Constructive CM and Canonical Lifts
ECC 2007

David R. Kohel
The University of Sydney

Complex Multiplication in Cryptography

In order to use elliptic curves in cryptography we need efficient methods of either constructing or calculating a curve with prime or nearly prime order.
The *random curve* method involves repeatedly choosing curves

$$E : y^2 + (a_1x + a_3)x = x^3 + a_2x^2 + a_4x + a_6$$

at random over a finite field $\mathbb{F}_q$, computing the number of points in $E(\mathbb{F}_q)$, until one has prime order. There exist efficient point counting methods for determining the number of points, namely:

- SEA (Schoof-Elkies-Atkin) method (any $\mathbb{F}_q$)
- Canonical lifting methods for p-adic point counting (small p).

Alternatively, one can apply the complex multiplication method...

Complex Multiplication in Cryptography

In the complex multiplication method, one precomputes the data of a Hilbert class polynomial $H_D(x)$. Any elliptic curve E whose j-invariant satisfies $H_D(j(E)) = 0$ has

$$Z[\frac{s+\sqrt{D}}{2}] \subseteq \mathrm{End}(E).$$

where we take s congruent to D modulo 2. Conversely, for any prime p such that

$$p = \mathrm{N}(x + \frac{s+\sqrt{D}}{2}y) = x^2 + sxy + \frac{(s^2-D)}{4}y^2,$$

the polynomial $H_D(x)$ splits completely into linear factors over $\mathbb{F}_p$. If $D \neq -3, -4$, then for every root j an elliptic curve over $\mathbb{F}_p$ with j-invariant j has number of points in

$$\left\{(x \pm 1)^2 + s(x \pm 1)y + \frac{(s-D)}{2}y^2\right\}.$$

Complex Multiplication in Cryptography

As an example, we have $1171 = x^2 + xy + 9y^2$ for $(x, y) = (17, 9)$, so the Hilbert class polynomial

$$H_{-35}(x) = x^2 + 117964800x - 134217728000$$

splits over $\mathbb{F}_{1171}$, with roots 861 and 879. There thus exist two quadratic twists of the elliptic curve with j-invariant 861 in $\mathbb{F}_{1171}$,

$$y^2 = x^3 + 109x + 57 \text{ and } y^2 = x^3 + 813x + 156,$$

having respective numbers of points

$1129 = (x-1)^2+(x-1)y+9y^2$ and $1215 = (x+1)^2+(x+1)y+9y^2$.

Bröker and Stevenhagen showed that, heuristically, the CM method can be used to construct any prime number of points.

Complex Multiplication in Cryptography

In the generalization from elliptic curves to Jacobians of genus 2 curves, we replace the j-invariant of an elliptic curve with a triple (j_1, j_2, j_3) of Igusa invariants.
The Hilbert class polynomial is replaced by an ideal of invariants among the (j_1, j_2, j_3). In particular this ideal contains each of the minimal polynomials $H_i(x)$ of j_i.
In order to find suitable primes (of ordinary reduction) one replaces the norm equation $p = \mathrm{N}\big(x + (s + \sqrt{D})y/2\big)$ with a relative norm equation

$$p = \pi\bar{\pi} = \mathrm{N}_F^K(\pi) = \mathrm{N}_F^K\big(x + \alpha_1 y + \alpha_2 z + \alpha_3 t\big)$$

from a quartic CM field K to its real quadratic subfield F. The number of points on $J(\mathbb{F}_p)$ is then given by $\mathrm{N}_F^K(\pi - 1)$.

Complex Multiplication in Genus 1

The Main Theorem of Complex Multiplication gives the relation between ideal classes and abelian varieties. For example, in genus 1, the j-variant of an elliptic curve with CM by a maximal order $\mathcal{O}_K$ in K, generates the Hilbert class field $H = K(j)/K$.

More precisely, an embedding $K \to \mathbb{C}$ gives the relation between ideals of $\mathcal{O}_K$ and isomorphism classes of elliptic curves over $\mathbb{C}$:

$$\mathfrak{a} \longmapsto E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}^{-1}.$$

The Artin isomorphism $\sigma : \mathrm{Gal}(H/K) \cong \mathrm{Cl}(\mathcal{O}_K)$, determines an action on $\{E_{\mathfrak{a}}\}$ compatible induced isogenies

$$E_{\mathfrak{a}} \to E_{\mathfrak{a}\mathfrak{p}} \cong_{\mathbb{C}} E_{\mathfrak{a}}^{\sigma(\mathfrak{p})}$$

N.B. The Galois action on $\{E_{\mathfrak{a}}\}$ is determined on any model $E_{\mathfrak{a}}/H$.

Complex Multiplication in Genus 1

A CM construction is an algorithm for the construction of invariants of an abelian variety with complex multiplication.

In genus 1, the traditional method is to evaluate the j-function at points τ in the upper half Poincaré plane, which correspond to lattices with complex multiplication.

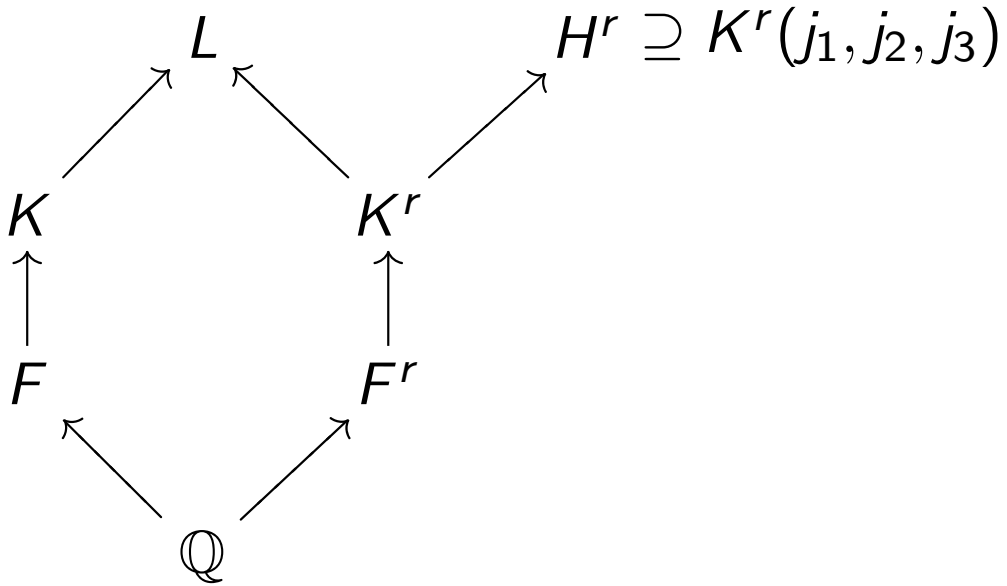
The objective of this algorithm is to determine the minimal polynomial $H_D(x)$ for $j(\tau)$ over $\mathbb{Q}$, called the Hilbert class polynomial. This polynomial defines a zero dimensional subscheme of $\mathbb{A}^1 \subset \mathbb{P}^1 \cong X(1)$.

For example, for $D = -23$ we find the following Hilbert class polynomial:

$$x^3 + 3491750x^2 - 5151296875x + 12771880859375.$$

Complex Multiplication in Genus 2

In genus 2 (i.e. Jacobian surfaces), a generic CM field K is non-Galois over $\mathbb{Q}$, and its normal closure is a degree 2 extension L/K with Galois group D_4 over $\mathbb{Q}$. There exist a triple of invariants (j_1, j_2, j_3) of any maximal order $\mathcal{O}_K$ (with associated CM type Φ), contained in the Hilbert class field H^r of the reflex field K^r:



The field K^r is constructed in terms of the CM type Φ.

Complex Multiplication in Genus 2

The abelian surfaces (with fixed polarization type) correspond to pairs $(\mathfrak{a}, \alpha)$ such that $\mathfrak{a}\bar{\mathfrak{a}} = (\alpha)$ for $(\alpha) \equiv (1)$ in $\mathrm{Cl}^+(\mathcal{O}_F)$. The set of pairs $(\mathfrak{a}, \alpha)$ forms a groupe $\mathfrak{C}(\mathcal{O}_K)$ with identity $(\mathcal{O}_K, 1)$.

The class group $\mathrm{Cl}(\mathcal{O}_{K^r})$ acts on the group $\mathfrak{C}(\mathcal{O}_K)$ by means of the homomorphism:

$$\begin{aligned} \mathrm{Gal}(H^r/K^r) \cong \mathrm{Cl}(\mathcal{O}_{K^r}) &\longrightarrow \mathfrak{C}(\mathcal{O}_K) \\ \mathfrak{c} &\longmapsto \left(\mathrm{N}_\Phi(\mathfrak{c}), \mathrm{N}_{\mathbb{Q}}^{K^r}(\mathfrak{c})\right) \end{aligned}$$

where $\mathrm{N}_\Phi(\mathfrak{c}) = \mathrm{N}_K^L(\mathfrak{c}\mathcal{O}_L)$. Composing with multiplication in $\mathfrak{C}(\mathcal{O}_K)$, we obtain the Galois action:

$$\mathrm{Gal}(H^r/K^r) \times \mathfrak{C}(\mathcal{O}_K) \to \mathfrak{C}(\mathcal{O}_K).$$

N.B. The above homomorphism can fail to be injective (hence $\{j_1, j_2, j_3\}$ does not generate H^r) or fail to be surjective (in which case there are multiple Galois orbits of invariants).

Complex Multiplication in Genus 2

An analytic construction for dimension 2 uses theta functions on Siegel to determine points (j_1, j_2, j_3) in $\mathcal{M}_2(\mathbb{C})$, the moduli space of curves of genus 2 (which we identify with its image in the moduli space $\mathcal{A}_2(\mathbb{C})$ of principally polarized abelian surfaces).

The result of a CM construction is an ideal in $\mathbb{Q}[x_1, x_2, x_3]$ defining the zero dimensional scheme over $\mathbb{Q}$ of the Galois orbit of the point (j_1, j_2, j_3).

Examples. The curves $y^2 = x^5 + 1$ and $y^2 = x^6 + 1$ have Igusa invariants

$$(0, 0, 0) \text{ and } (6400000/3, 440000/9, -32000/81).$$

Thus their respective defining ideals are

$$(x_1, x_2, x_3) \text{ and } (3x_1 - 6400000, 9x_2 - 440000, 81x_3 + 32000).$$

Canonical Lifts

Suppose that A/k is an ordinary, simple abelian variety over a finite field of characteristic p, and let R be its Witt ring, i.e. an extension of $\mathbb{Z}_p$ such that $[R : \mathbb{Z}_p] = [k : \mathbb{F}_p]$ and $\pi : R \to k$.

A canonical lift is an abelian variety $\tilde{A}$ over R such that

$$\tilde{A} \times_R k = A \text{ and } \mathrm{End}(\tilde{A}) = \mathrm{End}(A).$$

We construct the canonical lifted invariants, given x in $\mathcal{A}_g(k)$, by solving for $\tilde{x}$ in $\mathcal{A}_g(R)$ such that $(\tilde{x}, \tilde{x}^\sigma)$ lies on a subscheme of $\mathcal{A}_g \times \mathcal{A}_g$ defined by isogenies with kernel of type $(\mathbb{Z}/p\mathbb{Z})^g$.

Canonical Lifts

An algorithm pour the construction of the p-adic canonical lift of an elliptic curve was introduced by Satoh in 1999, to determine the number of points on a given $E/\mathbb{F}_q$ (in small characteristic p). The algorithm constructs the canonically lifted $\tilde{j}$ of an given ordinary j-invariant j in $\mathbb{F}_q$, as the unique point $(\tilde{j}, \tilde{j}^\sigma)$ on

$$X_0(p) \to X(1) \times X(1).$$

An algorithm of Mestre, in 2000, introduced the use of theta functions and the AGM. This algorithm determines canonically lifted invariants $(\tilde{x}, \tilde{x}^\sigma)$ on $X_0(8)$ (in residue characteristic 2).

Couveignes and Henocq in 2002 introduced the idea of p-adic lifting as a CM construction, to determine a high precision approximation to the Hilbert class polynomial on $X(1)$.

Canonical Lifts

In general, a p-adic algorithm for constructive CM must

- construct the lifted invariant (to some finite precision), and
- recognize an algebraic number from its approximation.

The first step replaces the p-adic numbers with complex numbers in analogous analytic constructions. Rather than a period lattice, the input is a suitable curve which we lift p-adically.

The second step uses an LLL reconstruction, from one or multiple points on the CM subscheme.

Constructive CM algorithms for genus 2

Currently several constructive CM algorithms for genus 2 CM moduli exist:

- 2-adic lifting of $(2,2)$-isogenies (Gaudry, Houtmann, K., Ritzenthaler, Weng).
- 3-adic lifting of $(3,3)$-isogenies (Carls, K., Lubicz),
- p-adic lifting of (ℓ,ℓ)-isogenies (K., adapting above to $\ell \neq p$).

The first is a variant of Mestre's 2-adic AGM lifting algorithm, using Richelot isogenies between Jacobians of curves in Rosenhain form:

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3).$$

The second, 3-adic, algorithm makes use of correspondence equations of algebraic theta functions.

The last algorithm applies the correspondence equations of the 2-adic and 3-adic algorithms in characteristic $p \neq \ell = 2, 3$.

Constructive CM algorithms for genus 2

The main advantages of the p-adic canonical lifting techniques are the numerical stability, since only arithmetic operations in R/p^nR are required.

The main challenge to the first phase of the p-adic algorithm is finding a suitable input curve, whose Jacobian has endomorphism ring which is a maximal order of low class number.

The height of the moduli points (hence the resulting output size) presents the major complexity limitation of the LLL phase (and the runtime of algorithm as a whole).

The LLL phase can be largely eliminated by using explicit isogenies and canonical lifting all representative moduli.

A canonical 3-adic lift of $(2,2)$-isogenies

Let $\mathbb{F}_{27} = \mathbb{F}_3[w]/(w^3 - w + 1)$, and let C be the curve

$$y^2 = x(x-1)(x-t_1)(x-t_2)(x-t_3),$$

where

$$(t_1, t_2, t_3) = (w^{14}, w^8, 2).$$

The point

$$(u_1, u_2, u_3) = (w^{16}, w^{24}, 2)$$

is the image (t_1, t_2, t_3) under Frobenius and defines a second curve

$$y^2 = x(x-1)(x-u_1)(x-u_2)(x-u_3),$$

connected to the first by a Richelot correspondence. Therefore the canonical lift of the invariants (t_1, t_2, t_3) give rise to a triple of absolute Igusa invariants (j_1, j_2, j_4), where $j_3 = j_2^2/j_1 + 4j_4$, satisfy:

A canonical 3-adic lift of $(2,2)$-isogenies

$$
\begin{aligned}
&10460353203j_1^6 - \\
&\quad 258057574371539210j_1^5 + \\
&\quad 247624672413238292031278 31j_1^4 - \\
&\quad 113152741542913622518874207616931j_1^3 - \\
&\quad 116142832015721679346443498802911666288j_1^2 - \\
&\quad 70782776480135088514937849133086022245140736j_1 - \\
&\quad 623173047080770359664027287795513118768324 6723072 = 0,
\end{aligned}
$$

$$
\begin{aligned}
&282429536481j_2^6 - \\
&\quad 101720638067873841 0j_2^5 + \\
&\quad 248812304560167623924547j_2^4 - \\
&\quad 935699011133114796109020340 73j_2^3 + \\
&\quad 216371077897466304252792736 3883074j_2^2 - \\
&\quad 112721460352929137586975806252985141388j_2 + \\
&\quad 222653772934163865823867589887247923630 81576 = 0,
\end{aligned}
$$

$$
\begin{aligned}
&843330077059682304j_4^6 - \\
&\quad 699281981805777701460 48j_4^5 - \\
&\quad 140267478713381926713599184j_4^4 + \\
&\quad 333222744806636241992331514 6997j_4^3 + \\
&\quad 194317558062962659254203520 17482148j_4^2 - \\
&\quad 324807531891753635438351846571893828 77j_4 + \\
&\quad 342957608759876088038084082162475778 19433 = 0,
\end{aligned}
$$

A canonical 3-adic lift of $(2,2)$-isogenies

Set $i_0 = i_2 i_3 / i_1$ where (i_1, i_2, i_3) are the absolute Igusa-Clebsch invariants. Then i_0 satisfies minimal polynomial

$$\begin{aligned} H(x) = {} & 2097152x^6 - 1353997189120x^5 - \\ & 1283649962073824 00x^4 - \\ & 8081508607729111 9625x^3 - \\ & 4185901441635615224 4632500x^2 + \\ & 3966639002290339376 15219250000x - \\ & 3057913457073576168488 111879000000 \end{aligned}$$

and the invariants i_2 and i_3 can be expressed as:

$$i_2 = H'(i_0)G_2(i_0)/27 \qquad i_3 = H'(i_0)G_3(i_0)/81$$

where $G_2(x)$ and $G_3(x)$ are the polynomials:

A canonical 3-adic lift of $(2,2)$-isogenies

$$G_2(x) = 4537252954767360x^5 + 29621247193480192000x^4 - 873069221996753826159200x^3 + 27424231130302780723899666000x^2 - 29868005451839820857404397256000000x + 8686743648741963364750789662856000000$$

$$G_3(x) = 3199579983446016x^5 + 1297541958927369625600x^4 - 1063348008541100992077320x^3 + 26664104695713090856402205400x^2 - 2396506629655727490148702447440000x + 57463721208140609754027557855128000000$$

A Cryptographic Example

Example. Let C be the curve $y^2 + h(x)y = f(x)$ over

$$\mathbb{F}_8 = \mathbb{F}_2[t]/(t^3 + t + 1),$$

with $h(x) = x(x+1)$ and $f(x) = x(x+1)(x^3 + x^2 + t^2x + t^3)$. The curve is ordinary and has complex multiplication by the maximal order of $K = \mathbb{Q}(i\sqrt{23 + 4\sqrt{5}})$. The maximal order has class number is 3, and there exist 6 isomorphism classes of principally polarized abelian varieties.

We construct the ideal of relations in Igusa invariants (j_1, j_2, j_3) from the canonical lift of the Jacobian of C. For example, the invariant j_1 satisfies a minimal polynomial:

$$\begin{aligned} H_1(x) = {} & 2^{18}5^{36}7^{24}\,x^6 \\ & - 1118773039927368977400974047014016967290290543651580810546875000\,x^5 \\ & + 501512527690591679504420832767471421512684501403834547644662988263671875000\,x^4 \\ & - 101124092427873917866762846337305750476145431355720256674682214327042638578082629 23\,x^3 \\ & + 11828700025058866756454074473940615439813597844779277192853554124079738699209182821352 1875\,x^2 \\ & - 2^1 3^{50} 5^{10} 11^1 13^1 53^1 701^1 16319^1 69938793494948953569198870004032131926868578084899317\,x \\ & + 3^{60}5^{15}23^5 409^5 179364113^5 \end{aligned}$$

A Cryptographic Example

Choosing the 120-bit prime

$$p = 954090659715830612807582649452910809,$$

and solving a norm equation in the endomorphism ring $\mathcal{O}_K$, we determine that the Jacobian of some curve over $\mathbb{F}_p$ with CM by $\mathcal{O}_K$ will have prime order

$$\begin{aligned}&9102889869569888857531185582844810291\\ &1141112827604802758431052540888444 9.\end{aligned}$$

A Cryptographic Example

Solving for a solution to the system of equations over $\mathbb{F}_p$, and applying Mestre's algorithm for reconstructing a curve from its invariants, we find

$$\begin{aligned} C : y^2 = x^6 &+ 827864728926129278937584622188769650\, x^4 \\ &+ 102877610579816483342116736180407060\, x^3 \\ &+ 335099510136640078379392471445640199\, x^2 \\ &+ 351831044709132324687022261714141411\, x \\ &+ 27453533043622555752730849345055308 5. \end{aligned}$$

A test of a random point on the Jacobian verifies the group order.

Cryptographic Database

Since the output of the CM construction only needs to be constructed as a one-time calculation, a comprehensive database for CM invariants in genera 1 and 2 is being developed:

`http://echidna.maths.usyd.edu.au/~kohel/dbs/`

For genus 2 this provides an interface for invariants of *quartic CM fields*, and *Igusa CM moduli*, and *genus 2 curves* over finite fields.

This combines output of both p-adic algorithms and complex analytic ones (using Paul van Wamelen in Magma and recently developed algorithms of Thomas Houtmann).

The END