Theta functions and applications in cryptography
Fonctions thêta et applications en cryptographie

Thèse d'informatique

Damien Robert[1]

[1]Caramel team, Nancy Universités, CNRS, INRIA Nancy Grand Est

21/07/2010 (Nancy)

Outline

Outline

A brief history of public-key cryptography

- Secret-key cryptography: Vigenère (1553), One time pad (1917), AES (NIST, 2001).
- Public-key cryptography:
  - Diffie–Hellman key exchange (1976).
  - RSA (1978): multiplication/factorisation.
  - ElGamal: exponentiation/discrete logarithm in $G = \mathbb{F}_q^*$.
  - ECC/HECC (1985): discrete logarithm in $G = A(\mathbb{F}_q)$.
  - Lattices, NTRU (1996), Ideal Lattices (2006): perturbate a lattice point/Closest Vector Problem, Bounded Distance Decoding.
  - Polynomial systems, HFE (1996): evaluating polynomials/finding roots.
  - Coding-based cryptography, McEliece (1978): Matrix.vector/decoding a linear code.

  $\Rightarrow$ Encryption, Signature (+Pseudo Random Number Generator, Zero Knowledge).
- Pairing-based cryptography (2000–2001).
- Homomorphic cryptography (2009).

RSA versus (H)ECC

Security (bits level)	RSA	ECC
72	1008	144
80	1248	160
96	1776	192
112	2432	224
128	3248	256
256	15424	512

Key length comparison between RSA and ECC

- Factorisation of a 768-bit RSA modulus [Kle+10].
- Currently: attempt to attack a 130-bit Koblitz elliptic curve.

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).
- $G = \mathbb{F}_p^*$: sub-exponential attacks.

$\Rightarrow$ Find secure groups with efficient law, compact representation.

Protocol [Diffie–Hellman Key Exchange]

Alice sends g^a, Bob sends g^b, the common key is

$$g^{ab} = (g^b)^a = (g^a)^b.$$

Pairing-based cryptography

Definition

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

- Identity-based cryptography [BF03].
- Short signature [BLS04].
- One way tripartite Diffie–Hellman [Jou04].
- Self-blindable credential certificates [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [Goy+06].

Tripartite Diffie–Helman

Alice sends g^a, Bob sends g^b, Charlie sends g^c. The common key is

$$e(g,g)^{abc} = e(g^b, g^c)^a = e(g^c, g^a)^b = e(g^a, g^b)^c \in G_2.$$

Outline

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.

$\Rightarrow$ Use $G = A(k)$ with $k = \mathbb{F}_q$ for the DLP.

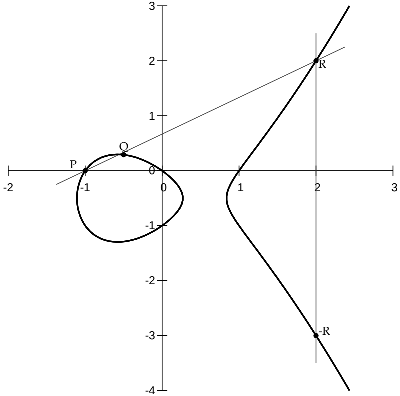
$\Rightarrow$ Pairing-based cryptography with the Weil or Tate pairing.
(Only available on abelian varieties.)

Elliptic curves

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

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

- An elliptic curve is a plane curve of genus 1.
- Elliptic curves = Abelian varieties of dimension 1.



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

Jacobian of hyperelliptic curves

$C : y^2 = f(x)$, hyperelliptic curve of genus g. $(\deg f = 2g - 1)$

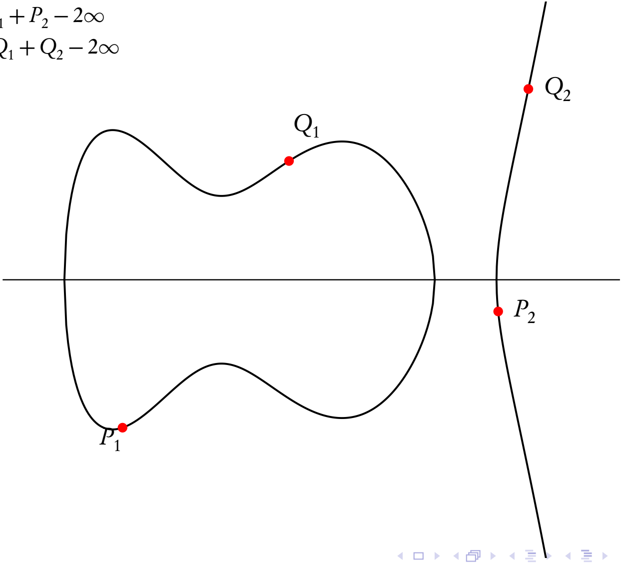
- Divisor: formal sum $D = \sum n_i P_i$, $P_i \in C(\overline{k})$.
  $\deg D = \sum n_i$.
- Principal divisor: $\sum_{P \in C(\overline{k})} v_P(f).P$; $f \in \overline{k}(C)$.
- Jacobian of C = Divisors of degree 0 modulo principal divisors
  = Abelian variety of dimension g.
- Divisor class $D \Rightarrow$ unique representative (Riemann–Roch):

$$D = \sum_{i=1}^{k} (P_i - P_\infty) \qquad k \leqslant g, \quad \text{symmetric } P_i \neq P_j$$

- Mumford coordinates: $D = (u, v) \Rightarrow u = \prod (x - x_i),\ v(x_i) = y_i$.
- Cantor algorithm: addition law.

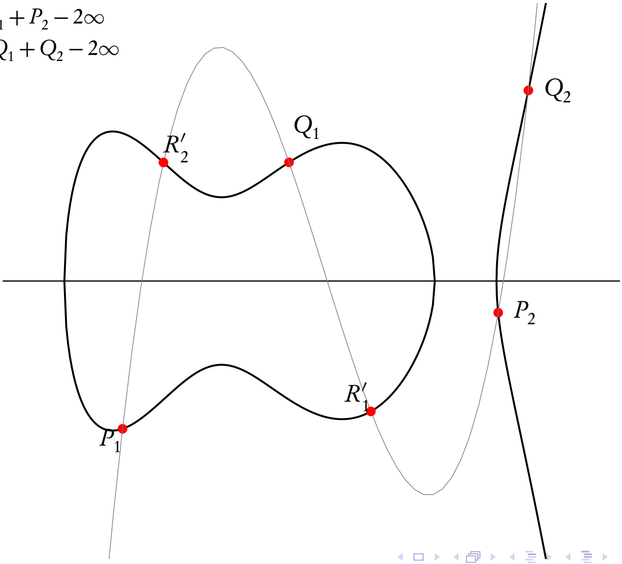
Example of the addition law in genus 2

$$D = P_1 + P_2 - 2\infty$$
$$D' = Q_1 + Q_2 - 2\infty$$



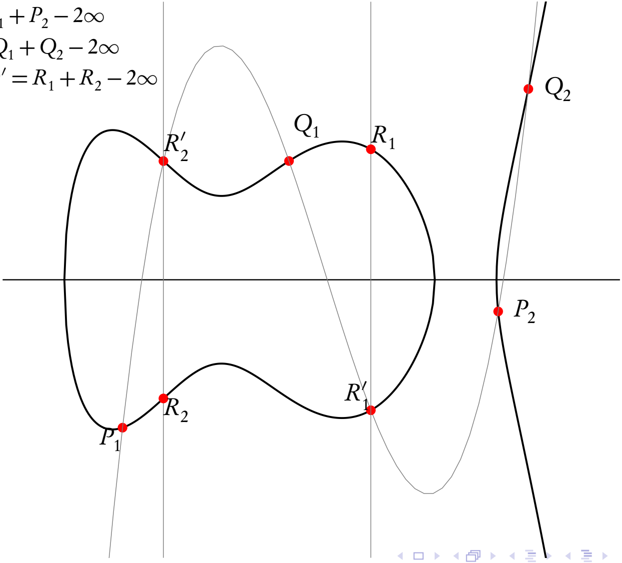
Example of the addition law in genus 2

$$D = P_1 + P_2 - 2\infty$$
$$D' = Q_1 + Q_2 - 2\infty$$



Example of the addition law in genus 2

$D = P_1 + P_2 - 2\infty$
$D' = Q_1 + Q_2 - 2\infty$
$D + D' = R_1 + R_2 - 2\infty$



Security of Jacobians

g	# points	DLP
1	$O(q)$	$\widetilde{O}(q^{1/2})$
2	$O(q^2)$	$\widetilde{O}(q)$
3	$O(q^3)$	$\widetilde{O}(q^{4/3})$ (Jacobian of hyperelliptic curve)
		$\widetilde{O}(q)$ (Jacobian of non hyperelliptic curve)
g	$O(q^g)$	$\widetilde{O}(q^{2-2/g})$
$g > \log(q)$		$L_{1/2}(q^g) = \exp(O(1)\log(x)^{1/2}\log\log(x)^{1/2})$

Security of the DLP

- Weak curves (MOV attack, Weil descent, anomal curves).

⇒ Public-key cryptography with the DLP: Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

⇒ Pairing-based cryptography: Abelian varieties of dimension $g \leqslant 4$.

Security of Jacobians

g	# points	DLP
1	$O(q)$	$\widetilde{O}(q^{1/2})$
2	$O(q^2)$	$\widetilde{O}(q)$
3	$O(q^3)$	$\widetilde{O}(q^{4/3})$ (Jacobian of hyperelliptic curve)
		$\widetilde{O}(q)$ (Jacobian of non hyperelliptic curve)
g	$O(q^g)$	$\widetilde{O}(q^{2-2/g})$
$g > \log(q)$		$L_{1/2}(q^g) = \exp(O(1)\log(x)^{1/2}\log\log(x)^{1/2})$

Security of the DLP

- Weak curves (MOV attack, Weil descent, anomal curves).

$\Rightarrow$ Public-key cryptography with the DLP: Elliptic curves, Jacobian of hyperelliptic curves of genus 2.

$\Rightarrow$ Pairing-based cryptography: Abelian varieties of dimension $g \leqslant 4$.

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.

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

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

Cryptographic usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms (ℓ-adic or p-adic) $\Rightarrow$ Verify a curve is secure.
- Compute the class field polynomials (CM-method) $\Rightarrow$ Construct a secure curve.
- Compute the modular polynomials $\Rightarrow$ Compute isogenies.
- Determine $\mathrm{End}(A)$ $\Rightarrow$ CRT method for class field polynomials.

Vélu's formula

Theorem

Let $E : y^2 = f(x)$ be an elliptic curve and $G \subset E(k)$ a finite subgroup. Then E/G is given by $Y^2 = g(X)$ where

$$X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} (x(P+Q) - x(Q))$$
$$Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} (y(P+Q) - y(Q)).$$

- Uses the fact that x and y are characterised in $k(E)$ by

$$\begin{aligned} v_{0_E}(x) &= -2 & \quad v_P(x) \geqslant 0 \quad \text{if } P \neq 0_E \\ v_{0_E}(y) &= -3 & \quad v_P(y) \geqslant 0 \quad \text{if } P \neq 0_E \\ y^2/x^3(0_E) &= 1 \end{aligned}$$

- No such characterisation in genus $g \geqslant 2$.

The modular polynomial

Definition

- Modular polynomial $\phi_n(x,y) \in \mathbb{Z}[x,y]$: $\phi_n(x,y) = 0 \Leftrightarrow x = j(E)$ and $y = j(E')$ with E and E' n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\phi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes.

$\Rightarrow$ Genus 2: $(2,2)$-isogenies [Richelot]. Genus 3: $(2,2,2)$-isogenies [Smi09].

$\Rightarrow$ Moduli space given by invariants with more structure.

$\Rightarrow$ Fix the form of the isogeny and look for compatible coordinates.

The modular polynomial

Definition

- Modular polynomial $\phi_n(x,y) \in \mathbb{Z}[x,y]$: $\phi_n(x,y) = 0 \Leftrightarrow x = j(E)$ and $y = j(E')$ with E and E' n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\phi_n(j(E),.) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes.

$\Rightarrow$ Genus 2: $(2,2)$-isogenies [Richelot]. Genus 3: $(2,2,2)$-isogenies [Smi09].

$\Rightarrow$ Moduli space given by invariants with more structure.

$\Rightarrow$ Fix the form of the isogeny and look for compatible coordinates.

Outline

Complex abelian varieties and theta functions of level n

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

Example ($k = \mathbb{C}$)

Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$; $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space (Ω symmetric, $\operatorname{Im}\Omega$ positive definite).

$$\vartheta_i := \Theta\left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](z, \Omega/n).$$

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

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

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

Arithmetic with low level theta functions (car $k \neq 2$)

	Mumford [Lan05]	Level 2 [Gau07]	Level 4
Doubling	$34M + 7S$	$7M + 12S + 9m_0$	$49M + 36S + 27m_0$
Mixed Addition	$37M + 6S$		

Multiplication cost in genus 2 (one step).

	Montgomery	Level 2	Jacobians	Level 4
Doubling	$5M + 4S + 1m_0$	$3M + 6S + 3m_0$	$3M + 5S$	$9M + 10S + 5m_0$
Mixed Addition			$7M + 6S + 1m_0$	

Multiplication cost in genus 1 (one step).

Arithmetic with high level theta functions [LR10a]

- Algorithms for
  - Additions and differential additions in level 4.
  - Computing $P \pm Q$ in level 2 (need one square root). [LR10b]
  - Fast differential multiplication.
- Compressing coordinates $O(1)$:
  - Level $2n$ theta null point $\Rightarrow 1 + g(g+1)/2$ level 2 theta null points.
  - Level $2n \Rightarrow 1 + g$ level 2 theta functions.
- Decompression: n^g differential additions.

Outline

Pairings on abelian varieties

E/k: elliptic curve.

- Weil pairing: $E[\ell] \times E[\ell] \to \mu_\ell$.

  $P, Q \in E[\ell]$. $\exists f_{\ell,P} \in k(E), (f_{\ell,P}) = \ell(P - 0_E)$.

$$e_{W,\ell}(P,Q) = \frac{f_{\ell,P}(Q - 0_E)}{f_{\ell,Q}(P - 0_E)}.$$

- Tate pairing: $e_{T,\ell}(P,Q) = f_{\ell,P}(Q - 0_E)$.
- Miller algorithm: pairing with Mumford coordinates.

The Weil and Tate pairing with theta coordinates [LR10b]

P and Q points of ℓ-torsion.

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

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

Comparison with Miller algorithm

$g=1$	$7\mathbf{M}+7\mathbf{S}+2\mathbf{m_0}$
$g=2$	$17\mathbf{M}+13\mathbf{S}+6\mathbf{m_0}$

Tate pairing with theta coordinates, $P, Q \in A[\ell](\mathbb{F}_{q^d})$ (one step)

		Miller		Theta coordinates
		Doubling	Addition	One step
$g=1$	d even	$1\mathbf{M}+1\mathbf{S}+1\mathbf{m}$	$1\mathbf{M}+1\mathbf{m}$	$1\mathbf{M}+2\mathbf{S}+2\mathbf{m}$
	d odd	$2\mathbf{M}+2\mathbf{S}+1\mathbf{m}$	$2\mathbf{M}+1\mathbf{m}$	
$g=2$	Q degenerate + denominator elimination	$1\mathbf{M}+1\mathbf{S}+3\mathbf{m}$	$1\mathbf{M}+3\mathbf{m}$	$3\mathbf{M}+4\mathbf{S}+4\mathbf{m}$
	General case	$2\mathbf{M}+2\mathbf{S}+18\mathbf{m}$	$2\mathbf{M}+18\mathbf{m}$	

$P \in A[\ell](\mathbb{F}_q)$, $Q \in A[\ell](\mathbb{F}_{q^d})$ (counting only operations in $\mathbb{F}_{q^d}$).

Outline

The isogeny theorem

Theorem

- *Let* $\ell \wedge n = 1$, *and* $\phi : Z(\overline{n}) \to Z(\overline{\ell n}), x \mapsto \ell.x$ *be the canonical embedding.* *Let* $K_0 = A[\ell]_2 \subset A[\ell n]_2$.
- *Let* $(\vartheta_i^A)_{i \in Z(\overline{\ell n})}$ *be the theta functions of level* ℓn *on* $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$.
- *Let* $(\vartheta_i^B)_{i \in Z(\overline{n})}$ *be the theta functions of level* n *of* $B = A/K_0 = \mathbb{C}^g / (\mathbb{Z}^g + \frac{\Omega}{\ell} \mathbb{Z}^g)$.
- *We have:*
$$(\vartheta_i^B(x))_{i \in Z(\overline{n})} = (\vartheta_{\phi(i)}^A(x))_{i \in Z(\overline{n})}$$

Example

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

The modular space of theta null points of level n (car $k \nmid n$)

Definition

The modular space $\mathcal{M}_{\overline{n}}$ of theta null points is:

$$\sum_{t \in Z(\overline{2})} a_{x+t} a_{y+t} \sum_{t \in Z(\overline{2})} a_{u+t} a_{v+t} = \sum_{t \in Z(\overline{2})} a_{x'+t} a_{y'+t} \sum_{t \in Z(\overline{2})} a_{u'+t} a_{v'+t},$$

with the relations of symmetry $a_x = a_{-x}$.

- Abelian varieties with a n-structure = open locus of $\mathcal{M}_{\overline{n}}$.

Isogenies and modular correspondence [FLR09]

$$
\begin{tikzcd}
A_k, A_k[\ell n] = A_k[\ell n]_1 \oplus A_k[\ell n]_2 \arrow[d, shift left, "\pi"] & & (a_i)_{i \in Z(\overline{\ell n})} \in \mathcal{M}_{\overline{\ell n}}(k) \arrow[ll, dotted, "\text{determines}"'] \arrow[d, "\phi_1"] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\widehat{\pi}"] & & (b_i)_{i \in Z(\overline{n})} \in \mathcal{M}_{\overline{n}}(k) \arrow[ll, dotted]
\end{tikzcd}
$$

- Every isogeny (with isotropic kernel K) comes from a modular solution.
- We can detect degenerate solutions.

Isogenies and modular correspondence [FLR09]

$$
\begin{tikzcd}
A_k, A_k[\ell n] = A_k[\ell n]_1 \oplus A_k[\ell n]_2 \arrow[d, shift left, "\pi"] & & (a_i)_{i \in Z(\overline{\ell n})} \in \mathcal{M}_{\overline{\ell n}}(k) \arrow[ll, dotted, "\text{determines}"'] \arrow[d, "\phi_1"] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\widehat{\pi}"] & & (b_i)_{i \in Z(\overline{n})} \in \mathcal{M}_{\overline{n}}(k) \arrow[ll, dotted]
\end{tikzcd}
$$

- Every isogeny (with isotropic kernel K) comes from a modular solution.
- We can detect degenerate solutions.

Isogenies and modular correspondence [FLR09]

$$
\begin{array}{ccc}
A_k, A_k[\ell n] = A_k[\ell n]_1 \oplus A_k[\ell n]_2 & \underset{\text{determines}}{\longleftarrow\cdots\cdots} & (a_i)_{i \in Z(\overline{\ell n})} \in \mathcal{M}_{\overline{\ell n}}(k) \\
\widehat{\pi} \uparrow \downarrow \pi & & \downarrow \phi_1 \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 & \longleftarrow\cdots\cdots & (b_i)_{i \in Z(\overline{n})} \in \mathcal{M}_{\overline{n}}(k)
\end{array}
$$

- Every isogeny (with isotropic kernel K) comes from a modular solution.
- We can detect degenerate solutions.

The contragredient isogeny [LR10a]

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\widehat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell.x$$

The contragredient isogeny [LR10a]

$$\begin{tikzcd}[column sep=small] x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\widehat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell.x$$

The contragredient isogeny [LR10a]

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\widehat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

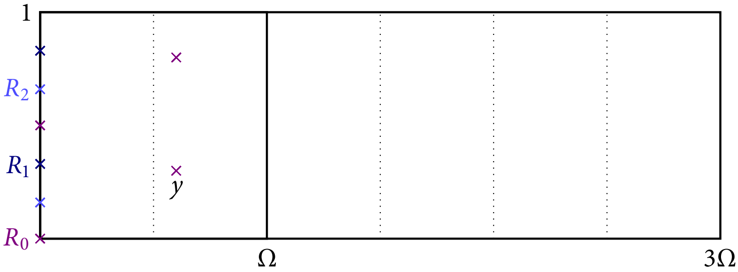
$$\widehat{\pi}(y) = \ell.x$$

The contragredient isogeny [LR10a]

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell.x$$

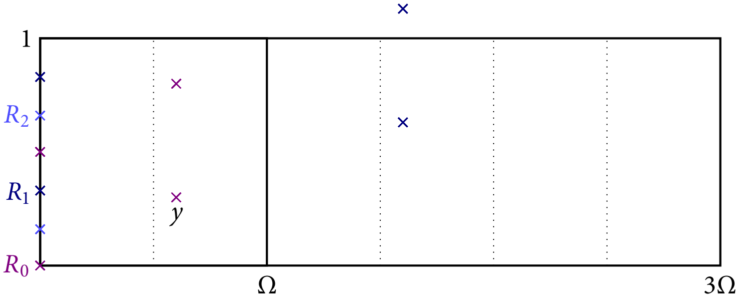


The contragredient isogeny [LR10a]

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$

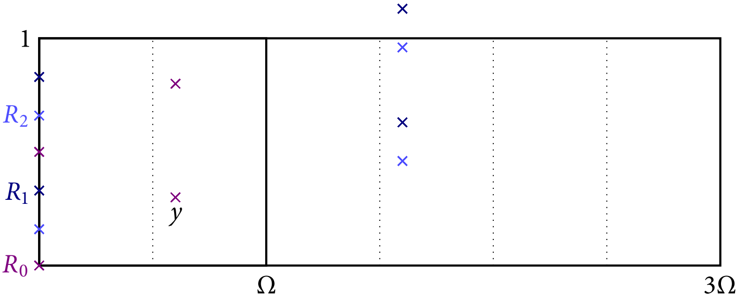


The contragredient isogeny [LR10a]

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\widehat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$

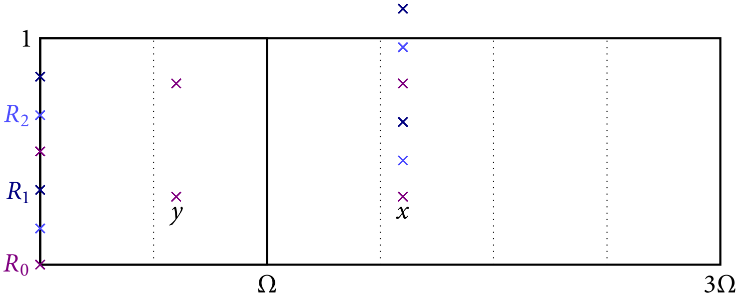


The contragredient isogeny [LR10a]

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\widehat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$



The contragredient isogeny [LR10a]

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\widehat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$

Explicit isogenies algorithm

- (Compressed) modular point from K: $g(g+1)/2$ ℓ^{th}-roots and $g(g+1)/2 \cdot O(\log(\ell))$ chain additions.

$\Rightarrow$ (Compressed) isogeny: $g \cdot O(\log(\ell))$ chain additions.

Example

- B: elliptic curve $y^2 = x^3 + 23x + 3$ over $k = \mathbb{F}_{31}$

  $\Rightarrow$ Theta null point of level 4: $(3 : 1 : 18 : 1) \in \mathcal{M}_4(\mathbb{F}_{31})$.
- $K = \{(3 : 1 : 18 : 1), (22 : 15 : 4 : 1), (18 : 29 : 23 : 1)\} \Rightarrow$ modular solution:

  $(3, \eta^{14233}, \eta^{2317}, 1, \eta^{1324}, \eta^{5296}, 18, \eta^{5296}, \eta^{1324}, 1, \eta^{2317}, \eta^{14233}) \quad (\eta^3 + \eta + 28 = 0)$.
- $y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1); \quad \widehat{\pi}(y)$?

Example

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y \oplus R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

Example

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y \oplus R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

$$y + 2R_1 = \lambda_1^2(\eta^{28758}, \eta^{11337}, \eta^{27602}, \eta^{22972})$$

$$y + 3R_1 = \lambda_1^3(\eta^{18374}, \eta^{18773}, \eta^{9688}, \eta^{28758}) = y/\eta^{1032} \quad \text{so } \lambda_1^3 = \eta^{28758}$$

Example

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y \oplus R_1 = \lambda_1 (\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

$$y + 2R_1 = \lambda_1^2 (\eta^{28758}, \eta^{11337}, \eta^{27602}, \eta^{22972})$$
$$y + 3R_1 = \lambda_1^3 (\eta^{18374}, \eta^{18773}, \eta^{9688}, \eta^{28758}) = y/\eta^{1032} \quad \text{so } \lambda_1^3 = \eta^{28758}$$

$$2y + R_1 = \lambda_1^2 (\eta^{17786}, \eta^{12000}, \eta^{16630}, \eta^{365})$$
$$3y + R_1 = \lambda_1^3 (\eta^{7096}, \eta^{11068}, \eta^{8089}, \eta^{20005}) = \eta^{5772} R_1$$

Example

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y \oplus R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

$$y + 2R_1 = \lambda_1^2(\eta^{28758}, \eta^{11337}, \eta^{27602}, \eta^{22972})$$
$$y + 3R_1 = \lambda_1^3(\eta^{18374}, \eta^{18773}, \eta^{9688}, \eta^{28758}) = y/\eta^{1032} \quad \text{so } \lambda_1^3 = \eta^{28758}$$

$$2y + R_1 = \lambda_1^2(\eta^{17786}, \eta^{12000}, \eta^{16630}, \eta^{365})$$
$$3y + R_1 = \lambda_1^3(\eta^{7096}, \eta^{11068}, \eta^{8089}, \eta^{20005}) = \eta^{5772} R_1$$

$$\widehat{\pi}(y) = (3, \eta^{21037}, \eta^{15925}, 1, \eta^{8128}, \eta^{18904}, 18, \eta^{12100}, \eta^{14932}, 1, \eta^{9121}, \eta^{27841})$$

Changing level by taking an isogeny

$$\begin{tikzcd}
B \arrow[dd, "{[\ell]}"'] \arrow[dr, "\widehat{\pi}"] & & \\
 & A, A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \arrow[dl, "\pi"'] \arrow[dr, "\pi_2"] \arrow[d, equal] & \\
B = A/A[\ell]_2 & A & C = A/A[\ell]_1
\end{tikzcd}$$

- $\pi_2 \circ \widehat{\pi}$: ℓ^2 isogeny in level n.
- Modular points (corresponding to K) $\Leftrightarrow A[\ell] = A[\ell]_1 \oplus \widehat{\pi}(B[\ell])$
  $\Leftrightarrow \ell^2$-isogenies $B \to C$.
- Isogeny graphs: $B[\ell] \Rightarrow \ell^{2g}$ differential additions.

Changing level by taking an isogeny

$$\begin{tikzcd}
B \arrow[dd, "{[\ell]}"'] \arrow[dr, "\widehat{\pi}"] & & \\
 & A, A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \arrow[dl, "\pi"'] \arrow[d, equal] \arrow[dr, "\pi_2"] & \\
B = A/A[\ell]_2 & A & C = A/A[\ell]_1
\end{tikzcd}$$

- $\pi_2 \circ \widehat{\pi}$: ℓ^2 isogeny in level n.
- Modular points (corresponding to K) $\Leftrightarrow A[\ell] = A[\ell]_1 \oplus \widehat{\pi}(B[\ell])$
  $\Leftrightarrow \ell^2$-isogenies $B \to C$.
- Isogeny graphs: $B[\ell] \Rightarrow \ell^{2g}$ differential additions.

Changing level without taking isogenies

Theorem (Koizumi-Kempf)

- *Let $\mathcal{L}$ be the space of theta functions of level ℓn and $\mathcal{L}'$ the space of theta functions of level n.*
- *Let $F \in \mathrm{M}_r(\mathbb{Z})$ be such that ${}^tFF = \ell \,\mathrm{Id}$, and $f : A^r \to A^r$ the corresponding isogeny.*

We have $\mathcal{L} = f^* \mathcal{L}'$ and the isogeny f is given by

$$f^*(\vartheta_{i_1}^{\mathcal{L}'} \star \ldots \star \vartheta_{i_r}^{\mathcal{L}'}) = \lambda \sum_{\substack{(j_1,\ldots,j_r) \in K_1(\mathcal{L}') \times \ldots \times K_1(\mathcal{L}') \\ f(j_1,\ldots,j_r) = (i_1,\ldots,i_r)}} \vartheta_{j_1}^{\mathcal{L}} \star \ldots \star \vartheta_{j_r}^{\mathcal{L}}$$

- $F = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ gives the Riemann relations. (For general ℓ, use the quaternions.)

$\Rightarrow$ Go up and down in level without taking isogenies [Cosset+R].

A complete generalisation of Vélu's algorithm [Cosset+R]

- Compute the isogeny $B \to A$ while staying in level n.
- No need of ℓ-roots. Need only $O(\#K)$ differential additions in B + $O(\ell^g)$ or $O(\ell^{2g})$ multiplications $\Rightarrow$ fast.
- The formulas are rational if the kernel K is rational.
- Blocking part: compute $K \Rightarrow$ compute all the ℓ-torsion on B. $g = 2$: ℓ-torsion, $\widetilde{O}(\ell^6)$ vs $O(\ell^2)$ for the isogeny.

$\Rightarrow$ Work in level 2.

$\Rightarrow$ Convert back and forth to Mumford coordinates:

$$\begin{tikzcd} B \arrow[r, "\widehat{\pi}"] \arrow[d, equal] & A \arrow[d, equal] \\ \mathrm{Jac}(C_1) \arrow[r, dotted] & \mathrm{Jac}(C_2) \end{tikzcd}$$

Example

The Igusa j-invariants $(3908, 2195, 648)$ correspond to an hyperelliptic curve over $\mathbb{F}_{4217}$ 1069-isogeneous to itself.

Outline

An improved modular correspondence?

$$
\begin{tikzcd}
 & \mathcal{M}_{\overline{\ell n}} \arrow[d] & \\
 & \mathcal{M}_{\overline{\ell n}}/\mathfrak{H}_1 \arrow[dl, "\phi_1"'] \arrow[d] \arrow[dr, "\phi_2"] & \\
\mathcal{M}_{\overline{n}} & \mathcal{M}_{\overline{\ell n}}/\mathfrak{H} \simeq \mathcal{M}_{\overline{n}}(\ell) \arrow[l] \arrow[d, "\text{Forget}"] & \mathcal{M}_{\overline{n}} \\
 & \mathcal{M}_{\overline{n}} &
\end{tikzcd}
$$

- $\# B_k[\ell] = \ell^{2g}$.
- Isotropic subspaces: $O(\ell^{g(g+1)/2})$.
- Modular solutions $\# \phi_1^{-1}((b_i)_{i \in Z(\overline{n})}) = O(\ell^{2g^2+g})$.

Linking theta null points and Jacobians

- Thomae formulas ⇒ link between Jacobian of hyperelliptic curves and theta functions.
- Equivalent for non hyperelliptic curves [She08]?

Application

Extends [Smi09] attack on hyperelliptic genus 3 curves.

Some more applications

- Explicit isogeny computation ⇒ endomorphism ring, Hilbert class polynomials.
- Modular space in level 2 and equations for the Kummer varieties.
- Improve the algorithm [CL08] for computing theta null points of the canonical lift of an ordinary abelian variety ⇒ point counting in small characteristic.
- Improve the pairing algorithm (Ate pairing).
- Faster additions law (level 3 theta functions, level $(2,4)$ in genus 2).
- Characteristic 2 [GL09].

The end

```
           /*   CARAMEL   */                  C,A,
           /*             */                 R,a,
           /*             */                M,E,
                                            L,i=
                                           5,e,
    d[5],Q[999                    ]={0};main(N          ){for
  (;i--;e=scanf("%"             "d",d+i));for(A         =*d;
 ++i<A          ;++Q[         i*i%          A],R=      i[Q]?
R:i);             for(;i     --;)            for(M     =A;M
--;N              +=!M*Q     [E%A            ],e+=     Q[(A
+E*E-            R*L*         L%A)           %A])       for(
  E=i,L=M,a=4;a;C=             i*E+R*M*L,L=(M*E         +i*L)
    %A,E=C%A+a                  --[d]);printf            ("%d"
                                                          "\n",
                                                           (e+N*
                                                             N)/2
     /* cc caramel.c; echo f3 f2 f1 f0 p | ./a.out */        -A);}
```

Thank you for your attention!

Bibliography

[BF03] 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. 7).

[BLS04] 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. 7).

[CL08] R. Carls and D. Lubicz. "A p-adic quasi-quadratic time and quadratic space point counting algorithm". In: *International Mathematics Research Notices* (2008). (Cit. on p. 57).

[FLR09] Jean-Charles Faugère, David Lubicz, and Damien Robert. *Computing modular correspondences for abelian varieties*. May 2009. arXiv: 0910.4668. (Cit. on pp. 34–36).

[Gau07] P. Gaudry. "Fast genus 2 arithmetic based on Theta functions". In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265. (Cit. on p. 25).

[GL09] P. Gaudry and D. Lubicz. "The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines". In: *Finite Fields and Their Applications* 15.2 (2009), pp. 246–260. (Cit. on p. 57).

[Goy+06] V. Goyal et al. "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. 7).

[Jou04] A. Joux. "A one round protocol for tripartite Diffie–Hellman". In: *Journal of Cryptology* 17.4 (2004), pp. 263–276. (Cit. on p. 7).

[Kle+10] T. Kleinjung et al. "Factorization of a 768-bit RSA modulus". In: (2010). (Cit. on p. 5).

[Lan05] T. Lange. "Formulae for arithmetic on genus 2 hyperelliptic curves". In: *Applicable Algebra in Engineering, Communication and Computing* 15.5 (2005), pp. 295–328. (Cit. on p. 25).

[LR10a] David Lubicz and Damien Robert. *Computing isogenies between abelian varieties*. Jan. 2010. arXiv: 1001.2016. (Cit. on pp. 26, 37–44).

[LR10b] David Lubicz and Damien Robert. *Efficient pairing computation with theta functions*. Ed. by Guillaume Hanrot, François Morain, and Emmanuel Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Jan. 2010. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. (Cit. on pp. 26, 29).

[SW05] A. Sahai and B. Waters. "Fuzzy identity-based encryption". In: *Advances in Cryptology–EUROCRYPT 2005* (2005), pp. 457–473. (Cit. on p. 7).

[She08] N. Shepherd-Barron. "Thomae's formulae for non-hyperelliptic curves and spinorial square roots of theta-constants on the moduli space of curves". In: (2008). (Cit. on p. 56).

[Smi09] Benjamin Smith. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*. Feb. 2009. arXiv: 0806.2995. (Cit. on pp. 20, 21, 56).

[Ver01] E. Verheul. "Self-blindable credential certificates from the Weil pairing". In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 533–551. (Cit. on p. 7).