The arithmetic of characteristic 2 Kummer surfaces

Pierrick Gaudry[1] David Lubicz[2]

[1]LORIA, Campus Scientifique, BP 239, 54506 Vandoeuvre-lès-Nancy, France

[2]Universté de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

Outline

Outline

The discrete logarithm problem

Let $(G, +)$ be a cyclic group of order n. Let g be a generator of $(G, +)$.

Definition

For $x \in G$ the unique k, $0 \leq k < n$, such that $x = kg$ is called the discrete logarithm of x in base g and denoted $\log_g x$.

Recovering k from the knowledge of g and x is the *discrete logarithm* problem.

Diffie-Hellman Protocol

Suppose that Alice and Bob want to share a common secret. Alice (resp. Bob) chose a random integer α (resp. β) and publish αg (resp. βg).

- public data: $(G, +)$, g, αg, βg.
- secret data: α, β.

- Alice computes $\alpha\beta g = \alpha(\beta g)$.
- Bob computes $\alpha\beta g = \beta(\alpha g)$.

The common secret is $\alpha\beta g$.
Recovering $\alpha\beta.g$ from the knowledge of $\alpha.g$ and $\beta.g$ is the *Diffie-Hellman* problem.

The discrete logarithm problem

Conditions to apply

In order to be able to use the preceding protocol, we need a family of groups with the following properties

- the groups law can be computed efficiently.
- the discrete logarithm problem is difficult in this family of groups.
- the computation of the carnality of a group in the family is easy.

In the preceding easy means polynomial time complexity and difficult is for exponential time complexity.

Known family of groups

There is not so many known family of groups which have the preceding properties. Essentially,

- the multiplicative groups of finite field $\mathbb{F}_{p^r}$.
- the group of rational points of an elliptic curves over a finite field $\mathbb{F}_{p^r}$.
- the group of rational points of Jacobian of hyperelliptic curves over $\mathbb{F}_{p^r}$.
- other more exotics and less interesting families...

Representation of a point

Let E be an elliptic curve over $\mathbb{F}_q$ ($\mathrm{char}(\mathbb{F}_q) \neq 2, 3$) given by a reduced Weierstrass equation:

$$Y^2 = X^3 + aX + b. \tag{1}$$

A point of E is just a couple $(x, y) \in \mathbb{F}_q^2$ satisfying 1. Actually, it is possible to save memory by representing a point by its affine coordinate x plus a bit b coding the sign of y. It appears that the y coordinate does not play an important role in the difficulty of the discrete logarithm problem in elliptic curves.

Montgomery representation

The idea of the Montgomery representation is just to drop any knowledge related to the y-coordinate. Let E be an elliptic curve expressed in Montgomery form:

$$E_M : By^2 = x^3 + Ax^2 + x. \tag{2}$$

Let P be a point of E_M. Let n be any positive integer, there exists formulas to computes $x(nP)$ iteratively from the knowledge of $x(P)$.
So for the discrete logarithm problem on elliptic curves there is no need to distinguish between a point and its inverse.

Outline

Definition

Let A_k be an abelian surface over a field k. The Kummer surface K associated to A_k is the quotient of A_k by the automorphism -1.
If k is a field of characteristic 0 it can be shown that K has a model in $\mathbb{P}^3$ given by an equation:

$$\Delta(x^4+y^4+z^4+t^4)+2Exyzt-F(x^2t^2+y^2z^2) \\ -G(x^2z^2+y^2t^2)-H(x^2y^2+z^2t^2)=0, \quad (3)$$

where Δ, E, F, G, H are elements of k.

Kummer surface over $\mathbb{C}$

Let $A_{\mathbb{C}}$ be an abelian surface over $\mathbb{C}$. As an analytic variety $A_{\mathbb{C}}$ is isomorphic to $\mathbb{C}^2/\Lambda$ with $\Lambda = \mathbb{Z}^2 + \Omega\mathbb{Z}^2$ where Ω is symmetric and $\mathrm{Im}\Omega > 0$.
It is possible to obtain a projective system of coordinate on $A_{\mathbb{C}}$ or $K_{A_{\mathbb{C}}}$ by the way of the theta functions.

Outline

Theta Functions

The Riemann theta function associated to Ω is the holomorphic function over $\mathbb{C}^2$ given the series

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

More generally for $a, b \in \mathbb{Q}^2$, we define the theta functions with rational characteristics as

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

A first important property of Theta functions with rational characteristics is that they give a homogeneous coordinate system and as such a projective embedding of $A_{\mathbb{C}}$.
For $l \geq 2$, consider the application

$$z \mapsto (\vartheta \begin{bmatrix} 0 \\ b/l \end{bmatrix} (z, \Omega/l))_{b \in (\mathbb{Z}/l\mathbb{Z})^2}.$$

For $l \geq 3$ this gives and embedding of $A_{\mathbb{C}}$ in $\mathbb{P}^{l^2-1}$. For $l = 2$, the image of the preceding application is exactly the Kummer surface associated to $A_{\mathbb{C}}$.

In this coordinate system it is possible to compute the group law of the abelian variety by using the Riemann duplications formulas (for application to Kummer surfaces see for instance [CC86]): first, we have the following duplication formulas due to Riemann [Fay73, p. 3], for $z_1, z_2, \in \mathbb{C}^2$ and $\eta, \eta', \varepsilon \in \frac{1}{2}\mathbb{Z}^2$,

$$\vartheta\left[\begin{smallmatrix}\eta\\ \varepsilon\end{smallmatrix}\right](2z_1, 2\Omega)\vartheta\left[\begin{smallmatrix}\eta'\\ \varepsilon\end{smallmatrix}\right](2z_2, 2\Omega) =$$
$$\frac{1}{4}\sum_{e\in(\mathbb{Z}/2\mathbb{Z})^2}(-1)^{4\,{}^t\eta e}\vartheta\left[\begin{smallmatrix}\eta+\eta'\\ \varepsilon+e\end{smallmatrix}\right](z_1+z_2,\Omega)\vartheta\left[\begin{smallmatrix}\eta+\eta'\\ e\end{smallmatrix}\right](z_1-z_2,\Omega), \tag{4}$$

Riemann Duplication Formula

To ease the notations we let:

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

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

Riemann Duplication Formula

The duplication formulas give:

$$\begin{aligned}
\vartheta_1(\mathbf{z})\vartheta_1(0) &= \Theta_1(\mathbf{z})^2 + \Theta_2(\mathbf{z})^2 + \Theta_3(\mathbf{z})^2 + \Theta_4(\mathbf{z})^2 \\
\vartheta_2(\mathbf{z})\vartheta_2(0) &= \Theta_1(\mathbf{z})^2 + \Theta_2(\mathbf{z})^2 - \Theta_3(\mathbf{z})^2 - \Theta_4(\mathbf{z})^2 \\
\vartheta_3(\mathbf{z})\vartheta_3(0) &= \Theta_1(\mathbf{z})^2 - \Theta_2(\mathbf{z})^2 + \Theta_3(\mathbf{z})^2 - \Theta_4(\mathbf{z})^2 \\
\vartheta_4(\mathbf{z})\vartheta_4(0) &= \Theta_1(\mathbf{z})^2 - \Theta_2(\mathbf{z})^2 - \Theta_3(\mathbf{z})^2 + \Theta_4(\mathbf{z})^2 \ ,
\end{aligned} \tag{5}$$

$$\begin{aligned}
4\Theta_1(2\mathbf{z})\Theta_1(0) &= \vartheta_1(\mathbf{z})^2 + \vartheta_2(\mathbf{z})^2 + \vartheta_3(\mathbf{z})^2 + \vartheta_4(\mathbf{z})^2 \\
4\Theta_2(2\mathbf{z})\Theta_2(0) &= \vartheta_1(\mathbf{z})^2 + \vartheta_2(\mathbf{z})^2 - \vartheta_3(\mathbf{z})^2 - \vartheta_4(\mathbf{z})^2 \\
4\Theta_3(2\mathbf{z})\Theta_3(0) &= \vartheta_1(\mathbf{z})^2 - \vartheta_2(\mathbf{z})^2 + \vartheta_3(\mathbf{z})^2 - \vartheta_4(\mathbf{z})^2 \\
4\Theta_4(2\mathbf{z})\Theta_4(0) &= \vartheta_1(\mathbf{z})^2 - \vartheta_2(\mathbf{z})^2 - \vartheta_3(\mathbf{z})^2 + \vartheta_4(\mathbf{z})^2 \ .
\end{aligned} \tag{6}$$

Pseudo-doubling formulas

Doubling Algorithm: odd characteristic case [Gau07]

`DoubleKummer`(P)

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

Output: The double $2P = (X, Y, Z, T)$ in $\mathcal{K}$.

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 (X, Y, Z, T).

Pseudo-addition formulas

Pseudo-addition Algorithm: odd characteristic case [Gau07] `PseudoAddKummer`(P, Q, R)

Input: Two points $P = (x, y, z, t)$ 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 $P - Q$, with $\bar{x}\bar{y}\bar{z}\bar{t} \neq 0$.

Output: The point (X, Y, Z, T) in $\mathcal{K}$ among $P + Q$ and $P - Q$ which is different from R.

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. $T = (x' - y' - z' + t')/\bar{t}$;

Finite field of odd characteristic

Using the Lefschetz principle, the preceding formulas actually work for any field of odd characteristic. In characteristic 2 they are not anymore valid.

Outline

Algebraic theta functions

Let A be an abelian variety over k. Let $\mathscr{L}$ be a degree d ample line bundle on A_k. There exists an isogeny $\phi_{\mathscr{L}}$ from A_k onto its dual $\hat{A}_k$ defined by $\phi_{\mathscr{L}} : A_k \to \hat{A}_k$, $x \mapsto \tau_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$. As $\mathscr{L}$ is ample, the kernel $K(\mathscr{L})$ of $\phi_{\mathscr{L}}$ is a finite group scheme. The theta group $G(\mathscr{L})$ is by definition the set of pairs (x, ψ) where x is a closed point of $K(\mathscr{L})$ and ψ is an isomorphism of line bundle $\psi : \mathscr{L} \to \tau_x^* \mathscr{L}$ together with the composition law $(x, \psi) \circ (y, \phi) = (x + y, \tau_y^* \psi \circ \phi)$. It is easy to see that $G(\mathscr{L})$ is a group which is a central extension of $K(\mathscr{L})$ by $\mathbb{G}_{m,k}$.

The Heisenberg group

Let $\delta = (d_1, \ldots, d_l)$ be a finite sequence of integers such that $d_i | d_{i+1}$, we consider the finite group scheme $Z_\delta = (\mathbb{Z}/d_1\mathbb{Z})_k \times_k \ldots \times_k (\mathbb{Z}/d_l\mathbb{Z})_k$ with elementary divisors given by δ. For a well chosen δ, the finite group scheme $K(\delta) = Z_\delta \times \hat{Z}_\delta$ where $\hat{Z}_\delta$ is the Cartier dual of Z_δ is isomorphic to $K(\mathscr{L})$ ([Mum70]). The Heisenberg group of type δ is the scheme $\mathcal{H}(\delta) = \mathbb{G}_{m,k} \times Z_\delta \times \hat{Z}_\delta$ together with the group law defined on closed points by $(\alpha, x_1, x_2).(\beta, y_1, y_2) = (\alpha.\beta.y_2(x_1), x_1 + y_1, x_2 + y_2)$.

Theta structures

A theta structure for $(A, \mathscr{L})$ is the data of the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & \mathcal{H}(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \Theta_\delta} & & \downarrow{\scriptstyle \overline{\Theta_\delta}} & & \\ 0 & \longrightarrow & \mathbb{G}_{m,k} & \longrightarrow & G(\mathscr{L}) & \longrightarrow & K(\mathscr{L}) & \longrightarrow & 0 \end{array}$$

The important thing about a theta structure is that it determines a basis a global sections of $\mathscr{L}$ and as such a projective embedding ϕ of A. The point $\phi(0)$ is called the theta null point defined by the theta structure Θ_δ.

Canonical lift

Let k be any finite algebraic extension of $\mathbb{F}_2$ and let $W(k)$ be the ring of Witt vectors with coefficients in k. Let A_k be an ordinary abelian surface over k. Denote by $\mathscr{A}_{A_k}^{loc}$ the local deformation space of A_k which is the set of isomorphism class of abelian schemes $A_{W(k)}$ over $W(k)$ whose special fiber is A_k. There exists a distinguished element in $\mathscr{A}_{A_k}^{loc}$ called the canonical lift $A_{W(k)}^{c}$ of A_k. The canonical lift is uniquely defined up to isomorphism by the property that all endomorphism of A_k lift to a relative endomorphism of $A_{W(k)}^{c}$.

Theta null point of the canonical lift

Suppose that $A_{W(k)}$ is a canonical lift of its special fiber. By a result of Carls [Car07] there exists a canonical theta structure Θ^c_δ of type $\delta = (2,2)$ such the theta null point defined by Θ^c_δ satisfy the following equations:

$$a_u^2 = \omega \sum_{v \in \mathbb{Z}/2\mathbb{Z}} \sigma(a_{v+u})\sigma(a_v), \tag{7}$$

$u \in (\mathbb{Z}/2\mathbb{Z})^2$. As a consequence we have the

Lemma

if $(a_u) \in W(k)^{Z_\delta}$ is the theta null point of an element of $\mathscr{A}^c_{\delta,\mathbb{Z}_2}$ then it reduces modulo 2 to the point with homogeneous coordinates $(1:0:0:0)$.

A correspondence

Let A_k be abelian variety over a field k of characteristic 2. We suppose that A_k comes wich a degree 2 totally symmetric ample line bundle $\mathscr{L}_k$. The following can be shown

Corollary

Let $\delta = (2,2)$. There is a one on one correspondence between the set of isomorphism classes of triples $(A_k, \mathscr{L}_k, \Theta_\delta)$ and the set of isomorphism classes of triples $(A^c_{W(k)}, \mathscr{L}^c_{W(k)}, \Theta^c_\delta)$.

Model of a Kummer surface

Let $W(k)$ be the ring of Witt vectors with coefficient in k. By a preceding result, the model of a Kummer surface K over $W(k)$ has the following form.

$$\Delta(x^4 + y^4 + z^4 + t^4) + 2Exyzt - F(x^2t^2 + y^2z^2) \\ - G(x^2z^2 + y^2t^2) - H(x^2y^2 + z^2t^2) = 0. \quad (8)$$

Because of the preceding lemma, the model has bad reduction modulo 2. After a blowing-up of the origin point of the special fiber, which correspond to the following change of variables:

$$X = 2.x, Y = 2.y, Z = 2.z, T = 2.t. \quad (9)$$

We obtain the equation

$$b'c'd'XYZT + c'^2b'^2(X^2T^2 + Y^2Z^2) + b'^2d'^2(X^2Z^2 + Y^2T^2) + c'^2d'^2(X^2Y^2 + T^2Z^2) = 0 \quad (10)$$

Because of the preceding correspondance this gives the model for an ordinary Kummer surface over k.

Model of a Kummer surface

Proposition

Let $\delta = (2,2)$. There is a bijective correspondence between

- *the set of triples $(A_k, \mathscr{L}_k, \Theta_\delta)$ where k is any finite algebraic extension of $\mathbb{F}_2$, A_k is an ordinary abelian variety over k, $\mathscr{L}_k$ a degree 2 totally symmetric ample line bundle and Θ_δ a theta structure of type δ defined over k' an extension of k*
- *and the set of triples of elements $(b', c', d') \in {k'}^3$*

Let $(b', c', d') \in {k'}^4$, an equation for the Kummer surface $K_{(1:b':c':d')}$ is given by

$$b'c'd'XYZT + c'^2b'^2(X^2T^2 + Y^2Z^2) + b'^2d'^2(X^2Z^2 + Y^2T^2) + c'^2d'^2(X^2Y^2 + T^2Z^2) = 0.$$

Doubling

Doubling Algorithm: `DoubleKummer(`$\overline{P}$`)`
Input: $\overline{P} = (x : y : z : t)$ a $\overline{k}$-point of $K_{(1:b':c':d')}$;
Output: The double $2\overline{P} = (x' : y' : z' : t')$ in $K_{(1:b':c':d')}$.

1. $x' = (x^2 + y^2 + z^2 + t^2)^2$;
2. $y' = \frac{1}{b'}(xy + zt)^2$;
3. $z' = \frac{1}{c'}(xz + yt)^2$;
4. $t' = \frac{1}{d'}(xt + yz)^2$;
5. Return $2\overline{P} = (x', y', z', t')$.

Pseudo-addition formulas

Pseudo-addition Algorithm: `PseudoAddKummer(`$\overline{P}$, $\overline{Q}$, $\overline{R}$`)`

Input: $\overline{P} = (x : y : z : t)$ and $\overline{Q} = (\underline{x} : \underline{y} : \underline{z} : \underline{t})$ two $\overline{k}$-points of $K_{(1:b':c':d')}$ and $\overline{R} = (\bar{x} : \bar{y} : \bar{z} : \bar{t})$ one of the $\pi(P+Q)$ or $\pi(P-Q)$.

Output: The point $(x' : y' : z' : t')$ among $\pi(P+Q)$ or $\pi(P-Q)$ which is different from $\overline{R}$.

1. $x' = (x\underline{x} + y\underline{y} + z\underline{z} + t\underline{t})^2/\bar{x}$;
2. $y' = (x\underline{y} + y\underline{x} + z\underline{t} + t\underline{z})^2/\bar{y}$;
3. $z' = (x\underline{z} + z\underline{x} + y\underline{t} + t\underline{y})^2/\bar{z}$;
4. $t' = (x\underline{t} + t\underline{x} + y\underline{z} + z\underline{y})^2/\bar{t}$;
5. Return $(x', y', z', t') = \pi(P+Q)$ or $\pi(P-Q)$.

Idea of the proof

In the duplication formula, we recognize the classical Borchardt mean twisted by the action of the Frobenius morphism. More precisely, because of the duplication formula, we have

$$\vartheta_2\left[\begin{smallmatrix}0\\ \epsilon\end{smallmatrix}\right](2z,1/2\Omega)\vartheta_2\left[\begin{smallmatrix}0\\ \epsilon\end{smallmatrix}\right](0,1/2\Omega) = \frac{1}{4}\sum_{e\in(\mathbb{Z}/2\mathbb{Z})^g}\vartheta_4\left[\begin{smallmatrix}0\\ \epsilon+e\end{smallmatrix}\right](z,1/4\Omega)\vartheta_4\left[\begin{smallmatrix}0\\ e\end{smallmatrix}\right](z,1/4\Omega). \quad (11)$$

We just need a way to relate $\vartheta_4\left[\begin{smallmatrix}0\\ e\end{smallmatrix}\right](z,1/4\Omega)$ with $\vartheta_4\left[\begin{smallmatrix}0\\ e\end{smallmatrix}\right](z,1/2\Omega)$. Modulo 2 this relation is exactly given by the action of Frobenius morphism.

Some computations

Cost per bit of scalar multiplication	
Elliptic, odd characteristic	3 M + 6 S + 3 D
Elliptic, even characteristic	5 M + 5 S + 1 D
Genus 2, odd characteristic	7 M + 12 S + 9 D
Genus 2, even characteristic	15 M + 9 S + 3 D

Conclusion and Perspectives

On the theoretical side, quartic's equation for a non ordinary Kummer surface is given in [LP04]. But the question of the pseudo-addition formulas on such non ordinary Kummer surfaces is still open. When using Mumford's coordinates and Cantor-based formulas, the group law can be more efficient in the non-ordinary case, so this is worth being investigated.


R. Carls.
Canonical coordinates on the canonical lift.
J. Ramanujan Math. Soc., 22(1):1–14, 2007.


D. V. Chudnovsky and G. V. Chudnovsky.
Sequences of numbers generated by addition in formal groups and new primality and factorization tests.
Adv. in Appl. Math., 7:385–434, 1986.


John D. Fay.
Theta functions on Riemann surfaces.
Springer-Verlag, Berlin, 1973.
Lecture Notes in Mathematics, Vol. 352.


P. Gaudry.
Fast genus 2 arithmetic based on Theta functions.
J. of Mathematical Cryptology, 1:243–265, 2007.


Y. Laszlo and C. Pauly.
The Frobenius map, rank 2 vector bundles and Kummer's quartic surface in characteristic 2 and 3.
Adv. Math., 185(2):246–269, 2004.


D. Mumford.
Abelian varieties.
Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.