Abelian varieties, theta functions and cryptography

Part 2

Damien Robert[1]

[1]LFANT team, INRIA Bordeaux Sud-Ouest

08/12/2010 (Bordeaux)

Outline

Outline

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).

$\Rightarrow$ Public key cryptography

$\Rightarrow$ Signature

$\Rightarrow$ Zero knowledge

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

$\Rightarrow$ Use $G = A(\mathbb{F}_q)$ where $A/\mathbb{F}_q$ is an abelian variety for the DLP.

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].

Example

The Weil and Tate pairings on abelian varieties are the only known examples of cryptographic pairings.

Security of abelian varieties

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 abelian varieties

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.

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

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

Cryptographic usage of isogenies

- Transfert 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.

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. $(Z(\overline{n}) \coloneqq \mathbb{Z}^g / n\mathbb{Z}^g)$
  $\Leftrightarrow A[n] = A_1[n] \oplus A_2[n]$: 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).

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

Jacobian of hyperelliptic curves

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

- 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 $D \Rightarrow$ 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.
- Thomae formula: convert between Mumford and theta coordinates of level 2 or 4.

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

Theorem (Mumford)

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 $\mathcal{M}_{\overline{n}}$.
- If $(a_u)_{u\in Z(\overline{n})}$ is a valid theta null point, the corresponding abelian variety is given by the following equations in $\mathbb{P}_k^{n^g-1}$:

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

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

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

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

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

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

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

Outline

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

1. Abelian varieties and cryptography
2. Theta functions
3. Arithmetic
4. Pairings
5. Isogenies
6. Perspectives

Explicit isogeny computation

- Given an isotropic subgroup $K \subset A(\overline{k})$ compute the isogeny $A \mapsto A/K$. (Vélu's formula.)
- Given an abelian variety compute all the isogeneous varieties. (Modular polynomials.)
- Given two isogeneous abelian variety A and B find the isogeny $A \mapsto B$. (Clever use of Vélu's formula $\Rightarrow$ SEA algorithm).

Explicit isogeny computation

- Given an isotropic subgroup $K \subset A(\overline{k})$ compute the isogeny $A \mapsto A/K$. (Vélu's formula.)
- Given an abelian variety compute all the isogeneous varieties. (Modular polynomials.)
- Given two isogeneous abelian variety A and B find the isogeny $A \mapsto B$. (Clever use of Vélu's formula $\Rightarrow$ SEA algorithm).

Explicit isogeny computation

- Given an isotropic subgroup $K \subset A(\overline{k})$ compute the isogeny $A \mapsto A/K$. (Vélu's formula.)
- Given an abelian variety compute all the isogeneous varieties. (Modular polynomials.)
- Given two isogeneous abelian variety A and B find the isogeny $A \mapsto B$. (Clever use of Vélu's formula $\Rightarrow$ SEA algorithm).

Explicit isogeny computation

- Given an isotropic subgroup $K \subset A(\overline{k})$ compute the isogeny $A \mapsto A/K$. (Vélu's formula.)
- Given an abelian variety compute all the isogeneous varieties. (Modular polynomials.)
- Given two isogeneous abelian variety A and B find the isogeny $A \mapsto B$. (Clever use of Vélu's formula $\Rightarrow$ SEA algorithm).

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

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

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

The isogeny theorem

Theorem (Mumford)

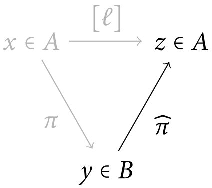
- *Let* $\ell \wedge n = 1$, *and* $\phi : Z(\overline{n}) \to Z(\overline{\ell n}), x \mapsto \ell.x$ *be the canonical embedding. Let* $K_0 = A[\ell]_2 \subset A[\ell n]_2$.
- *Let* $(\vartheta_i^A)_{i \in Z(\overline{\ell n})}$ *be the theta functions of level* ℓn *on* $A = \mathbb{C}^g/(\mathbb{Z}^g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

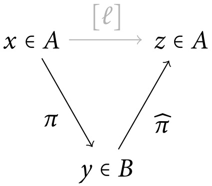
The contragredient isogeny [LR10a]



Let $\pi : A \rightarrow B$ 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

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

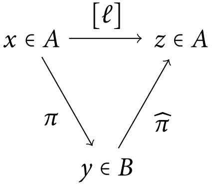
The contragredient isogeny [LR10a]



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

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

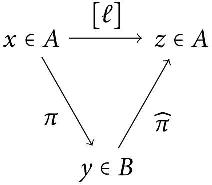
The contragredient isogeny [LR10a]



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

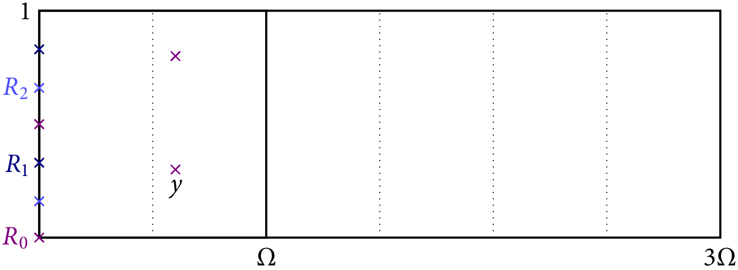
$$\widehat{\pi}(y) = \ell . x$$

The contragredient isogeny [LR10a]

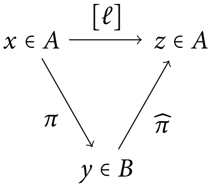


Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

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

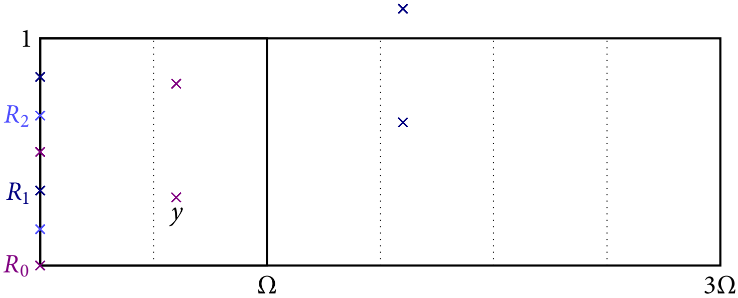


The contragredient isogeny [LR10a]

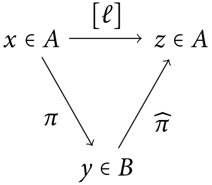


Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

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

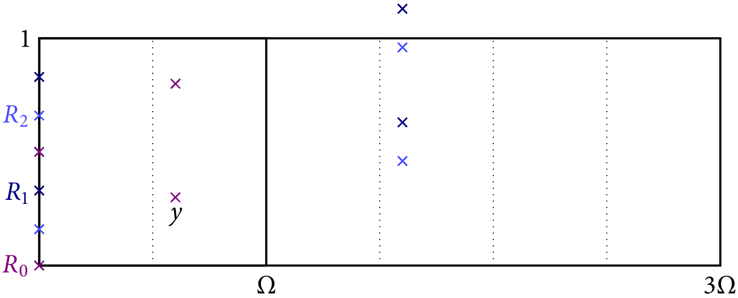


The contragredient isogeny [LR10a]

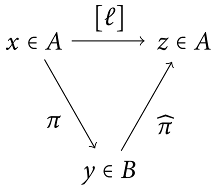


Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

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

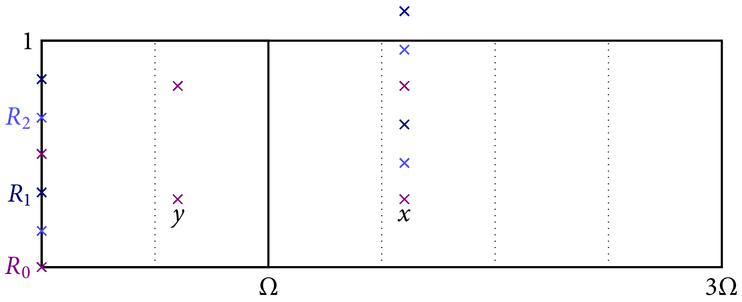


The contragredient isogeny [LR10a]



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

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



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 $F \in_r (\mathbb{Z})$ be such that ${}^t FF = \ell \operatorname{Id}$, and $f : A^r \to A^r$ the corresponding isogeny.*

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

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

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

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

Changing level and isogenies

Corollary

Let $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ *and* $B = \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g)$*. We can express the isogeny* $A \to B, z \mapsto \ell z$ *of kernel* $K = \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$ *in term of the theta functions of level* n *on* A *and* B*:*

$$\vartheta\left[\begin{smallmatrix}0\\i_1\end{smallmatrix}\right](\ell z, \ell\frac{\Omega}{n})\vartheta\left[\begin{smallmatrix}0\\i_2\end{smallmatrix}\right](0, \ell\frac{\Omega}{n})\ldots\vartheta\left[\begin{smallmatrix}0\\i_r\end{smallmatrix}\right](0, \ell\frac{\Omega}{n}) = \sum_{\substack{t_1,\ldots,t_r\in K\\F(t_1,\ldots,t_r)=(0,\ldots,0)}} \vartheta\left[\begin{smallmatrix}0\\j_1\end{smallmatrix}\right](X_1 + t_1, \frac{\Omega}{n})\ldots\vartheta\left[\begin{smallmatrix}0\\j_r\end{smallmatrix}\right]^{\mathcal{L}}(X_r + t_r, \frac{\Omega}{n}),$$

where $X = F^{-1}(\ell z, 0, \ldots, 0)$.

Remark

We compute the coordinates $\vartheta\left[\begin{smallmatrix}0\\j_i\end{smallmatrix}\right](X_i + t_i, \frac{\Omega}{n})$ *not in* A *but in* $\mathbb{C}^g$ *thanks to the differential additions.*

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

- Compute the isogeny $B \to A$ while staying in level n.
- $O(\ell^g)$ differential additions + $O(\ell^g)$ or $O(\ell^{2g}$ for the changing level.
- 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 $O(\ell^2)$ or $O(\ell^4)$ for the isogeny.

$\Rightarrow$ Work in level 2.

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

$$\begin{array}{ccc} B & \xrightarrow{\widehat{\pi}} & A \\ \| & & \| \\ \mathrm{Jac}(C_1) & \dashrightarrow & \mathrm{Jac}(C_2) \end{array}$$

Outline

The AGM and canonical lifts

- The elliptic curves $E_n : y^2 = x(x - a_n^2)(x - b_n^2)$ converges over $\mathbb{Q}_{2^\alpha}$ to the canonical lift of $(E_0)_{\mathbb{F}_{2^\alpha}}$ [Mes01], where $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ satisfy the Arithmetic Geometric Mean:

$$a_{n+1} = \frac{a_n + b_n}{2}$$
$$b_{n+1} = \sqrt{a_n b_n}$$

- Generalized in all genus by looking at theta null points [Mes02].
- Generalized in arbitrary characteristic p by [CL08] by looking at modular relations of degree p^2 on theta null points.

$\Rightarrow$ Point counting.

$\Rightarrow$ Class polynomials.

Some perspectives

- Improve the pairing algorithm (Ate pairing,optimal ate).
- Characteristic 2 [GL09].
- A SEA-like algorithm in genus 2?

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.

[BLS04] D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the Weil pairing". In: *Journal of Cryptology* 17.4 (2004), pp. 297–319.

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

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

[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.

[Goy+06] 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.

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

[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.

[LR10a] D. Lubicz and D. Robert. *Computing isogenies between abelian varieties*. HAL http://hal.archives-ouvertes.fr/hal-00446062/. Jan. 2010. arXiv:1001.2016. URL: http://www.normalesup.org/~robert/pro/publications/articles/isogenies.pdf.

[LR10b] D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: Lecture Notes in Comput. Sci. 6197 (Jan. 2010). Ed. by G. Hanrot, F. Morain, and E. Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. 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.

[Mes01] J.-F. Mestre. *Lettre à Gaudry et Harley*. 2001. URL: http://www.math.jussieu.fr/mestre.

[Mes02] J.-F. Mestre. *Notes of a talk given at the Cryptography Seminar Rennes*. 2002. URL: http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps.

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

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