Montgomery Addition for Genus Two Curves

Tanja Lange

ITSC - Information-Security and Cryptography

Ruhr-University of Bochum

lange@itsc.ruhr-uni-bochum.de

14.06.2004

Overview

- The aim
- Doubling
- Cantor's algorithm
- Montgomery arithmetic for elliptic curves
- Montgomery arithmetic for genus two curves

The Aim

- Main focus on countermeasure against SPA
- Use Montgomery ladder, i. e. keep two group elements with fixed difference
- Avoid increase of storage:
  in Mumford representation store only first polynomial u of $[u, v]$.
- Allow general equation of curve
  (prime group order wanted, no cofactor)

Doubling

For $D = [u, v]$, the m-th division polynomial allows to state mD as expression of u, v.

Elliptic curves: folklore (exercise in Silverman)

Hyperelliptic curves: Cantor 1994 (J. reine angewandte Mathematik)

First part of $2D$ depends only on first part of D

$\Rightarrow$ doubling no problem.

Arithmetic on hyperelliptic curves

Composition & Reduction (Cantor)

`IN:` $D_1 = [u_1, v_1], D_2 = [u_2, v_2], C : y^2 = f(x)$
`OUT:` $D = [u, v]$ reduced with $D \sim D_1 + D_2$

1. compute $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
2. compute $d = \gcd(d_1, v_1 + v_2) = c_1 d_1 + c_2(v_1 + v_2)$
3. let $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
4. $u = \frac{u_1 u_2}{d^2} \quad v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$
5. let $u' = \frac{f - v^2}{u} \quad b' = (-v) \bmod u'$
6. if $\deg u' > g$ put $u := u', v := v'$ goto step 5
7. make u monic

Montgomery Arithmetic for Elliptic Curves

Start with first polynomials of D_1, D_2

$$u_1 = x - x_1, u_2 = x - x_2 (x_1 \neq x_2)$$

and $u_- = x - x_-$ of $D_- = D_1 - D_2$.

Compute $D_+ = D_1 + D_2$ given by $u_+ = x - x_+$.
$d_1 = d = 1$ in Cantor's Algorithm and
$s_1 = e_1 = 1/(x_2 - x_1) = -e_2 = -s_2$, $s_3 = 0$. Thus in Step 4:

$$\begin{aligned}
\tilde{u}_+ &= \tilde{u}_- = u_1 u_2 \\
\tilde{v}_+ &= \frac{u_1 v_2 - u_2 v_1}{x_2 - x_1} \mod \tilde{u}_+ = \frac{u_1 v_2 - u_2 v_1}{x_2 - x_1} \\
\tilde{v}_- &= \frac{-u_1 v_2 - u_2 v_1}{x_2 - x_1} \mod \tilde{u}_- = \frac{-u_1 v_2 - u_2 v_1}{x_2 - x_1}
\end{aligned}$$

cont. ...

$v_i = y_i$ unknown, but $y_i^2 = f(x_i)$.
Take product of u'_+ and u'_-

$$
\begin{aligned}
u'_+ u'_- &= x^2 - (x_+ + x_-)x + x_+ x_- = \frac{(f - \tilde{v}_-^2)(f - \tilde{v}_+^2)}{u_1^2 u_2^2} \\
&= \frac{(f - (u_1^2 v_2^2 + u_2^2 v_1^2)/(x_2 - x_1)^2)^2 - 4u_1^2 u_2^2 v_1^2 v_2^2/(x_2 - x_1)^4}{u_1^2 u_2^2}.
\end{aligned}
$$

Multiplying out leads to

$$
x_+ = \frac{2}{(x_1 - x_2)^2}(2a_6 + (x_1 + x_2)(a_4 + x_1 x_2)) - x_-.
$$

Needs 4 multiplications and 1 inversion (saving of 2 M compared to Brier/Joye).

Projective Version

Allow further coordinate z, no field inversion needed

$$
\begin{aligned}
x_+ &= 2(2a_6(z_1 z_2)^2 + (x_1 z_2 + x_2 z_1)(a_4 z_1 z_2 + x_1 x_2)) - \\
&\quad - x_-(x_1 z_2 - x_2 z_1)^2, \\
z_+ &= (x_1 z_2 - x_2 z_1)^2
\end{aligned}
$$

This needs 7 multiplications and 3 multiplications by fixed constants just as the formulae by Brier/Joye

Montgomery Arithmetic for Genus 2 Curves

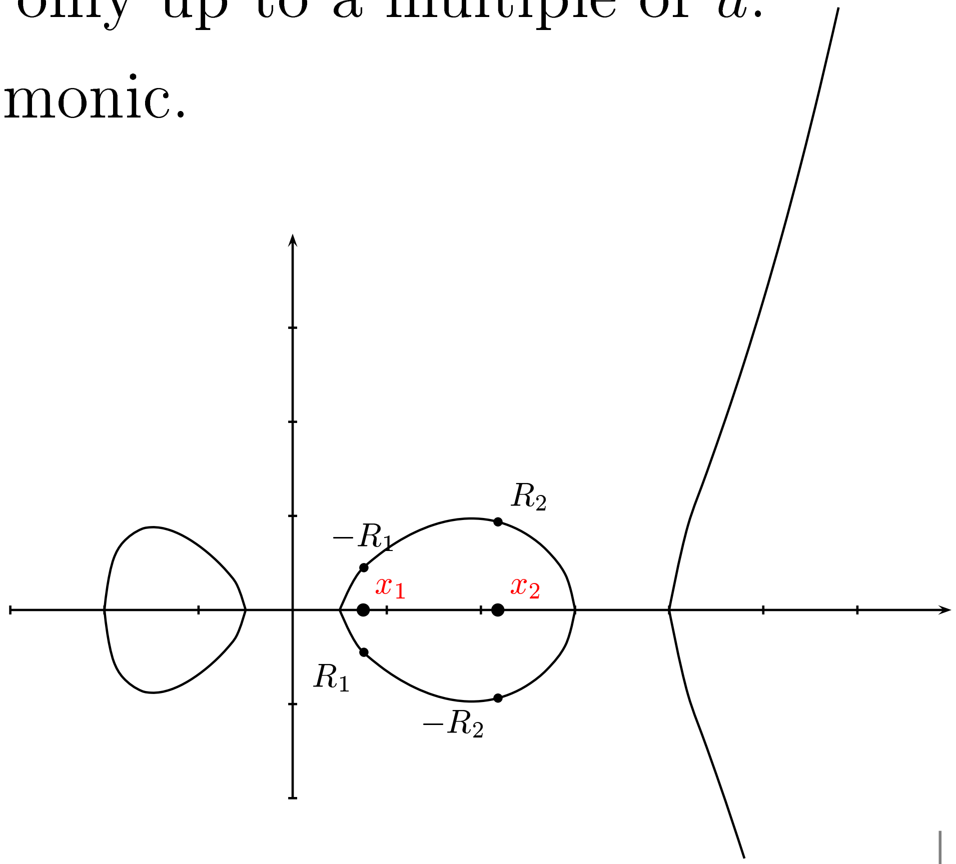
Problems:

- Reduction in $\tilde{v_\pm} = s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f) \bmod u_\pm$
- As $f \equiv v^2 \bmod u$, v^2 is given only up to a multiple of u.
- The resulting u'_+ will not be monic.

Reason:

Each u-polynomial belongs to 4 different divisor classes:

$$
\begin{array}{rcl}
P_1 + R_2 & - & 2P_\infty \\
(-R_1) + R_2 & - & 2P_\infty \\
R_1 + (-R_2) & - & 2P_\infty \\
(-R_1) + (-R_2) & - & 2P_\infty
\end{array}
$$



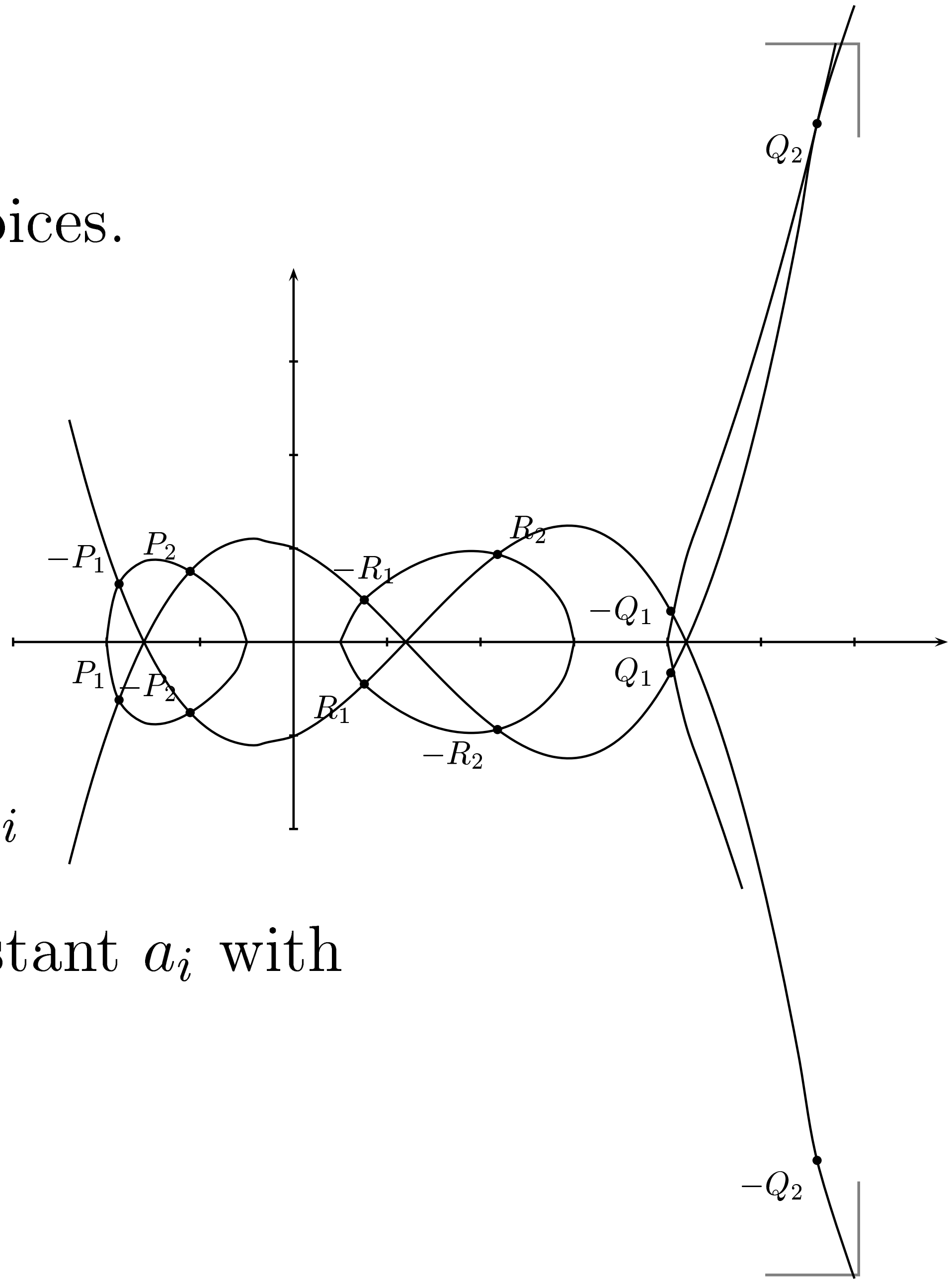
Genus Two cont.

Additionally known: u_-
$\Rightarrow$ cancels out all but 2 possible choices.

Introduce some variables:
e_i from Cantor's Algorithm

put $u_i = x^2 + u_{i1}x + u_{i0}$,

$$\begin{aligned} b_i &= b_{i1}x + b_{i0} \equiv (e_i v_{3-i})^2 \\ &\equiv e_i^2 f \bmod u_{3-i} \\ c_i &= c_{i1}x + c_{i0} \equiv e_i v_{3-i} \bmod u_{3-i} \end{aligned}$$



Then $c_i^2 = b_i + a_i u_{3-i}$ for some constant a_i with

$$\begin{aligned} c_{i1}^2 &= a_i (u \text{ is monic }) \\ 2c_{i1}c_{i0} &= b_{i1} + u_{(3-i)1}a_i \\ c_{i0}^2 &= b_{i0} + u_{(3-i)0}a_i. \end{aligned}$$

Genus Two cont.

…even more messy details (computation of resultants) …
$\Rightarrow u_+$.
Next step: make all computations explicit, use projective coordinates.
Advantages:

- Uniformity of side channel information
- Lower storage requirement
- General applicability (no cofactor)

Drawbacks:

- Many operations
- Slower than unshielded double-and-add
- No gain for special curves (see next talk)

The End

The END

Thanks!