Arithmetic on abelian varieties and related topics

2014/03/03 — Neuchâtel

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest

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.

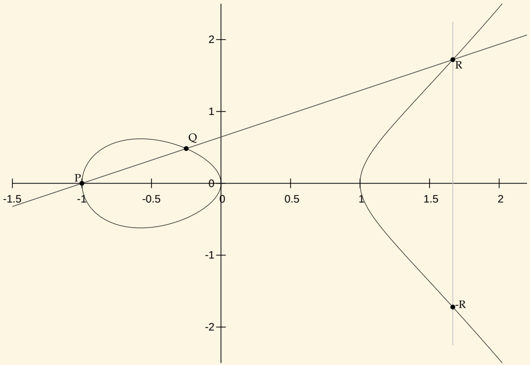
$\Rightarrow$ We want to find secure groups with efficient addition law and compact representation.

Elliptic curves

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

An elliptic curve is a plane curve with equation

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



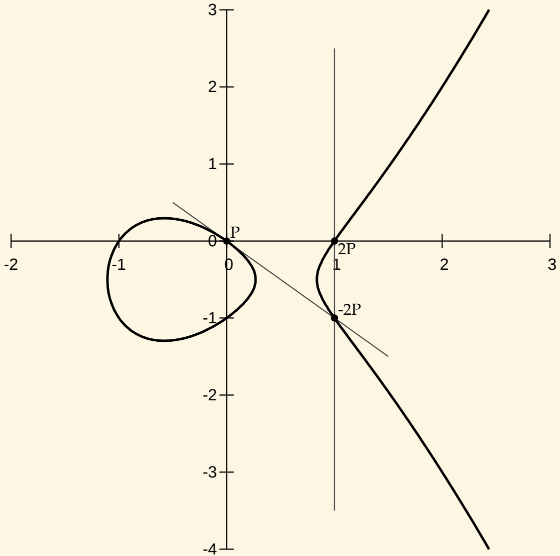
Exponentiation:

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

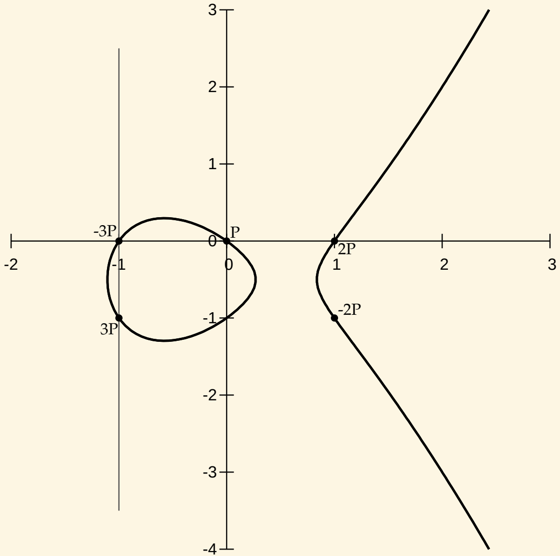
Discrete logarithm:

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

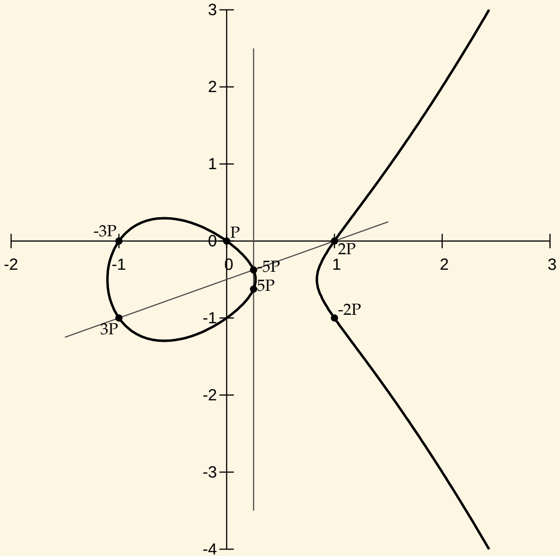
Scalar multiplication on an elliptic curve



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.

Pairing-based cryptography

Definition

A pairing is a bilinear application $e : G_1 \times G_1 \to G_2$.

Example

- If the pairing e can be computed easily, the difficulty of the DLP in G_1 reduces to the difficulty of the DLP in G_2.

$\Rightarrow$ MOV attacks on supersingular elliptic curves.

- One way tripartite Diffie–Hellman [Jou00].
- Identity-based cryptography [BF03].
- Short signature [BLS04].
- Self-blindable credential certificates [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [GPS+06].

Jacobian of curves

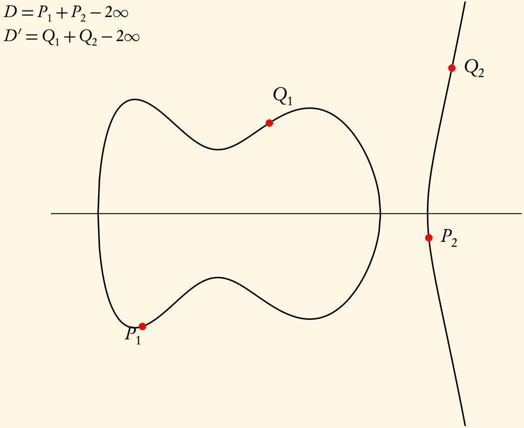
C a smooth irreducible projective curve of genus g.

- Divisor: formal sum $D = \sum n_i P_i, \qquad P_i \in C(\overline{k})$.
  $\deg D = \sum n_i$.
- Principal divisor: $\sum_{P \in C(\overline{k})} v_P(f).P; \qquad f \in \overline{k}(C)$.
- 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.

Example of Jacobians

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

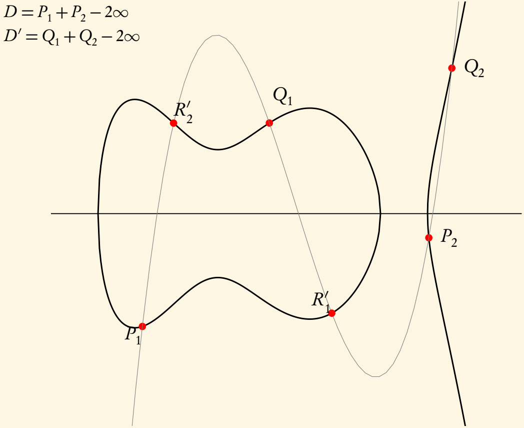
$$y^2 = f(x), \deg f = 5.$$



Example of Jacobians

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

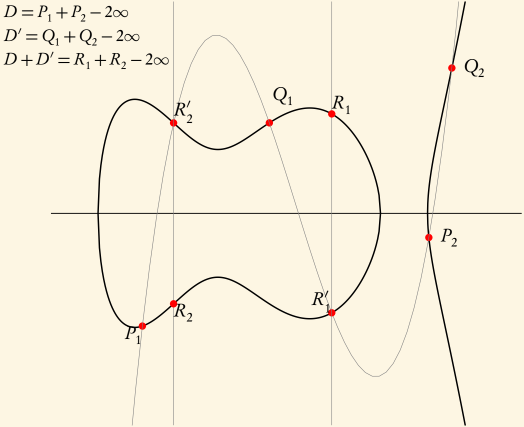
$$y^2 = f(x), \deg f = 5.$$



Example of Jacobians

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

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

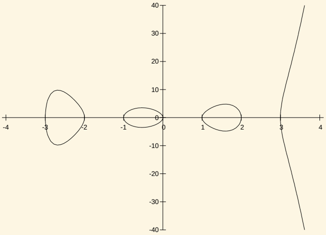


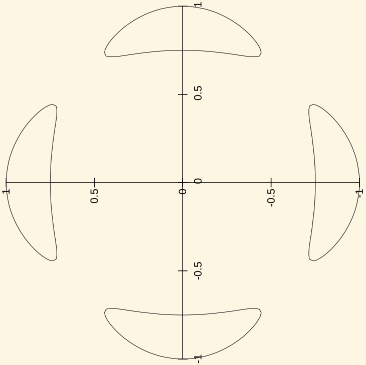
Example of Jacobians

Dimension 3

Jacobians of hyperelliptic curves of genus 3.

Jacobians of quartics.





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 $g \geqslant 4$, not every abelian variety is a Jacobian.

Isogenies

Definition

A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

- Isogenies = Rational map + group morphism + finite kernel.
- Isogenies $\Leftrightarrow$ Finite subgroups.

$$(f : A \rightarrow B) \mapsto \operatorname{Ker} f$$
$$(A \rightarrow A/H) \leftarrow H$$

- *Example:* Multiplication by ℓ ($\Rightarrow \ell$-torsion), Frobenius (non separable).

Polarised abelian varieties over $\mathbb{C}$

Definition

A complex abelian variety A of dimension g is isomorphic to a compact Lie group V/Λ with

- A complex vector space V of dimension g;
- A $\mathbb{Z}$-lattice Λ in V (of rank $2g$);

such that there exists an Hermitian form H on V with $E(\Lambda,\Lambda)\subset\mathbb{Z}$ where $E = \operatorname{Im} H$ is symplectic.

- Such an Hermitian form H is called a polarisation on A. Conversely, any symplectic form E on V such that $E(\Lambda,\Lambda)\subset\mathbb{Z}$ and $E(ix,iy)=E(x,y)$ for all $x,y\in V$ gives a polarisation H with $E=\operatorname{Im} H$.
- Over a symplectic basis of Λ, E is of the form.

  $$\begin{pmatrix} 0 & D_\delta \\ -D_\delta & 0 \end{pmatrix}$$

  where D_δ is a diagonal positive integer matrix $\delta=(\delta_1,\delta_2,\ldots,\delta_g)$, with $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_g$.
- The product $\prod \delta_i$ is the degree of the polarisation; H is a principal polarisation if this degree is 1.

Principal polarisations

- Let E_0 be the canonical principal symplectic form on $\mathbb{R}^{2g}$ given by $E_0((x_1,x_2),(y_1,y_2)) = {}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2$;
- If E is a principal polarisation on $A = V/\Lambda$, there is an isomorphism $j : \mathbb{Z}^{2g} \to \Lambda$ such that $E(j(x), j(y)) = E_0(x,y)$;
- There exists a basis of V such that $j((x_1,x_2)) = \Omega x_1 + x_2$ for a matrix Ω;
- In particular $E(\Omega x_1 + x_2, \Omega y_1 + y_2) = {}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2$;
- The matrix Ω is in $\mathfrak{H}_g$, the Siegel space of symmetric matrices Ω with $\operatorname{Im}\Omega$ positive definite;
- In this basis, $\Lambda = \Omega\mathbb{Z}^g + \mathbb{Z}^g$ and H is given by the matrix $(\operatorname{Im}\Omega)^{-1}$.

Action of the symplectic group

- Every principal symplectic form (hence symplectic basis) on $\mathbb{Z}^{2g}$ comes from the action of $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ on $(\mathbb{Z}^{2g}, E_0)$;
- This action gives a new equivariant bijection $j_M : \mathbb{Z}^{2g} \to \Lambda$ via $j_M((x_1, x_2)) = (A\Omega x_1 + B x_2, C\Omega x_1 + D x_2)$;
- Normalizing this embedding via the action of $(C\Omega + D)^{-1}$ on $\mathbb{C}^g$, we get that $j_M((x_1, x_2)) = \Omega_M x_1 + x_2$ with $\Omega_M = (A\Omega + B)(C\Omega + D)^{-1} \in \mathfrak{H}_g$;
- The moduli space of principally polarised abelian varieties is then isomorphic to $\mathfrak{H}_g / \mathrm{Sp}_{2g}(\mathbb{Z})$.

Isogenies

Let $A = V/\Lambda$ and $B = V'/\Lambda'$.

Definition

An isogeny $f : A \to B$ is a bijective linear map $f : V \to V'$ such that $f(\Lambda) \subset \Lambda'$. The kernel of the isogeny is $f^{-1}(\Lambda')/\Lambda \subset A$ and its degree is the cardinal of the kernel.

Remark

Up to a renormalization, we can always assume that $V = V' = \mathbb{C}^g$, $f = \mathrm{Id}$ and the isogeny is simply $\mathbb{C}^g/\Lambda \to \mathbb{C}^g/\Lambda'$ for $\Lambda \subset \Lambda'$.

The dual abelian variety

Definition

If $A = V/\Lambda$ is an abelian variety, its dual is $\widehat{A}_k = \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})/\Lambda^*$. Here $\mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})$ is the space of anti-linear forms and $\Lambda^* = \{f \mid f(\Lambda) \subset \mathbb{Z}\}$ is the orthogonal of Λ.

- If H is a polarisation on A, its dual H^* is a polarisation on $\widehat{A}$. Moreover, there is an isogeny $\Phi_H : A \to \widehat{A}$:
$$x \mapsto H(x, \cdot)$$
of degree $\deg H$. We note $K(H)$ its kernel.
- If $f : A \to B$ is an isogeny, then its dual is an isogeny $\widehat{f} : \widehat{B}_k \to \widehat{A}$ of the same degree.

Remark

There is a canonical polarisation on $A \times \widehat{A}$ (the Poincaré bundle):
$$(x, f) \mapsto f(x).$$

Projective embeddings

Proposition

Let $\Phi : A = V/\Lambda \mapsto \mathbb{P}^{m-1}$ be a projective embedding. Then the linear functions f associated to this embedding are Λ-automorphics:

$$f(x+\lambda) = a(\lambda, x) f(x) \quad x \in V, \lambda \in \Lambda;$$

for a fixed automorphy factor a:

$$a(\lambda+\lambda', x) = a(\lambda, x+\lambda') a(\lambda', x).$$

Theorem (Appell-Humbert)

All automorphy factors are of the form

$$a(\lambda, x) = \pm e^{\pi(H(x,\lambda) + \frac{1}{2} H(\lambda,\lambda))}$$

for a polarisation H on A.

Theta functions

- Let (A, H_0) be a principally polarised abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ with $\Omega \in \mathfrak{H}_g$.
- All automorphic forms corresponding to a multiple $\mathscr{L}$ of H_0 come from the theta functions with characteristics:

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

- Automorphic property:

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

Theta functions of level n

- Define $\vartheta_i = \vartheta\left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix}\right](., \frac{\Omega}{n})$ for $i \in Z(\overline{n}) = \mathbb{Z}^g / n\mathbb{Z}^g$;
- This is a basis of the automorphic functions for $H = nH_0$ (theta functions of level n);
- This is the unique basis such that in the projective coordinates:

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

  the translation by a point of n-torsion is normalized by

$$\vartheta_i(z + \frac{m_1}{n}\Omega + \frac{m_2}{n}) = e^{-\frac{2\pi i}{n}\,{}^t i \cdot m_1}\vartheta_{i+m_2}(z).$$

- $(\vartheta_i)_{i\in Z(\overline{n})} = \begin{cases} \text{coordinates system} & n \geqslant 3 \\ \text{coordinates on the Kummer variety } A/\pm 1 & n = 2 \end{cases}$
- $(\vartheta_i)_{i\in Z(\overline{n})}$: basis of the theta functions of level n
  $\Leftrightarrow A[n] = A_1[n] \oplus A_2[n]$: symplectic decomposition.
- Theta null point: $\vartheta_i(0)_{i\in Z(\overline{n})} =$ modular invariant.

The duplication formula

Theorem

Let $\xi : A \times A \to A \times A$, $(x, y) \mapsto (x+y, x-y)$. *The isogeny theorem applied to* ξ *gives for* $x, y \in \mathbb{C}^g$

$$\vartheta^{\mathscr{L}}_{i+j}(x+y)\vartheta^{\mathscr{L}}_{i-j}(x-y) = \frac{1}{2^g} \sum_{\chi \in \hat{Z}(\overline{2})} U^{\mathscr{L}^2}_{\chi,i}(x) U^{\mathscr{L}^2}_{\chi,j}(x)$$

$$U^{\mathscr{L}^2}_{\chi,i}(x) U^{\mathscr{L}^2}_{\chi,j}(y) = \sum_{t \in \hat{Z}(\overline{2})} \chi(t) \vartheta^{\mathscr{L}}_{i+j+t}(x+y)\vartheta^{\mathscr{L}}_{i-j+t}(x-y)$$

where $\vartheta^{\mathscr{L}}_i(x) = \vartheta\left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix}\right](x, \frac{\Omega}{n})$ *is a theta function of level* n *and* $U^{\mathscr{L}^2}_{\chi,i}(x) = \vartheta\left[\begin{smallmatrix} \frac{\chi}{2} \\ \frac{i}{n} \end{smallmatrix}\right](2x, \frac{2\Omega}{n})$ *is a theta function of level* $2n$ *on* A.

Multiplication of sections

- Let $\Delta : X \to X \times X$ be the diagonal;
- Δ induces the multiplication map
  $\Delta^* : \Gamma(A, \mathscr{L}) \otimes \Gamma(A, \mathscr{L}) \to \Gamma(X, \mathscr{L}^2)$, $\vartheta_i^{\mathscr{L}} \star \vartheta_j^{\mathscr{L}} \mapsto (\vartheta_i^{\mathscr{L}} \otimes \vartheta_j^{\mathscr{L}})$;
- if $S : A \to A \times A$ is the inclusion map $x \mapsto (x, 0)$ then Δ fits into the commutative diagram

$$\begin{tikzcd}
(A, \mathscr{L}^2) \arrow[d, "S"'] \arrow[dr, "\Delta"] & \\
(A \times A, \mathscr{L}^2 \star \mathscr{L}^2) \arrow[r, "\xi"] & (A \times A, \mathscr{L} \star \mathscr{L}).
\end{tikzcd}$$

  so $\Delta^* = S^* \xi^*$ where ξ^* is given by the duplication formula and
  $S^* : \Gamma(A, \mathscr{L}^2) \otimes \Gamma(A, \mathscr{L}^2) \to \Gamma(A, \mathscr{L}^2)$ is given by $\vartheta_i^{\mathscr{L}^2} \star \vartheta_j^{\mathscr{L}^2} \mapsto \vartheta_i^{\mathscr{L}^2} \vartheta_j^{\mathscr{L}^2}(0)$;
- We thus have that $\Gamma(A, \mathscr{L}) \otimes \Gamma(A, \mathscr{L}) \to \Gamma(X, \mathscr{L}^2)$ is given by

$$\sum_{t \in \hat{Z}(\overline{2})} \chi(t) \left(\vartheta_{i+t}^{\mathscr{L}} \star \vartheta_{j+t}^{\mathscr{L}} \right) \mapsto U_{\chi, \frac{i+j}{2}}^{\mathscr{L}^2} U_{\chi, \frac{i-j}{2}}^{\mathscr{L}^2}(0).$$

Projective normality

Theorem (Mumford–Kempf)

If $\mathscr{L}_0$ is a principal polarisation, then $\Gamma(A,\mathscr{L}_0^m)\otimes\Gamma(A,\mathscr{L}_0^n)\to\Gamma(A,\mathscr{L}_0^{n+m})$ is surjective whenever $m \geqslant 2$ and $n \geqslant 3$.

Corollary

If $\mathscr{L} = \mathscr{L}_0^n$ with $n \geqslant 3$, then $S^m\Gamma(A,\mathscr{L}) \to \Gamma(A,\mathscr{L}^m)$ is surjective for all m. Equivalently the homogeneous ring associated to $\mathscr{L}$ is integrally closed, we say that A is projectively normal.

Corollary (Restatement)

If $\mathscr{L} = \mathscr{L}_0^n$ with $n \geqslant 3$, then for every $u \in Z(2\overline{n})$, $\chi \in \hat{Z}(\overline{2})$, there exists $v \in Z(2\overline{n})$ congruent to u modulo $Z(\overline{n})$ such that $U_{\chi,v}^{\mathscr{L}^2}(0) \neq 0$.

Projective normality

Corollary (Restatement)

If $\mathscr{L} = \mathscr{L}_0^n$ with $n \geqslant 3$, then for every $u \in Z(2\overline{n})$, $\chi \in \hat{Z}(\overline{2})$, there exists $v \in Z(2\overline{n})$ congruent to u modulo $Z(\overline{n})$ such that $U_{\chi,v}^{\mathscr{L}^2}(0) \neq 0$.

Proof (Mumford).

For simplicity we assume here that $4 \mid n$. Let $F = \sum_{t \in Z(\overline{2})} \vartheta_{2u+t}^{\mathscr{L}^2}$ and $G = \sum_{t \in Z(\overline{2})} \chi(t) \vartheta_t^{\mathscr{L}^2}$. By the duplication formula, $F \star G = \sum_{v \in u + Z(\overline{4})} U_{\chi,v}^{\mathscr{L}^2}(0) \vartheta_v^{\mathscr{L}^2}$. Since the homogeneous ring is integral, $F \star G \neq 0$. Hence there exist $v \equiv u \pmod 4$ such that $U_{\chi,v}^{\mathscr{L}^2}(0) \neq 0$. □

The differential addition law ($k=\mathbb{C}$)

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

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

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

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

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

Proof.

Let i_0,j_0,k_0,l_0 be such that $i_0+j_0=i$, $i_0-j_0=j$, $k_0+l_0=k$, $k_0-l_0=l$; then (up to a change of variable) $i_0+l_0=i'$, $i_0-l_0=j'$, $k_0+j_0=k'$, $k_0-j_0=l'$. Thus both terms are equal to $U^{\mathscr{L}^2}_{\chi,i_0}(x)U^{\mathscr{L}^2}_{\chi,j_0}(y)U^{\mathscr{L}^2}_{\chi,k_0}(0)U^{\mathscr{L}^2}_{\chi,l_0}(0)$. □

The differential addition law ($k = \mathbb{C}$)

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big) = \Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

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

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

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

Remark

By the projective normality above, when $n \geqslant 4$, for all $\chi \in \hat{Z}(\overline{2})$, $k, l \in Z(\overline{n})$; there exists $k_1, l_1 \in Z(\overline{n})$ with $k_1 + l_1 \in 2Z(\overline{n})$ such that $\sum_{t\in Z(\overline{2})} \chi(t)\vartheta^{\mathscr{L}}_{k_2}(0)\vartheta^{\mathscr{L}}_{l_2}(0) \neq 0$ where $k_2 = k + k_1$, $l_2 = l + l_1$. Hence it is always possible to compute the addition law.

Example: addition in genus 1 and in level 2

Differential Addition Algorithm:
Input: $P=(x_1:z_1)$, $Q=(x_2:z_2)$
and $R=P-Q=(x_3:z_3)$ with $x_3z_3\neq 0$.
Output: $P+Q=(x':z')$.

1. $x_0=(x_1^2+z_1^2)(x_2^2+z_2^2)$;
2. $z_0=\frac{A^2}{B^2}(x_1^2-z_1^2)(x_2^2-z_2^2)$;
3. $x'=(x_0+z_0)/x_3$;
4. $z'=(x_0-z_0)/z_3$;
5. Return $(x':z')$.

Kummer varieties

- If the level $n = 2$, then the theta coordinates give an embedding of the Kummer variety $\mathscr{K} = A/\pm 1$;
- If $\mathscr{L}$ is totally symmetric, it descends to a section $\mathscr{M}$ on $\mathscr{K}$, and the sections of $\mathscr{M}^n$ are the symmetric sections $\Gamma(A, \mathscr{L}^n)^+$ of $\mathscr{L}^n$ (sections invariant under the action of $[-1]$);
- The functions $U_{\chi,i}$ appearing in the duplication and addition formulae corresponds to the classical theta functions of level four $\vartheta\left[\begin{smallmatrix} \frac{a}{2} \\ \frac{b}{2} \end{smallmatrix}\right](2x, \Omega)$. They are even (resp. odd) when $\chi(2i) = 1$ (resp. $\chi(2i) = -1$).

Theorem (Mumford–Koizumi)

The even theta null points $\{\vartheta\left[\begin{smallmatrix} \frac{a}{2} \\ \frac{b}{2} \end{smallmatrix}\right](0, \Omega) \mid (-1)^{{}^t ab} = 1\}$ *are non null if and only if* $\Gamma(A, \mathscr{L})^2 \to \Gamma(A, \mathscr{L}^2)^+$ *is surjective, if and only if* $(\mathscr{K}, \mathscr{M})$ *is projectively normal.*

Corollary ([Lubicz–R.])

- *In this case, from the theta coordinates of* x *and* y *we can recover all elements of the form* $\vartheta_i(x+y)\vartheta_j(x-y) + \vartheta_j(x+y)\vartheta_i(x-y)$*;*
- *While it is not possible to compute additions on the Kummer variety, it is always possible to compute differential additions.*

Isogenies and pairings

Let $f: A \to B$ be a separable isogeny with kernel K between two abelian varieties defined over k:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{f} & B & \longrightarrow & 0 \\ & & 0 & \longleftarrow & \hat{A} & \xleftarrow{\hat{f}} & \hat{B} & \longleftarrow & \hat{K} & \longleftarrow & 0 \end{array}$$

- Since $\hat{B} \simeq \mathrm{Ext}^1(B, \mathbb{G}_m)$, $\hat{K}$ is the Cartier dual of K, and we have a non degenerate pairing $e_f : K \times \hat{K} \to \overline{k}^*$:
  1. If $Q \in \hat{K}(\overline{k})$, Q defines a divisor D_Q on B;
  2. $\widehat{f}(Q) = 0$ means that $f^* D_Q$ is equal to a principal divisor (g_Q) on A;
  3. $e_f(P, Q) = g_Q(x)/g_Q(x+P)$. (This last function being constant in its definition domain).
- The Weil pairing $e_{W,\ell}$ is the pairing associated to the isogeny $[\ell]: A \to A$:

$$e_{W,\ell} : A[\ell] \times \hat{A}[\ell] \to \mu_\ell(\overline{k}).$$

Polarizations

If $\mathscr{L}$ is an ample line bundle, the polarization $\varphi_{\mathscr{L}}$ is a morphism $A \to \widehat{A}, x \mapsto t_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$.

Definition

Let $\mathscr{L}$ be a principal polarization on A. The (polarized) Weil pairing $e_{W,\mathscr{L},\ell}$ is the pairing

$$\begin{array}{rccc} e_{W,\mathscr{L},\ell} : A[\ell] \times A[\ell] & \longrightarrow & \mu_\ell(\overline{k}) \\ (P,Q) & \longmapsto & e_{W,\ell}(P, \varphi_{\mathscr{L}}(Q)) \end{array}.$$

associated to the polarization $\varphi_{\mathscr{L}^\ell}$:

$$A \xrightarrow{[\ell]} A \xrightarrow{\mathscr{L}} \widehat{A}_k$$

The Tate pairings on abelian varieties over finite fields

- From the exact sequence

$$0 \to A[\ell](\overline{\mathbb{F}}_{q^d}) \to A(\overline{\mathbb{F}}_{q^d}) \xrightarrow{[\ell]} A(\overline{\mathbb{F}}_{q^d}) \to 0$$

  we get from Galois cohomology a connecting morphism

$$\delta : A(\mathbb{F}_{q^d})/\ell A(\mathbb{F}_{q^d}) \to H^1(\mathrm{Gal}(\overline{\mathbb{F}}_{q^d}/\mathbb{F}_{q^d}), A[\ell]);$$

- Composing with the Weil pairing, we get a bilinear application

$$A[\ell](\mathbb{F}_{q^d}) \times A(\mathbb{F}_{q^d})/\ell A(\mathbb{F}_{q^d}) \to H^1(\mathrm{Gal}(\overline{\mathbb{F}}_{q^d}/\mathbb{F}_{q^d}), \mu_\ell) \simeq \mathbb{F}_{q^d}^*/\mathbb{F}_{q^d}^{*\,\ell} \simeq \mu_\ell$$

  where the last isomorphism comes from the Kummer sequence

$$1 \to \mu_\ell \to \overline{\mathbb{F}}_{q^d}^* \to \overline{\mathbb{F}}_{q^d}^* \to 1$$

  and Hilbert 90;

- Explicitely, if $P \in A[\ell](\mathbb{F}_{q^d})$ and $Q \in A(\mathbb{F}_{q^d})$ then the (reduced) Tate pairing is given by

$$e_T(P,Q) = e_W(P, \pi(Q_0) - Q_0)$$

  where Q_0 is any point such that $Q = [\ell]Q_0$ and π is the Frobenius of $\mathbb{F}_{q^d}$.

Cycles and Lang reciprocity

- Let $(A, \mathscr{L})$ be a principally polarized abelian variety;
- To a degree 0 cycle $\sum n_i(P_i)$ on A, we can associate the divisor $\sum t_{P_i}^* \mathscr{L}^{n_i}$ on A;
- The cycle $\sum n_i(P_i)$ corresponds to a trivial divisor iff $\sum n_i P_i = 0$ in A;
- If f is a function on A and $D = \sum(P_i)$ a cycle whose support does not contain a zero or pole of f, we let

$$f(D) = \prod f(P_i)^{n_i}.$$

(In the following, when we write $f(D)$ we will always assume that we are in this situation.)

Theorem ([Lan58])

Let D_1 and D_2 be two cycles equivalent to 0, and f_{D_1} and f_{D_2} be the corresponding functions on A. Then

$$f_{D_1}(D_2) = f_{D_2}(D_1)$$

The Weil and Tate pairings on abelian varieties

Theorem

Let $P, Q \in A[\ell]$. Let D_P and D_Q be two cycles equivalent to $(P)-(0)$ and $(Q)-(0)$. The Weil pairing is given by

$$e_W(P,Q) = \frac{f_{\ell D_P}(D_Q)}{f_{\ell D_Q}(D_P)}.$$

Theorem

Let $P \in A[\ell](\mathbb{F}_{q^d})$ and $Q \in A(\mathbb{F}_{q^d})$, and let D_P and D_Q be two cycles equivalent to $(P)-(0)$ and $(Q)-(0)$. The (non reduced) Tate pairing is given by

$$e_T(P,Q) = f_{\ell D_P}(D_Q).$$

Cryptographic usage of pairings on abelian varieties

- The moduli space of abelian varieties of dimension g is a space of dimension $g(g+1)/2$. We have more liberty to find optimal abelian varieties in function of the security parameters.
- Supersingular abelian varieties can have larger embedding degree than supersingular elliptic curves.
- Over a Jacobian, we can use twists even if they are not coming from twists of the underlying curve.
- If A is an abelian variety of dimension g, $A[\ell]$ is a $(\mathbb{Z}/\ell\mathbb{Z})$-module of dimension $2g \Rightarrow$ the structure of pairings on abelian varieties is richer.

The Weil and Tate pairing with theta coordinates (Lubicz–R. [LR10])

P and Q points of ℓ-torsion.

$$\begin{array}{ccccc}
z_0 & z_P & 2z_P & \dots & \ell z_P = \lambda_P^0 z_0 \\
z_Q & z_P \oplus z_Q & 2z_P + z_Q & \dots & \ell z_P + z_Q = \lambda_P^1 z_Q \\
2z_Q & z_P + 2z_Q & & & \\
\dots & \dots & & & \\
\ell Q = \lambda_Q^0 0_A & z_P + \ell z_Q = \lambda_Q^1 z_P & & &
\end{array}$$

- $e_{W,\ell}(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_P^0 \lambda_Q^1}$.
- $e_{T,\ell}(P,Q) = \frac{\lambda_P^1}{\lambda_P^0}$.

Why does it work?

$$
\begin{array}{ccccc}
z_0 & \alpha z_P & \alpha^4(2z_P) & \ldots & \alpha^{\ell^2}(\ell z_P) = \lambda'^0_P z_0 \\
\beta z_Q & \gamma(z_P \oplus z_Q) & \frac{\gamma^2\alpha^2}{\beta}(2z_P + z_Q) & \ldots & \frac{\gamma^\ell \alpha^{\ell(\ell-1)}}{\beta^{\ell-1}}(\ell z_P + z_Q) = \lambda'^1_P \beta z_Q \\
\beta^4(2z_Q) & \frac{\gamma^2\beta^2}{\alpha}(z_P + 2z_Q) & & & \\
\ldots & \ldots & & & \\
\beta^{\ell^2}(\ell z_Q) = \lambda'^0_Q z_0 & \frac{\gamma^\ell \beta^{\ell(\ell-1)}}{\alpha^{\ell-1}}(z_P + \ell z_Q) = \lambda'^1_Q \alpha z_P & & &
\end{array}
$$

We then have

$$
\lambda'^0_P = \alpha^{\ell^2}\lambda^0_P, \quad \lambda'^0_Q = \beta^{\ell^2}\lambda^0_Q, \quad \lambda'^1_P = \frac{\gamma^\ell \alpha^{(\ell(\ell-1))}}{\beta^\ell}\lambda^1_P, \quad \lambda'^1_Q = \frac{\gamma^\ell \beta^{(\ell(\ell-1))}}{\alpha^\ell}\lambda^1_Q,
$$

$$
e'_{W,\ell}(P,Q) = \frac{\lambda'^1_P \lambda'^0_Q}{\lambda'^0_P \lambda'^1_Q} = \frac{\lambda^1_P \lambda^0_Q}{\lambda^0_P \lambda^1_Q} = e_{W,\ell}(P,Q),
$$

$$
e'_{T,\ell}(P,Q) = \frac{\lambda'^1_P}{\lambda'^0_P} = \frac{\gamma^\ell}{\alpha^\ell \beta^\ell}\frac{\lambda^1_P}{\lambda^0_P} = \frac{\gamma^\ell}{\alpha^\ell \beta^\ell} e_{T,\ell}(P,Q).
$$

Ate pairing [LR13]

- Let $P \in G_2 = A[\ell] \bigcap \mathrm{Ker}(\pi_q - [q])$ and $Q \in G_1 = A[\ell] \bigcap \mathrm{Ker}(\pi_q - 1)$; $\lambda \equiv q \mod \ell$.
- In projective coordinates, we have $\pi_q^d(P+Q) = \lambda^d P + Q = P + Q$;
- Of course, in affine coordinates, $\pi_q^d(z_{P+Q}) \neq \lambda^d z_P + z_Q$.
- But if $\pi_q(z_{P+Q}) = C * (\lambda z_P + z_Q)$, then C is exactly the (non reduced) ate pairing (up to a renormalisation)!

Algorithm (Computing the ate pairing)

Input $P \in G_2$, $Q \in G_1$;

1. *Compute $z_Q + \lambda z_P$, λz_P using differential additions;*
2. *Find the projective factors C_1 and C_0 such that $z_Q + \lambda z_P = C_1 * \pi(z_{P+Q})$ and $\lambda z_P = C_0 * \pi(z_P)$ respectively;*

Return $(C_1/C_0)^{\frac{q^d-1}{\ell}}$.

Cryptographic usage of isogenies

- Transfer the Discrete Logarithm Problem from one Abelian variety to another;
- Point counting algorithms (ℓ-adic or p-adic) $\Rightarrow$ Verify an abelian variety is secure;
- Compute the class field polynomials (CM-method) $\Rightarrow$ Construct a secure abelian variety;
- Compute the modular polynomials $\Rightarrow$ Compute isogenies;
- Determine $\mathrm{End}(A)$ $\Rightarrow$ CRT method for class field polynomials;
- Speed up the arithmetic;
- Hash functions and cryptosystems based on isogeny graphs.

The isogeny theorem

Theorem

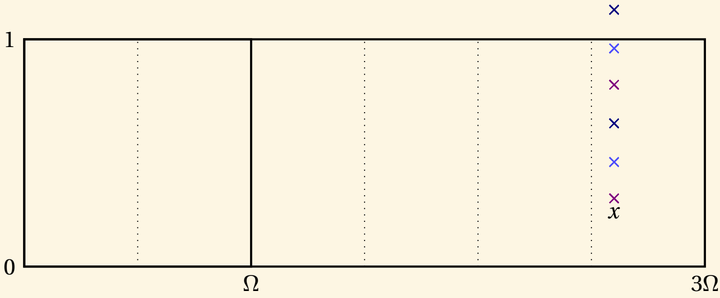
- *Let* $\varphi : Z(\overline{n}) \to Z(\overline{\ell n}), x \mapsto \ell.x$ *be the canonical embedding.*
  Let $K = A_2[\ell] \subset A_2[\ell n]$.
- *Let* $(\vartheta_i^A)_{i \in Z(\overline{\ell n})}$ *be the theta functions of level* ℓn *on* $A = \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g)$.
- *Let* $(\vartheta_i^B)_{i \in Z(\overline{n})}$ *be the theta functions of level* n *of* $B = A/K = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- *We have:*
$$(\vartheta_i^B(x))_{i \in Z(\overline{n})} = (\vartheta_{\varphi(i)}^A(x))_{i \in Z(\overline{n})}$$

Example

$f : (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) \mapsto (x_0, x_3, x_6, x_9)$ is a 3-isogeny between elliptic curves.

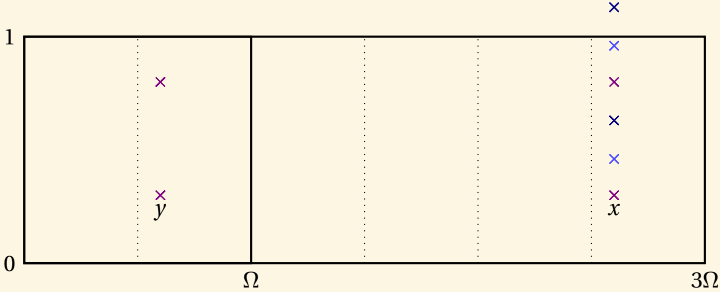
An example with $g=1$, $n=2$, $\ell=3$

$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "f"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$



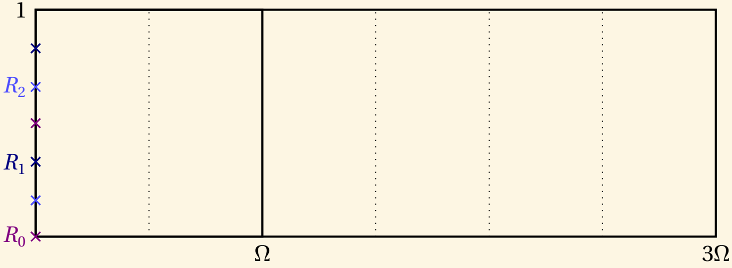
An example with $g=1$, $n=2$, $\ell=3$

$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "f"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$



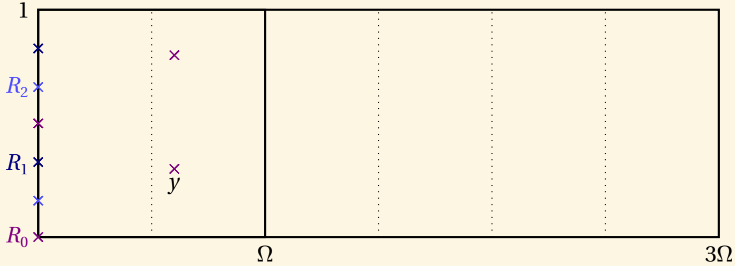
An example with $g=1$, $n=2$, $\ell=3$

$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "f"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$



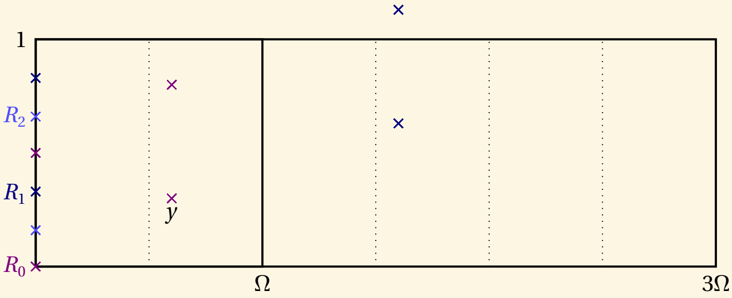
An example with $g=1$, $n=2$, $\ell=3$

$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "f"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g), \text{ level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g), \text{ level } n \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$



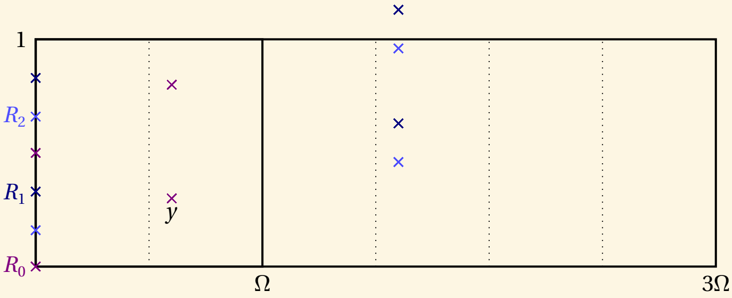
An example with $g=1$, $n=2$, $\ell=3$

$$\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g),\ \text{level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "f"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g),\ \text{level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g),\ \text{level } n \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}$$



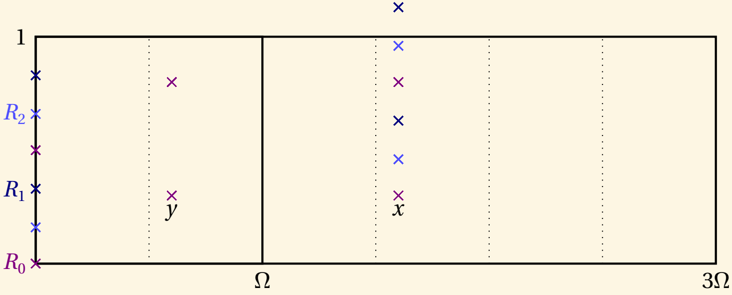
An example with $g=1$, $n=2$, $\ell=3$

$$
\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g),\ \text{level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "f"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g),\ \text{level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g),\ \text{level } n \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}
$$



An example with $g=1$, $n=2$, $\ell=3$

$$
\begin{tikzcd}
z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g),\ \text{level } \ell n \arrow[rr, "{[\ell]}"] \arrow[dr, "f"'] & & \ell z \in \mathbb{C}^g/(\mathbb{Z}^g+\ell\Omega\mathbb{Z}^g),\ \text{level } \ell n \\
& z \in \mathbb{C}^g/(\mathbb{Z}^g+\Omega\mathbb{Z}^g),\ \text{level } n \arrow[ur, "\tilde{f}"'] &
\end{tikzcd}
$$



Changing level

Theorem (Koizumi–Kempf)

Let F be a matrix of rank r such that ${}^t F F = \ell \operatorname{Id}_r$. Let $X \in (\mathbb{C}^g)^r$ and $Y = F(X) \in (\mathbb{C}^g)^r$. Let $j \in (\mathbb{Q}^g)^r$ and $i = F(j)$. Then we have

$$\vartheta\left[\begin{smallmatrix} 0 \\ i_1 \end{smallmatrix}\right]\left(Y_1, \frac{\Omega}{n}\right) \dots \vartheta\left[\begin{smallmatrix} 0 \\ i_r \end{smallmatrix}\right]\left(Y_r, \frac{\Omega}{n}\right) = \sum_{\substack{t_1,\dots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ F(t_1,\dots,t_r)=(0,\dots,0)}} \vartheta\left[\begin{smallmatrix} 0 \\ j_1 \end{smallmatrix}\right]\left(X_1 + t_1, \frac{\Omega}{\ell n}\right) \dots \vartheta\left[\begin{smallmatrix} 0 \\ j_r \end{smallmatrix}\right]\left(X_r + t_r, \frac{\Omega}{\ell n}\right),$$

(This is the isogeny theorem applied to $F_A : A^r \to A^r$.)

- If $\ell = a^2 + b^2$, we take $F = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$, so $r = 2$.
- In general, $\ell = a^2 + b^2 + c^2 + d^2$, we take F to be the matrix of multiplication by $a + bi + cj + dk$ in the quaternions, so $r = 4$.

The isogeny formula

$$\ell \wedge n = 1, \quad B = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \quad A = \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g)$$

$$\vartheta_b^B := \vartheta\left[\begin{smallmatrix} 0 \\ \frac{b}{n} \end{smallmatrix}\right]\left(\cdot, \frac{\Omega}{n}\right), \quad \vartheta_b^A := \vartheta\left[\begin{smallmatrix} 0 \\ \frac{b}{n} \end{smallmatrix}\right]\left(\cdot, \frac{\ell\Omega}{n}\right)$$

Proposition

Let F be a matrix of rank r such that ${}^tFF = \ell\,\mathrm{Id}_r$. Let X in $(\mathbb{C}^g)^r$ and $Y = XF^{-1} \in (\mathbb{C}^g)^r$. Let $i \in (Z(\overline{n}))^r$ and $j = iF^{-1}$. Then we have

$$\vartheta_{i_1}^A(Y_1)\dots\vartheta_{i_r}^A(Y_r) = \sum_{\substack{t_1,\dots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\dots,t_r)F=(0,\dots,0)}} \vartheta_{j_1}^B(X_1+t_1)\dots\vartheta_{j_r}^B(X_r+t_r),$$

Corollary

$$\vartheta_k^A(0)\vartheta_0^A(0)\dots\vartheta_0^A(0) = \sum_{\substack{t_1,\dots,t_r \in K \\ (t_1,\dots,t_r)F=(0,\dots,0)}} \vartheta_{j_1}^B(t_1)\dots\vartheta_{j_r}^B(t_r), \quad (j = (k,0,\dots,0)F^{-1} \in Z(\overline{n}))$$

The Algorithm (Cosset–R. [CR13])

$$
\begin{tikzcd}
 & x \in (A, \ell H_1) \arrow[dl, "f"] \arrow[dd, "{[\ell]}"] \arrow[r, dashed] & (x,0,\dots,0) \in (A^r, \ell H_1 \star \cdots \star \ell H_1) \arrow[d, "{}^t F"] \\
y \in (B, H_2) \arrow[dr, "\widetilde{f}"'] & & {}^t F(x,0,\dots,0) \in (A^r, \ell H_1 \star \cdots \star \ell H_1) \arrow[d, "F"] \\
 & \widetilde{f}(y) \in (A, H_1) & F \circ {}^t F(x,0,\dots,0) \in (A^r, H_1 \star \cdots \star H_1) \arrow[l, dashed]
\end{tikzcd}
$$

Complexity over $\mathbb{F}_q$

- The geometric points of the kernel live in a extension k' of degree at most $\ell^g - 1$ over $k = \mathbb{F}_q$;
- The isogeny formula assumes that the points are in affine coordinates. In practice, given $A/\mathbb{F}_q$ we only have projective coordinates $\Rightarrow$ we use differential additions to normalize the coordinates;
- Computing the normalization factors takes $O(\log \ell)$ operations in k';
- Computing the points of the kernel via differential additions take $O(\ell^g)$ operations in k';
- If $\ell \equiv 1 \pmod 4$, applying the isogeny formula take $O(\ell^g)$ operations in k';
- If $\ell \equiv 3 \pmod 4$, applying the isogeny formula take $O(\ell^{2g})$ operations in k';

$\Rightarrow$ The total cost is $\widetilde{O}(\ell^{2g})$ or $\widetilde{O}(\ell^{3g})$ operations in $\mathbb{F}_q$.

Remark

The complexity is much worse over a number field because we need to work with extensions of much higher degree.

Complexity over $\mathbb{F}_q$

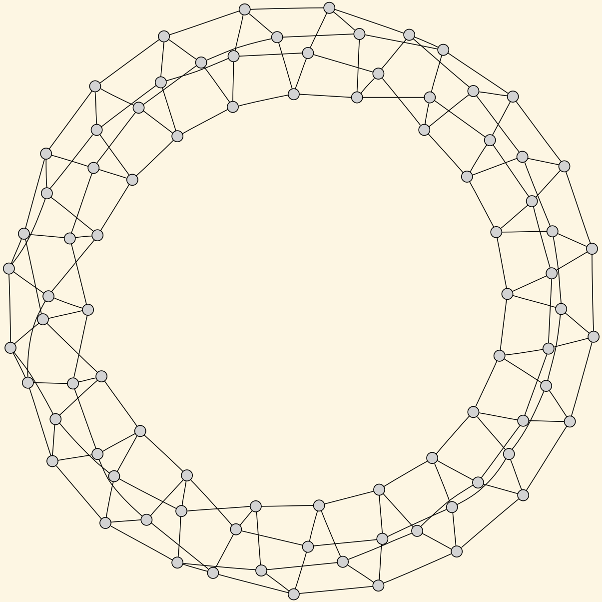
- The geometric points of the kernel live in a extension k' of degree at most $\ell^g - 1$ over $k = \mathbb{F}_q$;
- The isogeny formula assumes that the points are in affine coordinates. In practice, given $A/\mathbb{F}_q$ we only have projective coordinates $\Rightarrow$ we use differential additions to normalize the coordinates;
- Computing the normalization factors takes $O(\log \ell)$ operations in k';
- Computing the points of the kernel via differential additions take $O(\ell^g)$ operations in k';
- If $\ell \equiv 1 \pmod 4$, applying the isogeny formula take $O(\ell^g)$ operations in k';
- If $\ell \equiv 3 \pmod 4$, applying the isogeny formula take $O(\ell^{2g})$ operations in k';

$\Rightarrow$ The total cost is $\widetilde{O}(\ell^{2g})$ or $\widetilde{O}(\ell^{3g})$ operations in $\mathbb{F}_q$.

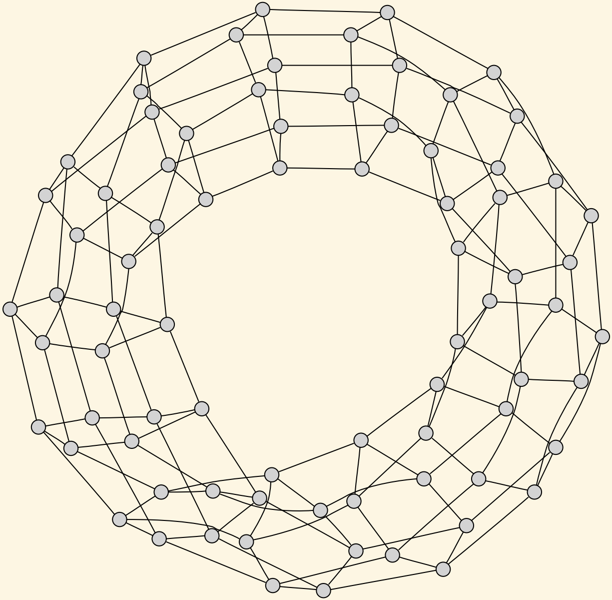
Theorem ([Lubicz–R.])

We can compute the isogeny directly given the equations (in a suitable form) of the kernel K of the isogeny. When K is rational, this gives a complexity of $\widetilde{O}(\ell^g)$ or $\widetilde{O}(\ell^{2g})$ operations in $\mathbb{F}_q$.

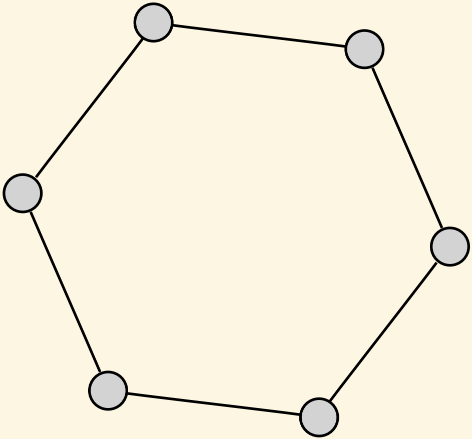
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



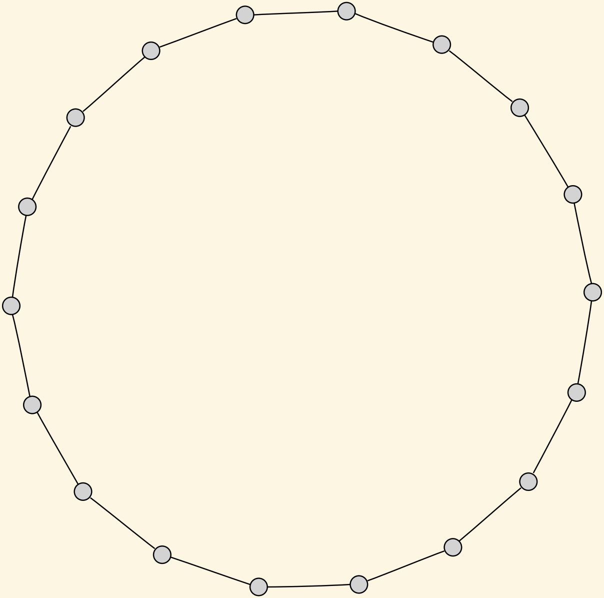
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



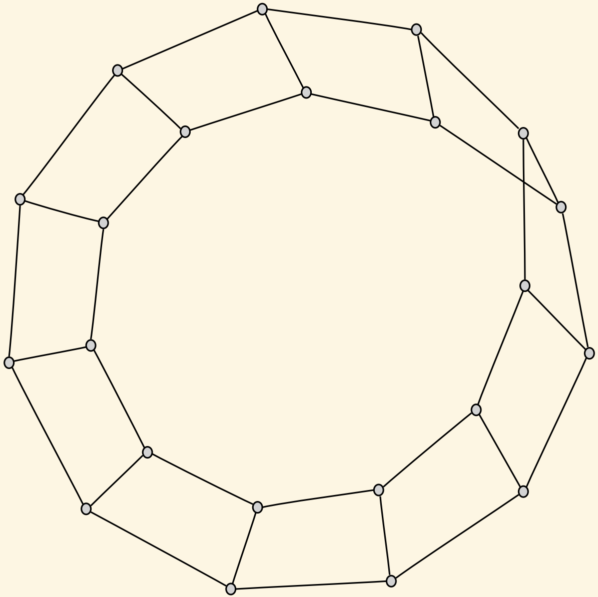
Horizontal isogeny graphs: $\ell = q = Q\overline{Q}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



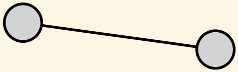
Horizontal isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2^2$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



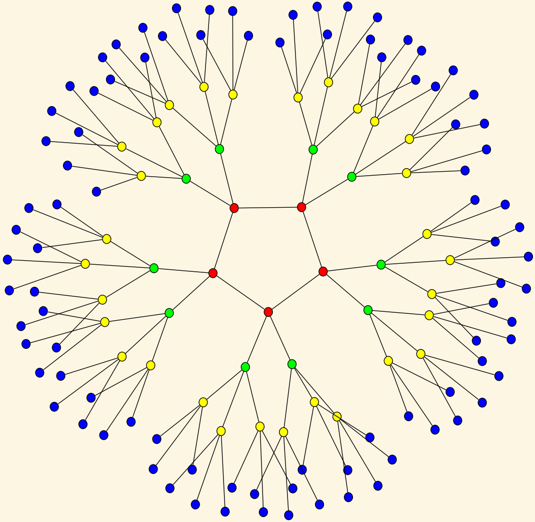
Horizontal isogeny graphs: $\ell = q^2 = Q^2\overline{Q}^2$

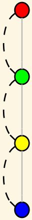


Horizontal isogeny graphs: $\ell = q^2 = Q^4$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$

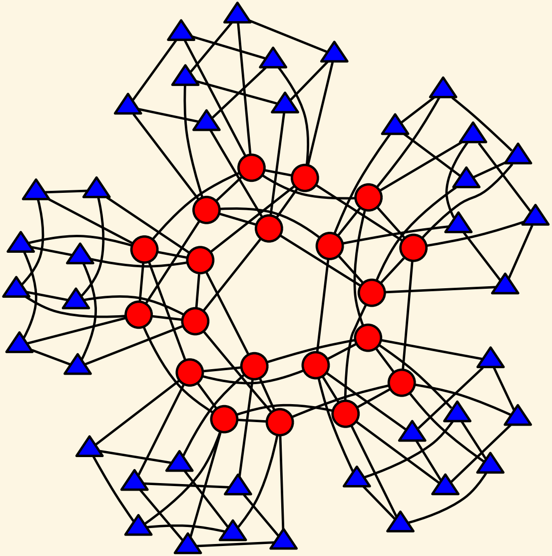


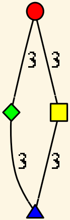
Isogeny graphs in dimension 1



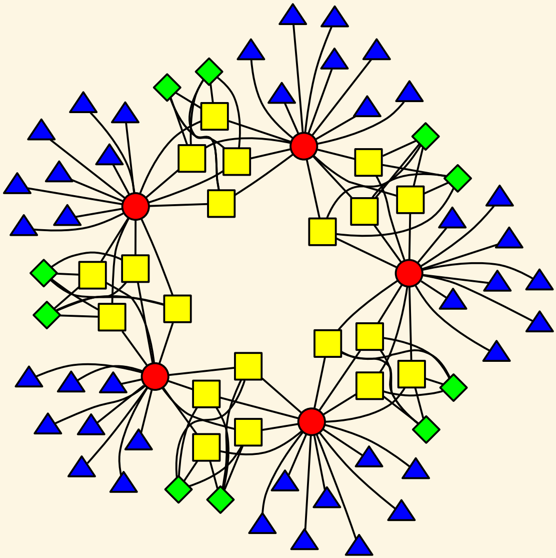


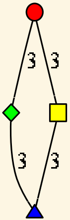
Isogeny graphs in dimension 2 ($\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$)



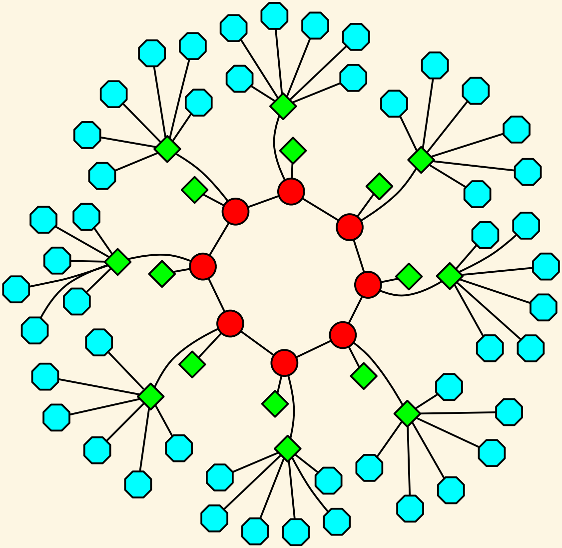


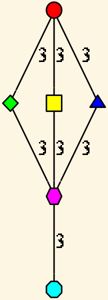
Isogeny graphs in dimension 2 ($\ell = q = Q\overline{Q}$)



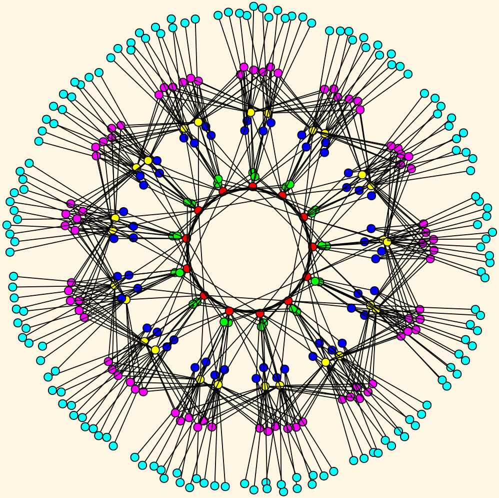


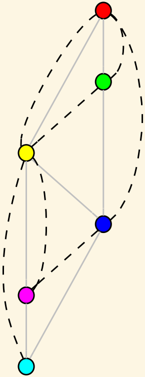
Isogeny graphs in dimension 2 ($\ell = q = Q\overline{Q}$)





Isogeny graphs and lattice of orders (Bisson–Cosset–R. [BCR10])





Bibliography

G. Bisson, R. Cosset, and D. Robert. "AVIsogenies (Abelian Varieties and Isogenies)". Magma package for explicit isogenies computation between abelian varieties. 2010. URL: http://avisogenies.gforge.inria.fr. Free software (LGPLv2+), registered to APP (reference IDDN.FR.001.440011.000.R.P.2010.000.10000) (cit. on p. 65).

D. Boneh and M. Franklin. "Identity-based encryption from the Weil pairing". In: *SIAM Journal on Computing* 32.3 (2003), pp. 586–615 (cit. on p. 8).

D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the Weil pairing". In: *Journal of Cryptology* 17.4 (2004), pp. 297–319 (cit. on p. 8).

R. Cosset and D. Robert. "An algorithm for computing (ℓ,ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". Accepted for publication at Mathematics of computation. Oct. 2013. URL: http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991, eprint: 2011/143 (cit. on p. 52).

V. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-based encryption for fine-grained access control of encrypted data". In: *Proceedings of the 13th ACM conference on Computer and communications security*. ACM. 2006, p. 98 (cit. on p. 8).

A. Joux. "A one round protocol for tripartite Diffie–Hellman". In: *Algorithmic number theory (ANTS IV* (2000), pp. 385–393 (cit. on p. 8).

S. Lang. "Reciprocity and Correspondences". In: *American Journal of Mathematics* 80.2 (1958), pp. 431–440 (cit. on p. 35).

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 http://www.normalesup.org/~robert/publications/slides/2010-07-ants.pdf (cit. on p. 38).

D. Lubicz and D. Robert. “A generalisation of Miller’s algorithm and applications to pairing computations on abelian varieties”. Mar. 2013. URL: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192 (cit. on p. 40).

A. Sahai and B. Waters. “Fuzzy identity-based encryption”. In: *Advances in Cryptology–EUROCRYPT 2005* (2005), pp. 457–473 (cit. on p. 8).

E. Verheul. “Self-blindable credential certificates from the Weil pairing”. In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 533–551 (cit. on p. 8).