Edwards Curves

Christiane Peters

Technische Universiteit Eindhoven

Séminaire de Cryptographie
Rennes
June 20, 2008

1. Elliptic curves in Edwards form

2. Addition law

3. Fast explicit formulas

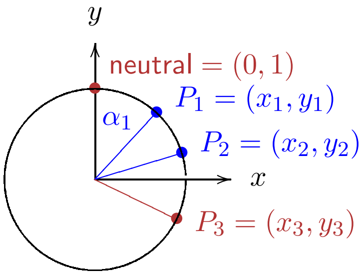
4. Twisted Edwards Curves

Addition on a clock

Unit circle $x^2 + y^2 = 1$.

Let $x_i = \sin(\alpha_i)$, $y_i = \cos(\alpha_i)$.

$$
\begin{aligned}
x_3 &= \sin(\alpha_1 + \alpha_2) \\
&= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \\
y_3 &= \cos(\alpha_1 + \alpha_2) \\
&= \cos(\alpha_1)\cos(\alpha_2) - \sin(\alpha_1)\sin(\alpha_2)
\end{aligned}
$$



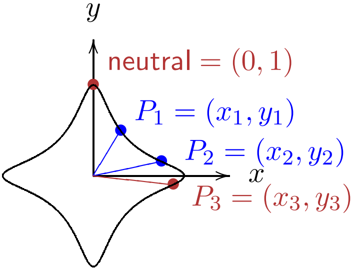
Addition of angles defines commutative group law $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2.$$

Fast but not elliptic; low security.

Elliptic curve in Edwards form over a non-binary field k

$x^2 + y^2 = 1 + d\,x^2y^2$,
where $d \in k \setminus \{0, 1\}$.



We add two points (x_1, y_1), (x_2, y_2) on E according to the Edwards addition law

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

Elliptic?

Short answer:

- Projective coordinates $(X^2+Y^2)Z^2 = Z^4 + dX^2Y^2$ imply at first glance two singular points at infinity: $(1:0:0)$, $(0:1:0)$.
- Blow up yields two points of order 2 and two points of order 4.
- Easy way to see is approach from curves in Montgomery form.

1. Elliptic curves in Edwards form

2. Addition law

3. Fast explicit formulas

4. Twisted Edwards Curves

Addition on Edwards curves

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

- The point $(0, 1)$ is the neutral element of the addition law and
- the negative of $P = (x_1, y_1)$ is $-P = (-x_1, y_1)$.

- If d is a non-square in k the addition law is complete.
- The addition law is strongly unified, i.e., it can be also used for doublings.

Complete? – (1)

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

Can the denominators be 0?

Claim: They are never 0 if d is not a square in k.

Proof: Let (x_1, y_1) and (x_2, y_2) be on the curve, i.e., $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$.
Write $\varepsilon = d x_1 x_2 y_1 y_2$ and suppose $\varepsilon \in \{-1, 1\}$.
Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} d x_1^2 y_1^2 (x_2^2 + y_2^2) &= d x_1^2 y_1^2 (1 + d x_2^2 y_2^2) \\ &= d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2 \\ &= d x_1^2 y_1^2 + \varepsilon^2 \\ &= 1 + d x_1^2 y_1^2 \qquad //(\varepsilon = \pm 1) \\ &= x_1^2 + y_1^2 \end{aligned}$$

Complete? – (2)

Show: $\varepsilon = dx_1x_2y_1y_2 = \pm 1$ implies d is a square.

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

We have $dx_1^2y_1^2(x_2^2 + y_2^2) = x_1^2 + y_1^2$.

Proof (continued): It follows that

$$\begin{aligned} (x_1 + \varepsilon y_1)^2 &= x_1^2 + y_1^2 + 2\varepsilon x_1y_1 \\ &= dx_1^2y_1^2(x_2^2 + y_2^2) + 2x_1y_1dx_1x_2y_1y_2 \\ &= dx_1^2y_1^2(x_2^2 + 2x_2y_2 + y_2^2) = dx_1^2y_1^2(x_2 + y_2)^2 \end{aligned}$$

$x_2 + y_2 \neq 0 \;\Rightarrow\; d = ((x_1 + \varepsilon y_1)/x_1y_1(x_2 + y_2))^2 \;\Rightarrow\; d = \square$

$x_2 - y_2 \neq 0 \;\Rightarrow\; d = ((x_1 - \varepsilon y_1)/x_1y_1(x_2 - y_2))^2 \;\Rightarrow\; d = \square$

If $x_2 + y_2 = 0$ and $x_2 - y_2 = 0$, then $x_2 = y_2 = 0$, contradiction.

1. Elliptic curves in Edwards form

2. Addition law

3. Fast explicit formulas

4. Twisted Edwards Curves

Inversion-free addition

Consider the homogenized Edwards equation

$$E:\ (X^2+Y^2)Z^2 = Z^4 + dX^2Y^2$$

A point $(X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$ on E corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$.

$$\begin{aligned}
A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2;\\
E &= (X_1+Y_1)\cdot(X_2+Y_2) - C - D;\ F = d \cdot C \cdot D;\\
X_{P+Q} &= A \cdot E \cdot (B-F);\\
Y_{P+Q} &= A \cdot (D-C) \cdot (B+F);\\
Z_{P+Q} &= (B-F)\cdot(B+F).
\end{aligned}$$

Costs 10M+1S+1D (mixed ADD needs 9M+1S+1D).

Explicit fast doubling and tripling formulas

(Non-unified) Doubling of a point (x_1, y_1) on $x^2 + y^2 = 1 + dx^2y^2$:

$$\begin{aligned}[2](x_1, y_1) &= \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - dx_1^2y_1^2}\right) \\ &= \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)}\right).\end{aligned}$$

Inversion-free version needs 3M + 4S.

Tripling:

$$[3](x_1, y_1) = \left(\frac{((x_1^2 + y_1^2)^2 - (2y_1)^2)}{4(x_1^2 - 1)x_1^2 - (x_1^2 - y_1^2)^2} x_1, \frac{((x_1^2 + y_1^2)^2 - (2x_1)^2)}{-4(y_1^2 - 1)y_1^2 + (x_1^2 - y_1^2)^2} y_1\right).$$

Inversion-free explicit formulas cost 9M + 4S.

Inverted Edwards

A point $(X_1 : Y_1 : Z_1)$ with $X_1Y_1Z_1 \neq 0$ on

$$(X^2 + Y^2)Z^2 = X^2Y^2 + dZ^4$$

corresponds to $(Z_1/X_1, Z_1/Y_1)$ on the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$.

Costs: 9M + 1S for ADD, 8M + 1S for mixed ADD, 3M + 4S for DBL and 9M + 4S for TRI.

1. Elliptic curves in Edwards form

2. Addition law

3. Fast explicit formulas

4. Twisted Edwards Curves

What about Montgomery form?

- So far fastest ECC methods use curves in Montgomery form $Bv^2 = u^3 + Au^2 + u$.
- Differential addition formulas for computing nP use 5M + 4S + 1A for each bit of n.
- Setting 1S = 0.8 M: Edwards faster than Montgomery curves when using scalars with more than 160 bits.
- $nP + n'P'$ is hard to compute for $n \neq n'$ and $P \neq P'$. Big advantage for Edwards.

Counting elliptic curves over $\mathbb{F}_p$ if $p \equiv 1 \pmod 4$

$\approx 2p$ elliptic curves.
$\approx 5p/6$ curves with order $\in 4\mathbb{Z}$.
$\approx 5p/6$ Montgomery curves.
$\approx 2p/3$ Edwards curves.
$\approx p/2$ complete Edwards curves.
$\approx p/24$ original Edwards curves.

(more detailed description and more experiments in Bernstein, Birkner, Joye, Lange, P.: *Twisted Edwards Curves* in AFRICACRYPT '08)

Counting elliptic curves over $\mathbb{F}_p$ if $p \equiv 3 \pmod 4$

$\approx 2p$ elliptic curves.
$\approx 5p/6$ curves with order $\in 4\mathbb{Z}$.
$\approx 3p/4$ Montgomery curves.
$\approx 3p/4$ Edwards curves.
$\approx p/2$ complete Edwards curves.
$\approx p/4$ original Edwards curves.

Can we achieve Edwards-like speeds for more curves?

Twisted curves

Points of order 4 restrict the number of elliptic curves in Edwards form over k.

Define twisted Edwards curves

$$ax^2 + y^2 = 1 + dx^2y^2,$$

with $a, d \neq 0$ and $a \neq d$.

Every Edwards curve is a twisted Edwards curve $(a = 1)$.

Why "twisted"?

- $E' : \bar{x}^2 + \bar{y}^2 = 1 + (d/a)\bar{x}^2\bar{y}^2$ over k
  with $a = \alpha^2$ for some $\alpha \in k$ is isomorphic to
  $E : ax^2 + y^2 = 1 + dx^2y^2$ by $x = \bar{x}/\alpha$ and $y = \bar{y}$.

- In general: E' and E are quadratic twists of each other,
  i.e., isomorphic over a quadratic extension of k.
  We have $E' : \bar{a}\bar{x}^2 + \bar{y}^2 = 1 + \bar{d}\bar{x}^2\bar{y}^2$ and
  $E : ax^2 + y^2 = 1 + dx^2y^2$ are quadratic twists
  if $a\bar{d} = \bar{a}d$.

Convert Edwards curves into twisted form

Get rid of huge denominators mod large primes p:

E.g. Given $x^2 + y^2 = 1 + dx^2y^2$ with $d = n/m$. Assume m "small".

Then m^{-1} mod p is almost as big as p!

Bernstein's Curve25519: $v^2 = u^3 + 486662u^2 + u$ over $\mathbb{F}_p$ where $p = 2^{255} - 19$.

Bernstein/Lange: Curve25519 is birationally equivalent to $x^2 + y^2 = 1 + (121665/121666)x^2y^2$.

But $121665/121666 \equiv$

$20800338683988658368647408995589388737092878452977063003340006470870624536394$

mod p.

Write curve as $121666\ x^2 + y^2 = 1 + 121665\ x^2y^2$.

Addition on twisted Edwards curves

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$$

Costs for inversion-free formulas: 10M + 1S + 1A + 1D for ADD, 3M + 4S + 1A for DBL.

Speed in inverted coordinates: 9M + 1S + 1A + 1D for ADD, 3M + 4S + 1A + 1D for DBL.

Birational equivalence

The Montgomery curve $Bv^2 = u^3 + Au^2 + u$ is birationally equivalent to an Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ where $a = (A+2)/B$ and $d = (A-2)/B$.

- $(u, v) \mapsto (x, y) = (u/v, (u-1)/(u+1))$.
- inverse map
  $(x, y) \mapsto ((1+y)/(1-y), (1+y)/((1-y)x))$.
  ($B = 4/(a-d)$ and $A = 2(a+d)/(a-d)$.)

Exceptional points

Birational maps $(u, v) \mapsto (x, y) = (u/v, (u-1)/(u+1))$.
Exceptional points satisfy $v(u+1) = 0$.

- $(0, 0) \in E_M$ corresponds to $(0, -1)$.

- If $E_M(k)$ contains two more points of order 2, they are mapped to two points of order 2 at infinity of the desingularization of E.

- If $d = \delta^2$ in k: The point with $u = -1$ corresponds to points $(-1, \pm\delta)$ which have order 4. They correspond to two points of order 4 at infinity of the desingularization of E.

Twisted Edwards speed for curves having group order $\in 4\mathbb{Z}$

Not every curve with group order $\in 4\mathbb{Z}$ can be written as a Montgomery curve.

That's the case iff $p \equiv 3 \bmod 4$ and the curve has 2-torsion $\mathbb{Z}/2 \times \mathbb{Z}/2$.

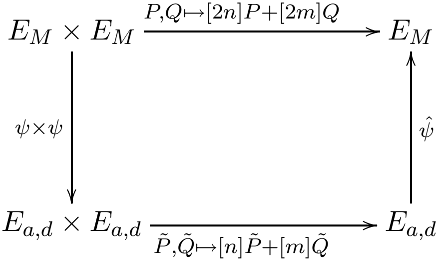
Write curve as $v^2 = u^3 - (a+d)u^2 + (ad)u$.

This curve is 2-isogenous to $ax^2 + y^2 = 1 + dx^2y^2$:

$$(u, v) \mapsto (2v/(ad - u^2), (v^2 - (a-d)u^2)/(v^2 + (a-d)u^2).$$

Make use of fast arithmetic on twisted Edwards curves

Given $n, m \in \mathbb{Z}$ and two points P, Q on the Montgomery curve E_M and a 2-isogeny ψ to a twisted Edwards curve $E_{a,d}$.



Benefits of twisted Edwards curves

- Fast addition formulas for a greater range of elliptic curves.
- Some Edwards curves are sped up by twists.
- All Montgomery curves can be written as twisted Edwards curves.
- Can use isogenies to achieve similar speeds for all curves where 4 divides group order.

Merci beaucoup!