Variants of the Montgomery form based on Theta functions

Pierrick Gaudry

gaudry@lix.polytechnique.fr

LORIA

Contents

- Motivation
- The Montgomery form for elliptic curves
- Background on Theta
- Genus 1, odd characteristic
- Genus 1, characteristic 2
- Genus 2, odd characteristic
- Genus 2, characteristic 2

Motivation

ECC and HECC

- Advantages of ECC vs finite fields in DL-based systems:
  - Better speed, bandwidth, key sizes, for similar security.
  - Slightly more complicated to generate parameters (point counting).
  - Better scalability for high security levels (AES-256).
- HECC vs ECC:
  - Bandwidth and key sizes similar to elliptic curves.
  - Parameter generation (point counting) is difficult – especially in large characteristic.
  - Speed? (See talk by T. Lange, last ECC conference)

Soft- vs Hard-ware

- Software
  - Prime field arithmetic faster than characteristic 2.
  - No real need to consider SCA (but still... there are some attacks using the behaviour of the memory hierarchy)
  - Some parallelism might be used, but very limited.
- Hardware
  - Characteristic 2 is cheaper than prime field arithmetic.
  - SCA is usually a crucial threat.
  - If area / power consumption is not the main issue, then one can put several multiplication units on the same chip, thus allowing parallelism.

The Montgomery form for elliptic curves

Curves with a particular equation

Def. An elliptic curve is in Montgomery form if it has an equation

$$E \ : \ By^2 = x^3 + Ax^2 + x,$$

with $B(A^2 - 4) \neq 0$.

Arithmetic considerations show that E and its twist have order divisible by 4.

If $p \equiv 1 \mod 4$, then one is even divisible by 8.

Abscissa-only formulae

Let $P = (x_P, y_P)$ be a point on E. Then the abscissa x_n/z_n of the n-th multiple of P is obtained with the following recurrence formulae:

$$x_1 = x_P, \qquad z_1 = 1,$$

$$\begin{cases} x_{2n} &= (x_n^2 - z_n^2)^2, \\ z_{2n} &= 4x_n z_n (x_n^2 + A x_n z_n + z_n^2), \end{cases}$$

$$\begin{cases} x_{n+m}x_{n-m} &= 4(x_n x_m - z_n z_m)^2, \\ z_{n+m}z_{n-m} &= 4(x_n z_m - z_n x_m)^2. \end{cases}$$

Particular case: $m = n + 1$.

Operation count

After some reorganization of the formulae, obtaining $(x_{2n}, z_{2n}, x_{2n+1}, z_{2n+1})$ or $(x_{2n+1}, z_{2n+1}, x_{2n+2}, z_{2n+2})$ from $(x_n, z_n, x_{n+1}, z_{n+1})$ can be done in

- 4 squares,
- 4 multiplications,
- 1 multiplication by $(A-2)/4$ (usually a small integer),
- 1 multiplication by x_1.
- 1 multiplication by z_1 (usually equal to 1),

Total: 5 P + 4 S + 1 sP per bit for a scalar multiplication (binary ladder).

Extensions

- Montgomery form is used in:
  - Implementation of ECM for factoring;
  - Implementation of ECC, e.g. `curve25519` by D. Bernstein.
- Extensions to genus 2 ?
  - Chudnovsky and Chudnovsky suggested Kummer surface in 1986, in the context of primality proving;
  - Siksek and Smart in 1999;
  - Duquesne, Lange in 2004;

Here: use Theta functions to get Montgomery-like formulae in various contexts.

Background on Theta

Definition of ϑ

In the following few slides, we work over $\mathbb{C}$.

Let Ω be a matrix in the g-dimensional Siegel upper-half-space $\mathcal{H}_2$, i.e. Ω is a symmetric $g \times g$ matrix with $\mathrm{Im}(\Omega) > 0$.

Def. The Riemann Theta function is, for $\mathbf{z} \in \mathbb{C}^g$,

$$\vartheta(\mathbf{z}, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i\, {}^t n \Omega n + 2\pi i\, {}^t n \cdot \mathbf{z}\right).$$

If $\mathbf{z}$ is set to 0, we obtain a Theta constant.

ϑ is "almost" periodic:

$$\vartheta(\mathbf{z} + \Omega m + n, \Omega) = \exp(-i\pi^t m \Omega m - 2i\pi^t m \cdot \mathbf{z}) \cdot \vartheta(\mathbf{z}, \Omega).$$

$\Longrightarrow$ "almost defined" on the abelian variety $\mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$.

Theta functions with characteristics

For a and b, two vectors in $\{0, \frac{1}{2}\}^g$, we define

$$\vartheta[a;b](\mathbf{z},\Omega) = \exp\left(\pi i\, {}^t a\Omega a + 2\pi i\, {}^t a\cdot(\mathbf{z}+b)\right)\cdot\vartheta(\mathbf{z}+\Omega a+b,\Omega).$$

There are 2^{2g} of them, yielding 2^{2g} Theta functions with characteristic and 2^{2g} Theta constants.

Among them, $2^{g-1}(2^g+1)$ are even and $2^{g-1}(2^g-1)$ are odd.

Obviously, the odd Theta functions with characteristics give trivial Theta constants.

Theta functions with characteristics

$$
\begin{array}{lccccc}
 & & & \text{even} & & \text{odd} \\
g=1: & 4 & = & 3 & + & 1 \\
g=2: & 16 & = & 10 & + & 6 \\
g=3: & 64 & = & 36 & + & 28
\end{array}
$$

A projective embedding

For a fixed Ω, let φ be the map from $\mathbb{C}^g$ to $\mathbb{P}^{2^g-1}(\mathbb{C})$ defined by

$$\varphi(\mathbf{z}) = \Big(\vartheta[0;b](2\mathbf{z},\Omega)\Big)_{b\in\{0,\frac{1}{2}\}^g}.$$

By periodicity, one checks that up to a multiplicative constant,

$$\varphi(\mathbf{z}+\Omega m+n)=\varphi(\mathbf{z}), \qquad \text{for } (m,n)\in\mathbb{Z}^g\times\mathbb{Z}^g,$$

so that φ is well-defined from $\mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g)$ to $\mathbb{P}^{2^g-1}(\mathbb{C})$.

Rem. Since all the $\vartheta[0;b]$ are even, φ is even: $-\mathbf{z}$ and $\mathbf{z}$ are sent to the same point. *[and this is essentially the only injectivity defect]*

The Kummer variety

Def. The image of φ is called the Kummer variety of the abelian variety $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.

Rem. This is a complicated way to say that the Kummer variety of an abelian variety A is $A/\{\pm 1\}$.

Our main interest in using Theta functions is. . .

The Kummer variety

Def. The image of φ is called the Kummer variety of the abelian variety $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.

Rem. This is a complicated way to say that the Kummer variety of an abelian variety A is $A/\{\pm 1\}$.

Our main interest in using Theta functions is. . .

Formulae

Formulae

Taken from Mumford's *Tata lectures on Theta (I)*, for genus 1:

RIEMANN'S THETA FORMULAE

I. (R_1): $\sum_{\eta=0,\frac{1}{2},\frac{\tau}{2},\frac{1+\tau}{2}} e_\eta \vartheta(x+\eta)\vartheta(y+\eta)\vartheta(u+\eta)\vartheta(v+\eta) = 2\vartheta(x_1)\vartheta(y_1)\vartheta(u_1)\vartheta(v_1)$

where $e_\eta = 1$ for $\eta = 0, \frac{1}{2}$ and $e_\eta = \exp(\pi i\tau + \pi i(x+y+u+v))$ for $\eta = \frac{1}{2}(1+\tau)$, and

$x_1 = \frac{1}{2}(x+y+u+v)$, $y_1 = \frac{1}{2}(x+y-u-v)$, $u_1 = \frac{1}{2}(x-y+u-v)$ and $v_1 = \frac{1}{2}(x-y-u+v)$.

II. Via Half-integer thetas:

$\vartheta^x_{oo} = \vartheta(x,\tau) = \Sigma\exp(\pi i n^2\tau + 2\pi i n x)$, $\vartheta^x_{01} = \Sigma\exp(\pi i n^2\tau + 2\pi i n(x+\frac{1}{2}))$,

$\vartheta^x_{10} = \Sigma\exp(\pi i(n+\frac{1}{2})^2\tau + 2\pi i(n+\frac{1}{2})x)$ and $\vartheta^x_{11} = \Sigma\exp(\pi i(n+\frac{1}{2})^2\tau + 2\pi i(n+\frac{1}{2})(x+\frac{1}{2}))$

(R_2): $\vartheta^x_{oo}\vartheta^y_{oo}\vartheta^u_{oo}\vartheta^v_{oo} + \vartheta^x_{01}\vartheta^y_{01}\vartheta^u_{01}\vartheta^v_{01} + \vartheta^x_{10}\vartheta^y_{10}\vartheta^u_{10}\vartheta^v_{10} + \vartheta^x_{11}\vartheta^y_{11}\vartheta^u_{11}\vartheta^v_{11} = 2\vartheta^{x_1}_{oo}\vartheta^{y_1}_{oo}\vartheta^{u_1}_{oo}\vartheta^{v_1}_{oo}$

" + " − " − " $= 2\vartheta^{x_1}_{01}\vartheta^{y_1}_{01}\vartheta^{u_1}_{01}\vartheta^{v_1}_{01}$

" − " + " − " $= 2\vartheta^{x_1}_{10}\vartheta^{y_1}_{10}\vartheta^{u_1}_{10}\vartheta^{v_1}_{10}$

" − " − " + " $= 2\vartheta^{z_1}_{11}\vartheta^{y_1}_{11}\vartheta^{u_1}_{11}\vartheta^{v_1}_{11}$

(R_6): $\vartheta^x_{oo}\vartheta^y_{oo}\vartheta^u_{01}\vartheta^v_{01} + \vartheta^x_{01}\vartheta^y_{01}\vartheta^u_{oo}\vartheta^v_{oo} + \vartheta^x_{10}\vartheta^y_{10}\vartheta^u_{11}\vartheta^v_{11} + \vartheta^x_{11}\vartheta^y_{11}\vartheta^u_{10}\vartheta^v_{10} = 2\vartheta^{z_1}_{01}\vartheta^{y_1}_{01}\vartheta^{u_1}_{oo}\vartheta^{v_1}_{oo}$

" + " − " − " $= 2\vartheta^{x_1}_{oo}\vartheta^{y_1}_{oo}\vartheta^{u_1}_{01}\vartheta^{v_1}_{01}$

" − " + " − " $= -2\vartheta^{x_1}_{11}\vartheta^{y_1}_{11}\vartheta^{u_1}_{10}\vartheta^{v_1}_{10}$

" − " − " + " $= -2\vartheta^{x_1}_{10}\vartheta^{y_1}_{10}\vartheta^{u_1}_{11}\vartheta^{v_1}_{11}$

(R_{10}): $\vartheta^x_{oo}\vartheta^y_{oo}\vartheta^u_{10}\vartheta^v_{10} + \vartheta^x_{01}\vartheta^y_{01}\vartheta^u_{11}\vartheta^v_{11} + \vartheta^x_{10}\vartheta^y_{10}\vartheta^u_{oo}\vartheta^v_{oo} + \vartheta^x_{11}\vartheta^y_{11}\vartheta^u_{01}\vartheta^v_{01} = 2\vartheta^{x_1}_{oo}\vartheta^{y_1}_{oo}\vartheta^{u_1}_{10}\vartheta^{v_1}_{10}$

" + " − " − " $= 2\vartheta^{x_1}_{01}\vartheta^{y_1}_{01}\vartheta^{u_1}_{11}\vartheta^{v_1}_{11}$

" − " + " − " $= 2\vartheta^{x_1}_{10}\vartheta^{y_1}_{10}\vartheta^{u_1}_{oo}\vartheta^{v_1}_{oo}$

" − " − " + " $= 2\vartheta^{x_1}_{11}\vartheta^{y_1}_{11}\vartheta^{u_1}_{01}\vartheta^{v_1}_{01}$

(R_{14}): $\vartheta^x_{oo}\vartheta^y_{oo}\vartheta^u_{11}\vartheta^v_{11} + \vartheta^x_{01}\vartheta^y_{01}\vartheta^u_{10}\vartheta^v_{10} + \vartheta^x_{10}\vartheta^y_{10}\vartheta^u_{01}\vartheta^v_{01} + \vartheta^x_{11}\vartheta^y_{11}\vartheta^u_{oo}\vartheta^v_{oo} = 2\vartheta^{x_1}_{01}\vartheta^{y_1}_{01}\vartheta^{u_1}_{10}\vartheta^{v_1}_{10}$

" + " − " − " $= 2\vartheta^{x_1}_{oo}\vartheta^{y_1}_{oo}\vartheta^{u_1}_{11}\vartheta^{v_1}_{11}$

" − " + " − " $= -2\vartheta^{x_1}_{11}\vartheta^{y_1}_{11}\vartheta^{u_1}_{oo}\vartheta^{v_1}_{oo}$

" − " − " + " $= -2\vartheta^{x_1}_{10}\vartheta^{y_1}_{10}\vartheta^{u_1}_{01}\vartheta^{v_1}_{01}$

(R_{18}): $\vartheta^x_{oo}\vartheta^y_{01}\vartheta^u_{11}\vartheta^v_{11} + \vartheta^x_{01}\vartheta^y_{oo}\vartheta^u_{10}\vartheta^v_{10} + \vartheta^x_{10}\vartheta^y_{11}\vartheta^u_{oo}\vartheta^v_{01} + \vartheta^x_{11}\vartheta^y_{10}\vartheta^u_{01}\vartheta^v_{oo} = 2\vartheta^{x_1}_{11}\vartheta^{y_1}_{10}\vartheta^{u_1}_{01}\vartheta^{v_1}_{oo}$

" + " − " − " $= -2\vartheta^{x_1}_{10}\vartheta^{y_1}_{11}\vartheta^{u_1}_{oo}\vartheta^{v_1}_{01}$

" − " + " − " $= -2\vartheta^{x_1}_{01}\vartheta^{y_1}_{oo}\vartheta^{u_1}_{11}\vartheta^{v_1}_{10}$

(R_{21}): " − " − " + " $= 2\vartheta^{x_1}_{oo}\vartheta^{y_1}_{01}\vartheta^{u_1}_{10}\vartheta^{v_1}_{11}$

III. Addition Formulae

(A_1): $\vartheta_{oo}(x+u)\vartheta_{oo}(x-u)\vartheta^2_{oo}(0) = \vartheta^2_{oo}(x)\vartheta^2_{oo}(u) + \vartheta^2_{11}(x)\vartheta^2_{11}(u) = \vartheta^2_{01}(x)\vartheta^2_{01}(u) + \vartheta^2_{10}(x)\vartheta^2_{10}(u)$

$\vartheta_{01}(x+u)\vartheta_{01}(x-u)\vartheta^2_{01}(0) = \vartheta^2_{oo}(x)\vartheta^2_{oo}(u) - \vartheta^2_{10}(x)\vartheta^2_{10}(u) = \vartheta^2_{01}(x)\vartheta^2_{01}(u) - \vartheta^2_{11}(x)\vartheta^2_{11}(u)$

$\vartheta_{10}(x+u)\vartheta_{10}(x-u)\vartheta^2_{10}(0) = \vartheta^2_{oo}(x)\vartheta^2_{oo}(u) - \vartheta^2_{01}(x)\vartheta^2_{01}(u) = \vartheta^2_{10}(x)\vartheta^2_{10}(u) - \vartheta^2_{11}(x)\vartheta^2_{11}(u)$

$\vartheta_{oo}(x+u)\vartheta_{01}(x-u)\vartheta_{oo}(0)\vartheta_{01}(0) = \vartheta_{oo}(x)\vartheta_{01}(x)\vartheta_{oo}(u)\vartheta_{01}(u) - \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$

$\vartheta_{01}(x+u)\vartheta_{oo}(x-u)\vartheta_{oo}(0)\vartheta_{01}(0) = \vartheta_{oo}(x)\vartheta_{01}(x)\vartheta_{00}(u)\vartheta_{01}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$

$\vartheta_{oo}(x+u)\vartheta_{10}(x-u)\vartheta_{oo}(0)\vartheta_{01}(0) = \vartheta_{oo}(x)\vartheta_{10}(x)\vartheta_{oo}(u)\vartheta_{10}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$

$\vartheta_{10}(x+u)\vartheta_{oo}(x-u)\vartheta_{oo}(0)\vartheta_{10}(0) = \vartheta_{oo}(x)\vartheta_{10}(x)\vartheta_{oo}(u)\vartheta_{10}(u) - \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$

$\vartheta_{01}(x+u)\vartheta_{10}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{oo}(x)\vartheta_{11}(x)\vartheta_{oo}(u)\vartheta_{11}(u) + \vartheta_{01}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{10}(u)$

$\vartheta_{10}(x+u)\vartheta_{01}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = -\vartheta_{oo}(x)\vartheta_{11}(x)\vartheta_{oo}(u)\vartheta_{11}(u) + \vartheta_{01}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{10}(u)$

(A_{10}): $\vartheta_{11}(x+u)\vartheta_{11}(x-u)\vartheta^2_{oo}(0) = \vartheta^2_{11}(x)\vartheta^2_{oo}(u) - \vartheta^2_{oo}(x)\vartheta^2_{11}(u) = \vartheta^2_{01}(x)\vartheta^2_{10}(u) - \vartheta^2_{10}(x)\vartheta^2_{01}(u)$

$\vartheta_{11}(x+u)\vartheta_{oo}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{oo}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{10}(u) + \vartheta_{10}(x)\vartheta_{01}(x)\vartheta_{oo}(u)\vartheta_{11}(u)$

$\vartheta_{oo}(x+u)\vartheta_{u}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{oo}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{10}(u) - \vartheta_{10}(x)\vartheta_{01}(x)\vartheta_{oo}(u)\vartheta_{11}(u)$

$\vartheta_{11}(x+u)\vartheta_{01}(x-u)\vartheta_{oo}(0)\vartheta_{10}(0) = \vartheta_{oo}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{11}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{oo}(u)\vartheta_{10}(u)$

$\vartheta_{01}(x+u)\vartheta_{11}(x-u)\vartheta_{oo}(0)\vartheta_{10}(0) = -\vartheta_{oo}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{11}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{oo}(u)\vartheta_{10}(u)$

$\vartheta_{11}(x+u)\vartheta_{10}(x-u)\vartheta_{oo}(0)\vartheta_{01}(0) = \vartheta_{oo}(x)\vartheta_{01}(x)\vartheta_{10}(u)\vartheta_{11}(u) + \vartheta_{10}(x)\vartheta_{11}(x)\vartheta_{oo}(u)\vartheta_{01}(u)$

$\vartheta_{10}(x+u)\vartheta_{11}(x-u)\vartheta_{oo}(0)\vartheta_{01}(0) = -\vartheta_{oo}(x)\vartheta_{01}(x)\vartheta_{10}(u)\vartheta_{11}(u) + \vartheta_{10}(x)\vartheta_{11}(x)\vartheta_{oo}(u)\vartheta_{01}(u)$

IV. Equations for ϑ

(E_1): $\vartheta^2_{oo}(x)\vartheta^2_{oo}(0) = \vartheta^2_{01}(x)\vartheta^2_{01}(0) + \vartheta^2_{10}(x)\vartheta^2_{10}(0)$

(E_2): $\vartheta^2_{11}(x)\vartheta^2_{oo}(0) = \vartheta^2_{01}(x)\vartheta^2_{10}(0) - \vartheta^2_{10}(x)\vartheta^2_{01}(x)$ and

(J_1): $\vartheta^4_{oo}(0) = \vartheta^4_{01}(0) + \vartheta^4_{10}(0)$

Formulae

Fact: For many of the usual curve-related algebraic objects one like to manipulate explicitly, there exist corresponding formulae with Theta functions (and often, already in the literature).

- Algebraic parametrization of the abelian variety (Weierstraß $\wp$ function);
- Modular equations (AGM as the most spectacular example);
- Isogenies (well...)
- Group law.

and for any genus!

The case of genus 1

Formulae in genus 1

In genus 1, for $\mathrm{Im}(\tau) > 0$, the map φ is

$$\varphi \ : \ \mathbf{z} \mapsto (\vartheta[0;0](2\mathbf{z},\tau), \vartheta[0;\frac{1}{2}](2\mathbf{z},\tau)),$$

from $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ to $\mathbb{P}^1(\mathbb{C})$.

Give names to some Theta constants:

$$a = \vartheta[0;0](0,\tau), \quad b = \vartheta[0;\frac{1}{2}](0,\tau),$$

$$A = \vartheta[0;0](0,2\tau), \quad B = \vartheta[\frac{1}{2};0](0,2\tau).$$

The pseudo-group law on $\mathbb{P}^1(\mathbb{C})$ is given by the following formulae.

Rem. $2A^2 = a^2 + b^2$ and $2B^2 = a^2 - b^2$.

Doubling

$$a\vartheta[0;0](\mathbf{z},\tau) = \vartheta[0;0](\mathbf{z},2\tau)^2 + \vartheta[\frac{1}{2};0](\mathbf{z},2\tau)^2$$

$$b\vartheta[0;\frac{1}{2}](\mathbf{z},\tau) = \vartheta[0;0](\mathbf{z},2\tau)^2 - \vartheta[\frac{1}{2};0](\mathbf{z},2\tau)^2$$

$$2A\vartheta[0;0](2\mathbf{z},2\tau) = \vartheta[0;0](\mathbf{z},\tau)^2 + \vartheta[0;\frac{1}{2}](\mathbf{z},\tau)^2$$

$$2B\vartheta[\frac{1}{2};0](2\mathbf{z},2\tau) = \vartheta[0;0](\mathbf{z},\tau)^2 - \vartheta[0;\frac{1}{2}](\mathbf{z},\tau)^2$$

Doubling (deciphered)

Input: A point $P = (x : y)$ with $P = \varphi(\mathbf{z})$;

Output: The double $2P = (X : Y)$, i.e. $2P = \varphi(2\mathbf{z})$.

1. $x' = (x^2 + y^2)^2$;
2. $y' = \frac{B^2}{A^2}(x^2 - y^2)^2$;
3. $X = (x' + y')$;
4. $Y = \frac{b}{a}(x' - y')$;
5. Return $(X : Y)$.

Cost: 4S + 2sP.

Pseudo-addition

Input: Two points $P = (x : y) = \varphi(\mathbf{z})$ and $Q = (\underline{x} : \underline{y}) = \varphi(\underline{\mathbf{z}})$, and $R = (\bar{x} : \bar{y})$ one of $\varphi(\mathbf{z} + \underline{\mathbf{z}})$ and $\varphi(\mathbf{z} - \underline{\mathbf{z}})$, with $\bar{x}\bar{y} \neq 0$;

Output: The point $(X : Y)$ among $\varphi(\mathbf{z} + \underline{\mathbf{z}})$ and $\varphi(\mathbf{z} - \underline{\mathbf{z}})$ which is different from R.

1. $x' = (x^2 + y^2)(\underline{x}^2 + \underline{y}^2)$;
2. $y' = \frac{B^2}{A^2}(x^2 - y^2)(\underline{x}^2 - \underline{y}^2)$;
3. $X = (x' + y')/\bar{x}$;
4. $Y = (x' - y')/\bar{y}$;
5. Return $(X : Y)$.

Cost: 4S + 3P + 1sP (2S + 3P + 1sP).

Alternate representation

- To simplify, we can manipulate squares of coordinates of points. This makes it easier to count products.
- We could also store $(x^2 + y^2, x^2 - y^2)$ to make clear that we can share some additions.

Rem. In some formulae below, I sometimes use this alternate representation.

Scalar multiplication

Thm. Multiplying a point by a scalar n on the Kummer line of E costs $6 \log n$ squarings, $3 \log n$ multiplications, and $3 \log n$ multiplications by constants.

Rem. Compared to Montgomery's formulae, that's 1 P replaced by 1 S, but 2 more sP.

- For ECC implementation on PC, DJB's cycle count for `curve25519` give similar results for both;
- For different context, this might be different;
- For ECM, when the modulus gets large, at some point this should become better than Montgomery.

Validity of the formulae over a finite field

The formulae are valid on $\mathbb{C}$, but one wants to use them over a finite field.

Two lines of proof:

- Make explicit the map with a Weierstraß equation;
- Lift/reduce approach.

The first approach is useful to use point-counting, and guarantee that the DLP is equivalent on Kummer and on the curve.

The second is useful to avoid heavy computations (for higher genus), and to derive formulae in characteristic 2.

Link with classical Weierstraß equation

Let $\lambda = \frac{a^4}{a^4 - b^4}$ and E_λ the curve of equation

$$E_\lambda \ : \ Y^2 = X(X-1)(X-\lambda).$$

Then the map from the Kummer line to E_λ is given by

$$(x:y) \mapsto \left(\frac{a^2 x}{a^2 x - b^2 y}, \ \ldots \right).$$

From these formulae, it is easy to check that the formulae are valid, using the group law on E_λ.

The case of genus 1, characteristic 2

Problems with characteristic 2

- The plain formulae lead quickly to the non-point $(0:0)$.
- The link with the Weierstraß equation implies a full rational 2-torsion subgroup, which is impossible in characteristic 2.

General strategy

- Start with a curve E over $\mathbb{F}_{2^n}$;
- Lift E to a curve $\mathcal{E}$ defined over a number field K;
- Since $K \subset \mathbb{C}$, define the Kummer line associated to $\mathcal{E}$;
- Use the explicit maps to do the following
  - Take a point P on E;
  - Lift it to a point Q of $\mathcal{E}$ (a 2-adic approximation is enough);
  - Map Q to the Kummer line (again using 2-adic approximation);
  - Apply appropriate transformations to make the coordinates of Q reducible modulo 2;
  - Apply appropriate transformations to make the group law reducible modulo 2.

Let's do it...

We start with an ordinary curve E_{a_6} defined over $\mathbb{F}_q$ of characteristic 2 by

$$E_{a_6} \ : \ y^2 + xy = x^3 + a_6.$$

We consider now a curve E_λ with

$$\lambda \equiv 1 + 16\sqrt{a_6} \mod 32,$$

such that E_λ is isomorphic to a lift of E_{a_6} to $\mathbb{Q}_q$.

The explicit transformations to the Kummer line give (modulo 8):

$$a^2 \equiv 1, \quad b^2 \equiv 4\sqrt[4]{a_6}, \quad A^2 \equiv B^2 \equiv 1.$$

One checks that a point $P = (x, y)$ on E_{a_6} is mapped to a point on the Kummer line where all the coordinates are integral and the information is contained in the value modulo 2.

Let's do it...

Let $P = (x : y)$ be a point on the Kummer line, with integral 2-adic coordinates.

$$x' = (x + y)^2$$
$$y' = \frac{A^2}{B^2}(x - y)^2$$

$$X = (x' + y')^2$$
$$Y = \frac{a^2}{b^2}(x' - y')^2$$

Let's do it...

Let $P = (x : y)$ be a point on the Kummer line, with integral 2-adic coordinates.

$$x' = (x+y)^2 \equiv x^2 + y^2 + 2xy \mod 8$$
$$y' = \tfrac{A^2}{B^2}(x-y)^2 \equiv x^2 + y^2 - 2xy \mod 8.$$

$$x' + y' = 2(x^2 + y^2) \mod 8,$$
$$x' - y' = 4xy \mod 8.$$

$$X = (x' + y')^2 \equiv 4(x^4 + y^4) \mod 8,$$
$$Y = \tfrac{a^2}{b^2}(x' - y')^2 \equiv 16x^2y^2/4\sqrt[4]{a_6} \mod 8.$$

Now, since we are in projective, we can divide both X and Y by 4. We get:

$$X \equiv (x^2 + y^2)^2 \quad \text{and} \quad Y \equiv x^2y^2/\sqrt[4]{a_6} \mod 2,$$

which are valid also over $\mathbb{F}_q$.

Same business with pseudo-addition

For the pseudo-addition, we get:

[. . . some more 2-adic abstract non-sense . . .]

$$X = (x\underline{x} + y\underline{y})^2/\bar{x} \qquad \text{and} \qquad Y = ((x+y)(\underline{x}+\underline{y}) + x\underline{x} + y\underline{y})^2/\bar{y}.$$

Total Cost: 5S + 5P + 1sP per bit in scalar multiplication.

Same business with pseudo-addition

For the pseudo-addition, we get:

[. . . some more 2-adic abstract non-sense . . .]

$$X = (x\underline{x} + y\underline{y})^2/\bar{x} \qquad \text{and} \qquad Y = ((x+y)(\underline{x}+\underline{y}) + x\underline{x} + y\underline{y})^2/\bar{y}.$$

Total Cost: 5S + 5P + 1sP per bit in scalar multiplication.

Cool, but. . .

These formulae have already been discovered by Stam (PKC'03) as a variant of Lopez-Dahab (SAC'98).

The case of genus 2

A projective embedding

For a fixed Ω, let φ be the map from $\mathbb{C}^g$ to $\mathbb{P}^{2^g-1}(\mathbb{C})$ defined by

$$\varphi(\mathbf{z}) = \Big(\vartheta[0;b](2\mathbf{z},\Omega)\Big)_{b\in\{0,\frac{1}{2}\}^g}.$$

By periodicity, one checks that up to a multiplicative constant,

$$\varphi(\mathbf{z}+\Omega m+n)=\varphi(\mathbf{z}), \qquad \text{for } (m,n)\in\mathbb{Z}^g\times\mathbb{Z}^g,$$

so that φ is well-defined from $\mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g)$ to $\mathbb{P}^{2^g-1}(\mathbb{C})$.

Rem. Since all the $\vartheta[0;b]$ are even, φ is even: $-\mathbf{z}$ and $\mathbf{z}$ are sent to the same point. *[and this is essentially the only injectivity defect]*

Eight particular Theta functions

The functions used to map A to $\mathbb{P}^3(\mathbb{C})$:

$$\begin{aligned}
\vartheta_1(\mathbf{z}) &= \vartheta[(0,0);(0,0)](\mathbf{z},\Omega) \\
\vartheta_2(\mathbf{z}) &= \vartheta[(0,0);(\tfrac{1}{2},\tfrac{1}{2})](\mathbf{z},\Omega) \\
\vartheta_3(\mathbf{z}) &= \vartheta[(0,0);(\tfrac{1}{2},0)](\mathbf{z},\Omega) \\
\vartheta_4(\mathbf{z}) &= \vartheta[(0,0);(0,\tfrac{1}{2})](\mathbf{z},\Omega)\ .
\end{aligned}$$

Dual functions on the isogenous abelian variety:

$$\begin{aligned}
\Theta_1(\mathbf{z}) &= \vartheta[(0,0);(0,0)](\mathbf{z},2\Omega) \\
\Theta_2(\mathbf{z}) &= \vartheta[(\tfrac{1}{2},\tfrac{1}{2});(0,0)](\mathbf{z},2\Omega) \\
\Theta_3(\mathbf{z}) &= \vartheta[(0,\tfrac{1}{2});(0,0)](\mathbf{z},2\Omega) \\
\Theta_4(\mathbf{z}) &= \vartheta[(\tfrac{1}{2},0);(0,0)](\mathbf{z},2\Omega)\ .
\end{aligned}$$

Some constants

Let us give names to a few Theta constants:

$$a = \vartheta_1(0),\ b = \vartheta_2(0),\ c = \vartheta_3(0),\ d = \vartheta_4(0),$$

and

$$A = \Theta_1(0),\ B = \Theta_2(0),\ C = \Theta_3(0),\ D = \Theta_4(0).$$

Put also

$$y_0 = a/b,\ z_0 = a/c,\ t_0 = a/d,$$

and

$$y_0' = (A/B)^2,\ z_0' = (A/C)^2,\ t_0' = (A/D)^2,$$

Some more equations

It can be shown that

$$4A^2 = a^2 + b^2 + c^2 + d^2,$$
$$4B^2 = a^2 + b^2 - c^2 - d^2,$$
$$4C^2 = a^2 - b^2 + c^2 - d^2,$$
$$4D^2 = a^2 - b^2 - c^2 + d^2.$$

Then, we define furthermore E, F, G, H by

$$E = abcdA^2B^2C^2D^2/(a^2d^2 - b^2c^2)(a^2c^2 - b^2d^2)(a^2b^2 - c^2d^2)$$
$$F = (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2)$$
$$G = (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2)$$
$$H = (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2)\,.$$

Equation for the Kummer surface

The abelian variety has dimension 2, so has its image by φ.

4 projective coordinates + dimension 2 $\Longrightarrow$ one equation.

It can be shown that this equation is (for a point (x, y, z, t) in the image $\mathcal{K}$ of φ):

$$\mathcal{K} \ : \ (x^4 + y^4 + z^4 + t^4) + 2Exyzt - F(x^2t^2 + y^2z^2) \\ - G(x^2z^2 + y^2t^2) - H(x^2y^2 + z^2t^2) = 0.$$

Doubling formula

Input: A point $P = (x, y, z, t)$ on $\mathcal{K}$;

1. $x' = (x^2 + y^2 + z^2 + t^2)^2$;
2. $y' = y'_0(x^2 + y^2 - z^2 - t^2)^2$;
3. $z' = z'_0(x^2 - y^2 + z^2 - t^2)^2$;
4. $t' = t'_0(x^2 - y^2 - z^2 + t^2)^2$;
5. $X = (x' + y' + z' + t')$;
6. $Y = y_0(x' + y' - z' - t')$;
7. $Z = z_0(x' - y' + z' - t')$;
8. $T = t_0(x' - y' - z' + t')$;
9. Return $2P = (X, Y, Z, T)$.

Pseudo-add formula

Input: $P = (x, y, z, t)$ and $Q = (\underline{x}, \underline{y}, \underline{z}, \underline{t})$ on $\mathcal{K}$ and $R = (\bar{x}, \bar{y}, \bar{z}, \bar{t})$ one of $P + Q$ and $P - Q$.

1. $x' = (x^2 + y^2 + z^2 + t^2)(\underline{x}^2 + \underline{y}^2 + \underline{z}^2 + \underline{t}^2)$;
2. $y' = y'_0(x^2 + y^2 - z^2 - t^2)(\underline{x}^2 + \underline{y}^2 - \underline{z}^2 - \underline{t}^2)$;
3. $z' = z'_0(x^2 - y^2 + z^2 - t^2)(\underline{x}^2 - \underline{y}^2 + \underline{z}^2 - \underline{t}^2)$;
4. $t' = t'_0(x^2 - y^2 - z^2 + t^2)(\underline{x}^2 - \underline{y}^2 - \underline{z}^2 + \underline{t}^2)$;
5. $X = (x' + y' + z' + t')/\bar{x}$;
6. $Y = (x' + y' - z' - t')/\bar{y}$;
7. $Z = (x' - y' + z' - t')/\bar{z}$;
8. $T = (x' - y' - z' + t')/\bar{t}$;
9. Return $(X, Y, Z, T) = P + Q$ or $P - Q$.

Operation count

Thm. Multiplying a point by a scalar n on the Kummer surface costs $9 \log n$ squarings, $10 \log n$ multiplications, and $6 \log n$ multiplications by constants. 9S + 10P + 6 sP.

Alternate choice of organizing the computation: 12S + 7P + 9sP.

Problem: having small constants (and cheap sP), require point counting in genus 2, for which the current record is 162 bits.

Still: Can already beat ECC on a PC implementation (DJB's ECC-06 talk).

Rosenhain invariants

Given $a = \vartheta_1(0), b = \vartheta_2(0), c = \vartheta_3(0), d = \vartheta_4(0)$, four theta constants corresponding to a matrix Ω, then define:

$$\lambda = \frac{a^2c^2}{b^2d^2};\ \mu = \frac{c^2e^2}{d^2f^2};\ \nu = \frac{a^2e^2}{b^2f^2},$$

where

$$\frac{e^2}{f^2} = \frac{1 + \frac{CD}{AB}}{1 - \frac{CD}{AB}}.$$

Then the curve $\mathcal{C}$ of equation

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

has a Jacobian isomorphic to $\mathbb{C}^2/(\mathbb{Z}^2 + \Omega\mathbb{Z}^2)$. [Thomae]

Mapping points from $\mathcal{K}$ to $\mathrm{Jac}(\mathcal{C})$

$$(x, y, z, t) \mapsto \langle u(x), v^2(x) \rangle$$

The formula is a consequence of some formulae in Mumford's book. More details in van Wamelen's work.

- I won't give the formulae here...
- Some precomputation that depends only on $\mathcal{K}$ (a few hundreds of multiplications and a few dozens of inversions);
- Then, mapping a point of $\mathcal{K}$ to $\mathrm{Jac}(\mathcal{C})$ involves about 50 multiplications and a few inversions.
- Of course, the v-polynomial is computed up to sign.

Genus 2 / characteristic 2

Genus 2 – characteristic 2

The lifting/reduce technique also works in genus 2. In the following, some of the formulae have been guessed (not yet proven), but they should be correct (works on practical examples).

Let α, β, γ, δ be 4 elements of $\mathbb{F}_q^*$ of characteristic 2.

The equation of the Kummer surface is

$$\sqrt{\alpha\beta\gamma\delta}\,xyzt = \beta\gamma(xt+yz)^2 + \alpha\gamma(xz+yt)^2 + \alpha\beta(xy+zt)^2.$$

Doubling

Input: A point $P = (x, y, z, t)$ on $\mathcal{K}$;

1. $X = (xt + yz)^2$;
2. $Y = \frac{\alpha}{\gamma}(xz + yt)^2$;
3. $Z = \frac{\alpha}{\beta}(xy + zt)^2$;
4. $T = \frac{\alpha}{\delta}(x + y + z + t)^4$;
5. Return $2P = (X, Y, Z, T)$.

Cost: 4P+5S+3sP.

Pseudo-addition

Input: $P = (x, y, z, t)$ and $Q = (\underline{x}, \underline{y}, \underline{z}, \underline{t})$ on $\mathcal{K}$ and $R = (\bar{x}, \bar{y}, \bar{z}, \bar{t})$ one of $P + Q$ and $P - Q$.

1. $X = (x\underline{t} + t\underline{x} + y\underline{z} + z\underline{y})^2/\bar{x}$;
2. $Y = (x\underline{z} + z\underline{x} + y\underline{t} + t\underline{y})^2/\bar{y}$;
3. $Z = (x\underline{y} + y\underline{x} + z\underline{t} + t\underline{z})^2/\bar{z}$;
4. $T = (x\underline{x} + y\underline{y} + z\underline{z} + t\underline{t})^2/\bar{t}$;
5. Return $(X, Y, Z, T) = P + Q$ or $P - Q$.

Cost: 12P + 4S (have to rearrange things quite a bit!).

Total cost for scalar mult: 16P + 9S + 3sP per bit.

Link with the underlying genus 2 curve

Let

$$f_0 = \frac{\alpha\gamma}{\beta\delta}, \quad f_1 = \frac{\alpha}{\delta}\frac{(\beta+\gamma)^2}{\beta\gamma}, \quad f_2 = f_3 = \frac{\beta\gamma}{\alpha\delta}.$$

Then the curve $\mathcal{C}$ of equation

$$y^2 + x(x+1)y = x(x+1)(f_3x^3 + f_2x^2 + f_1x + f_0).$$

corresponds to $\mathcal{K}$.

Rem. All the ordinary genus 2 curves with rational 2-torsion can be put in this form.

Additional remarks

- Beside the operation count, Montgomery-ladder formulae are nice for SCA resistance;
- Theta-based formulae can be easily parallelized:
  - Char $\neq 2$: depth of $2P + 1S + 1sP$ (with 4 squaring units, 8 small-multipliers and 4 multipliers);
  - Char 2: depth of $2P + 1S$ (with 8 squaring units, 22 multipliers);

Conclusion

The same formulae (addition and duplication of theta functions) have given nice Montgomery-like applications in many context, that compare well to state-of-the-art:

	genus 1	genus 2
char $\neq 2$	different but as good	improvement
char $= 2$	recover the best	improvement

Further questions

- We have asked for full rational 2-torsion.

  Is it really necessary?

- We have asked for ordinary curves.

  Is it really necessary?

- Genus 3 and genus 4.

  Group law can be easily guessed. Need to work out formulae for the Kummer variety and correspondence with curves.