Edwards Curves

Christiane Peters

Technische Universiteit Eindhoven

S^{3}CM

July 10, 2008

Motivation: Elliptic Curve Cryptography

Given a group G and an element $P \in G$ of finite order.
Compute the scalar multiple

$$Q = [n]P = \underbrace{P + P + \cdots + P}_{n \text{ times}}.$$

Discrete logarithm problem (DLP): Given Q, find n modulo the order of P.

- Cryptographic protocols such as e-voting or digital signatures often use discrete logarithm systems.
- G is usually one of the following groups: $\mathbb{F}_p^\times$, $\mathbb{F}_q^\times$, $E(\mathbb{F}_q)$ or $\mathrm{Pic}_C^0(\mathbb{F}_q)$
- $E(\mathbb{F}_q)$ has "somewhat" slower arithmetic than $\mathbb{F}_q^\times$; but much smaller key sizes for same security level.

1. Elliptic curves in Edwards form

2. Addition law

3. Fast explicit formulas

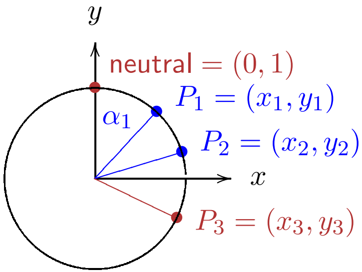
4. Using Edwards curves

Addition on a clock

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

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

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



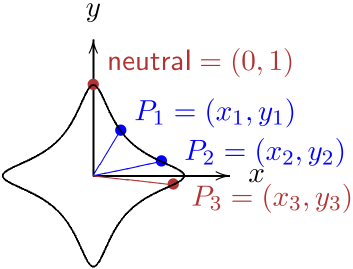
Addition of angles defines commutative group law $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

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

Fast but not elliptic; low security (solve DLP using index calculus attacks).

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

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

What about singular points?

Projective coordinates $(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$ imply at first glance two singular points at infinity: $(1 : 0 : 0)$, $(0 : 1 : 0)$.

What about singular points?

Projective coordinates $(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$ imply at first glance two singular points at infinity: $(1 : 0 : 0)$, $(0 : 1 : 0)$.

Take a closer look at $(1 : 0 : 0)$.
Dehomogenize defining equation by setting $X = 1$:

$$G = (1 + Y^2)Z^2 - Z^4 - dY^2.$$

Partial derivatives: $\frac{\partial G}{\partial Y} = 2YZ^2 - 2Y$ and

$\frac{\partial G}{\partial Z} = 2(1 + Y^2)Z - 4Z^3.$

Both partial derivatives vanish at $(0, 0)$! $\longrightarrow$ singular point!

Blow up

Given $G = (1 + y^2)z^2 - z^4 - dy^2$.

Replace $y = uz$ and get $G(uz, z) = (1 + u^2 z^2)z^2 - z^4 - du^2 z^2$.
Get new equation:

$$H = 1 + u^2 z^2 - z^2 - du^2.$$

What happens at $z = 0$?

$$1 - du^2 = 0 \Rightarrow u = \pm\frac{1}{\sqrt{d}}.$$

Resolved points lie in a quadratic extension of k, namely $k(\sqrt{d})$.

We get $\frac{\partial H}{\partial u} = 2(uz^2 - du)$ which is non-zero for $u = \pm\frac{1}{\sqrt{d}}$.

Blow-up is non-singular.

1. Elliptic curves in Edwards form

2. Addition law

3. Fast explicit formulas

4. Using Edwards curves

Addition on an Edwards curve

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

- The point $(0, 1)$ is the neutral element of the addition law. The point $(0, -1)$ has order 2. The points $(1, 0)$ and $(-1, 0)$ have order 4.
- The inverse 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. (points at infinity in an extension of the ground field)
- The addition law is strongly unified, i.e., it can be also used for doublings. (protection against side-channel attacks)

1. Elliptic curves in Edwards form

2. Addition law

3. Fast explicit formulas

4. Using 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).

(M: general multiplications, S: squarings, D: multiplication with d)

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. Using Edwards curves

Twisted Edwards curves

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

Bernstein, Birkner, Joye, Lange, P.: "Twisted Edwards Curves" in AFRICACRYPT '08):

- generalize Edwards curves to $ax^2 + y^2 = 1 + dx^2y^2$, with $a, d \neq 0$ and $a \neq d$
- show that twisted Edwards curves include more curves over finite fields, and in particular every elliptic curve in Montgomery form
- cover even more curves via isogenies
- fast explicit formulas for twisted Edwards curves in projective and inverted coordinates

Elliptic Curve Factoring Method using Edwards curves

Bernstein-Birkner-Lange-P., "ECM using Edwards curves": Better curves for ECM; and twisted-Edwards ECM software, faster than state-of-the-art GMP-ECM Montgomery software.

Edwards curves in characteristic 2

Bernstein-Lange-Rezaeian Farashahi, "Binary Edwards curves": Edwards-like curve shape for all ordinary elliptic curves over fields $\mathbb{F}_{2^n}$ if $n \geq 3$.

Interested in Elliptic Curve Cryptography?

The 12th Workshop on Elliptic Curve Cryptography (ECC 2008)

September 22-24, 2008,

Utrecht, The Netherlands

`http://www.hyperelliptic.org/tanja/conf/ECC08/`