Elliptic-curve cryptography VI

Montgomery curves and birational equivalence

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Montgomery curves

Montgomery curves are a special form of elliptic curves which can be written in the form

$$M_{A,B} : Bv^2 = u^3 + Au^2 + u, \quad B \neq 0, A \neq \pm 2.$$

This almost matches the general Weierstrass equation given in talk V.

Montgomery curves

Montgomery curves are a special form of elliptic curves which can be written in the form

$$M_{A,B} : Bv^2 = u^3 + Au^2 + u, \quad B \neq 0, A \neq \pm 2.$$

This almost matches the general Weierstrass equation given in talk V.
The addition law is very similar: The first 3 cases match, the others are

If $u_1 = u_2$ and $v_1 = v_2 \neq 0$ then $\lambda = (3u_1^2 + 2Au_1 + 1)/(2Bv_1)$.
If $u_1 \neq u_2$ then $\lambda = (v_1 - v_2)/(u_1 - u_2)$.
In both cases

$$u_3 = B\lambda^2 - A - u_1 - u_2, v_3 = \lambda(u_1 - u_3) - v_1$$

As on Weierstrass curves:
$-(u_1, v_1) = (u_1, -v_1)$ and ∞ is the neutral element.

Montgomery curves

Montgomery curves are a special form of elliptic curves which can be written in the form

$$M_{A,B} : Bv^2 = u^3 + Au^2 + u, \quad B \neq 0, A \neq \pm 2.$$

This almost matches the general Weierstrass equation given in talk V. The addition law is very similar: The first 3 cases match, the others are

If $u_1 = u_2$ and $v_1 = v_2 \neq 0$ then $\lambda = (3u_1^2 + 2Au_1 + 1)/(2Bv_1)$.
If $u_1 \neq u_2$ then $\lambda = (v_1 - v_2)/(u_1 - u_2)$.
In both cases

$$u_3 = B\lambda^2 - A - u_1 - u_2, v_3 = \lambda(u_1 - u_3) - v_1$$

As on Weierstrass curves:
$-(u_1, v_1) = (u_1, -v_1)$ and ∞ is the neutral element.

Montgomery curves always have a point $(0, 0)$ of order 2. Over a finite field they have at least one of the following (see next page for proof)

- Two more points of order 2.
- Two points of order 4 doubling to $(0, 0)$.

Hence, the group order is always divisible by 4.

Proof

Want to show that $Bv^2 = u^3 + Au^2 + u$ has more points of order 2 or points of order 4.

If $A^2 - 4$ is a square then

$$u^3 + Au^2 + u = u(u^2 + Au + 1) = u(u - u_1)(u - u_2),$$

with $u_{1,2} = (-A \pm \sqrt{A^2 - 4})/2$ and $(u_1, 0), (u_2, 0)$ have order 2.

Proof

Want to show that $Bv^2 = u^3 + Au^2 + u$ has more points of order 2 or points of order 4.

If $A^2 - 4$ is a square then

$$u^3 + Au^2 + u = u(u^2 + Au + 1) = u(u - u_1)(u - u_2),$$

with $u_{1,2} = (-A \pm \sqrt{A^2 - 4})/2$ and $(u_1, 0), (u_2, 0)$ have order 2.

Else if $(A + 2)/B$ is a square then $(1, \pm\sqrt{(A + 2)/B})$ double to $(0, 0)$, hence have order 4

Proof

Want to show that $Bv^2 = u^3 + Au^2 + u$ has more points of order 2 or points of order 4.

If $A^2 - 4$ is a square then

$$u^3 + Au^2 + u = u(u^2 + Au + 1) = u(u - u_1)(u - u_2),$$

with $u_{1,2} = (-A \pm \sqrt{A^2 - 4})/2$ and $(u_1, 0), (u_2, 0)$ have order 2.

Else if $(A + 2)/B$ is a square then $(1, \pm\sqrt{(A + 2)/B})$ double to $(0, 0)$, hence have order 4

Else $(A - 2)/B$ is a square and $(-1, \pm\sqrt{(A - 2)/B})$ double to $(0, 0)$, hence have order 4.

Easy to see that these are on curve. Small computation for doubling.

Proof

Want to show that $Bv^2 = u^3 + Au^2 + u$ has more points of order 2 or points of order 4.

If $A^2 - 4$ is a square then

$$u^3 + Au^2 + u = u(u^2 + Au + 1) = u(u - u_1)(u - u_2),$$

with $u_{1,2} = (-A \pm \sqrt{A^2 - 4})/2$ and $(u_1, 0), (u_2, 0)$ have order 2.

Else if $(A + 2)/B$ is a square then $(1, \pm\sqrt{(A + 2)/B})$ double to $(0, 0)$, hence have order 4

Else $(A - 2)/B$ is a square and $(-1, \pm\sqrt{(A - 2)/B})$ double to $(0, 0)$, hence have order 4.

Easy to see that these are on curve. Small computation for doubling.

Let $a, b \in \mathbf{F}_p^*$. Then either ab is a square or exactly one of a and b is.
Prove this via $\mathbf{F}_p^* = \langle g \rangle$ and that any even power of g is a square.
Thus at least one of $(A + 2)/B, (A - 2)/B$, and $(A^2 - 4)/B^2$ is square.

Birational equivalences

Two curves are *birationally equivalent* if there exist maps between the curves given by fractions of polynomials (rational maps) which map almost all points on one curve to the other and almost all points of the other to the first and which are compatible with the group law, i.e.

$$\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1, \phi_i(P+Q) = \phi_i(P) + \phi_i(Q),$$

where ϕ_i are rational maps and for all $P, Q, P+Q$ on E_i where ϕ_i is defined.

Birational equivalences

Two curves are *birationally equivalent* if there exist maps between the curves given by fractions of polynomials (rational maps) which map almost all points on one curve to the other and almost all points of the other to the first and which are compatible with the group law, i.e.

$$\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1, \phi_i(P+Q) = \phi_i(P) + \phi_i(Q),$$

where ϕ_i are rational maps and for all $P, Q, P+Q$ on E_i where ϕ_i is defined.

Twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to Montgomery curve $M_{A,B} : Bv^2 = u^3 + Au^2 + u$ for

$$A = 2(a+d)/(a-d), B = 4/(a-d) \Leftrightarrow a = (A+2)/B, d = (A-2)/B$$

mapping

$$u = (1+y)/(1-y), v = u/x \Leftrightarrow x = u/v, y = (u-1)/(u+1).$$

These have exceptions at

Birational equivalences

Two curves are *birationally equivalent* if there exist maps between the curves given by fractions of polynomials (rational maps) which map almost all points on one curve to the other and almost all points of the other to the first and which are compatible with the group law, i.e.

$$\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1, \phi_i(P+Q) = \phi_i(P) + \phi_i(Q),$$

where ϕ_i are rational maps and for all $P, Q, P+Q$ on E_i where ϕ_i is defined.

Twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to Montgomery curve $M_{A,B} : Bv^2 = u^3 + Au^2 + u$ for

$$A = 2(a+d)/(a-d), B = 4/(a-d) \Leftrightarrow a = (A+2)/B, d = (A-2)/B$$

mapping

$$u = (1+y)/(1-y), v = u/x \Leftrightarrow x = u/v, y = (u-1)/(u+1).$$

These have exceptions at $(0,0), (u_1, 0), (u_2, 0), (-1, \pm\sqrt{(A-2)/B}), \infty$ on $M_{A,B}$ and

Birational equivalences

Two curves are *birationally equivalent* if there exist maps between the curves given by fractions of polynomials (rational maps) which map almost all points on one curve to the other and almost all points of the other to the first and which are compatible with the group law, i.e.

$$\phi_1 : E_1 \to E_2, \phi_2 : E_2 \to E_1, \phi_i(P+Q) = \phi_i(P) + \phi_i(Q),$$

where ϕ_i are rational maps and for all $P, Q, P+Q$ on E_i where ϕ_i is defined.

Twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to Montgomery curve $M_{A,B} : Bv^2 = u^3 + Au^2 + u$ for

$$A = 2(a+d)/(a-d), B = 4/(a-d) \Leftrightarrow a = (A+2)/B, d = (A-2)/B$$

mapping

$$u = (1+y)/(1-y), v = u/x \Leftrightarrow x = u/v, y = (u-1)/(u+1).$$

These have exceptions at $(0,0), (u_1,0), (u_2,0), (-1, \pm\sqrt{(A-2)/B}), \infty$ on $M_{A,B}$ and $(0,1), (0,-1)$ and any points at infinity on $E_{a,d}$ if those points exist.