Genus 2 formulae based on Theta functions and their implementation

Pierrick Gaudry

pierrick.gaudry@loria.fr

LORIA – CACAO

(Nancy, France)

Genus 2 formulae based on Theta functions and RM Kummer surfaces

Pierrick Gaudry

pierrick.gaudry@loria.fr

LORIA – CACAO

(Nancy, France)

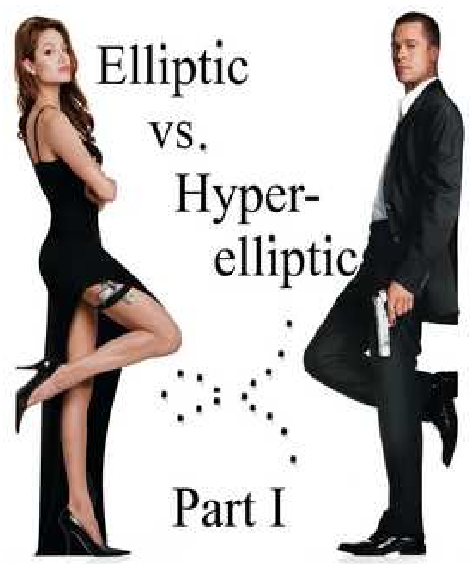
Contents

- Motivation
- Background on Theta over $\mathbb{C}$
- Formulae for genus 2
- Kummer surfaces with RM by $\sqrt{2}$

Motivation

2 > 1 ?

Remember last ECC conference... Dan and Tanja talked about:



ⓒ Danja 2006

The most famous duo in cryptography is now playing for elliptic curves.

(see their talk of Friday).

Somebody has to defend hyperelliptic curves!

Looking for formulae

- Until recently, Montgomery form for ECC is the most appropriate for key exchange implementation in genus 1.
- Fast, good SCA properties.
- Does not cover all curves; no plain addition.
- Goal: find similar formulae for genus 2. (prev work by Smart-Siksek, Duquesne, Lange).
- Following Chudnovsky and Chudnovsky: use Theta functions.

Rem. One should probably look for genus 2 formulae analogous to Edwards form, now.

Point counting becomes a question of speed

Most of the formulae involves multiplications by coeffs of the equation.

$\Longrightarrow$ If these are small integers, the formulae get faster.

Rem. Particularly true for genus 2 formulae based on Theta (DJB's last year talk).

Problem: «easy-to-count» curves (CM) usually don't have such a small coefficient equation.

Point counting of random curves is not only a question of non-trusting CM curves, but a question of SPEED.

Current record for genus 2 over $\mathbb{F}_p$ gives a 162 bit group (GaSc04).

Genus 2 RM curves

Def. A genus 2 RM curve $\mathcal{C}$ is such that $\mathrm{End}_{\mathbb{Q}}\mathrm{Jac}(\mathcal{C})$ is isomorphic to a real quadratic field.

- CM curves + easy pt counting: no choice in p / size of coeffs. Dim 0.
- Random curves + hard pt counting: choose p / small coeffs. Dim 3.
- RM curves + medium pt counting: choose p / small coeffs. Dim 2.

Rem. The additional endomorphism can be used to speed-up scalar multiplication. (Takashima, Kohel-Smith).

Background on Theta

Siegel upper-half-space

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 $\mathrm{Im}(\Omega) > 0$.

Rem. In dim 1, Ω is in the upper-half plane (and Ω is denoted by τ...)

Then $\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ is an abelian variety A.

If A is the Jacobian of a curve $\mathcal{C}$, then Ω is called the period matrix of $\mathcal{C}$.

Rem. The action of the symplectic group on Ω does not change the isomorphism class of A.

In dim 1, this is $SL_2(\mathbb{Z})$ acting on τ.

Definition of ϑ

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

			even		odd
$g = 1:$	4	$=$	3	$+$	1
$g = 2:$	16	$=$	10	$+$	6
$g = 3:$	64	$=$	36	$+$	28

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

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:

$\vartheta_{00}^{x} = \vartheta(x,\tau) = \sum\exp(\pi i n^2\tau + 2\pi i n x)$, $\vartheta_{01}^{x} = \sum\exp(\pi i n^2\tau + 2\pi i n(x+\frac{1}{2}))$,

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

(R_2): $\vartheta_{00}^{x}\vartheta_{00}^{y}\vartheta_{00}^{u}\vartheta_{00}^{v}+\vartheta_{01}^{x}\vartheta_{01}^{y}\vartheta_{01}^{u}\vartheta_{01}^{v}+\vartheta_{10}^{x}\vartheta_{10}^{y}\vartheta_{10}^{u}\vartheta_{10}^{v}+\vartheta_{11}^{x}\vartheta_{11}^{y}\vartheta_{11}^{u}\vartheta_{11}^{v} = 2\vartheta_{00}^{x_i}\vartheta_{00}^{y_1}\vartheta_{00}^{u_1}\vartheta_{00}^{v_1}$

$'' \;+\; '' \;-\; '' \;-\; '' \;= 2\vartheta_{01}^{x_1}\vartheta_{01}^{y_1}\vartheta_{01}^{u_1}\vartheta_{01}^{v_1}$

$'' \;-\; '' \;+\; '' \;-\; '' \;= 2\vartheta_{10}^{x_1}\vartheta_{10}^{y_1}\vartheta_{10}^{u_1}\vartheta_{10}^{v_1}$

$'' \;-\; '' \;-\; '' \;+\; '' \;= 2\vartheta_{11}^{z_1}\vartheta_{11}^{y_1}\vartheta_{11}^{u_1}\vartheta_{11}^{v_1}$

(R_6): $\vartheta_{00}^{x}\vartheta_{00}^{y}\vartheta_{01}^{u}\vartheta_{01}^{v}+\vartheta_{01}^{x}\vartheta_{01}^{y}\vartheta_{00}^{u}\vartheta_{00}^{v}+\vartheta_{10}^{x}\vartheta_{10}^{y}\vartheta_{11}^{u}\vartheta_{11}^{v}+\vartheta_{11}^{x}\vartheta_{11}^{y}\vartheta_{10}^{u}\vartheta_{10}^{v} = 2\vartheta_{01}^{z_1}\vartheta_{01}^{y_1}\vartheta_{00}^{u_1}\vartheta_{00}^{v_1}$

$'' \;+\; '' \;-\; '' \;-\; '' \;= 2\vartheta_{00}^{x_1}\vartheta_{00}^{y_1}\vartheta_{01}^{u_1}\vartheta_{01}^{v_1}$

$'' \;-\; '' \;+\; '' \;-\; '' \;= -2\vartheta_{11}^{x_1}\vartheta_{11}^{y_1}\vartheta_{10}^{u_1}\vartheta_{10}^{v_1}$

$'' \;-\; '' \;-\; '' \;+\; '' \;= -2\vartheta_{10}^{x_1}\vartheta_{10}^{y_1}\vartheta_{11}^{u_1}\vartheta_{11}^{v_1}$

(R_{10}): $\vartheta_{00}^{x}\vartheta_{00}^{y}\vartheta_{10}^{u}\vartheta_{10}^{v}+\vartheta_{01}^{x}\vartheta_{01}^{y}\vartheta_{11}^{u}\vartheta_{11}^{v}+\vartheta_{10}^{x}\vartheta_{10}^{y}\vartheta_{00}^{u}\vartheta_{00}^{v}+\vartheta_{11}^{x}\vartheta_{11}^{y}\vartheta_{01}^{u}\vartheta_{01}^{v} = 2\vartheta_{00}^{x_1}\vartheta_{00}^{y_1}\vartheta_{10}^{u_1}\vartheta_{10}^{v_1}$

$'' \;+\; '' \;-\; '' \;-\; '' \;= 2\vartheta_{01}^{x_1}\vartheta_{01}^{y_1}\vartheta_{11}^{u_1}\vartheta_{11}^{v_1}$

$'' \;-\; '' \;+\; '' \;-\; '' \;= 2\vartheta_{10}^{x_1}\vartheta_{10}^{y_1}\vartheta_{00}^{u_1}\vartheta_{00}^{v_1}$

$'' \;-\; '' \;-\; '' \;+\; '' \;= 2\vartheta_{11}^{x_1}\vartheta_{11}^{y_1}\vartheta_{01}^{u_1}\vartheta_{01}^{v_1}$

(R_{14}): $\vartheta_{00}^{x}\vartheta_{00}^{y}\vartheta_{11}^{u}\vartheta_{11}^{v}+\vartheta_{01}^{x}\vartheta_{01}^{y}\vartheta_{10}^{u}\vartheta_{10}^{v}+\vartheta_{10}^{x}\vartheta_{10}^{y}\vartheta_{01}^{u}\vartheta_{01}^{v}+\vartheta_{11}^{x}\vartheta_{11}^{y}\vartheta_{00}^{u}\vartheta_{00}^{v} = 2\vartheta_{01}^{x_1}\vartheta_{01}^{y_1}\vartheta_{10}^{u_1}\vartheta_{10}^{v_1}$

$'' \;+\; '' \;-\; '' \;-\; '' \;= 2\vartheta_{00}^{x_1}\vartheta_{00}^{y_1}\vartheta_{11}^{u_1}\vartheta_{11}^{v_1}$

$'' \;-\; '' \;+\; '' \;-\; '' \;= -2\vartheta_{11}^{x_1}\vartheta_{11}^{y_1}\vartheta_{00}^{u_1}\vartheta_{00}^{v_1}$

$'' \;-\; '' \;-\; '' \;+\; '' \;= -2\vartheta_{10}^{x_1}\vartheta_{10}^{y_1}\vartheta_{01}^{u_1}\vartheta_{01}^{v_1}$

(R_{18}): $\vartheta_{00}^{x}\vartheta_{01}^{y}\vartheta_{10}^{u}\vartheta_{11}^{v}+\vartheta_{01}^{x}\vartheta_{00}^{y}\vartheta_{11}^{u}\vartheta_{10}^{v}+\vartheta_{10}^{x}\vartheta_{11}^{y}\vartheta_{00}^{u}+\vartheta_{01}^{v}+\vartheta_{11}^{x}\vartheta_{10}^{y}\vartheta_{01}^{u}\vartheta_{00}^{v} = 2\vartheta_{11}^{x_1}\vartheta_{10}^{y_1}\vartheta_{01}^{u_1}\vartheta_{00}^{v_1}$

$'' \;+\; '' \;-\; '' \;-\; '' \;= -2\vartheta_{10}^{x_1}\vartheta_{11}^{y_1}\vartheta_{00}^{u_1}\vartheta_{01}^{v_1}$

$'' \;-\; '' \;+\; '' \;-\; '' \;= -2\vartheta_{01}^{x_1}\vartheta_{00}^{y_1}\vartheta_{11}^{u_1}\vartheta_{10}^{v_1}$

(R_{21}): $'' \;-\; '' \;-\; '' \;+\; '' \;= 2\vartheta_{00}^{x_1}\vartheta_{01}^{y_1}\vartheta_{10}^{u_1}\vartheta_{11}^{v_1}$

III. Addition Formulae

(A_1): $\vartheta_{00}(x+u)\,\vartheta_{00}(x-u)\,\vartheta_{00}^2(0) = \vartheta_{00}^2(x)\vartheta_{00}^2(u)+\vartheta_{11}^2(x)\vartheta_{11}^2(u) = \vartheta_{01}^2(x)\vartheta_{01}^2(u)+\vartheta_{10}^2(x)\vartheta_{10}^2(u)$

$\vartheta_{01}(x+u)\,\vartheta_{01}(x-u)\,\vartheta_{01}^2(0) = \vartheta_{00}^2(x)\vartheta_{00}^2(u)-\vartheta_{10}^2(x)\vartheta_{10}^2(u) = \vartheta_{01}^2(x)\vartheta_{01}^2(u)-\vartheta_{11}^2(x)\vartheta_{11}^2(u)$

$\vartheta_{10}(x+u)\,\vartheta_{10}(x-u)\,\vartheta_{10}^2(0) = \vartheta_{00}^2(x)\vartheta_{00}^2(u)-\vartheta_{01}^2(x)\vartheta_{01}^2(u) = \vartheta_{10}^2(x)\vartheta_{10}^2(u)-\vartheta_{11}^2(x)\vartheta_{11}^2(u)$

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

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

$\vartheta_{00}(x+u)\vartheta_{10}(x-u)\vartheta_{00}(0)\vartheta_{01}(0) = \vartheta_{00}(x)\vartheta_{10}(x)\vartheta_{00}(u)\vartheta_{10}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$

$\vartheta_{10}(x+u)\vartheta_{00}(x-u)\vartheta_{00}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{10}(x)\vartheta_{00}(u)\vartheta_{10}(u) - \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{11}(u)$

$\vartheta_{01}(x+u)\vartheta_{10}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{11}(u)+\vartheta_{01}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{10}(u)$

$\vartheta_{10}(x+u)\vartheta_{01}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = -\vartheta_{00}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{11}(u)+\vartheta_{01}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{10}(u)$

(A_{10}): $\vartheta_{11}(x+u)\vartheta_{11}(x-u)\vartheta_{00}^2(0) = \vartheta_{11}^2(x)\vartheta_{00}^2(u) - \vartheta_{00}^2(x)\vartheta_{11}^2(u) = \vartheta_{01}^2(x)\vartheta_{10}^2(u)-\vartheta_{10}^2(x)\vartheta_{01}^2(u)$

$\vartheta_{11}(x+u)\vartheta_{00}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{10}(u) + \vartheta_{10}(x)\vartheta_{01}(x)\vartheta_{00}(u)\vartheta_{11}(u)$

$\vartheta_{00}(x+u)\vartheta_{u}(x-u)\vartheta_{01}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{11}(x)\vartheta_{01}(u)\vartheta_{10}(u) - \vartheta_{10}(x)\vartheta_{01}(x)\vartheta_{00}(u)\vartheta_{11}(u)$

$\vartheta_{11}(x+u)\vartheta_{01}(x-u)\vartheta_{00}(0)\vartheta_{10}(0) = \vartheta_{00}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{11}(u) + \vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{10}(u)$

$\vartheta_{01}(x+u)\vartheta_{11}(x-u)\vartheta_{00}(0)\vartheta_{10}(0) = -\vartheta_{00}(x)\vartheta_{10}(x)\vartheta_{01}(u)\vartheta_{11}(u)+\vartheta_{01}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{10}(u)$

$\vartheta_{11}(x+u)\vartheta_{10}(x-u)\vartheta_{00}(0)\vartheta_{01}(0) = \vartheta_{00}(x)\vartheta_{01}(x)\vartheta_{10}(u)\vartheta_{11}(u)+\vartheta_{10}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{01}(u)$

$\vartheta_{10}(x+u)\vartheta_{11}(x-u)\vartheta_{00}(0)\vartheta_{01}(0) = -\vartheta_{00}(x)\vartheta_{01}(x)\vartheta_{10}(u)\vartheta_{11}(u)+\vartheta_{10}(x)\vartheta_{11}(x)\vartheta_{00}(u)\vartheta_{01}(u)$

IV. Equations for ϑ

(E_1): $\vartheta_{00}^2(x)\,\vartheta_{00}^2(0) = \vartheta_{01}^2(x)\,\vartheta_{01}^2(0) + \vartheta_{10}^2(x)\,\vartheta_{10}^2(0)$

(E_2): $\vartheta_{11}^2(x)\,\vartheta_{00}^2(0) = \vartheta_{01}^2(x)\,\vartheta_{10}^2(0) - \vartheta_{10}^2(x)\,\vartheta_{01}^2(x)$ and

(J_1): $\vartheta_{00}^4(0) = \vartheta_{01}^4(0) + \vartheta_{10}^4(0)$

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 2

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):

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

Rem. Only a pseudo-group law available on $\mathcal{K}$, similar to Montgomery form.

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 $2P = (X, Y, Z, T)$.

Interpretation in terms of isogeny

The first 4 steps of the doubling comes from:

$$\begin{aligned}
4\Theta_1(2\mathbf{z})\Theta_1(0) &= \vartheta_1(\mathbf{z})^2 + \vartheta_2(\mathbf{z})^2 + \vartheta_3(\mathbf{z})^2 + \vartheta_4(\mathbf{z})^2 \\
4\Theta_2(2\mathbf{z})\Theta_2(0) &= \vartheta_1(\mathbf{z})^2 + \vartheta_2(\mathbf{z})^2 - \vartheta_3(\mathbf{z})^2 - \vartheta_4(\mathbf{z})^2 \\
4\Theta_3(2\mathbf{z})\Theta_3(0) &= \vartheta_1(\mathbf{z})^2 - \vartheta_2(\mathbf{z})^2 + \vartheta_3(\mathbf{z})^2 - \vartheta_4(\mathbf{z})^2 \\
4\Theta_4(2\mathbf{z})\Theta_4(0) &= \vartheta_1(\mathbf{z})^2 - \vartheta_2(\mathbf{z})^2 - \vartheta_3(\mathbf{z})^2 + \vartheta_4(\mathbf{z})^2 \,.
\end{aligned}$$

$(\Theta_1(2\mathbf{z}), \Theta_2(2\mathbf{z}), \Theta_3(2\mathbf{z}), \Theta_4(2\mathbf{z}))$ is a point on the Kummer surface

associated to $\mathbb{C}^2/(\mathbb{Z}^2 + 2\Omega\mathbb{Z}^2)$, isogenous to A.

Doubling is the composition of this isogeny and its dual.

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).

Implementation

(joint work with É. Thomé)

The Theta based formulae have been implemented using the $\mathtt{mp}\mathbb{F}_q$ library and submitted to eBATS. Results in cycles:

	`curve25519`	`surf127eps`	`curve2251`	`surf2113`
Opteron K8	310,000	296,000	1,400,000	1,200,000
Core2	386,000	405,000	888,000	687,000
Pentium 4	3,570,000	3,300,000	3,085,000	2,815,000
Pentium M	1,708,000	2,000,000	2,480,000	2,020,000

E.g.: `surf127eps` does 10,000 scalar mult per sec. on a 3 GHz Opteron (waiting for AMD's K10...)

Rem. Optimized only for 64 bit architecture.

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.

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:

- Use the explicit map to Rosenhain form and check the algebra.
- 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, and to derive formulae in characteristic 2.

RM Kummer surfaces

Thanks: É. Schost, D. Kohel

Characteristic polynomial considerations

Let $\mathcal{C}$ be the reduction modulo p of a genus 2 curve with RM by $\sqrt{d}$.

Assume $\mathrm{Jac}(\mathcal{C})$ is ordinary and absolutely simple.

The characteristic polynomial of Frobenius π is of the form

$$\chi(t) = t^4 - s_1 t^3 + s_2 t^2 - p s_1 + p^2,$$

with $|s_1| \leq 4\sqrt{p}$ and $|s_2| \leq 6p$.

$\chi(t)$ is irreducible and defines a CM field K. Its real subfield is isomorphic to $\mathbb{Q}(\sqrt{d})$ and can be defined by the minimal polynomial of $\pi + \bar{\pi}$:

$$P(t) = t^2 - s_1 t + (s_2 - 2p).$$

$$\mathrm{disc}(P) = s_1^2 - 4s_2 + 8p = n^2 d, \quad \text{for some integer } n.$$

RM baby-step giant-step algorithm

The classical genus 2 BSGS algorithm looks for s_1 and s_2.

Search space has size $O(p^{3/2})$, so the complexity is $O(p^{3/4})$.

Main idea: Look for s_1 and n (and deduce s_2).

Bounds on s_1 and s_2 give:

$$n \in \{1, \ldots, \sqrt{48p/d}\}.$$

Since $P(\pi + \bar{\pi}) = 0$, one gets

$$(2(\pi + \bar{\pi}) - s_1)^2 = {s_1}^2 - 4(s_2 - p) = n^2 d.$$

Multiply by π^2 and use $\pi\bar{\pi} = p$:

$$\left(2(\pi^2 + p) - s_1\pi\right)^2 = n^2 d\pi^2.$$

RM baby-step giant-step algorithm (2)

Let D be a random divisor (defined over $\mathbb{F}_p$), since π acts trivially on D, one gets

$$(2(1+p) - s_1)^2 D = n^2 dD.$$

There are $O(\sqrt{p})$ possibilities for the LHS and the RHS.

$\Longrightarrow$ Complexity in $O(\sqrt{p})$ instead of $O(p^{3/4})$.

Rem. $dD, 4dD, 9dD, 16dD, \ldots$ can be computed in linear time.

Low memory version

Assumption: The $\sqrt{d}$ endomorphism is explicit and efficient.

Rewrite equation as

$$(2(1+p) - s_1)\, D = \pm n\sqrt{d}D.$$

This is then exactly the context of the Bidimensional collision search (aka cockroach algorithm) of GaSc04 (inspired by Matsuo-Chao-Tsujii).

Furthermore: if s_1 and n are known modulo m, the whole running time is reduced by a factor of m.

Adapting Schoof's algorithm

If we call the general Schoof's algorithm, one computes s_1 and s_2 modulo ℓ.

But, this gives only n modulo ℓ up to sign.

CRT after k primes ℓ: get 2^k possibilities for n modulo product of ℓ's.

Solution: Test the RM equality to find the sign of n mod ℓ:

$$\left(2(\pi^2 + p) - s_1\pi\right) P = n\sqrt{d}\pi P,$$

for P an ℓ-torsion point.

$\Longrightarrow$ Don't lose the 2^k factor.

Quick estimates for $d = 2$

Schoof's part:

$m = 2^{10} \times 3^4 \times 5^2 \times 7 \times 11 \times 13 \times 17 \times 19 \times 23 \times 29 = 447185196057600 \approx 2^{48}$, sounds feasible in a dozen of core-days.

Cost of collision search is about $32\sqrt{p}/m$. Let us allow 10 core-days for these, that is 10^{12} group operations.

This gives $p \approx 2^{165}$, hence a group of size $\approx 2^{330}$.

$\Longrightarrow$ In two months on 20 cores, one expects to find a suitable Kummer surface, with more than enough security.

A nice family with RM by $\sqrt{2}$

Choose (a, b, c, d) so that doubling in the Kummer surface is the composition of an endomorphism with itself (it has to be $\sqrt{2}$).

Assume that (a, b, c, d) is such that (A, B, C, D) is proportionnal to (a, b, c, d). Then Doubling is twice the following algorithm:

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

1. $X = \quad (x^2 + y^2 + z^2 + t^2)$;
2. $Y = (a/b)(x^2 + y^2 - z^2 - t^2)$;
3. $Z = (a/c)(x^2 - y^2 + z^2 - t^2)$;
4. $T = (a/d)(x^2 - y^2 - z^2 + t^2)$;
5. Return $\sqrt{2}P = (X, Y, Z, T)$.

A nice family with RM by $\sqrt{2}$

Let H be the matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

so that $(A^2, B^2, C^2, D^2) = 4H(a^2, b^2, c^2, d^2)$.

The eigenvalues of H are -2 (simple) and 2 (triple). The eigenspace for 2 is the dimension 3 space defined by

$$a^2 = b^2 + c^2 + d^2.$$

Since we are in a projective world, this gives a 2-parameter family of Kummer surfaces with RM by $\sqrt{2}$.

Conclusion

- With efficient point counting, genus 2 would be very fast, thanks to Theta based formulae;
- RM curves / Kummer surfaces provide small coeffs and efficient point counting;
- Implementation is on the way (the point counting part, first).
- Important speed-up expected – new eBAT to come!