Pairings III

Supersingular curves

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Definition

Let E be an elliptic curve defined over $\mathbf{F}_q, q = p^r$.
E is supersingular if $t \equiv 0 \bmod p$ for $\#E(\mathbf{F}_q) = q + 1 - t$.

Otherwise it is ordinary.

Examples:

$$y^2 = x(x^2 + a_4), \text{ for } p \equiv 3 \bmod 4$$

has $p + 1$ points, thus is supersingular.

Definition

Let E be an elliptic curve defined over $\mathbf{F}_q, q = p^r$.
E is supersingular if $t \equiv 0 \bmod p$ for $\#E(\mathbf{F}_q) = q + 1 - t$.

Otherwise it is ordinary.

Examples:

$$y^2 = x(x^2 + a_4), \text{ for } p \equiv 3 \bmod 4$$

has $p + 1$ points, thus is supersingular.
Proof:
$x = 0$ and $x = \pm\sqrt{-a_4}$ (if defined) give one point $(x, 0)$ each.
For all other x, exactly one of x and $-x$ gives 2 points,
the other one none,

Definition

Let E be an elliptic curve defined over $\mathbf{F}_q, q = p^r$.
E is supersingular if $t \equiv 0 \bmod p$ for $\#E(\mathbf{F}_q) = q + 1 - t$.

Otherwise it is ordinary.

Examples:

$$y^2 = x(x^2 + a_4), \text{ for } p \equiv 3 \bmod 4$$

has $p + 1$ points, thus is supersingular.
Proof:
$x = 0$ and $x = \pm\sqrt{-a_4}$ (if defined) give one point $(x, 0)$ each.
For all other x, exactly one of x and $-x$ gives 2 points,
the other one none, because $p \equiv 3 \bmod 4$ implies $\sqrt{-1} \neq \mathbf{F}_p$.

Definition

Let E be an elliptic curve defined over $\mathbf{F}_q, q = p^r$.
E is supersingular if $t \equiv 0 \bmod p$ for $\#E(\mathbf{F}_q) = q + 1 - t$.

Otherwise it is ordinary.

Examples:

$$y^2 = x(x^2 + a_4), \text{ for } p \equiv 3 \bmod 4$$

has $p + 1$ points, thus is supersingular.
Proof:
$x = 0$ and $x = \pm\sqrt{-a_4}$ (if defined) give one point $(x, 0)$ each.
For all other x, exactly one of x and $-x$ gives 2 points,
the other one none, because $p \equiv 3 \bmod 4$ implies $\sqrt{-1} \not\in \mathbf{F}_p$.
Total of p points with $x \in \mathbf{F}_p$ and plus 1 point ∞.

$$y^2 = x^3 + a_6, for\ p \equiv 2 \bmod 3$$

has $p + 1$ points, thus is supersingular.

Definition

Let E be an elliptic curve defined over $\mathbf{F}_q, q = p^r$.
E is supersingular if $t \equiv 0 \bmod p$ for $\#E(\mathbf{F}_q) = q + 1 - t$.

Otherwise it is ordinary.

Examples:

$$y^2 = x(x^2 + a_4), \text{ for } p \equiv 3 \bmod 4$$

has $p + 1$ points, thus is supersingular.
Proof:
$x = 0$ and $x = \pm\sqrt{-a_4}$ (if defined) give one point $(x, 0)$ each.
For all other x, exactly one of x and $-x$ gives 2 points,
the other one none, because $p \equiv 3 \bmod 4$ implies $\sqrt{-1} \not\in \mathbf{F}_p$.
Total of p points with $x \in \mathbf{F}_p$ and plus 1 point ∞.

$$y^2 = x^3 + a_6, for\ p \equiv 2 \bmod 3$$

has $p + 1$ points, thus is supersingular.
Proof uses that $\mathbf{F}_p$ has unique cube roots as there are no cube roots of unity in $\mathbf{F}_p$.

Embedding degrees for supersingular curves

Let E be supersingular and $p \geq 5$, i.e $p > 2\sqrt{p}$.

Hasse's Theorem states $|t| \leq 2\sqrt{q}$ and E supersingular implies $t \equiv 0 \bmod p$, so $t = 0$ and

$$|E(\mathbf{F}_p)| = p + 1.$$

Obviously $(p+1) \mid p^2 - 1 = (p+1)(p-1)$.

Embedding degrees for supersingular curves

Let E be supersingular and $p \geq 5$, i.e $p > 2\sqrt{p}$.

Hasse's Theorem states $|t| \leq 2\sqrt{q}$ and E supersingular implies $t \equiv 0 \bmod p$, so $t = 0$ and

$$|E(\mathbf{F}_p)| = p + 1.$$

Obviously $(p+1) \mid p^2 - 1 = (p+1)(p-1)$.
So for any $\ell|(p+1)$ we have $\ell|(p^2-1)$ and $G_2 \subset E(\mathbf{F}_{p^2})$.

Embedding degree (recall from Pairings I) $k \leq 2$ for supersingular curves over large prime fields.

Embedding degrees for supersingular curves

Let E be supersingular and $p \geq 5$, i.e $p > 2\sqrt{p}$.

Hasse's Theorem states $|t| \leq 2\sqrt{q}$ and E supersingular implies $t \equiv 0 \bmod p$, so $t = 0$ and

$$|E(\mathbf{F}_p)| = p + 1.$$

Obviously $(p+1) \mid p^2 - 1 = (p+1)(p-1)$.
So for any $\ell|(p+1)$ we have $\ell|(p^2-1)$ and $G_2 \subset E(\mathbf{F}_{p^2})$.

Embedding degree (recall from Pairings I) $k \leq 2$ for supersingular curves over large prime fields.

For these curves we have efficient distortion maps:

- $\phi(x, y) = (-x, iy)$ for $i^2 = -1$
  on $y^2 = x^3 + a_4x$ for $p \equiv 3 \bmod 4$
- $\phi(x, y) = (jx, y)$ for $j^3 = 1, j \neq 1$
  on $y^2 = x^3 + a_6$ for $p \equiv 2 \bmod 3$.

Thus can use BLS short signatures, but need very large p.

Example

Curve from DLP lectures:
$p = 1000003 \equiv 3 \bmod 4$ and $y^2 = x^3 - x$ over $\mathbf{F}_p$.
Has $1000004 = p + 1$ points.
$P = (101384, 614510)$ is a point of order 500002.
$aP = (670366, 740819)$.

Construct $\mathbf{F}_{p^2}$ as $\mathbf{F}_p(i)$.
$\phi(P) = (898619, 614510i)$.

Then
$e(P, \phi(P)) = 387265 + 276048i$;
$e(aP, \phi(P)) = 609466 + 807033i$.
Solve with index calculus to get $a = 78654$.
(Btw. G_T for this example is the clock).

Embedding degrees for other curves

Let $E/\mathbf{F}_q$ be supersingular.
Menezes, Okamoto, and Vanstone show:

- in characteristic 2 we have $k \leq 4$,
- in characteristic 3 we have $k \leq 6$,
- over prime fields $\mathbf{F}_p$ with $p \geq 5$ we have $k \leq 2$,

and these bounds are attained.

Also ordinary curves can have small embedding degrees.
Very unlikely for randomly chosen curves, but curves constructed for pairings have small k. These do not have distortion maps.

Example:
Barreto–Naehrig curves have $k = 12$.