Arithmetic on Elliptic Curves, Abelian varieties and Kummer varieties

2015/03/26 — EMA, Franceville, Gabon

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest
Institut de Mathématiques de Bordeaux
Équipe MACISA, Laboratoire International de Recherche en Informatique et Mathématiques Appliquées

Discrete logarithm

Definition (DLP)

Let $G = \langle g \rangle$ be a cyclic group of prime order. Let $x \in \mathbb{N}$ and $h = g^x$. The discrete logarithm $\log_g(h)$ is x.

- Exponentiation: $O(\log p)$. DLP: $\widetilde{O}(\sqrt{p})$ (in a generic group). So we can use the DLP for public key cryptography.

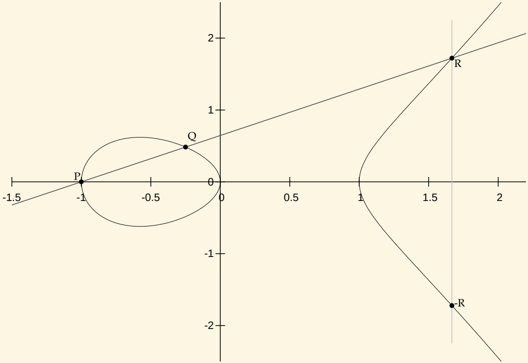
$\Rightarrow$ We want to find secure groups with efficient addition law and compact representation.

Elliptic curves

Definition (char $k \neq 2,3$)

An elliptic curve is a plane curve with equation

$$y^2 = x^3 + ax + b \qquad 4a^3 + 27b^2 \neq 0.$$



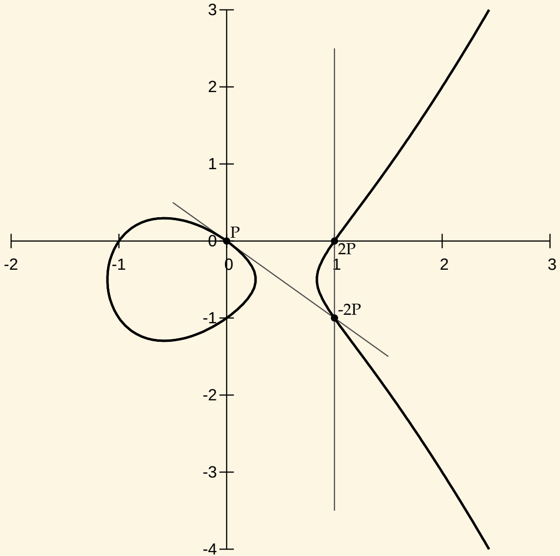
Exponentiation:

$$(\ell, P) \mapsto \ell P$$

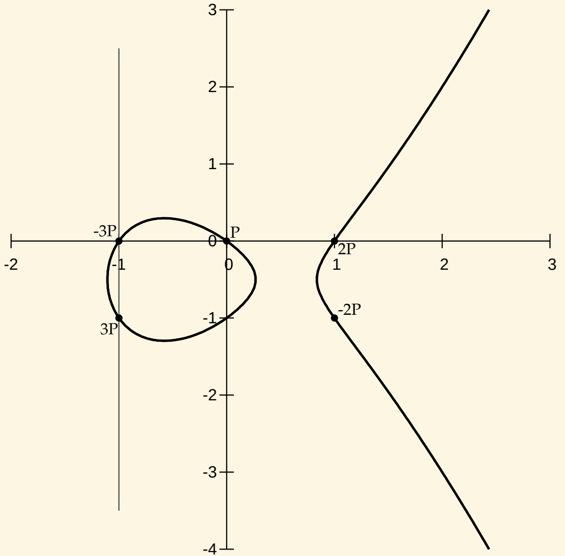
Discrete logarithm:

$$(P, \ell P) \mapsto \ell$$

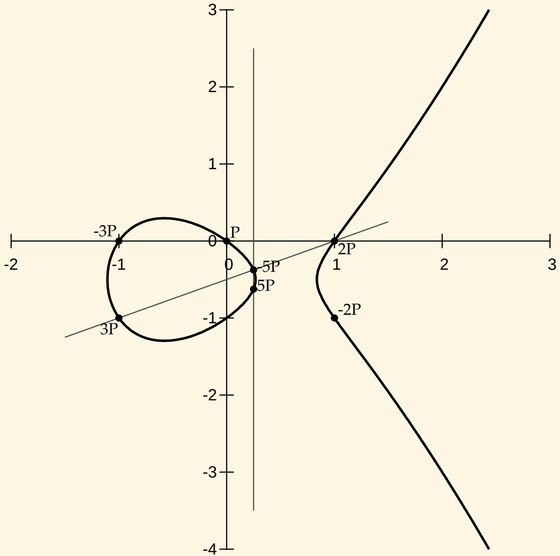
Scalar multiplication on an elliptic curve



Scalar multiplication on an elliptic curve



Scalar multiplication on an elliptic curve



ECC (Elliptic curve cryptography)

Example (NIST-p-256)

- E elliptic curve $y^2 = x^3 - 3x + 41058363725152142129326129780047268409114441015993725554835256314039467401291$ over $\mathbb{F}_{115792089210356248762697446949407573530086143415290314195533631308867097853951}$
- Public key:
$$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286,\\ 36134250956749795798585127919587881956611106672985015071877198253568414405109),$$
$$Q = (76028141830806192577282777898750452406210805147329580134802140726480409897389,\\ 85583728422624684878257214555223946135008937421540868848199576276874939903729)$$
- Private key: ℓ such that $Q = \ell P$.

- Used by the NSA;
- Used in Europeans biometric passports.

Addition law on the Weierstrass model

$E : y^2 = x^3 + ax + b$ (short Weierstrass form).

- Distinct points P and Q:

$$P + Q = -R = (x_R, -y_R)$$
$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$
$$x_R = \lambda^2 - x_P - x_Q$$
$$y_R = y_P + \lambda(x_R - x_P)$$

(If $x_P = x_Q$ then $P = -Q$ and $P + Q = 0_E$).

- If $P = Q$, then λ comes from the tangent at P:

$$\lambda = \frac{3x_P^2 + b}{2y_P}$$
$$x_R = \lambda^2 - 2x_P$$
$$y_R = y_P + \lambda(x_R - x_P)$$

$\Rightarrow$ Avoid divisions by working with projective coordinates $(X : Y : Z)$:

$$E : Y^2 Z = X^3 + aXZ^2 + bZ^3.$$

Scalar multiplication

- The scalar multiplication $P \mapsto n.P$ is computed via the standard double and add algorithm;
- On average $\log n$ doubling and $1/2 \log n$ additions;
- Standard tricks to speed-up include NAF form, windowing ...
- The multiscalar multiplication $(P,Q) \mapsto n.P + m.Q$ can also be computed via doubling and the addition of P, Q or $P+Q$ according to the bits of n and m;
- On average $\log N$ doubling and $3/4 \log N$ additions where $N = \max(n,m)$;
- GLV idea: if there exists an efficiently computable endomorphism α such that $\alpha(P) = u.P$ where $u \approx \sqrt{n}$, then replace the scalar multiplication $n.P$ by the multiscalar multiplication $n_1 P + n_2 \alpha(P)$;
- One can expect n_1 and n_2 to be half the size of $n \Rightarrow$ from $\log n$ doubling and $1/2 \log n$ additions to $1/2 \log n$ doubling and $3/8 \log n$ additions.

Edwards curves

$E : x^2 + y^2 = 1 + d x^2 y^2$, $d \neq 0, -1$.

- Addition of $P = (x_1, y_1)$ and $Q = (x_2, y_2)$:

$$P + Q = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

- When $d = 0$ we get a circle (a curve of genus 0) and we find back the addition law on the circle coming from the sine and cosine laws;
- Neutral element: $(0, 1)$; $-(x, y) = (x, y)$; $T = (1, 0)$ has order 4, $2T = (0, 1)$.
- If d is not a square in K, then there are no exceptional points: the denominators are always nonzero ⇒ complete addition laws;

⇒ Very useful to prevent some Side Channel Attacks.

Twisted Edwards curves

- $E : a x^2 + y^2 = 1 + d x^2 y^2$;
- Extensively studied by Bernstein and Lange;
- Addition of $P = (x_1, y_1)$ and $Q = (x_2, y_2)$:

$$P + Q = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

- Neutral element: $(0, 1)$; $-(x, y) = (x, y)$; $T = (0, -1)$ has order 2;
- Complete addition if a is a square and d not a square.

Montgomery

- $E : By^2 = x^3 + Ax^2 + x$;
- Birationally equivalent to twisted Edwards curves;
- The map $E \to \mathbb{A}^1, (x, y) \mapsto (x)$ maps E to the Kummer line $K_E = E/\pm 1$;
- We represent a point $\pm P \in K_E$ by the projective coordinates $(X : Z)$ where $x = X/Z$;
- Differential addition: Given $\pm P_1 = (X_1 : Z_1)$, $\pm P_2 = (X_2 : Z_2)$ and $\pm(P_1 - P_2) = (X_3 : Z_3)$; then one can compute $\pm(P_1 + P_2) = (X_4 : Z_4)$ by

$$X_4 = Z_3\left((X_1 - Z_1)(X_2 + Z_2) + (X_1 + Z_1)(X_2 - Z_2)\right)^2$$
$$Z_4 = X_3\left((X_1 - Z_1)(X_2 + Z_2) - (X_1 + Z_1)(X_2 - Z_2)\right)^2$$

Montgomery's scalar multiplication

- The scalar multiplication $\pm P \mapsto \pm n.P$ can be computed through differential additions if we can construct a differential chain;
- If $\pm[n]P = (X_n - Z_n)$, then

$$X_{m+n} = Z_{m-n}\left((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)\right)^2$$
$$Z_{m+n} = X_{m-n}\left((X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)\right)^2$$

- Montgomery's ladder use the chain nP, $(n+1)P$;
- From $nP, (n+1)P$ the next iteration computes $2nP$, $(2n+1)P$ or $(2n+1)P$, $(2n+2)P$ via one doubling and one differential addition.

Jacobian of curves

C a smooth irreducible projective curve of genus g.

- Divisor: formal sum $D = \sum n_i P_i$, $\quad P_i \in C(\overline{k})$.
  $\deg D = \sum n_i$.
- Principal divisor: $\sum_{P \in C(\overline{k})} v_P(f).P$; $\quad f \in \overline{k}(C)$.
- Jacobian of C = Divisors of degree 0 modulo principal divisors
  \+ Galois action
  = Abelian variety of dimension g.
- Divisor class of a divisor $D \in \mathrm{Jac}(C)$ is generically represented by a sum of g points.

Higher dimension

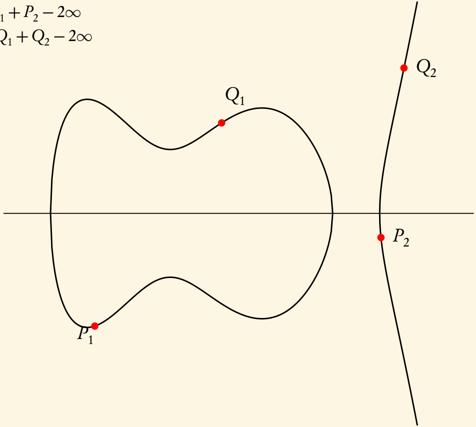
Dimension 2:

Addition law on the Jacobian of an hyperelliptic curve of genus 2:

$$y^2 = f(x),\ \deg f = 5.$$

$D = P_1 + P_2 - 2\infty$

$D' = Q_1 + Q_2 - 2\infty$

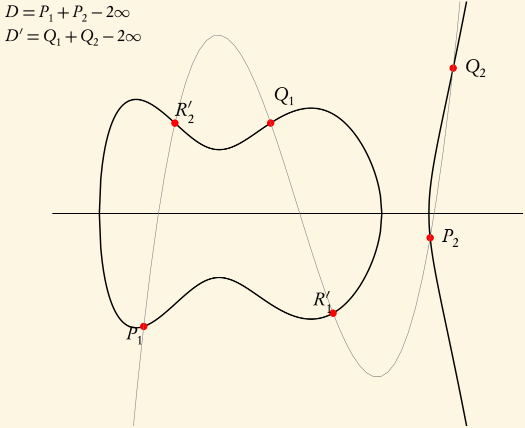


Higher dimension

Dimension 2:

Addition law on the Jacobian of an hyperelliptic curve of genus 2:

$$y^2 = f(x), \deg f = 5.$$

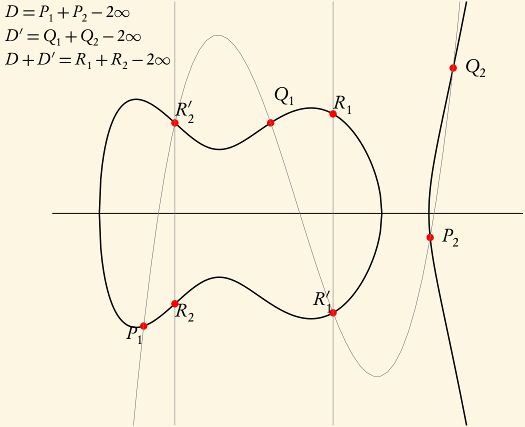


Higher dimension

Dimension 2:

Addition law on the Jacobian of an hyperelliptic curve of genus 2:

$$y^2 = f(x),\ \deg f = 5.$$



Hyperelliptic curves

- $H : y^2 = f(x)$, $\deg f = 2g+1$: hyperelliptic curve of genus g with a rational point at infinity;
- Every divisor D can be represented by a reduced divisor

$$\sum_{i=1}^{r} (P_i) - r(\infty)$$

  where $r \leqslant g$ and $P_i \neq -P_j$ for $i \neq j$;
- The divisor D is represented by its Mumford coordinates (u, v) where if $P_i = (x_i, y_i)$:

$$u(x) = \prod (x - x_i)$$
$$v(x_i) = y_i$$
$$\deg v < \deg u \leqslant g$$
$$u(x) \mid v(x)^2 - f(x);$$

  The last condition encodes that $y - v(x)$ has multiplicity $m_i = \mathrm{v}_{P_i}(D)$ at P_i.

Cantor's algorithm

Algorithm

Input $D_1 = (u_1, v_1)$, $D_2 = (u_2, v_2)$;

Output $D = (u, v)$ *such that* $D \sim D_1 + D_2$;

1. ***Semireduce****: Compute the extended gcd of* u_1, u_2, $v_1 + v_2$

$$d = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2)$$
$$u = \frac{u_1 u_2}{d^2}$$
$$v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \textit{ modulo } u$$

2. ***Reduce****:*

$$u = \frac{f - v^2}{u}$$
$$v = -v \textit{ modulo } u$$

until $\deg u \leqslant g$.

Abelian varieties

Definition

An Abelian variety is a complete connected group variety over a base field k.

- Abelian variety = points on a projective space (locus of homogeneous polynomials) + an abelian group law given by rational functions.

Example

- Elliptic curves= Abelian varieties of dimension 1;
- If C is a (smooth) curve of genus g, its Jacobian is an abelian variety of dimension g;
- In dimension $g = 2$, every (absolutely simple principally polarised) abelian variety is the Jacobian of an hyperelliptic curve of genus 2;
- In dimension $g \geqslant 4$, not every abelian variety is a Jacobian.

Abelian surfaces

- For the same level of security, abelian surfaces need fields half the size as for elliptic curves (good for embedded devices);
- The moduli space is of dimension 3 compared to $1 \Rightarrow$ more possibilities to find efficient parameters;
- Potential speed record (the record holder often change between elliptic curves and abelian surfaces);
- But lot of algorithms still lacking compared to elliptic curves!

Complex abelian varieties

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, where $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space.
- The theta functions with characteristic are analytic (quasi periodic) functions on $\mathbb{C}^g$.

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega) = \sum_{n\in\mathbb{Z}^g} e^{\pi i\, {}^t(n+a)\Omega(n+a) + 2\pi i\, {}^t(n+a)(z+b)} \qquad a,b \in \mathbb{Q}^g$$

Quasi-periodicity:

$$\vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + m_1\Omega + m_2, \Omega) = e^{2\pi i({}^t a\cdot m_2 - {}^t b\cdot m_1) - \pi i\, {}^t m_1 \Omega m_1 - 2\pi i\, {}^t m_1\cdot z}\, \vartheta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\Omega).$$

- Projective coordinates: theta functions of level n

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}^{n^g-1}_{\mathbb{C}} \\ z & \longmapsto & (\vartheta_i(z))_{i\in Z(\overline{n})} \end{array}$$

where $Z(\overline{n}) = \mathbb{Z}^g/n\mathbb{Z}^g$ and $\vartheta_i = \vartheta\left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix}\right](., \frac{\Omega}{n})$.

Riemann relations ($k=\mathbb{C}$)

$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big)=$$

$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

where $\chi\in\hat{Z}(\overline{2}), i,j,k,l\in Z(\overline{n})$

$$(i',j',k',l')=A(i,j,k,l)$$

$$A=\frac{1}{2}\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}$$

Example: differential addition in dimension 1 and in level 2

Algorithm

Input $z_P = (x_0, x_1)$, $z_Q = (y_0, y_1)$ and $z_{P-Q} = (z_0, z_1)$ with $z_0 z_1 \neq 0$;
$z_0 = (a, b)$ and $A = 2(a^2 + b^2)$, $B = 2(a^2 - b^2)$.

Output $z_{P+Q} = (t_0, t_1)$.

1. $t'_0 = (x_0^2 + x_1^2)(y_0^2 + y_2^2)/A$
2. $t'_1 = (x_0^2 - x_1^2)(y_0^2 - y_1^2)/B$
3. $t_0 = (t'_0 + t'_1)/z_0$
4. $t_1 = (t'_0 - t'_1)/z_1$

Return (t_0, t_1)

Projective normality

- To use Riemann relations, one needs non zero theta null points;
- If the level n is even and $n > 2$ then the embedding given by the theta functions of level n is always projectively normal (Mumford-Kempf);
- Projective normality is linked to the non annulation of some theta null points;
- It is thus always possible to compute the addition law on the abelian variety from Riemann relations.

Kummer varieties

- If the level $n=2$, then the theta coordinates give an embedding of the Kummer variety $\mathscr{K}=A/\pm 1$;
- No addition law on the Kummer variety;
- But still possible to define differential additions: from $\pm P$, $\pm Q$ and $\pm(P-Q)$ then $\pm(P+Q)$ is well defined;
- How to compute it?
- In Riemann relations, the theta constants appearing to the formulas correspond to the classical theta functions of level four $\vartheta\begin{bmatrix}\frac{a}{2}\\ \frac{b}{2}\end{bmatrix}(2x,\Omega)$. They are even (resp. odd) when $a\cdot b=0 \pmod 2$ (resp $a\cdot b=1 \pmod 2$).

Theorem (Mumford–Koizumi)

The even theta null points $\{\vartheta\begin{bmatrix}\frac{a}{2}\\ \frac{b}{2}\end{bmatrix}(0,\Omega)\,|\,(-1)^{{}^t ab}=1\}$ are non null if and only if the embedding given by the theta functions of level 2 is projectively normal.

Corollary ([Lubicz–R.])

- *In this case, from the theta coordinates of P and Q we can recover all elements of the form $\vartheta_i(P+Q)\vartheta_j(P-Q)+\vartheta_j(P+Q)\vartheta_i(P-Q)$;*

$\Rightarrow$ *Differential additions, Scalar multiplication.*

Cost of the arithmetic with low level theta functions (char $k \neq 2$)

	Montgomery	Level 2	Jacobians coordinates
Doubling	$5M+4S+1m_0$	$3M+6S+3m_0$	$3M+5S$
Mixed Addition			$7M+6S+1m_0$

Table: Multiplication cost in dimension 1 (one step).

	Mumford	Level 2	Level 4
Doubling	$34M+7S$	$7M+12S+9m_0$	$49M+36S+27m_0$
Mixed Addition	$37M+6S$		

Table: Multiplication cost in dimension 2 (one step).

Arithmetic on Kummer and abelian varieties

We assume for simplicity from now on that $g = 2$.

- An abelian surface A can be embedded into projective space via theta functions of level 4 in $\mathbb{P}^{15}$ $\Rightarrow$ expensive arithmetic;
- If we use level 2, we get an embedding of the Kummer surface K_A into $\mathbb{P}^3$ $\Rightarrow$ very efficient arithmetic, but no general addition law;
- Mumford coordinates (u, v) yields an embedding of the non degenerate divisors into $\mathbb{A}^4$, somewhat efficient arithmetic;
- The image of a divisor in K_A can be represented by the coordinates (u, v^2), but there is no efficient differential addition;

Summary

On the Kummer variety, very efficient scalar multiplication given by theta functions of level 2, competitive with the scalar multiplication on elliptic curves. But going back to the abelian variety means using level 4 theta functions. Do we really need 12 extra functions just to encode a choice of sign? Recall that in dimension 1, going from the Kummer line to the elliptic curve is simply adding y to x.

Arithmetic from Riemann relations

From now on we assume n even and that if $n=2$ then we are projectively normal.

Given $x=(\vartheta_i(x))$ and $y=(\vartheta_i(y))$, one can recover

- All $\vartheta_i(x+y)\vartheta_j(x-y)$ when $n>2$;
- All $\vartheta_i(x+y)\vartheta_j(x-y)+\vartheta_j(x+y)\vartheta_i(x-y)$ when $n=2$.

Proposition ($2 \mid n$)

- *Given $x=(\vartheta_i(x))$, one can compute $-x=(\vartheta_{-i}(x)$ (Opposite);*
- *Given the points x, y and $x-y$, one can compute $x+y$ (Differential addition);*
- *Given the points $x_1,\dots,x_n$ and the two by two sums x_i+x_j, one can recover $x_1+\ldots+x_n$ (Multiway addition).*
  (Multiway additions use a generalised version of Riemann relations.)

Remark

The previous arithmetic actually can be defined over affine lifts of the projective theta coordinates. These lifts correspond to the lift of the projection $\mathbb{C}^g \to \mathbb{C}^g/\Lambda$ when $\overline{k}=\mathbb{C}$. This extra affine data is crucial for isogenies or pairings computations [LR10; LR15].

(Projective) additions

Given x and y, we want to compute $x+y$.

- When $4 \mid n$, we can always compute $x+y$ by using Riemann relations;
- When $n=2$, we can compute the (sub-scheme) $\{x+y, x-y\}$ as follows:
- Let $\kappa_{ij} = \vartheta_i(x+y)\vartheta_j(x-y) + \vartheta_j(x+y)\vartheta_i(x-y)$;
- The roots of $\mathfrak{P}_i(X) = X^2 - 2\frac{\kappa_{i0}}{\kappa_{00}}X + \frac{\kappa_{ii}}{\kappa_{00}}$ are $\frac{\vartheta_i(z_P+z_Q)}{\vartheta_0(z_P+z_Q)}$ and $\frac{\vartheta_i(z_P-z_Q)}{\vartheta_0(z_P-z_Q)}$;
- We recover the subscheme $\{x+y, x-y\}$ via the equation $\mathfrak{P}_\alpha(X)=0$ and the linear relations coming from

$$\begin{pmatrix} \vartheta_0(x+y) & \vartheta_0(x-y) \\ \vartheta_\alpha(x+y) & \vartheta_\alpha(x-y) \end{pmatrix} \begin{pmatrix} \vartheta_i(x-y) \\ \vartheta_i(x+y) \end{pmatrix} = \begin{pmatrix} \kappa_{0i} \\ \kappa_{\alpha i} \end{pmatrix};$$

- Recovering the set $\{x+y, x-y\}$ explicitly costs a square root in k.

Compatible additions

We work on the Kummer variety $K = A/\pm 1$.

Theorem

Let x, y, z, t be geometric points on A such that $x + y = z + t$ and $x - y \neq z - t$. Then one can compute $x + y = z + t$ on K.

Proof.

The corresponding point is just the intersection of $\{x + y, x - y\}$ and $\{z + t, z - t\}$. In practice this is just a gcd computation between two quadratic polynomials! $\square$

Projective multiway additions

Corollary (Projective multiway addition)

Let x_0 be a point not of 2-torsion. Then from $x_1, \ldots, x_n \in K$ and $x_0 + x_1, \ldots, x_0 + x_n \in K$, one can compute $x_1 + \ldots x_n$ and $x_0 + x_1 + \ldots x_n$.

Proof.

By an easy recursion, it suffices to look at the case $n = 2$. In the previous theorem set $x = x_1, y = x_2, z = x_0 + x_1, t = -x_0 + x_2$ to recover $x_1 + x_2$, and $x = x_1, y = x_0 + x_2, z = x_2, t = x_0 + x_1$ to recover $x_0 + x_1 + x_2$. □

Remark

- The arithmetic here works only in the projective setting, that's why the projective multiway addition needs less input than the affine multiway addition;
- In the $n = 2$ case above, one can also recover the point $x_0 + x_1 + x_2$ or $x_1 + x_2$ once the other is computed by using Riemann relations for the three-way addition.

Double scalar multiplication

In a Kummer variety, how to compute $\alpha P + \beta Q$? (Think GLV/GLS). We assume that we are given P, Q and $P+Q$.

1. A Montgomery square $mP+nQ$, $(m+1)P+nQ$, $mP+(n+1)Q$, $(m+1)P+(n+1)Q$, adding the correct element to the square depending on the current bits of (α, β);
2. A cleverer way is to use a triangle (Bernstein);
3. But actually we only need to keep track of two elements in the square.

Example

From $nP+(m+1)Q, (n+1)P+mQ$, one can recover $nP+mQ$ by using a compatible addition with $x = nP+(m+1)Q$, $y = -Q$, $z = (n+1)P+mQ$, $t = -P$.

Remark

We expect to need to reconstruct a missing element in the square with probability $1/2$, but when we do that we can be clever in the two elements we keep, so the probability is actually higher.

Multi scalar multiplication

- In a Kummer variety, we want to compute $\sum \alpha_i P_i$. (Think higher dimensional GLV/GLS).
- We assume that we are given the two by two sums $P_i + P_j$ (actually, we just need the $P_1 + P_i$, we can recover the others via compatible additions);
- The trivial way would be to use an hypercube;
- But as previously, we just need two elements in the hypercube, say $\sum m_i P_i$ and $P_1 + \sum m_i P_i$;
- At each step we do one compatible addition to recover the element we need in the hypercube, and then use it for two differential additions;
- The total cost is 2 differential additions $+1$ compatible addition by bits.

An efficient representation

Definition

Let A be an abelian variety with a point $T \in A(k)$ not of two torsion, and let $K = A/\pm 1$ be the associated Kummer variety. We represent a point $x \in A(\overline{k})$ by the couple $(x, x+T) \in K^2$.

Remark

To represent $x+T$ we just need to give a root of $\mathfrak{P}_1(X)$, hence this representation needs only $1+2^g$ coordinates.

Efficient arithmetic

- Differential addition: From $(x, x+T), y, (x-y, x-y+T)$, recover $(x+y, x+y+T)$ via two level 2 differential additions;
- Addition: this uses two compatible additions (or one compatible addition + one threeway addition);
- Scalar multiplication:
  1. Do a Montgomery ladder: One doubling and two differential additions at each step (adding the same point, so some savings – $23M+13S$ by bits);
  2. Use a standard level 2 multiplication to compute $(m-1)P, mP$ ($16M+9S$ by bits) and recover $mP+T$ as a compatible addition

$$mP+T=(mP)+T=(m-1)P+(P+T);$$

- Multi scalar multiplication: likewise, do a level 2 multiscalar multiplication to compute $(\sum m_i P_i)-P_1, \sum m_i P_i$ and recover $\sum m_i P_i + T$ as

$$\sum m_i P_i + T = (\sum m_i P_i) + T = ((\sum m_i P_i) - P_1) + (P_1 + T);$$

$\Rightarrow$ This representation only add a small overhead compared to the level 2 representation, but allows to compute additions!

Differential addition

- Notations: $x, y, X = x + y, Y = x - y, 0_A = (a_i)$;
- $$z_i^\chi = \Big(\sum_{t \in Z(\overline{2})} \chi(t) x_{i+t} x_t\Big)\Big(\sum_{t \in Z(\overline{2})} \chi(t) y_{i+t} y_t\Big) / \Big(\sum_{t \in Z(\overline{2})} \chi(t) a_{i+t} a_t\Big).$$
- $$\begin{aligned} 4X_{00}Y_{00} &= z_{00}^{00} + z_{00}^{01} + z_{00}^{10} + z_{00}^{11}; \\ 4X_{01}Y_{01} &= z_{00}^{00} - z_{00}^{01} + z_{00}^{10} + z_{00}^{11}; \\ 4X_{10}Y_{10} &= z_{00}^{00} + z_{00}^{01} - z_{00}^{10} - z_{00}^{11}; \\ 4X_{11}Y_{11} &= z_{00}^{00} - z_{00}^{01} - z_{00}^{10} + z_{00}^{11}; \end{aligned}$$

$\Rightarrow$ $7M + 12S + 9M_0$ for the differential addition (here we neglect multiplications by constants).

Remark

$\left(\sum_t \chi(t) a_{i+t} a_t\right)$ is simply the classical theta null point $\vartheta\left[\begin{smallmatrix}\chi/2 \\ i/2\end{smallmatrix}\right](0,\Omega)^2$.

Normal additions

- $$\begin{aligned}
2(X_{10}Y_{00}+X_{00}Y_{10}) &= z_{10}^{00}+z_{10}^{01};\\
2(X_{11}Y_{01}+X_{01}Y_{11}) &= z_{10}^{00}-z_{10}^{01};\\
2(X_{01}Y_{00}+X_{00}Y_{01}) &= z_{01}^{00}+z_{01}^{10};\\
2(X_{11}Y_{10}+X_{10}Y_{11}) &= z_{01}^{00}-z_{01}^{10};\\
2(X_{11}Y_{00}+X_{00}Y_{11}) &= z_{11}^{00}+z_{11}^{11};\\
2(X_{01}Y_{10}+X_{10}Y_{01}) &= z_{11}^{00}-z_{11}^{11};
\end{aligned}$$

$\Rightarrow$ $(4M+8S+3M_0)+3\times(2M+4S+2M_0)=10M+20S+9M_0$ to compute all the κ_{ij}.

Normal additions, explicit coordinates

- $\mathfrak{P}_\alpha(Z) = Z^2 - 2\frac{\kappa_{\alpha 0}}{\kappa_{00}} Z + \frac{\kappa_{\alpha\alpha}}{\kappa_{00}}$ whose roots are $\{\frac{X_\alpha}{X_0}, \frac{Y_\alpha}{Y_0}\}$;
- We can recover the coordinates X_i, Y_i by solving the equation

$$\begin{pmatrix} 1 & 1 \\ Z & Z' \end{pmatrix} \begin{pmatrix} Y_i/Y_0 \\ X_i/X_0 \end{pmatrix} = \begin{pmatrix} 2\kappa_{0i}/\kappa_{00} \\ 2\kappa_{\alpha i}/\kappa_{00} \end{pmatrix};$$

- We find

$$X_i = \frac{X_\alpha \kappa_{0i} - X_0 \kappa_{\alpha i}}{X_\alpha \kappa_{00} - X_0 \kappa_{\alpha 0}}.$$

$\Rightarrow$ $(10M + 20S + 9M_0) + 8M = 18M + 20S + 9M_0$ to compute X once we know Z.

Compatible additions

- Let $P_1 = X^2 + aX + b$ and $P_2 = X^2 + cX + d$. Then P_1 and P_2 have a common root iff $(ad - bc)(c - a) = (d - b)^2$, in this case this root is $(d - b)/(a - c)$.
- A compatible addition amount to computing a normal addition $x + y$, and finding a root of $\mathfrak{P}_\alpha$ as a common root of the polynomial $\mathfrak{P}'_\alpha$ coming from the addition of $(x + t, y + t)$;
- So for a compatible addition we need the extra computation of $\mathfrak{P}'_\alpha \Rightarrow 6M + 12S + 5M_0$;
- The common root is
$$\frac{\kappa'_{\alpha\alpha}\kappa'_{00} - \kappa_{\alpha\alpha}\kappa_{00}}{2(\kappa'_{\alpha 0} - \kappa_{\alpha 0})};$$

$\Rightarrow$ $28M + 32S + 14M_0$;

- In the $(x, x + t)$ representation, once we have computed $x + y$ via a compatible addition, we can reuse some operations in the computation of $x + y + t$;
- Still, it is more efficient to use a three way addition to compute $x + y + t$ rather than another compatible addition.
- More details in [LR14];
- Possible improvements: find better normalisations, use the equation of the Kummer surface ...

Bibliography

D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: ed. by G. Hanrot, F. Morain, and E. Thomé. Vol. 6197. Lecture Notes in Comput. Sci. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Springer–Verlag, July 2010. DOI: 10.1007/978-3-642-14518-6_21. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. Slides: 2010-07-ANTS-Nancy.pdf (30min, Nancy), HAL: hal-00528944. (Cit. on p. 29).

D. Lubicz and D. Robert. "Arithmetic on Abelian and Kummer Varieties". June 2014. URL: http://www.normalesup.org/~robert/pro/publications/articles/arithmetic.pdf. HAL: hal-01057467, eprint: 2014/493. (Cit. on p. 40).

D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". Mar. 2015. URL: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192. (Cit. on p. 29).