLP must be computationally infeasible.
- A *cryptographic pairing* is map

$$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$$

that is

- 1 Bilinear: $e(x^a, y^b) = e(x, y)^{ab}$ in $\mathbb{G}_T$.
- 2 Nondegenerate: for any $x \in \mathbb{G}$, $x \neq 1$, there is a $y \in \mathbb{G}$ such that $e(x, y) \neq 1$ in $\mathbb{G}_T$.

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
 - Compute $e(x, x^a) = e(x, x)^a$ and $e(x, x^b) = e(x, x)^b$.
 - $e(x, x^c) = e(x, x)^{ab}$ and only if the two values are equal in $\mathbb{G}_T$.

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - 1 Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - 2 Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - 3 Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
 (By computing $e(x, x^a) = e(x, x^b)$ and $e(x^a, x^b) = e(x, x^c)$.
 If $ab = c$ and only if the two values are equal in $\mathbb{G}_T$.)

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - 1 Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - 2 Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - 3 Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
 (We know $e(x, x^a) = e(x, x^b)$ and $e(x^a, x^b) = e(x, x^{ab})$.
 If $ab = c$ and given x and x^c , we can verify $e(x, x^c) = e(x^a, x^b)$.)

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - 1 Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - 2 Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - 3 Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
 (If $c = ab$, then $e(x, x^c) = e(x, x^{ab}) = e(x^a, x^b) = e(x, x^c)$.
 If $c \neq ab$, then $e(x, x^c) \neq e(x, x^{ab}) = e(x^a, x^b) = e(x, x^c)$.)

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - 1 Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - 2 Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - 3 Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
(The pairing e is a bilinear map: $e(x, x^a) = e(x, x)^a$ and $e(x, x^b) = e(x, x)^b$.
If $c = ab$ then $e(x, x^c) = e(x, x)^{ab} = e(x, x^a)^b = e(x, x^b)^a$.

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - 1 Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - 2 Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - 3 Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
 - Compute $e(x, x^c) = e(x, x)^c$ and $e(x^a, x^b) = e(x, x)^{ab}$.
 - $ab = c$ if and only if the two pairings are equal in $\mathbb{G}_T$.

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - 1 Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - 2 Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - 3 Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
 - 1 Compute $e(x, x^c) = e(x, x)^c$ and $e(x^a, x^b) = e(x, x)^{ab}$.
 - 2 $ab = c$ if and only if the two pairings are equal in $\mathbb{G}_T$.

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - 1 Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - 2 Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - 3 Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
 - 1 Compute $e(x, x^c) = e(x, x)^c$ and $e(x^a, x^b) = e(x, x)^{ab}$.
 - 2 $ab = c$ if and only if the two pairings are equal in $\mathbb{G}_T$.

How to Use a Pairing

- A cryptographic pairing maps the discrete logarithm problem in $\mathbb{G}$ to the DLP in $\mathbb{G}_T$:
 - Given x and $y = x^a$ in $\mathbb{G}$:
 - 1 Choose a $z \in \mathbb{G}$ with $e(x, z) \neq 1$.
 - 2 Compute $x' = e(x, z)$, $y' = e(y, z)$.
 - 3 Try to compute a from x' and $y' = x'^a$.
- The pairing solves the *Decision Diffie-Hellman Problem* in $\mathbb{G}$:
 - Given x, x^a, x^b, x^c , determine if $c = ab$.
 - 1 Compute $e(x, x^c) = e(x, x)^c$ and $e(x^a, x^b) = e(x, x)^{ab}$.
 - 2 $ab = c$ if and only if the two pairings are equal in $\mathbb{G}_T$.

Applications of Pairings

- Attack on discrete logarithm problem for supersingular elliptic curves (Menezes-Okamoto-Vanstone).
 - Map discrete log on elliptic curve to easier discrete log 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, threshold cryptography, broadcast encryption, private information retrieval, electronic voting, etc.

Applications of Pairings

- Attack on discrete logarithm problem for supersingular elliptic curves (Menezes-Okamoto-Vanstone).
 - Map discrete log on elliptic curve to easier discrete log 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, threshold cryptography, broadcast encryption, private information retrieval, electronic voting, etc.

Applications of Pairings

- Attack on discrete logarithm problem for supersingular elliptic curves (Menezes-Okamoto-Vanstone).
 - Map discrete log on elliptic curve to easier discrete log 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, threshold cryptography, broadcast encryption, private information retrieval, electronic voting, etc.

Applications of Pairings

- Attack on discrete logarithm problem for supersingular elliptic curves (Menezes-Okamoto-Vanstone).
 - Map discrete log on elliptic curve to easier discrete log 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, threshold cryptography, broadcast encryption, private information retrieval, electronic voting, etc.

Applications of Pairings

- Attack on discrete logarithm problem for supersingular elliptic curves (Menezes-Okamoto-Vanstone).
 - Map discrete log on elliptic curve to easier discrete log 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, threshold cryptography, broadcast encryption, private information retrieval, electronic voting, etc.

Applications of Pairings

- Attack on discrete logarithm problem for supersingular elliptic curves (Menezes-Okamoto-Vanstone).
 - Map discrete log on elliptic curve to easier discrete log 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, threshold cryptography, broadcast encryption, private information retrieval, electronic voting, etc.

Applications of Pairings

- Attack on discrete logarithm problem for supersingular elliptic curves (Menezes-Okamoto-Vanstone).
 - Map discrete log on elliptic curve to easier discrete log 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, threshold cryptography, broadcast encryption, private information retrieval, electronic voting, etc.

Requirements for Pairings

- To be useful in applications using the Decision Diffie-Hellman property, we need:
 - 1 the discrete logarithm problem in $\mathbb{G}$ to be computationally infeasible,
 - 2 the discrete logarithm problem in $\mathbb{G}_T$ to be computationally infeasible, and
 - 3 the pairing to be easy to compute.

Requirements for Pairings

- To be useful in applications using the Decision Diffie-Hellman property, we need:
 - 1 the discrete logarithm problem in $\mathbb{G}$ to be computationally infeasible,
 - 2 the discrete logarithm problem in $\mathbb{G}_T$ to be computationally infeasible, and
 - 3 the pairing to be easy to compute.

Requirements for Pairings

- To be useful in applications using the Decision Diffie-Hellman property, we need:
 - 1 the discrete logarithm problem in $\mathbb{G}$ to be computationally infeasible,
 - 2 the discrete logarithm problem in $\mathbb{G}_T$ to be computationally infeasible, and
 - 3 the pairing to be easy to compute.

Requirements for Pairings

- To be useful in applications using the Decision Diffie-Hellman property, we need:
 - 1 the discrete logarithm problem in $\mathbb{G}$ to be computationally infeasible,
 - 2 the discrete logarithm problem in $\mathbb{G}_T$ to be computationally infeasible, and
 - 3 the pairing to be easy to compute.

Outline

- 1 **Pairings in Cryptography**
 - Introduction to Pairings
 - **Pairings on Elliptic Curves**
- 2 **How to Construct Pairing-Friendly Elliptic Curves**
 - Ordinary vs. Supersingular
 - The Complex Multiplication Method
 - Classification of Pairing-Friendly Elliptic Curves
- 3 **Construction Methods**
 - Curves with Arbitrary Embedding Degree
 - Cocks-Pinch and Dupont-Engge-Morain Methods
 - Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
 - Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

Elliptic Curves in Cryptography

- An *elliptic curve* E over a finite field $\mathbb{F}_p$ is defined by an equation

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- The set of points (x, y) on E , plus a “point at infinity” O , forms a group (usually written additively).
 - Adding two points P, Q gives a third point $R = P + Q$.
 - Adding a point to itself repeatedly gives multiplication: $P + \cdots + P$ (m times) $= mP$.
- If P has prime order r , then computing a from P and aP takes time $\sim \sqrt{r}$.
 - If r is a large prime, then discrete log in elliptic curve subgroup of order r is infeasible.

Elliptic Curves in Cryptography

- An *elliptic curve* E over a finite field $\mathbb{F}_p$ is defined by an equation

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- The set of points (x, y) on E , plus a “point at infinity” O , forms a group (usually written additively).
 - Adding two points P, Q gives a third point $R = P + Q$.
 - Adding a point to itself repeatedly gives multiplication:
 $P + \dots + P$ (m times) $= mP$.
- If P has prime order r , then computing a from P and aP takes time $\sim \sqrt{r}$.
 - If r is a large prime, then discrete log in elliptic curve subgroup of order r is infeasible.

Elliptic Curves in Cryptography

- An *elliptic curve* E over a finite field $\mathbb{F}_p$ is defined by an equation

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- The set of points (x, y) on E , plus a “point at infinity” O , forms a group (usually written additively).
 - Adding two points P, Q gives a third point $R = P + Q$.
 - Adding a point to itself repeatedly gives multiplication:
 $P + \dots + P$ (m times) $= mP$.
- If P has prime order r , then computing a from P and aP takes time $\sim \sqrt{r}$.
 - If r is a large prime, then discrete log in elliptic curve subgroup of order r is infeasible.

Elliptic Curves in Cryptography

- An *elliptic curve* E over a finite field $\mathbb{F}_p$ is defined by an equation

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- The set of points (x, y) on E , plus a “point at infinity” O , forms a group (usually written additively).
 - Adding two points P, Q gives a third point $R = P + Q$.
 - Adding a point to itself repeatedly gives multiplication:
 $P + \dots + P$ (m times) $= mP$.
- If P has prime order r , then computing a from P and aP takes time $\sim \sqrt{r}$.
 - If r is a large prime, then discrete log in elliptic curve subgroup of order r is infeasible.

Elliptic Curves in Cryptography

- An *elliptic curve* E over a finite field $\mathbb{F}_p$ is defined by an equation

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- The set of points (x, y) on E , plus a “point at infinity” O , forms a group (usually written additively).
 - Adding two points P, Q gives a third point $R = P + Q$.
 - Adding a point to itself repeatedly gives multiplication:
 $P + \dots + P$ (m times) $= mP$.
- If P has prime order r , then computing a from P and aP takes time $\sim \sqrt{r}$.
 - If r is a large prime, then discrete log in elliptic curve subgroup of order r is infeasible.

Elliptic Curves in Cryptography

- An *elliptic curve* E over a finite field $\mathbb{F}_p$ is defined by an equation

$$E : y^2 = x^3 + ax + b \pmod{p}$$

- The set of points (x, y) on E , plus a “point at infinity” O , forms a group (usually written additively).
 - Adding two points P, Q gives a third point $R = P + Q$.
 - Adding a point to itself repeatedly gives multiplication:
 $P + \dots + P$ (m times) $= mP$.
- If P has prime order r , then computing a from P and aP takes time $\sim \sqrt{r}$.
 - If r is a large prime, then discrete log in elliptic curve subgroup of order r is infeasible.

The Weil and Tate Pairings

- Let E be an elliptic curve defined over a finite field $\mathbb{F}$.
- For any integer r the *Weil pairing* $e_{r,weil}$ is a bilinear map sending pairs of points of order r to r -th roots of unity in $\overline{\mathbb{F}}$:

$$e_{r,weil}: E[r] \times E[r] \rightarrow \mu_r.$$

- The *Tate pairing* $e_{r,tate}$ is similar:

$$e_{r,tate}: E(\mathbb{F})[r] \times E(\mathbb{F})/rE(\mathbb{F}) \rightarrow \mathbb{F}^\times/(\mathbb{F}^\times)^r.$$

- If r is prime and $\mathbb{F}_{p^k}$ is the smallest field containing μ_r , then both pairings take values in $\mathbb{F}_{p^k}^\times$.
- Tate pairing generally can be computed more efficiently.

The Weil and Tate Pairings

- Let E be an elliptic curve defined over a finite field $\mathbb{F}$.
- For any integer r the *Weil pairing* $e_{r,weil}$ is a bilinear map sending pairs of points of order r to r -th roots of unity in $\overline{\mathbb{F}}$:

$$e_{r,weil}: E[r] \times E[r] \rightarrow \mu_r.$$

- The *Tate pairing* $e_{r,tate}$ is similar:

$$e_{r,tate}: E(\mathbb{F})[r] \times E(\mathbb{F})/rE(\mathbb{F}) \rightarrow \mathbb{F}^\times / (\mathbb{F}^\times)^r.$$

- If r is prime and $\mathbb{F}_{p^k}$ is the smallest field containing μ_r , then both pairings take values in $\mathbb{F}_{p^k}^\times$.
- Tate pairing generally can be computed more efficiently.

The Weil and Tate Pairings

- Let E be an elliptic curve defined over a finite field $\mathbb{F}$.
- For any integer r the *Weil pairing* $e_{r,weil}$ is a bilinear map sending pairs of points of order r to r -th roots of unity in $\overline{\mathbb{F}}$:

$$e_{r,weil}: E[r] \times E[r] \rightarrow \mu_r.$$

- The *Tate pairing* $e_{r,tate}$ is similar:

$$e_{r,tate}: E(\mathbb{F})[r] \times E(\mathbb{F})/rE(\mathbb{F}) \rightarrow \mathbb{F}^\times/(\mathbb{F}^\times)^r.$$

- If r is prime and $\mathbb{F}_{p^k}$ is the smallest field containing μ_r , then both pairings take values in $\mathbb{F}_{p^k}^\times$.
- Tate pairing generally can be computed more efficiently.

The Weil and Tate Pairings

- Let E be an elliptic curve defined over a finite field $\mathbb{F}$.
- For any integer r the *Weil pairing* $e_{r,weil}$ is a bilinear map sending pairs of points of order r to r -th roots of unity in $\overline{\mathbb{F}}$:

$$e_{r,weil}: E[r] \times E[r] \rightarrow \mu_r.$$

- The *Tate pairing* $e_{r,tate}$ is similar:

$$e_{r,tate}: E(\mathbb{F})[r] \times E(\mathbb{F})/rE(\mathbb{F}) \rightarrow \mathbb{F}^\times/(\mathbb{F}^\times)^r.$$

- If r is prime and $\mathbb{F}_{p^k}$ is the smallest field containing μ_r , then both pairings take values in $\mathbb{F}_{p^k}^\times$.
- Tate pairing generally can be computed more efficiently.

The Weil and Tate Pairings

- Let E be an elliptic curve defined over a finite field $\mathbb{F}$.
- For any integer r the *Weil pairing* $e_{r,weil}$ is a bilinear map sending pairs of points of order r to r -th roots of unity in $\overline{\mathbb{F}}$:

$$e_{r,weil}: E[r] \times E[r] \rightarrow \mu_r.$$

- The *Tate pairing* $e_{r,tate}$ is similar:

$$e_{r,tate}: E(\mathbb{F})[r] \times E(\mathbb{F})/rE(\mathbb{F}) \rightarrow \mathbb{F}^\times / (\mathbb{F}^\times)^r.$$

- If r is prime and $\mathbb{F}_{p^k}$ is the smallest field containing μ_r , then both pairings take values in $\mathbb{F}_{p^k}^\times$.
- Tate pairing generally can be computed more efficiently.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \# \text{bits of } p / \# \text{bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \# \text{bits of } p / \# \text{bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \text{\#bits of } p / \text{\#bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \# \text{bits of } p / \# \text{bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \# \text{bits of } p / \# \text{bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \# \text{bits of } p / \# \text{bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \# \text{bits of } p / \# \text{bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \# \text{bits of } p / \# \text{bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Embedding degrees

- Elliptic curve pairings used in cryptography use curves $E/\mathbb{F}_p$ with a point of order r , and map into the r th roots of unity in $\mathbb{F}_{p^k}$.
- 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 discrete log in $\mathbb{F}_{p^k}^\times$ is computationally infeasible, but small enough so that pairing is easy to compute.
- r is a large prime dividing $\#E(\mathbb{F}_p)$
 - Define $\rho = \log p / \log r = \# \text{bits of } p / \# \text{bits of } r$.
 - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want ρ small to save bandwidth.
 - If curve has prime order, $\rho = 1$.

Pairing-friendly elliptic curves

- Balasubramanian-Koblitz: 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 ($k \leq 50$).
- Problem: construct pairing-friendly elliptic curves for specified values of k and number of bits in r .

Pairing-friendly elliptic curves

- Balasubramanian-Koblitz: 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 ($k \leq 50$).
- Problem: construct pairing-friendly elliptic curves for specified values of k and number of bits in r .

Pairing-friendly elliptic curves

- Balasubramanian-Koblitz: 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 ($k \leq 50$).
- Problem: construct pairing-friendly elliptic curves for specified values of k and number of bits in r .

Pairing-friendly elliptic curves

- Balasubramanian-Koblitz: 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 ($k \leq 50$).
- Problem: construct pairing-friendly elliptic curves for specified values of k and number of bits in r .

Our Goal

- Provide a supply of pairing-friendly curves suitable for many different performance and security requirements.
- Since discrete logarithm problem is easier in finite fields than on elliptic curves, finite field size $\mathbb{F}_{p^k}$ should be larger than subgroup size r .
- How much larger depends on level of security desired:

Security level (in bits)	Subgroup size r (in bits)	Extension field size p^k (in bits)	Embedding degree k	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960 – 1280	6 – 8	3 – 4
112	224	2200 – 3600	10 – 16	5 – 8
128	256	3000 – 5000	12 – 20	6 – 10
192	384	8000 – 10000	20 – 26	10 – 13
256	512	14000 – 18000	28 – 36	14 – 18

Our Goal

- Provide a supply of pairing-friendly curves suitable for many different performance and security requirements.
- Since discrete logarithm problem is easier in finite fields than on elliptic curves, finite field size $\mathbb{F}_{p^k}$ should be larger than subgroup size r .
- How much larger depends on level of security desired:

Security level (in bits)	Subgroup size r (in bits)	Extension field size p^k (in bits)	Embedding degree k	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960 – 1280	6 – 8	3 – 4
112	224	2200 – 3600	10 – 16	5 – 8
128	256	3000 – 5000	12 – 20	6 – 10
192	384	8000 – 10000	20 – 26	10 – 13
256	512	14000 – 18000	28 – 36	14 – 18

Our Goal

- Provide a supply of pairing-friendly curves suitable for many different performance and security requirements.
- Since discrete logarithm problem is easier in finite fields than on elliptic curves, finite field size $\mathbb{F}_{p^k}$ should be larger than subgroup size r .
- How much larger depends on level of security desired:

Security level (in bits)	Subgroup size r (in bits)	Extension field size p^k (in bits)	Embedding degree k	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960 – 1280	6 – 8	3 – 4
112	224	2200 – 3600	10 – 16	5 – 8
128	256	3000 – 5000	12 – 20	6 – 10
192	384	8000 – 10000	20 – 26	10 – 13
256	512	14000 – 18000	28 – 36	14 – 18

Our Goal

- Provide a supply of pairing-friendly curves suitable for many different performance and security requirements.
- Since discrete logarithm problem is easier in finite fields than on elliptic curves, finite field size $\mathbb{F}_{p^k}$ should be larger than subgroup size r .
- How much larger depends on level of security desired:

Security level (in bits)	Subgroup size r (in bits)	Extension field size p^k (in bits)	Embedding degree k	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960 – 1280	6 – 8	3 – 4
112	224	2200 – 3600	10 – 16	5 – 8
128	256	3000 – 5000	12 – 20	6 – 10
192	384	8000 – 10000	20 – 26	10 – 13
256	512	14000 – 18000	28 – 36	14 – 18

Our Goal

- Provide a supply of pairing-friendly curves suitable for many different performance and security requirements.
- Since discrete logarithm problem is easier in finite fields than on elliptic curves, finite field size $\mathbb{F}_{p^k}$ should be larger than subgroup size r .
- How much larger depends on level of security desired:

Security level (in bits)	Subgroup size r (in bits)	Extension field size p^k (in bits)	Embedding degree k	
			$\rho \approx 1$	$\rho \approx 2$
80	160	960 – 1280	6 – 8	3 – 4
112	224	2200 – 3600	10 – 16	5 – 8
128	256	3000 – 5000	12 – 20	6 – 10
192	384	8000 – 10000	20 – 26	10 – 13
256	512	14000 – 18000	28 – 36	14 – 18

Outline

- 1 Pairings in Cryptography
 - Introduction to Pairings
 - Pairings on Elliptic Curves
- 2 How to Construct Pairing-Friendly Elliptic Curves
 - Ordinary vs. Supersingular
 - The Complex Multiplication Method
 - Classification of Pairing-Friendly Elliptic Curves
- 3 Construction Methods
 - Curves with Arbitrary Embedding Degree
 - Cocks-Pinch and Dupont-Engge-Morain Methods
 - Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
 - Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

Supersingular Curves

- An elliptic curve over $\mathbb{F}_p$ ($p \geq 5$) is *supersingular* if $\#E(\mathbb{F}_p) = p + 1$.
 - Supersingular curves easy to construct; e.g., $y^2 = x^3 + 1$ for any $p \equiv 2 \pmod{3}$.
- If $p \geq 5$, then supersingular curves over $\mathbb{F}_p$ have embedding degree 2.
- Supersingular curves over non-prime fields have embedding degree ≤ 6 .
- To obtain other embedding degrees, we must use ordinary (i.e., non-supersingular) elliptic curves.

Supersingular Curves

- An elliptic curve over $\mathbb{F}_p$ ($p \geq 5$) is *supersingular* if $\#E(\mathbb{F}_p) = p + 1$.
 - Supersingular curves easy to construct; e.g., $y^2 = x^3 + 1$ for any $p \equiv 2 \pmod{3}$.
- If $p \geq 5$, then supersingular curves over $\mathbb{F}_p$ have embedding degree 2.
- Supersingular curves over non-prime fields have embedding degree ≤ 6 .
- To obtain other embedding degrees, we must use ordinary (i.e., non-supersingular) elliptic curves.

Supersingular Curves

- An elliptic curve over $\mathbb{F}_p$ ($p \geq 5$) is *supersingular* if $\#E(\mathbb{F}_p) = p + 1$.
 - Supersingular curves easy to construct; e.g., $y^2 = x^3 + 1$ for any $p \equiv 2 \pmod{3}$.
- If $p \geq 5$, then supersingular curves over $\mathbb{F}_p$ have embedding degree 2.
- Supersingular curves over non-prime fields have embedding degree ≤ 6 .
- To obtain other embedding degrees, we must use ordinary (i.e., non-supersingular) elliptic curves.

Supersingular Curves

- An elliptic curve over $\mathbb{F}_p$ ($p \geq 5$) is *supersingular* if $\#E(\mathbb{F}_p) = p + 1$.
 - Supersingular curves easy to construct; e.g., $y^2 = x^3 + 1$ for any $p \equiv 2 \pmod{3}$.
- If $p \geq 5$, then supersingular curves over $\mathbb{F}_p$ have embedding degree 2.
- Supersingular curves over non-prime fields have embedding degree ≤ 6 .
- To obtain other embedding degrees, we must use ordinary (i.e., non-supersingular) elliptic curves.

Supersingular Curves

- An elliptic curve over $\mathbb{F}_p$ ($p \geq 5$) is *supersingular* if $\#E(\mathbb{F}_p) = p + 1$.
 - Supersingular curves easy to construct; e.g., $y^2 = x^3 + 1$ for any $p \equiv 2 \pmod{3}$.
- If $p \geq 5$, then supersingular curves over $\mathbb{F}_p$ have embedding degree 2.
- Supersingular curves over non-prime fields have embedding degree ≤ 6 .
- To obtain other embedding degrees, we must use ordinary (i.e., non-supersingular) elliptic curves.

Ordinary Elliptic Curves: The General Strategy

To construct pairing-friendly ordinary elliptic curves:

- 1 Fix k , find primes p and r such that there exists a curve $E/\mathbb{F}_p$ with a subgroup of order r and embedding degree k .
- 2 Use Complex Multiplication method to construct the equation for E .

Ordinary Elliptic Curves: The General Strategy

To construct pairing-friendly ordinary elliptic curves:

- 1 Fix k , find primes p and r such that there exists a curve $E/\mathbb{F}_p$ with a subgroup of order r and embedding degree k .
- 2 Use Complex Multiplication method to construct the equation for E .

Outline

- 1 Pairings in Cryptography
 - Introduction to Pairings
 - Pairings on Elliptic Curves
- 2 How to Construct Pairing-Friendly Elliptic Curves
 - Ordinary vs. Supersingular
 - **The Complex Multiplication Method**
 - Classification of Pairing-Friendly Elliptic Curves
- 3 Construction Methods
 - Curves with Arbitrary Embedding Degree
 - Cocks-Pinch and Dupont-Engge-Morain Methods
 - Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
 - Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

The Complex Multiplication Method

- Originally due to Atkin and Morain for primality testing application.
- Define the *trace* of E to be t such that $\#E(\mathbb{F}_p) = p + 1 - t$.
 - Hasse bound: if E ordinary then $|t| < 2\sqrt{p}$.
- Define the *Complex Multiplication (CM) discriminant* of E to be the square-free part of $4p - t^2$.
- For given square-free $D > 0$, Complex Multiplication (CM) method constructs elliptic curve with CM discriminant D .
 - Used to construct curves with specified number of points.

The Complex Multiplication Method

- Originally due to Atkin and Morain for primality testing application.
- Define the *trace* of E to be t such that $\#E(\mathbb{F}_p) = p + 1 - t$.
 - Hasse bound: if E ordinary then $|t| < 2\sqrt{p}$.
- Define the *Complex Multiplication (CM) discriminant* of E to be the square-free part of $4p - t^2$.
- For given square-free $D > 0$, Complex Multiplication (CM) method constructs elliptic curve with CM discriminant D .
 - Used to construct curves with specified number of points.

The Complex Multiplication Method

- Originally due to Atkin and Morain for primality testing application.
- Define the *trace* of E to be t such that $\#E(\mathbb{F}_p) = p + 1 - t$.
 - Hasse bound: if E ordinary then $|t| < 2\sqrt{p}$.
- Define the *Complex Multiplication (CM) discriminant* of E to be the square-free part of $4p - t^2$.
- For given square-free $D > 0$, Complex Multiplication (CM) method constructs elliptic curve with CM discriminant D .
 - Used to construct curves with specified number of points.

The Complex Multiplication Method

- Originally due to Atkin and Morain for primality testing application.
- Define the *trace* of E to be t such that $\#E(\mathbb{F}_p) = p + 1 - t$.
 - Hasse bound: if E ordinary then $|t| < 2\sqrt{p}$.
- Define the *Complex Multiplication (CM) discriminant* of E to be the square-free part of $4p - t^2$.
- For given square-free $D > 0$, Complex Multiplication (CM) method constructs elliptic curve with CM discriminant D .
 - Used to construct curves with specified number of points.

The Complex Multiplication Method

- Originally due to Atkin and Morain for primality testing application.
- Define the *trace* of E to be t such that $\#E(\mathbb{F}_p) = p + 1 - t$.
 - Hasse bound: if E ordinary then $|t| < 2\sqrt{p}$.
- Define the *Complex Multiplication (CM) discriminant* of E to be the square-free part of $4p - t^2$.
- For given square-free $D > 0$, Complex Multiplication (CM) method constructs elliptic curve with CM discriminant D .
 - Used to construct curves with specified number of points.

The Complex Multiplication Method

- Originally due to Atkin and Morain for primality testing application.
- Define the *trace* of E to be t such that $\#E(\mathbb{F}_p) = p + 1 - t$.
 - Hasse bound: if E ordinary then $|t| < 2\sqrt{p}$.
- Define the *Complex Multiplication (CM) discriminant* of E to be the square-free part of $4p - t^2$.
- For given square-free $D > 0$, Complex Multiplication (CM) method constructs elliptic curve with CM discriminant D .
 - Used to construct curves with specified number of points.

Effectiveness of the CM Method

- Running time of CM method 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 $h_D = 10^5$.
 - Equivalent to $D \approx 10^{10}$.

Effectiveness of the CM Method

- Running time of CM method 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 $h_D = 10^5$.
 - Equivalent to $D \approx 10^{10}$.

Effectiveness of the CM Method

- Running time of CM method 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 $h_D = 10^5$.
 - Equivalent to $D \approx 10^{10}$.

Effectiveness of the CM Method

- Running time of CM method 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 $h_D = 10^5$.
 - Equivalent to $D \approx 10^{10}$.

Effectiveness of the CM Method

- Running time of CM method 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 $h_D = 10^5$.
 - Equivalent to $D \approx 10^{10}$.

Effectiveness of the CM Method

- Running time of CM method 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 $h_D = 10^5$.
 - Equivalent to $D \approx 10^{10}$.

Existence Conditions for Pairing-Friendly Curves

- Fix an embedding degree k , and look for parameters $t = \text{trace}$, $r = \text{subgroup size}$, $p = \text{field size}$, satisfying:
 - 1 p and r are prime.
 - 2 r divides $p + 1 - t$.
 - $E(\mathbb{F}_p)$ has a point of order r .
 - 3 r divides $\Phi_k(p)$, where Φ_k is the k th cyclotomic polynomial.
 - p has exact order k in $(\mathbb{Z}/r\mathbb{Z})^\times$.
 - 4 $4p - t^2 = Dy^2$ for some sufficiently small D and some $y \in \mathbb{Z}$. (This is the “CM equation.”)
- For such t, r, p , if D is not too large ($\sim 10^{10}$) we can construct an elliptic curve E over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .

Existence Conditions for Pairing-Friendly Curves

- Fix an embedding degree k , and look for parameters $t = \text{trace}$, $r = \text{subgroup size}$, $p = \text{field size}$, satisfying:
 - 1 p and r are prime.
 - 2 r divides $p + 1 - t$.
 - $E(\mathbb{F}_p)$ has a point of order r .
 - 3 r divides $\Phi_k(p)$, where Φ_k is the k th cyclotomic polynomial.
 - p has exact order k in $(\mathbb{Z}/r\mathbb{Z})^\times$.
 - 4 $4p - t^2 = Dy^2$ for some sufficiently small D and some $y \in \mathbb{Z}$. (This is the “CM equation.”)
- For such t, r, p , if D is not too large ($\sim 10^{10}$) we can construct an elliptic curve E over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .

Existence Conditions for Pairing-Friendly Curves

- Fix an embedding degree k , and look for parameters $t = \text{trace}$, $r = \text{subgroup size}$, $p = \text{field size}$, satisfying:
 - 1 p and r are prime.
 - 2 r divides $p + 1 - t$.
 - $E(\mathbb{F}_p)$ has a point of order r .
 - 3 r divides $\Phi_k(p)$, where Φ_k is the k th cyclotomic polynomial.
 - p has exact order k in $(\mathbb{Z}/r\mathbb{Z})^\times$.
 - 4 $4p - t^2 = Dy^2$ for some sufficiently small D and some $y \in \mathbb{Z}$. (This is the “CM equation.”)
- For such t, r, p , if D is not too large ($\sim 10^{10}$) we can construct an elliptic curve E over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .

Existence Conditions for Pairing-Friendly Curves

- Fix an embedding degree k , and look for parameters $t = \text{trace}$, $r = \text{subgroup size}$, $p = \text{field size}$, satisfying:
 - 1 p and r are prime.
 - 2 r divides $p + 1 - t$.
 - $E(\mathbb{F}_p)$ has a point of order r .
 - 3 r divides $\Phi_k(p)$, where Φ_k is the k th cyclotomic polynomial.
 - p has exact order k in $(\mathbb{Z}/r\mathbb{Z})^\times$.
 - 4 $4p - t^2 = Dy^2$ for some sufficiently small D and some $y \in \mathbb{Z}$. (This is the “CM equation.”)
- For such t, r, p , if D is not too large ($\sim 10^{10}$) we can construct an elliptic curve E over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .

Existence Conditions for Pairing-Friendly Curves

- Fix an embedding degree k , and look for parameters $t = \text{trace}$, $r = \text{subgroup size}$, $p = \text{field size}$, satisfying:
 - 1 p and r are prime.
 - 2 r divides $p + 1 - t$.
 - $E(\mathbb{F}_p)$ has a point of order r .
 - 3 r divides $\Phi_k(p)$, where Φ_k is the k th cyclotomic polynomial.
 - p has exact order k in $(\mathbb{Z}/r\mathbb{Z})^\times$.
 - 4 $4p - t^2 = Dy^2$ for some sufficiently small D and some $y \in \mathbb{Z}$. (This is the “CM equation.”)
- For such t, r, p , if D is not too large ($\sim 10^{10}$) we can construct an elliptic curve E over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .

Existence Conditions for Pairing-Friendly Curves

- Fix an embedding degree k , and look for parameters $t = \text{trace}$, $r = \text{subgroup size}$, $p = \text{field size}$, satisfying:
 - 1 p and r are prime.
 - 2 r divides $p + 1 - t$.
 - $E(\mathbb{F}_p)$ has a point of order r .
 - 3 r divides $\Phi_k(p)$, where Φ_k is the k th cyclotomic polynomial.
 - p has exact order k in $(\mathbb{Z}/r\mathbb{Z})^\times$.
 - 4 $4p - t^2 = Dy^2$ for some sufficiently small D and some $y \in \mathbb{Z}$. (This is the “CM equation.”)
- For such t, r, p , if D is not too large ($\sim 10^{10}$) we can construct an elliptic curve E over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .

Existence Conditions for Pairing-Friendly Curves

- Fix an embedding degree k , and look for parameters $t = \text{trace}$, $r = \text{subgroup size}$, $p = \text{field size}$, satisfying:
 - 1 p and r are prime.
 - 2 r divides $p + 1 - t$.
 - $E(\mathbb{F}_p)$ has a point of order r .
 - 3 r divides $\Phi_k(p)$, where Φ_k is the k th cyclotomic polynomial.
 - p has exact order k in $(\mathbb{Z}/r\mathbb{Z})^\times$.
 - 4 $4p - t^2 = Dy^2$ for some sufficiently small D and some $y \in \mathbb{Z}$. (This is the “CM equation.”)
- For such t, r, p , if D is not too large ($\sim 10^{10}$) we can construct an elliptic curve E over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .

Existence Conditions for Pairing-Friendly Curves

- Fix an embedding degree k , and look for parameters $t = \text{trace}$, $r = \text{subgroup size}$, $p = \text{field size}$, satisfying:
 - 1 p and r are prime.
 - 2 r divides $p + 1 - t$.
 - $E(\mathbb{F}_p)$ has a point of order r .
 - 3 r divides $\Phi_k(p)$, where Φ_k is the k th cyclotomic polynomial.
 - p has exact order k in $(\mathbb{Z}/r\mathbb{Z})^\times$.
 - 4 $4p - t^2 = Dy^2$ for some sufficiently small D and some $y \in \mathbb{Z}$. (This is the “CM equation.”)
- For such t, r, p , if D is not too large ($\sim 10^{10}$) we can construct an elliptic curve E over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .

Observations about the CM Method

- The embedding degree condition $r \mid \Phi_k(p)$ can be replaced with $r \mid \Phi_k(t - 1)$.
 - r divides $p + 1 - t$ implies $p \equiv t - 1 \pmod{r}$.
- We can use $\#E(\mathbb{F}_p) = p + 1 - t$ to write the “CM equation” in two ways:

$$\begin{aligned} Dy^2 &= 4p - t^2 \\ Dy^2 &= 4hr - (t - 2)^2. \end{aligned}$$

- h is a “cofactor” satisfying $\#E(\mathbb{F}_p) = hr$.
- Set $h = 1$ if we want $\#E(\mathbb{F}_p)$ to be prime.

Observations about the CM Method

- The embedding degree condition $r \mid \Phi_k(p)$ can be replaced with $r \mid \Phi_k(t - 1)$.
 - r divides $p + 1 - t$ implies $p \equiv t - 1 \pmod{r}$.
- We can use $\#E(\mathbb{F}_p) = p + 1 - t$ to write the “CM equation” in two ways:

$$\begin{aligned} Dy^2 &= 4p - t^2 \\ Dy^2 &= 4hr - (t - 2)^2. \end{aligned}$$

- h is a “cofactor” satisfying $\#E(\mathbb{F}_p) = hr$.
- Set $h = 1$ if we want $\#E(\mathbb{F}_p)$ to be prime.

Observations about the CM Method

- The embedding degree condition $r \mid \Phi_k(p)$ can be replaced with $r \mid \Phi_k(t - 1)$.
 - r divides $p + 1 - t$ implies $p \equiv t - 1 \pmod{r}$.
- We can use $\#E(\mathbb{F}_p) = p + 1 - t$ to write the “CM equation” in two ways:

$$\begin{aligned} Dy^2 &= 4p - t^2 \\ Dy^2 &= 4hr - (t - 2)^2. \end{aligned}$$

- h is a “cofactor” satisfying $\#E(\mathbb{F}_p) = hr$.
- Set $h = 1$ if we want $\#E(\mathbb{F}_p)$ to be prime.

Observations about the CM Method

- The embedding degree condition $r \mid \Phi_k(p)$ can be replaced with $r \mid \Phi_k(t - 1)$.
 - r divides $p + 1 - t$ implies $p \equiv t - 1 \pmod{r}$.
- We can use $\#E(\mathbb{F}_p) = p + 1 - t$ to write the “CM equation” in two ways:

$$\begin{aligned} Dy^2 &= 4p - t^2 \\ Dy^2 &= 4hr - (t - 2)^2. \end{aligned}$$

- h is a “cofactor” satisfying $\#E(\mathbb{F}_p) = hr$.
- Set $h = 1$ if we want $\#E(\mathbb{F}_p)$ to be prime.

Observations about the CM Method

- The embedding degree condition $r \mid \Phi_k(p)$ can be replaced with $r \mid \Phi_k(t - 1)$.
 - r divides $p + 1 - t$ implies $p \equiv t - 1 \pmod{r}$.
- We can use $\#E(\mathbb{F}_p) = p + 1 - t$ to write the “CM equation” in two ways:

$$\begin{aligned} Dy^2 &= 4p - t^2 \\ Dy^2 &= 4hr - (t - 2)^2. \end{aligned}$$

- h is a “cofactor” satisfying $\#E(\mathbb{F}_p) = hr$.
- Set $h = 1$ if we want $\#E(\mathbb{F}_p)$ to be prime.

Outline

1 Pairings in Cryptography

- Introduction to Pairings
- Pairings on Elliptic Curves

2 How to Construct Pairing-Friendly Elliptic Curves

- Ordinary vs. Supersingular
- The Complex Multiplication Method
- Classification of Pairing-Friendly Elliptic Curves

3 Construction Methods

- Curves with Arbitrary Embedding Degree
 - Cocks-Pinch and Dupont-Engge-Morain Methods
- Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
- Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

Our Classification

- 1 Curves not in families: Construction gives t, r, p directly; repeat construction to get different curve parameters.
- 2 Families of curves: Parametrize t, r, p as polynomials $t(x), r(x), p(x)$; plug in x to get curve parameters.
 - 1 Sparse families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ grow exponentially.
 - 2 Complete families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ exist for any x .
 - Further classified by properties of $r(x)$.

Our Classification

- 1 Curves not in families: Construction gives t, r, p directly; repeat construction to get different curve parameters.
- 2 Families of curves: Parametrize t, r, p as polynomials $t(x), r(x), p(x)$; plug in x to get curve parameters.
 - 1 Sparse families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ grow exponentially.
 - 2 Complete families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ exist for any x .
 - Further classified by properties of $r(x)$.

Our Classification

- 1 Curves not in families: Construction gives t, r, p directly; repeat construction to get different curve parameters.
- 2 Families of curves: Parametrize t, r, p as polynomials $t(x), r(x), p(x)$; plug in x to get curve parameters.
 - 1 Sparse families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ grow exponentially.
 - 2 Complete families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ exist for any x .
 - Further classified by properties of $r(x)$.

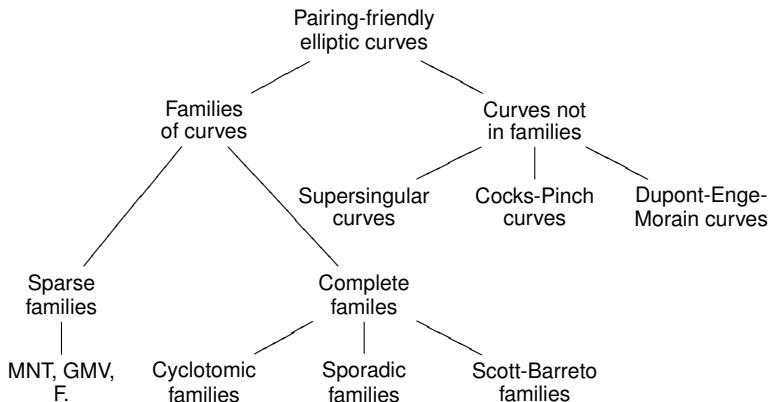
Our Classification

- 1 Curves not in families: Construction gives t, r, p directly; repeat construction to get different curve parameters.
- 2 Families of curves: Parametrize t, r, p as polynomials $t(x), r(x), p(x)$; plug in x to get curve parameters.
 - 1 Sparse families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ grow exponentially.
 - 2 Complete families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ exist for any x .
 - Further classified by properties of $r(x)$.

Our Classification

- 1 Curves not in families: Construction gives t, r, p directly; repeat construction to get different curve parameters.
- 2 Families of curves: Parametrize t, r, p as polynomials $t(x), r(x), p(x)$; plug in x to get curve parameters.
 - 1 Sparse families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ grow exponentially.
 - 2 Complete families: Solutions (x, y) to $4p(x) - t(x)^2 = Dy^2$ exist for any x .
 - Further classified by properties of $r(x)$.

Classification of Pairing-Friendly Elliptic Curves



Outline

1 Pairings in Cryptography

- Introduction to Pairings
- Pairings on Elliptic Curves

2 How to Construct Pairing-Friendly Elliptic Curves

- Ordinary vs. Supersingular
- The Complex Multiplication Method
- Classification of Pairing-Friendly Elliptic Curves

3 Construction Methods

- **Curves with Arbitrary Embedding Degree**
 - Cocks-Pinch and Dupont-Enge-Morain Methods
- Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
- Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

Overview of the Cocks-Pinch Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2.$$

- Cocks-Pinch strategy: Choose r , compute t satisfying divisibility conditions, compute y, p satisfying CM equation.
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order; usually $p \approx 2$.
 - Many curves possible, easy to specify bit sizes.
 - Has been generalized to produce families of curves.

Overview of the Cocks-Pinch Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2.$$

- Cocks-Pinch strategy: Choose r , compute t satisfying divisibility conditions, compute y, p satisfying CM equation.
 - 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.
 - Has been generalized to produce families of curves.

Overview of the Cocks-Pinch Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2.$$

- Cocks-Pinch strategy: Choose r , compute t satisfying divisibility conditions, compute y, p satisfying CM equation.
 - 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.
 - Has been generalized to produce families of curves.

Overview of the Cocks-Pinch Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2.$$

- Cocks-Pinch strategy: Choose r , compute t satisfying divisibility conditions, compute y, p satisfying CM equation.
 - 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.
 - Has been generalized to produce families of curves.

Overview of the Cocks-Pinch Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2.$$

- Cocks-Pinch strategy: Choose r , compute t satisfying divisibility conditions, compute y, p satisfying CM equation.
 - 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.
 - Has been generalized to produce families of curves.

Overview of the Cocks-Pinch Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2.$$

- Cocks-Pinch strategy: Choose r , compute t satisfying divisibility conditions, compute y, p satisfying CM equation.
 - 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.
 - Has been generalized to produce families of curves.

The Cocks-Pinch Method

- 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 $y' = (t' - 2)/\sqrt{-D} \pmod{r}$.
- 4 Lift t', y' to integers t, y , and compute $p = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
- 5 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup.
 - y is constructed so that CM equation $Dy^2 = 4p - t^2$ is automatically satisfied.
 - Since t', y' are essentially random integers in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Cocks-Pinch Method

- 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 $y' = (t' - 2)/\sqrt{-D} \pmod{r}$.
- 4 Lift t', y' to integers t, y , and compute $p = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
- 5 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup.
 - y is constructed so that CM equation $Dy^2 = 4p - t^2$ is automatically satisfied.
 - Since t', y' are essentially random integers in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Cocks-Pinch Method

- 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 $y' = (t' - 2)/\sqrt{-D} \pmod{r}$.
- 4 Lift t', y' to integers t, y , and compute $p = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
- 5 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup.
 - y is constructed so that CM equation $Dy^2 = 4p - t^2$ is automatically satisfied.
 - Since t', y' are essentially random integers in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Cocks-Pinch Method

- 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 $y' = (t' - 2)/\sqrt{-D} \pmod{r}$.
 - 4 Lift t', y' to integers t, y , and compute $p = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
 - 5 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup.
- y is constructed so that CM equation $Dy^2 = 4p - t^2$ is automatically satisfied.
 - Since t', y' are essentially random integers in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Cocks-Pinch Method

- 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 $y' = (t' - 2)/\sqrt{-D} \pmod{r}$.
 - 4 Lift t' , y' to integers t , y , and compute $p = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
 - 5 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup.
- y is constructed so that CM equation $Dy^2 = 4p - t^2$ is automatically satisfied.
 - Since t' , y' are essentially random integers in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Cocks-Pinch Method

- 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 $y' = (t' - 2)/\sqrt{-D} \pmod{r}$.
 - 4 Lift t', y' to integers t, y , and compute $p = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
 - 5 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup.
- y is constructed so that CM equation $Dy^2 = 4p - t^2$ is automatically satisfied.
 - Since t', y' are essentially random integers in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Cocks-Pinch Method

- 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 $y' = (t' - 2)/\sqrt{-D} \pmod{r}$.
- 4 Lift t', y' to integers t, y , and compute $p = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
- 5 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup.
 - y is constructed so that CM equation $Dy^2 = 4p - t^2$ is automatically satisfied.
 - Since t', y' are essentially random integers in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Cocks-Pinch Method

- 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 $y' = (t' - 2)/\sqrt{-D} \pmod{r}$.
- 4 Lift t' , y' to integers t , y , and compute $p = (t^2 + Dy^2)/4$ (in $\mathbb{Q}$).
- 5 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup.
 - y is constructed so that CM equation $Dy^2 = 4p - t^2$ is automatically satisfied.
 - Since t' , y' are essentially random integers in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

Overview of the Dupont-Engge-Morain Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2$$

- Dupont-Engge-Morain strategy: Choose D, y , use resultants to find t and r simultaneously, compute p such that CM equation is satisfied.
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order; usually $p \approx 2$.
 - Has not been generalized to produce families of curves.

Overview of the Dupont-Engge-Morain Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2$$

- Dupont-Engge-Morain strategy: Choose D, y , use resultants to find t and r simultaneously, compute p 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.

Overview of the Dupont-Enge-Morain Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2$$

- Dupont-Enge-Morain strategy: Choose D, y , use resultants to find t and r simultaneously, compute p 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.

Overview of the Dupont-Enge-Morain Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2$$

- Dupont-Enge-Morain strategy: Choose D, y , use resultants to find t and r simultaneously, compute p 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.

Overview of the Dupont-Enge-Morain Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2$$

- Dupont-Enge-Morain strategy: Choose D, y , use resultants to find t and r simultaneously, compute p 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.

The Dupont-Enge-Morain Method

- 1 Fix k , 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 $\Phi_k(t-1) \equiv Dy^2 - (t-2)^2 \equiv 0 \pmod{r}$.
 - 3 Lift t' to integer t , compute $p = (t^2 + Dy^2)/4$.
 - 4 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .
- Since t' is essentially random in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Dupont-Enge-Morain Method

- 1 Fix k , 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 $\Phi_k(t-1) \equiv Dy^2 - (t-2)^2 \equiv 0 \pmod{r}$.
 - 3 Lift t' to integer t , compute $p = (t^2 + Dy^2)/4$.
 - 4 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .
- Since t' is essentially random in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Dupont-Enge-Morain Method

- 1 Fix k , 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 $\Phi_k(t-1) \equiv Dy^2 - (t-2)^2 \equiv 0 \pmod{r}$.
 - 3 Lift t' to integer t , compute $p = (t^2 + Dy^2)/4$.
 - 4 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .
- Since t' is essentially random in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Dupont-Enge-Morain Method

- 1 Fix k , 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 $\Phi_k(t-1) \equiv Dy^2 - (t-2)^2 \equiv 0 \pmod{r}$.
 - 3 Lift t' to integer t , compute $p = (t^2 + Dy^2)/4$.
 - 4 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .
- Since t' is essentially random in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

The Dupont-Enge-Morain Method

- 1 Fix k , 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 $\Phi_k(t-1) \equiv Dy^2 - (t-2)^2 \equiv 0 \pmod{r}$.
 - 3 Lift t' to integer t , compute $p = (t^2 + Dy^2)/4$.
 - 4 If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order- r subgroup and embedding degree k .
- Since t' is essentially random in $[0, r)$, $p \approx r^2$, so $\rho \approx 2$.

Outline

- 1 Pairings in Cryptography
 - Introduction to Pairings
 - Pairings on Elliptic Curves
- 2 How to Construct Pairing-Friendly Elliptic Curves
 - Ordinary vs. Supersingular
 - The Complex Multiplication Method
 - Classification of Pairing-Friendly Elliptic Curves
- 3 Construction Methods
 - Curves with Arbitrary Embedding Degree
 - Cocks-Pinch and Dupont-Engge-Morain Methods
 - Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
 - Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

Overview of the Miyaji-Nakabayashi-Takano Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Miyaji-Nakabayashi-Takano method: 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 4 possible embedding degrees: $k = 3, 4, 6, 10$.
 - Solutions to CM equation grow exponentially.

Overview of the Miyaji-Nakabayashi-Takano Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Miyaji-Nakabayashi-Takano method: 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 4 possible embedding degrees: $k = 3, 4, 6, 10$.
 - Solutions to CM equation grow exponentially.

Overview of the Miyaji-Nakabayashi-Takano Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Miyaji-Nakabayashi-Takano method: 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 4 possible embedding degrees: $k = 3, 4, 6, 10$.
 - Solutions to CM equation grow exponentially.

Overview of the Miyaji-Nakabayashi-Takano Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Miyaji-Nakabayashi-Takano method: 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 4 possible embedding degrees: $k = 3, 4, 6, 10$.
 - Solutions to CM equation grow exponentially.

Overview of the Miyaji-Nakabayashi-Takano Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Miyaji-Nakabayashi-Takano method: 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 4 possible embedding degrees: $k = 3, 4, 6, 10$.
 - Solutions to CM equation grow exponentially.

Overview of the Miyaji-Nakabayashi-Takano Method

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Miyaji-Nakabayashi-Takano method: 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 4 possible embedding degrees: $k = 3, 4, 6, 10$.
 - Solutions to CM equation grow exponentially.

The Miyaji-Nakabayashi-Takano (MNT) Method

- 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 $p(x) = h(x)r(x) + t(x) - 1$.
- 4 Find integer solutions (x_0, y_0) to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
- 5 If $p(x_0)$, $r(x_0)$ are both prime for some x_0 , use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with $h(x_0)r(x_0)$ points.
- For the rest of this section, we will assume $h(x)$ is a constant.

The Miyaji-Nakabayashi-Takano (MNT) Method

- 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 $p(x) = h(x)r(x) + t(x) - 1$.
- 4 Find integer solutions (x_0, y_0) to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
- 5 If $p(x_0)$, $r(x_0)$ are both prime for some x_0 , use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with $h(x_0)r(x_0)$ points.
- For the rest of this section, we will assume $h(x)$ is a constant.

The Miyaji-Nakabayashi-Takano (MNT) Method

- 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 $p(x) = h(x)r(x) + t(x) - 1$.
 - 4 Find integer solutions (x_0, y_0) to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
 - 5 If $p(x_0)$, $r(x_0)$ are both prime for some x_0 , use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with $h(x_0)r(x_0)$ points.
- For the rest of this section, we will assume $h(x)$ is a constant.

The Miyaji-Nakabayashi-Takano (MNT) Method

- 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 $p(x) = h(x)r(x) + t(x) - 1$.
 - 4 Find integer solutions (x_0, y_0) to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
 - 5 If $p(x_0)$, $r(x_0)$ are both prime for some x_0 , use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with $h(x_0)r(x_0)$ points.
- For the rest of this section, we will assume $h(x)$ is a constant.

The Miyaji-Nakabayashi-Takano (MNT) Method

- 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 $p(x) = h(x)r(x) + t(x) - 1$.
 - 4 Find integer solutions (x_0, y_0) to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
 - 5 If $p(x_0)$, $r(x_0)$ are both prime for some x_0 , use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with $h(x_0)r(x_0)$ points.
- For the rest of this section, we will assume $h(x)$ is a constant.

The Miyaji-Nakabayashi-Takano (MNT) Method

- 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 $p(x) = h(x)r(x) + t(x) - 1$.
 - 4 Find integer solutions (x_0, y_0) to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
 - 5 If $p(x_0)$, $r(x_0)$ are both prime for some x_0 , use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with $h(x_0)r(x_0)$ points.
- For the rest of this section, we will assume $h(x)$ is a constant.

The Miyaji-Nakabayashi-Takano (MNT) Method

- 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 $p(x) = h(x)r(x) + t(x) - 1$.
 - 4 Find integer solutions (x_0, y_0) to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
 - 5 If $p(x_0)$, $r(x_0)$ are both prime for some x_0 , use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with $h(x_0)r(x_0)$ points.
- For the rest of this section, we will assume $h(x)$ is a constant.

Obstacles to the MNT Method

- Step 4 is the difficult part: finding integer solutions (x_0, y_0) to

$$Dy^2 = 4hr(x) - (t(x) - 2)^2.$$

- If $f(x) = 4hr(x) - (t(x) - 2)^2$ has degree ≥ 3 and no multiple roots, then $Dy^2 = f(x)$ has only a finite number of integer solutions! (Siegel's Theorem)
- Consequence: 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 $\deg r(x)$ must be a multiple of $\deg \Phi_k > 2$.

Obstacles to the MNT Method

- Step 4 is the difficult part: finding integer solutions (x_0, y_0) to

$$Dy^2 = 4hr(x) - (t(x) - 2)^2.$$

- If $f(x) = 4hr(x) - (t(x) - 2)^2$ has degree ≥ 3 and no multiple roots, then $Dy^2 = f(x)$ has only a finite number of integer solutions! (Siegel's Theorem)
- Consequence: 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 $\deg r(x)$ must be a multiple of $\deg \Phi_k > 2$.

Obstacles to the MNT Method

- Step 4 is the difficult part: finding integer solutions (x_0, y_0) to

$$Dy^2 = 4hr(x) - (t(x) - 2)^2.$$

- If $f(x) = 4hr(x) - (t(x) - 2)^2$ has degree ≥ 3 and no multiple roots, then $Dy^2 = f(x)$ has only a finite number of integer solutions! (Siegel's Theorem)
- Consequence: 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 $\deg r(x)$ must be a multiple of $\deg \Phi_k > 2$.

Obstacles to the MNT Method

- Step 4 is the difficult part: finding integer solutions (x_0, y_0) to

$$Dy^2 = 4hr(x) - (t(x) - 2)^2.$$

- If $f(x) = 4hr(x) - (t(x) - 2)^2$ has degree ≥ 3 and no multiple roots, then $Dy^2 = f(x)$ has only a finite number of integer solutions! (Siegel's Theorem)
- Consequence: 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 $\deg r(x)$ must be a multiple of $\deg \Phi_k > 2$.

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:
 - Choose $t(x)$ linear; then $r(x)$ is quadratic, and so is $f(x)$.
 - Use standard algorithms to find solutions (x_0, y_0) to $Dy^2 = f(x)$.
 - If no solutions of appropriate size, or $p(x)$ 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).
- Galbraith-McKee-Valena, Scott-Barreto extend MNT idea by allowing cofactor $h(x) \neq 1$, so that $\#E(\mathbb{F}_p) = h(x)r(x)$.
 - Find many more suitable curves than original MNT construction.

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_0, y_0) to $Dy^2 = f(x)$.
 - 3 If no solutions of appropriate size, or $p(x)$ 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).
- Galbraith-McKee-Valença, Scott-Barreto extend MNT idea by allowing cofactor $h(x) \neq 1$, so that $\#E(\mathbb{F}_p) = h(x)r(x)$.
 - Find many more suitable curves than original MNT construction.

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_0, y_0) to $Dy^2 = f(x)$.
 - 3 If no solutions of appropriate size, or $p(x)$ 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).
- Galbraith-McKee-Valença, Scott-Barreto extend MNT idea by allowing cofactor $h(x) \neq 1$, so that $\#E(\mathbb{F}_p) = h(x)r(x)$.
 - Find many more suitable curves than original MNT construction.

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_0, y_0) to $Dy^2 = f(x)$.
 - 3 If no solutions of appropriate size, or $p(x)$ 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).
- Galbraith-McKee-Valença, Scott-Barreto extend MNT idea by allowing cofactor $h(x) \neq 1$, so that $\#E(\mathbb{F}_p) = h(x)r(x)$.
 - Find many more suitable curves than original MNT construction.

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_0, y_0) to $Dy^2 = f(x)$.
 - 3 If no solutions of appropriate size, or $p(x)$ 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).
- Galbraith-McKee-Valença, Scott-Barreto extend MNT idea by allowing cofactor $h(x) \neq 1$, so that $\#E(\mathbb{F}_p) = h(x)r(x)$.
 - Find many more suitable curves than original MNT construction.

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_0, y_0) to $Dy^2 = f(x)$.
 - 3 If no solutions of appropriate size, or $p(x)$ 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).
- Galbraith-McKee-Valença, Scott-Barreto extend MNT idea by allowing cofactor $h(x) \neq 1$, so that $\#E(\mathbb{F}_p) = h(x)r(x)$.
 - Find many more suitable curves than original MNT construction.

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_0, y_0) to $Dy^2 = f(x)$.
 - 3 If no solutions of appropriate size, or $p(x)$ 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).
- Galbraith-McKee-Valença, Scott-Barreto extend MNT idea by allowing cofactor $h(x) \neq 1$, so that $\#E(\mathbb{F}_p) = h(x)r(x)$.
 - Find many more suitable curves than original MNT construction.

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_0, y_0) to $Dy^2 = f(x)$.
 - 3 If no solutions of appropriate size, or $p(x)$ 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).
- Galbraith-McKee-Valena, Scott-Barreto extend MNT idea by allowing cofactor $h(x) \neq 1$, so that $\#E(\mathbb{F}_p) = h(x)r(x)$.
 - Find many more suitable curves than original MNT construction.

F. 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- Galbraith-McKee-Valena: 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.
 - Can't be extended to allow cofactors $h \neq 1$.

F. 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- Galbraith-McKee-Valena: 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.
 - Can't be extended to allow cofactors $h \neq 1$.

F. 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- 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.
 - Can't be extended to allow cofactors $h \neq 1$.

F. 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- Galbraith-McKee-Valena: 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.
 - Can't be extended to allow cofactors $h \neq 1$.

F. 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- Galbraith-McKee-Valena: 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.
 - Can't be extended to allow cofactors $h \neq 1$.

F. 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- Galbraith-McKee-Valena: 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.
 - Can't be extended to allow cofactors $h \neq 1$.

F. 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- Galbraith-McKee-Valena: 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.
 - Can't be extended to allow cofactors $h \neq 1$.

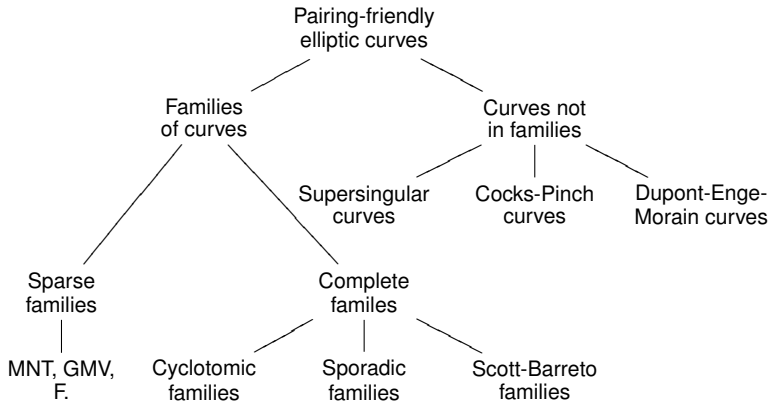
F. Solution for $k = 10$

- 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- Galbraith-McKee-Valena: 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.
 - Can't be extended to allow cofactors $h \neq 1$.

F. 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 irred. factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x)$, $t(x)$ such that the leading terms of $4r$ and t^2 cancel out.
 - Smallest possible case: $\deg r = 4$, $\deg t = 2$.
- Galbraith-McKee-Valena: 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.
 - Can't be extended to allow cofactors $h \neq 1$.

Classification of Pairing-Friendly Elliptic Curves



Outline

- 1 Pairings in Cryptography
 - Introduction to Pairings
 - Pairings on Elliptic Curves
- 2 How to Construct Pairing-Friendly Elliptic Curves
 - Ordinary vs. Supersingular
 - The Complex Multiplication Method
 - Classification of Pairing-Friendly Elliptic Curves
- 3 Construction Methods
 - Curves with Arbitrary Embedding Degree
 - Cocks-Pinch and Dupont-Engge-Morain Methods
 - Sparse Families of Pairing-Friendly Curves
 - The Miyaji-Nakabayashi-Takano Method and Extensions
 - Complete Families of Curves
 - Cyclotomic, Sproadic, and Scott-Barreto Families

Overview of Complete Families

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Complete families method: Choose $r(x)$, use properties of the number field $K = \mathbb{Q}[x]/(r(x))$ to compute $t(x), p(x)$ satisfying CM equation for any x .
 - Good for constructing curves with arbitrary k .
 - Usually gives curves with $1 < \rho < 2$.
 - Easy to specify bit sizes of curves (if k not too large).

Overview of Complete Families

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Complete families method: Choose $r(x)$, use properties of the number field $K = \mathbb{Q}[x]/(r(x))$ to compute $t(x), p(x)$ satisfying CM equation for any x .
 - Good for constructing curves with arbitrary k .
 - Usually gives curves with $1 < \rho < 2$.
 - Easy to specify bit sizes of curves (if k not too large).

Overview of Complete Families

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Complete families method: Choose $r(x)$, use properties of the number field $K = \mathbb{Q}[x]/(r(x))$ to compute $t(x), p(x)$ satisfying CM equation for any x .
 - Good for constructing curves with arbitrary k .
 - Usually gives curves with $1 < \rho < 2$.
 - Easy to specify bit sizes of curves (if k not too large).

Overview of Complete Families

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Complete families method: Choose $r(x)$, use properties of the number field $K = \mathbb{Q}[x]/(r(x))$ to compute $t(x), p(x)$ satisfying CM equation for any x .
 - Good for constructing curves with arbitrary k .
 - Usually gives curves with $1 < \rho < 2$.
 - Easy to specify bit sizes of curves (if k not too large).

Overview of Complete Families

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Complete families method: Choose $r(x)$, use properties of the number field $K = \mathbb{Q}[x]/(r(x))$ to compute $t(x), p(x)$ satisfying CM equation for any x .
 - Good for constructing curves with arbitrary k .
 - Usually gives curves with $1 < \rho < 2$.
 - Easy to specify bit sizes of curves (if k not too large).

Overview of Complete Families

- Recall: for fixed D, k , we are looking for t, r, p satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4p - t^2 = 4hr - (t - 2)^2$$

for some y .

- Idea: Parametrize t, r, p, h as polynomials $t(x), r(x), p(x), h(x)$.
- Complete families method: Choose $r(x)$, use properties of the number field $K = \mathbb{Q}[x]/(r(x))$ to compute $t(x), p(x)$ satisfying CM equation for any x .
 - Good for constructing curves with arbitrary k .
 - Usually gives curves with $1 < \rho < 2$.
 - Easy to specify bit sizes of curves (if k not too large).

Constructing Complete Families of Curves

- 1 Fix D, k , choose an irreducible polynomial $r(x)$.
 - Let K be the number field $\mathbb{Q}[x]/(r(x))$.
 - Require that K contain a k th root of unity ζ_k .
- 2 Choose $t(x)$ to be a polynomial representing $1 + \zeta_k \in K$.
- 3 Compute $y(x)$ so that CM equation is satisfied in K .
- 4 Compute $p(x) = (t(x)^2 + Dy(x)^2)/4$ (in $\mathbb{Q}[x]$).
- 5 If $p(x_0)$ is an integer for some x_0 and $p(x_0), r(x_0)$ are prime, use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with an order- $r(x_0)$ subgroup and embedding degree k .

Constructing Complete Families of Curves

- 1 Fix D, k , choose an irreducible polynomial $r(x)$.
 - Let K be the number field $\mathbb{Q}[x]/(r(x))$.
 - Require that K contain a k th root of unity ζ_k .
- 2 Choose $t(x)$ to be a polynomial representing $1 + \zeta_k \in K$.
- 3 Compute $y(x)$ so that CM equation is satisfied in K .
- 4 Compute $p(x) = (t(x)^2 + Dy(x)^2)/4$ (in $\mathbb{Q}[x]$).
- 5 If $p(x_0)$ is an integer for some x_0 and $p(x_0), r(x_0)$ are prime, use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with an order- $r(x_0)$ subgroup and embedding degree k .

Constructing Complete Families of Curves

- 1 Fix D, k , choose an irreducible polynomial $r(x)$.
 - Let K be the number field $\mathbb{Q}[x]/(r(x))$.
 - Require that K contain a k th root of unity ζ_k .
- 2 Choose $t(x)$ to be a polynomial representing $1 + \zeta_k \in K$.
- 3 Compute $y(x)$ so that CM equation is satisfied in K .
- 4 Compute $p(x) = (t(x)^2 + Dy(x)^2)/4$ (in $\mathbb{Q}[x]$).
- 5 If $p(x_0)$ is an integer for some x_0 and $p(x_0), r(x_0)$ are prime, use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with an order- $r(x_0)$ subgroup and embedding degree k .

Constructing Complete Families of Curves

- 1 Fix D, k , choose an irreducible polynomial $r(x)$.
 - Let K be the number field $\mathbb{Q}[x]/(r(x))$.
 - Require that K contain a k th root of unity ζ_k .
- 2 Choose $t(x)$ to be a polynomial representing $1 + \zeta_k \in K$.
- 3 Compute $y(x)$ so that CM equation is satisfied in K .
- 4 Compute $p(x) = (t(x)^2 + Dy(x)^2)/4$ (in $\mathbb{Q}[x]$).
- 5 If $p(x_0)$ is an integer for some x_0 and $p(x_0), r(x_0)$ are prime, use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with an order- $r(x_0)$ subgroup and embedding degree k .

Constructing Complete Families of Curves

- 1 Fix D, k , choose an irreducible polynomial $r(x)$.
 - Let K be the number field $\mathbb{Q}[x]/(r(x))$.
 - Require that K contain a k th root of unity ζ_k .
- 2 Choose $t(x)$ to be a polynomial representing $1 + \zeta_k \in K$.
- 3 Compute $y(x)$ so that CM equation is satisfied in K .
- 4 Compute $p(x) = (t(x)^2 + Dy(x)^2)/4$ (in $\mathbb{Q}[x]$).
- 5 If $p(x_0)$ is an integer for some x_0 and $p(x_0), r(x_0)$ are prime, use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with an order- $r(x_0)$ subgroup and embedding degree k .

Constructing Complete Families of Curves

- 1 Fix D, k , choose an irreducible polynomial $r(x)$.
 - Let K be the number field $\mathbb{Q}[x]/(r(x))$.
 - Require that K contain a k th root of unity ζ_k .
- 2 Choose $t(x)$ to be a polynomial representing $1 + \zeta_k \in K$.
- 3 Compute $y(x)$ so that CM equation is satisfied in K .
- 4 Compute $p(x) = (t(x)^2 + Dy(x)^2)/4$ (in $\mathbb{Q}[x]$).
- 5 If $p(x_0)$ is an integer for some x_0 and $p(x_0), r(x_0)$ are prime, use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with an order- $r(x_0)$ subgroup and embedding degree k .

Constructing Complete Families of Curves

- 1 Fix D, k , choose an irreducible polynomial $r(x)$.
 - Let K be the number field $\mathbb{Q}[x]/(r(x))$.
 - Require that K contain a k th root of unity ζ_k .
- 2 Choose $t(x)$ to be a polynomial representing $1 + \zeta_k \in K$.
- 3 Compute $y(x)$ so that CM equation is satisfied in K .
- 4 Compute $p(x) = (t(x)^2 + Dy(x)^2)/4$ (in $\mathbb{Q}[x]$).
- 5 If $p(x_0)$ is an integer for some x_0 and $p(x_0), r(x_0)$ are prime, use CM method to construct elliptic curve over $\mathbb{F}_{p(x_0)}$ with an order- $r(x_0)$ subgroup and embedding degree k .

Properties of Complete Families

- For large x , $\rho \approx \deg p / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg p \leq 2 \deg r - 2$.
 - Can always get $\rho < 2$, improving on CP, DEM methods.
 - With clever choices of $r(x)$, $t(x)$, ρ can be decreased even further.
 - Best current results: $\rho = \frac{k+1}{k-1}$ for k prime $\equiv 3 \pmod{4}$.
- No restrictions on k , and many values of x_0, D produce curves.
 - Compare with sparse families: $k \leq 10$, and values of x_0 grow exponentially.
- Complete families subdivided according to type of number field $K = \mathbb{Q}[x]/(r(x))$.

Properties of Complete Families

- For large x , $\rho \approx \deg p / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg p \leq 2 \deg r - 2$.
 - Can always get $\rho < 2$, improving on CP, DEM methods.
 - With clever choices of $r(x)$, $t(x)$, ρ can be decreased even further.
 - Best current results: $\rho = \frac{k+1}{k-1}$ for k prime $\equiv 3 \pmod{4}$.
- No restrictions on k , and many values of x_0, D produce curves.
 - Compare with sparse families: $k \leq 10$, and values of x_0 grow exponentially.
- Complete families subdivided according to type of number field $K = \mathbb{Q}[x]/(r(x))$.

Properties of Complete Families

- For large x , $\rho \approx \deg p / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg p \leq 2 \deg r - 2$.
 - Can always get $\rho < 2$, improving on CP, DEM methods.
 - With clever choices of $r(x)$, $t(x)$, ρ can be decreased even further.
 - Best current results: $\rho = \frac{k+1}{k-1}$ for k prime $\equiv 3 \pmod{4}$.
- No restrictions on k , and many values of x_0, D produce curves.
 - Compare with sparse families: $k \leq 10$, and values of x_0 grow exponentially.
- Complete families subdivided according to type of number field $K = \mathbb{Q}[x]/(r(x))$.

Properties of Complete Families

- For large x , $\rho \approx \deg p / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg p \leq 2 \deg r - 2$.
 - Can always get $\rho < 2$, improving on CP, DEM methods.
 - With clever choices of $r(x)$, $t(x)$, ρ can be decreased even further.
 - Best current results: $\rho = \frac{k+1}{k-1}$ for k prime $\equiv 3 \pmod{4}$.
- No restrictions on k , and many values of x_0, D produce curves.
 - Compare with sparse families: $k \leq 10$, and values of x_0 grow exponentially.
- Complete families subdivided according to type of number field $K = \mathbb{Q}[x]/(r(x))$.

Properties of Complete Families

- For large x , $\rho \approx \deg p / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg p \leq 2 \deg r - 2$.
 - Can always get $\rho < 2$, improving on CP, DEM methods.
 - With clever choices of $r(x), t(x)$, ρ can be decreased even further.
 - Best current results: $\rho = \frac{k+1}{k-1}$ for k prime $\equiv 3 \pmod{4}$.
- No restrictions on k , and many values of x_0, D produce curves.
 - Compare with sparse families: $k \leq 10$, and values of x_0 grow exponentially.
- Complete families subdivided according to type of number field $K = \mathbb{Q}[x]/(r(x))$.

Properties of Complete Families

- For large x , $\rho \approx \deg p / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg p \leq 2 \deg r - 2$.
 - Can always get $\rho < 2$, improving on CP, DEM methods.
 - With clever choices of $r(x), t(x)$, ρ can be decreased even further.
 - Best current results: $\rho = \frac{k+1}{k-1}$ for k prime $\equiv 3 \pmod{4}$.
- No restrictions on k , and many values of x_0, D produce curves.
 - Compare with sparse families: $k \leq 10$, and values of x_0 grow exponentially.
- Complete families subdivided according to type of number field $K = \mathbb{Q}[x]/(r(x))$.

Properties of Complete Families

- For large x , $\rho \approx \deg p / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg p \leq 2 \deg r - 2$.
 - Can always get $\rho < 2$, improving on CP, DEM methods.
 - With clever choices of $r(x), t(x)$, ρ can be decreased even further.
 - Best current results: $\rho = \frac{k+1}{k-1}$ for k prime $\equiv 3 \pmod{4}$.
- No restrictions on k , and many values of x_0, D produce curves.
 - Compare with sparse families: $k \leq 10$, and values of x_0 grow exponentially.
- Complete families subdivided according to type of number field $K = \mathbb{Q}[x]/(r(x))$.

Properties of Complete Families

- For large x , $\rho \approx \deg p / \deg r$.
- Working modulo $r(x)$, we can choose $t(x), y(x)$ such that $\deg t, \deg y < \deg r$, so $\deg p \leq 2 \deg r - 2$.
 - Can always get $\rho < 2$, improving on CP, DEM methods.
 - With clever choices of $r(x), t(x)$, ρ can be decreased even further.
 - Best current results: $\rho = \frac{k+1}{k-1}$ for k prime $\equiv 3 \pmod{4}$.
- No restrictions on k , and many values of x_0, D produce curves.
 - Compare with sparse families: $k \leq 10$, and values of x_0 grow exponentially.
- Complete families subdivided according to type of number field $K = \mathbb{Q}[x]/(r(x))$.

Cyclotomic Families

- Idea of Barreto-Lynn-Scott, Brezing-Weng: Fix k, D , choose $r(x)$ to be cyclotomic polynomial $\Phi_\ell(x)$ with $k \mid \ell$, $4D \mid \ell$.
 - Then $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$, and K contains $\zeta_k, \sqrt{-D}$.
 - E.g., $k = 8, D = 3, r(x) = \Phi_{24}(x), K \cong \mathbb{Q}(\zeta_{24})$.
- CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$ factors in K as

$$(\zeta_k - 1 + y\sqrt{-D})(\zeta_k - 1 - y\sqrt{-D}) \equiv 0 \pmod{r(x)}.$$

- If $y(x)$ is a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K , then CM equation automatically satisfied.
- Restriction: $\sqrt{-D}$ in $\mathbb{Q}(\zeta_\ell)$ implies D divides ℓ .
 - In practice, usually set $D = 1, 2$, or 3 .

Cyclotomic Families

- Idea of Barreto-Lynn-Scott, Brezing-Weng: Fix k, D , choose $r(x)$ to be cyclotomic polynomial $\Phi_\ell(x)$ with $k \mid \ell$, $4D \mid \ell$.
 - Then $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$, and K contains $\zeta_k, \sqrt{-D}$.
 - E.g., $k = 8, D = 3, r(x) = \Phi_{24}(x), K \cong \mathbb{Q}(\zeta_{24})$.
- CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$ factors in K as

$$\left(\zeta_k - 1 + y\sqrt{-D}\right) \left(\zeta_k - 1 - y\sqrt{-D}\right) \equiv 0 \pmod{r(x)}.$$

- If $y(x)$ is a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K , then CM equation automatically satisfied.
- Restriction: $\sqrt{-D}$ in $\mathbb{Q}(\zeta_\ell)$ implies D divides ℓ .
 - In practice, usually set $D = 1, 2$, or 3 .

Cyclotomic Families

- Idea of Barreto-Lynn-Scott, Brezing-Weng: Fix k, D , choose $r(x)$ to be cyclotomic polynomial $\Phi_\ell(x)$ with $k \mid \ell$, $4D \mid \ell$.
 - Then $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$, and K contains $\zeta_k, \sqrt{-D}$.
 - E.g., $k = 8, D = 3, r(x) = \Phi_{24}(x), K \cong \mathbb{Q}(\zeta_{24})$.
- CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$ factors in K as

$$\left(\zeta_k - 1 + y\sqrt{-D}\right) \left(\zeta_k - 1 - y\sqrt{-D}\right) \equiv 0 \pmod{r(x)}.$$

- If $y(x)$ is a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K , then CM equation automatically satisfied.
- Restriction: $\sqrt{-D}$ in $\mathbb{Q}(\zeta_\ell)$ implies D divides ℓ .
 - In practice, usually set $D = 1, 2$, or 3 .

Cyclotomic Families

- Idea of Barreto-Lynn-Scott, Brezing-Weng: Fix k, D , choose $r(x)$ to be cyclotomic polynomial $\Phi_\ell(x)$ with $k \mid \ell$, $4D \mid \ell$.
 - Then $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$, and K contains $\zeta_k, \sqrt{-D}$.
 - E.g., $k = 8, D = 3, r(x) = \Phi_{24}(x), K \cong \mathbb{Q}(\zeta_{24})$.
- CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$ factors in K as

$$(\zeta_k - 1 + y\sqrt{-D})(\zeta_k - 1 - y\sqrt{-D}) \equiv 0 \pmod{r(x)}.$$

- If $y(x)$ is a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K , then CM equation automatically satisfied.
- Restriction: $\sqrt{-D}$ in $\mathbb{Q}(\zeta_\ell)$ implies D divides ℓ .
 - In practice, usually set $D = 1, 2$, or 3 .

Cyclotomic Families

- Idea of Barreto-Lynn-Scott, Brezing-Weng: Fix k, D , choose $r(x)$ to be cyclotomic polynomial $\Phi_\ell(x)$ with $k \mid \ell$, $4D \mid \ell$.
 - Then $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$, and K contains $\zeta_k, \sqrt{-D}$.
 - E.g., $k = 8, D = 3, r(x) = \Phi_{24}(x), K \cong \mathbb{Q}(\zeta_{24})$.
- CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$ factors in K as

$$(\zeta_k - 1 + y\sqrt{-D})(\zeta_k - 1 - y\sqrt{-D}) \equiv 0 \pmod{r(x)}.$$

- If $y(x)$ is a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K , then CM equation automatically satisfied.
- Restriction: $\sqrt{-D}$ in $\mathbb{Q}(\zeta_\ell)$ implies D divides ℓ .
 - In practice, usually set $D = 1, 2$, or 3 .

Cyclotomic Families

- Idea of Barreto-Lynn-Scott, Brezing-Weng: Fix k, D , choose $r(x)$ to be cyclotomic polynomial $\Phi_\ell(x)$ with $k \mid \ell$, $4D \mid \ell$.
 - Then $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$, and K contains $\zeta_k, \sqrt{-D}$.
 - E.g., $k = 8, D = 3, r(x) = \Phi_{24}(x), K \cong \mathbb{Q}(\zeta_{24})$.
- CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$ factors in K as

$$\left(\zeta_k - 1 + y\sqrt{-D}\right) \left(\zeta_k - 1 - y\sqrt{-D}\right) \equiv 0 \pmod{r(x)}.$$

- If $y(x)$ is a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K , then CM equation automatically satisfied.
- Restriction: $\sqrt{-D}$ in $\mathbb{Q}(\zeta_\ell)$ implies D divides ℓ .
 - In practice, usually set $D = 1, 2$, or 3 .

Cyclotomic Families

- Idea of Barreto-Lynn-Scott, Brezing-Weng: Fix k, D , choose $r(x)$ to be cyclotomic polynomial $\Phi_\ell(x)$ with $k \mid \ell$, $4D \mid \ell$.
 - Then $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_\ell)$, and K contains $\zeta_k, \sqrt{-D}$.
 - E.g., $k = 8, D = 3, r(x) = \Phi_{24}(x), K \cong \mathbb{Q}(\zeta_{24})$.
- CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$ factors in K as

$$(\zeta_k - 1 + y\sqrt{-D})(\zeta_k - 1 - y\sqrt{-D}) \equiv 0 \pmod{r(x)}.$$

- If $y(x)$ is a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in K , then CM equation automatically satisfied.
- Restriction: $\sqrt{-D}$ in $\mathbb{Q}(\zeta_\ell)$ implies D divides ℓ .
 - In practice, usually set $D = 1, 2$, or 3 .

Example of a Cyclotomic Family (Brezing-Weng)

- Fix $k = 8$, $D = 3$.
- $r(x) = \Phi_{24}(x) = x^8 - x^4 + 1$ defines $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{24})$.
- $\zeta_8 \mapsto x^5 - x$ in K , so choose $t(x) = x^5 - x + 1$.
- $\sqrt{-3} \mapsto 2x^4 - 1$ in K , so choose

$$y(x) = \frac{\zeta_8 - 1}{\sqrt{-3}} = \frac{1}{3}(x^5 + 2x^4 + x - 1)$$

- Compute

$$p(x) = \frac{t(x)^2 + Dy(x)^2}{4} = \frac{1}{3}(x-1)^2(x^8 - x^4 + 1) + x^9$$

- Evaluating at $x = 1000726$ gives 160-bit prime r and 198-bit prime p .
 - $y^2 = x^3 + 14$ over $\mathbb{F}_p$ has point of order r , embedding degree 8, and $\rho \approx 5/4$

Example of a Cyclotomic Family (Brezing-Weng)

- Fix $k = 8$, $D = 3$.
- $r(x) = \Phi_{24}(x) = x^8 - x^4 + 1$ defines $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{24})$.
- $\zeta_8 \mapsto x^5 - x$ in K , so choose $t(x) = x^5 - x + 1$.
- $\sqrt{-3} \mapsto 2x^4 - 1$ in K , so choose

$$y(x) = \frac{\zeta_8 - 1}{\sqrt{-3}} = \frac{1}{3}(x^5 + 2x^4 + x - 1)$$

- Compute

$$p(x) = \frac{t(x)^2 + Dy(x)^2}{4} = \frac{1}{3}(x - 1)^2(x^8 - x^4 + 1) + x^9$$

- Evaluating at $x = 1000726$ gives 160-bit prime r and 198-bit prime p .
 - $y^2 = x^3 + 14$ over $\mathbb{F}_p$ has point of order r , embedding degree 8, and $\rho \approx 5/4$

Example of a Cyclotomic Family (Brezing-Weng)

- Fix $k = 8$, $D = 3$.
- $r(x) = \Phi_{24}(x) = x^8 - x^4 + 1$ defines $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{24})$.
- $\zeta_8 \mapsto x^5 - x$ in K , so choose $t(x) = x^5 - x + 1$.
- $\sqrt{-3} \mapsto 2x^4 - 1$ in K , so choose

$$y(x) = \frac{\zeta_8 - 1}{\sqrt{-3}} = \frac{1}{3}(x^5 + 2x^4 + x - 1)$$

- Compute

$$p(x) = \frac{t(x)^2 + Dy(x)^2}{4} = \frac{1}{3}(x - 1)^2(x^8 - x^4 + 1) + x^9$$

- Evaluating at $x = 1000726$ gives 160-bit prime r and 198-bit prime p .
 - $y^2 = x^3 + 14$ over $\mathbb{F}_p$ has point of order r , embedding degree 8, and $\rho \approx 5/4$

Example of a Cyclotomic Family (Brezing-Weng)

- Fix $k = 8$, $D = 3$.
- $r(x) = \Phi_{24}(x) = x^8 - x^4 + 1$ defines $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{24})$.
- $\zeta_8 \mapsto x^5 - x$ in K , so choose $t(x) = x^5 - x + 1$.
- $\sqrt{-3} \mapsto 2x^4 - 1$ in K , so choose

$$y(x) = \frac{\zeta_8 - 1}{\sqrt{-3}} = \frac{1}{3}(x^5 + 2x^4 + x - 1)$$

- Compute

$$p(x) = \frac{t(x)^2 + Dy(x)^2}{4} = \frac{1}{3}(x-1)^2(x^8 - x^4 + 1) + x^9$$

- Evaluating at $x = 1000726$ gives 160-bit prime r and 198-bit prime p .

- $y^2 = x^3 + 14$ over $\mathbb{F}_p$ has point of order r , embedding degree 8, and $\rho \approx 5/4$

Example of a Cyclotomic Family (Brezing-Weng)

- Fix $k = 8$, $D = 3$.
- $r(x) = \Phi_{24}(x) = x^8 - x^4 + 1$ defines $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{24})$.
- $\zeta_8 \mapsto x^5 - x$ in K , so choose $t(x) = x^5 - x + 1$.
- $\sqrt{-3} \mapsto 2x^4 - 1$ in K , so choose

$$y(x) = \frac{\zeta_8 - 1}{\sqrt{-3}} = \frac{1}{3}(x^5 + 2x^4 + x - 1)$$

- Compute

$$p(x) = \frac{t(x)^2 + Dy(x)^2}{4} = \frac{1}{3}(x - 1)^2(x^8 - x^4 + 1) + x^9$$

- Evaluating at $x = 1000726$ gives 160-bit prime r and 198-bit prime p .
 - $y^2 = x^3 + 14$ over $\mathbb{F}_p$ has point of order r , embedding degree 8, and $\rho \approx 5/4$

Example of a Cyclotomic Family (Brezing-Weng)

- Fix $k = 8$, $D = 3$.
- $r(x) = \Phi_{24}(x) = x^8 - x^4 + 1$ defines $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{24})$.
- $\zeta_8 \mapsto x^5 - x$ in K , so choose $t(x) = x^5 - x + 1$.
- $\sqrt{-3} \mapsto 2x^4 - 1$ in K , so choose

$$y(x) = \frac{\zeta_8 - 1}{\sqrt{-3}} = \frac{1}{3}(x^5 + 2x^4 + x - 1)$$

- Compute

$$p(x) = \frac{t(x)^2 + Dy(x)^2}{4} = \frac{1}{3}(x - 1)^2(x^8 - x^4 + 1) + x^9$$

- Evaluating at $x = 1000726$ gives 160-bit prime r and 198-bit prime p .
 - $y^2 = x^3 + 14$ over $\mathbb{F}_p$ has point of order r , embedding degree 8, and $\rho \approx 5/4$

Example of a Cyclotomic Family (Brezing-Weng)

- Fix $k = 8$, $D = 3$.
- $r(x) = \Phi_{24}(x) = x^8 - x^4 + 1$ defines $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{24})$.
- $\zeta_8 \mapsto x^5 - x$ in K , so choose $t(x) = x^5 - x + 1$.
- $\sqrt{-3} \mapsto 2x^4 - 1$ in K , so choose

$$y(x) = \frac{\zeta_8 - 1}{\sqrt{-3}} = \frac{1}{3}(x^5 + 2x^4 + x - 1)$$

- Compute

$$p(x) = \frac{t(x)^2 + Dy(x)^2}{4} = \frac{1}{3}(x - 1)^2(x^8 - x^4 + 1) + x^9$$

- Evaluating at $x = 1000726$ gives 160-bit prime r and 198-bit prime p .
 - $y^2 = x^3 + 14$ over $\mathbb{F}_p$ has point of order r , embedding degree 8, and $\rho \approx 5/4$

Sporadic Families

- Idea of Barreto-Naehrig: Fix k, D , choose $r(x)$ so that $K = \mathbb{Q}[x]/(r(x))$ is an *extension* of a cyclotomic field containing $\zeta_k, \sqrt{-D}$.
- How? Choose $u(x)$ so that $\Phi_k(u(x)) = r(x)r'(x)$, set $K = \mathbb{Q}(x)/(r(x))$.
- Construct $t(x), y(x), p(x)$ as with cyclotomic families.

Sporadic Families

- Idea of Barreto-Naehrig: Fix k, D , choose $r(x)$ so that $K = \mathbb{Q}[x]/(r(x))$ is an *extension* of a cyclotomic field containing $\zeta_k, \sqrt{-D}$.
- How? Choose $u(x)$ so that $\Phi_k(u(x)) = r(x)r'(x)$, set $K = \mathbb{Q}(x)/(r(x))$.
- Construct $t(x), y(x), p(x)$ as with cyclotomic families.

Sporadic Families

- Idea of Barreto-Naehrig: Fix k, D , choose $r(x)$ so that $K = \mathbb{Q}[x]/(r(x))$ is an *extension* of a cyclotomic field containing $\zeta_k, \sqrt{-D}$.
- How? Choose $u(x)$ so that $\Phi_k(u(x)) = r(x)r'(x)$, set $K = \mathbb{Q}(x)/(r(x))$.
- Construct $t(x), y(x), p(x)$ as with cyclotomic families.

Example: Barreto-Naehrig Curves

- Set $k = 12$, $D = 3$. Look for $u(x)$ such that $\Phi_{12}(u(x))$ factors.
- Galbraith-McKee-Valença: only 2 such quadratic $u(x)$.
- $u(x) = 6x^2$ gives $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$.
- Compute $t(x) = 6x^2 + 1$,
 $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
- Since $p(x) + 1 - t(x) = r(x)$ (not just divisible by $r(x)$),
 $r(x)$ is the size of the full group of points.
 - When $p(x_0), r(x_0)$ are both prime for some x_0 , E is a curve of prime order and $k = 12$.
- BN family is only family of prime-order curves that is not sparse – easy to specify the bit sizes of p, r .

Example: Barreto-Naehrig Curves

- Set $k = 12$, $D = 3$. Look for $u(x)$ such that $\Phi_{12}(u(x))$ factors.
- Galbraith-McKee-Valença: only 2 such quadratic $u(x)$.
- $u(x) = 6x^2$ gives $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$.
- Compute $t(x) = 6x^2 + 1$,
 $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
- Since $p(x) + 1 - t(x) = r(x)$ (not just divisible by $r(x)$),
 $r(x)$ is the size of the full group of points.
 - When $p(x_0), r(x_0)$ are both prime for some x_0 , E is a curve of prime order and $k = 12$.
- BN family is only family of prime-order curves that is not sparse – easy to specify the bit sizes of p, r .

Example: Barreto-Naehrig Curves

- Set $k = 12$, $D = 3$. Look for $u(x)$ such that $\Phi_{12}(u(x))$ factors.
- Galbraith-McKee-Valença: only 2 such quadratic $u(x)$.
- $u(x) = 6x^2$ gives $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$.
- Compute $t(x) = 6x^2 + 1$,
 $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
- Since $p(x) + 1 - t(x) = r(x)$ (not just divisible by $r(x)$),
 $r(x)$ is the size of the full group of points.
 - When $p(x_0), r(x_0)$ are both prime for some x_0 , E is a curve of prime order and $k = 12$.
- BN family is only family of prime-order curves that is not sparse – easy to specify the bit sizes of p, r .

Example: Barreto-Naehrig Curves

- Set $k = 12$, $D = 3$. Look for $u(x)$ such that $\Phi_{12}(u(x))$ factors.
- Galbraith-McKee-Valença: only 2 such quadratic $u(x)$.
- $u(x) = 6x^2$ gives $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$.
- Compute $t(x) = 6x^2 + 1$,
 $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
- Since $p(x) + 1 - t(x) = r(x)$ (not just divisible by $r(x)$),
 $r(x)$ is the size of the full group of points.
 - When $p(x_0), r(x_0)$ are both prime for some x_0 , E is a curve of prime order and $k = 12$.
- BN family is only family of prime-order curves that is not sparse – easy to specify the bit sizes of p, r .

Example: Barreto-Naehrig Curves

- Set $k = 12$, $D = 3$. Look for $u(x)$ such that $\Phi_{12}(u(x))$ factors.
- Galbraith-McKee-Valença: only 2 such quadratic $u(x)$.
- $u(x) = 6x^2$ gives $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$.
- Compute $t(x) = 6x^2 + 1$,
 $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
- Since $p(x) + 1 - t(x) = r(x)$ (not just divisible by $r(x)$),
 $r(x)$ is the size of the full group of points.
 - When $p(x_0), r(x_0)$ are both prime for some x_0 , E is a curve of prime order and $k = 12$.
- BN family is only family of prime-order curves that is not sparse – easy to specify the bit sizes of p, r .

Example: Barreto-Naehrig Curves

- Set $k = 12$, $D = 3$. Look for $u(x)$ such that $\Phi_{12}(u(x))$ factors.
- Galbraith-McKee-Valença: only 2 such quadratic $u(x)$.
- $u(x) = 6x^2$ gives $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$.
- Compute $t(x) = 6x^2 + 1$,
 $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
- Since $p(x) + 1 - t(x) = r(x)$ (not just divisible by $r(x)$),
 $r(x)$ is the size of the full group of points.
 - When $p(x_0), r(x_0)$ are both prime for some x_0 , E is a curve of prime order and $k = 12$.
- BN family is only family of prime-order curves that is not sparse – easy to specify the bit sizes of p, r .

Example: Barreto-Naehrig Curves

- Set $k = 12$, $D = 3$. Look for $u(x)$ such that $\Phi_{12}(u(x))$ factors.
- Galbraith-McKee-Valença: only 2 such quadratic $u(x)$.
- $u(x) = 6x^2$ gives $r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$.
- Compute $t(x) = 6x^2 + 1$,
 $p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$.
- Since $p(x) + 1 - t(x) = r(x)$ (not just divisible by $r(x)$),
 $r(x)$ is the size of the full group of points.
 - When $p(x_0), r(x_0)$ are both prime for some x_0 , E is a curve of prime order and $k = 12$.
- BN family is only family of prime-order curves that is not sparse – easy to specify the bit sizes of p, r .

Scott-Barreto Families

- Scott-Barreto idea: Fix k , choose $r(x)$ so that $K = \mathbb{Q}(x)/(r(x))$ is an extension of a cyclotomic field containing ζ_k and *not containing* $\sqrt{-D}$ for small D .
- Compute $t(x)$, search (via computer) for $h(x)$ that makes right side of CM equation

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

a linear factor times a perfect square.

- Compute D and $y(x)$ such that CM equation is satisfied for any x .
- Method gives families with $1 < \rho < 2$.
 - Known examples have $k \leq 6$.

Scott-Barreto Families

- Scott-Barreto idea: Fix k , choose $r(x)$ so that $K = \mathbb{Q}(x)/(r(x))$ is an extension of a cyclotomic field containing ζ_k and *not containing* $\sqrt{-D}$ for small D .
- Compute $t(x)$, search (via computer) for $h(x)$ that makes right side of CM equation

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

a linear factor times a perfect square.

- Compute D and $y(x)$ such that CM equation is satisfied for any x .
- Method gives families with $1 < \rho < 2$.
 - Known examples have $k \leq 6$.

Scott-Barreto Families

- Scott-Barreto idea: Fix k , choose $r(x)$ so that $K = \mathbb{Q}(x)/(r(x))$ is an extension of a cyclotomic field containing ζ_k and *not containing* $\sqrt{-D}$ for small D .
- Compute $t(x)$, search (via computer) for $h(x)$ that makes right side of CM equation

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

a linear factor times a perfect square.

- Compute D and $y(x)$ such that CM equation is satisfied for any x .
- Method gives families with $1 < \rho < 2$.
 - Known examples have $k \leq 6$.

Scott-Barreto Families

- Scott-Barreto idea: Fix k , choose $r(x)$ so that $K = \mathbb{Q}(x)/(r(x))$ is an extension of a cyclotomic field containing ζ_k and *not containing* $\sqrt{-D}$ for small D .
- Compute $t(x)$, search (via computer) for $h(x)$ that makes right side of CM equation

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

a linear factor times a perfect square.

- Compute D and $y(x)$ such that CM equation is satisfied for any x .
- Method gives families with $1 < \rho < 2$.
 - Known examples have $k \leq 6$.

Scott-Barreto Families

- Scott-Barreto idea: Fix k , choose $r(x)$ so that $K = \mathbb{Q}(x)/(r(x))$ is an extension of a cyclotomic field containing ζ_k and *not containing* $\sqrt{-D}$ for small D .
- Compute $t(x)$, search (via computer) for $h(x)$ that makes right side of CM equation

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

a linear factor times a perfect square.

- Compute D and $y(x)$ such that CM equation is satisfied for any x .
- Method gives families with $1 < \rho < 2$.
 - Known examples have $k \leq 6$.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Can construct pairing-friendly curves with $\rho = 1/2$.
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Can't construct pairing-friendly curves with $k = 1, 2$.
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Can't construct pairing-friendly curves with $\rho = 1$.
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Can't construct curves with $\rho = 2$.
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Exception: Barreto-Naehrig curves with $k = 12$.
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Exception: Barreto-Naehrig curves with $k = 12$.
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Exception: Barreto-Naehrig curves with $k = 12$.
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Exception: Barreto-Naehrig curves with $k = 12$.
 - Many curves possible, easy to specify bit sizes.

Summary: Pairing-Friendly Elliptic Curves

- 1 Curves not in families (Cocks-Pinch, Dupont-Engge-Morain):
 - Good for constructing curves with arbitrary k .
 - Can't construct curves of prime order ($\rho \approx 2$).
 - Many curves possible, easy to specify bit sizes.
- 2 Sparse families (Miyaji-Nakabayashi-Takano, F.):
 - Good for constructing curves of prime order.
 - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
 - Curves are rare.
- 3 Complete families (Barreto-Lynn-Scott, Brezing-Weng, Scott-Barreto, others):
 - Good for constructing curves with arbitrary k .
 - Usually can't construct curves of prime order ($1 < \rho < 2$).
 - Exception: Barreto-Naehrig curves with $k = 12$.
 - Many curves possible, easy to specify bit sizes.

The State of the Art

Smallest known ρ -values for families with even embedding degrees k .

k	ρ	Type	k	ρ	Type
4	1	Sparse	22	13/10	Cyclotomic
6	1	Sparse	24	5/4	Cyclotomic
8	5/4	Cyclotomic	26	7/6	Cyclotomic
10	1	Sparse	28	4/3	Cyclotomic
12	1	Sporadic	30	3/2	Cyclotomic
14	4/3	Cyclotomic	32	17/16	Cyclotomic
16	5/4	Cyclotomic	34	9/8	Cyclotomic
18	4/3	Cyclotomic	36	17/12	Cyclotomic
20	11/8	Cyclotomic	38	7/6	Cyclotomic