Abelian varieties, Theta functions and cryptography

MSR presentation

Damien Robert[1]

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

07/07/2010 (MSR)

Outline

Outline

A brief history of 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): Closest Vector Problem, Bounded Distance Decoding.
- Polynomial systems, HFE (1996): evaluating polynomials/finding roots.
- Coding-based cryptography, McEliece (1978): decoding a linear code.

⇒ 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).

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

$\Rightarrow$ $G = \mathbb{F}_q^*$: subexponential attacks.

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.

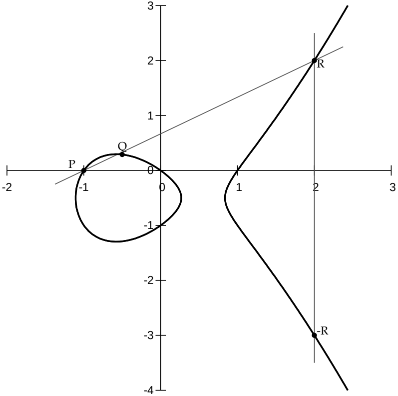
$\Rightarrow$ Pairing-based cryptography with the Weil or Tate pairing. (Only available on abelian varieties.)

Elliptic curves

Definition (car $k \neq 2$)

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

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



$$P + Q = -R = (x_R, -y_R)$$

$$\lambda = \frac{y_Q - y_P}{x_P - x_Q}$$

$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = y_P + \lambda(x_R - x_P)$$

Jacobian of hyperelliptic curves

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

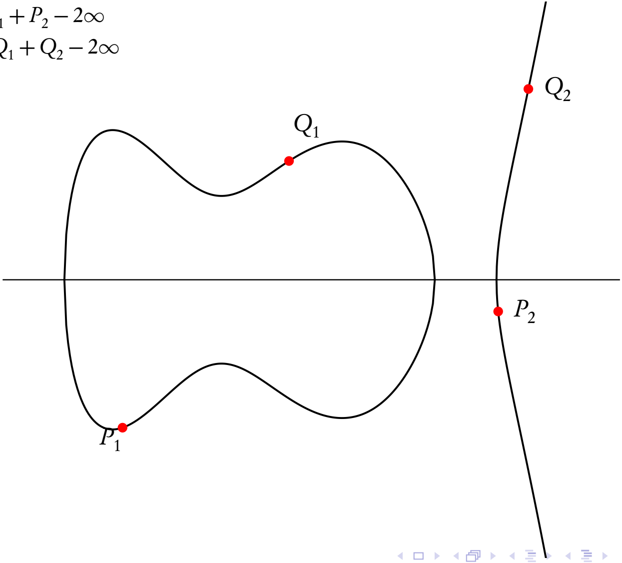
- Divisor: formal sum $D = \sum n_i P_i$, $P_i \in C(\overline{k})$.
  $\deg D = \sum n_i$.
- Principal divisor: $\sum_{P \in C(\overline{k})} v_P(f).P$; $f \in \overline{k}(C)$.
- Jacobian of C = Divisors of degree 0 modulo principal divisors
  = Abelian variety of dimension g.
- Mumford coordinates:

$$D = \sum_{i=1}^{k} (P_i - P_\infty) \qquad k \leqslant g, \quad \text{symmetric } P_i \neq P_j$$
$$= (u, v) \text{ with } u = \prod (x - x_i), v(x_i) = y_i.$$

- Cantor algorithm: addition law.

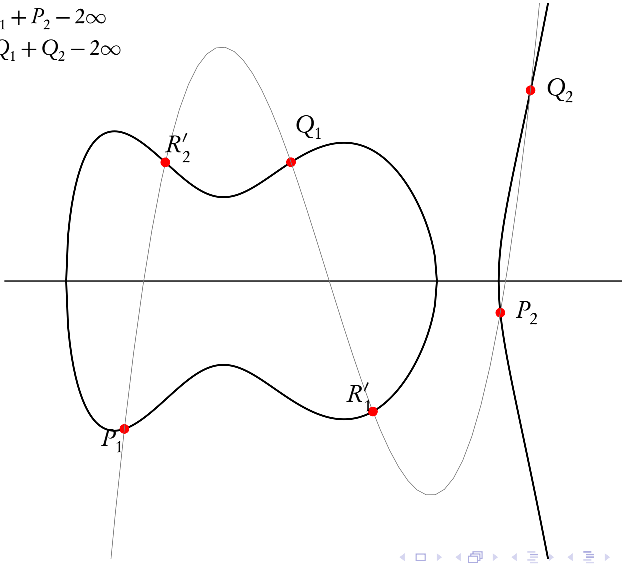
Exemple of the addition law in genus 2

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

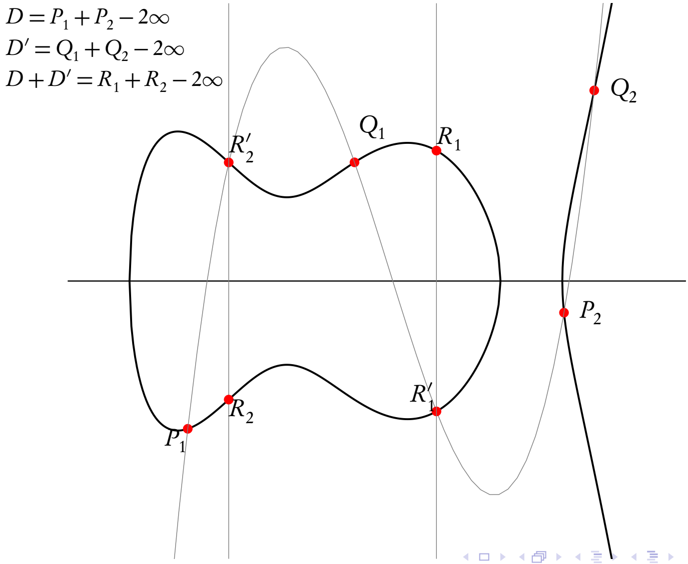


Exemple of the addition law in genus 2

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



Exemple of the addition law in genus 2



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 $g > \log(q)$	$O(q^g)$	$\widetilde{O}(q^{2-2/g})$ $L_{1/2}(q^g) = \exp(O(1)\log(x)^{1/2}\log\log(x)^{1/2})$

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).

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

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

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 ($\Rightarrow \ell$-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.

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 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], more recently $(3,3)$-isogenies [BGL09]. Genus 3: $(2,2,2)$-isogenies [Smi09].

Outline

Complex abelian varieties

- 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).
- Theta functions with characteristic:

$$\vartheta(z,\Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i \, {}^t n \Omega n + 2\pi i \, {}^t n z},$$

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

- $(\vartheta_i)_{i \in Z(\overline{n})}$: basis of the theta functions of level n. $(Z(\overline{n}) \coloneqq \mathbb{Z}^g / n\mathbb{Z}^g)$.

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

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	Level $(2,4)$
Doubling	$34M + 7S$	$7M + 12S + 9m_0$	$49M + 36S + 27m_0$	$21M + 20S + 15m_0$
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).

Pairings on abelian varieties

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

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

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

- 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

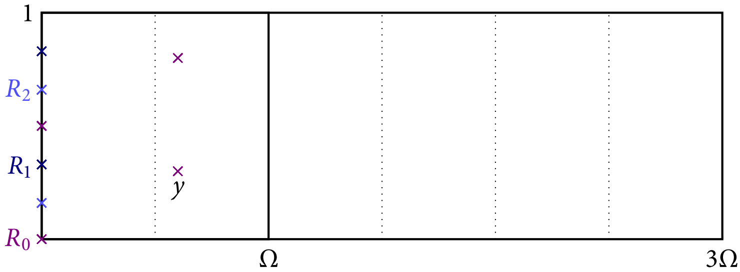
$g = 1$	$7\mathbf{M} + 7\mathbf{S} + 2\mathbf{m_0}$
$g = 2$	$17\mathbf{M} + 13\mathbf{S} + 6\mathbf{m_0}$

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

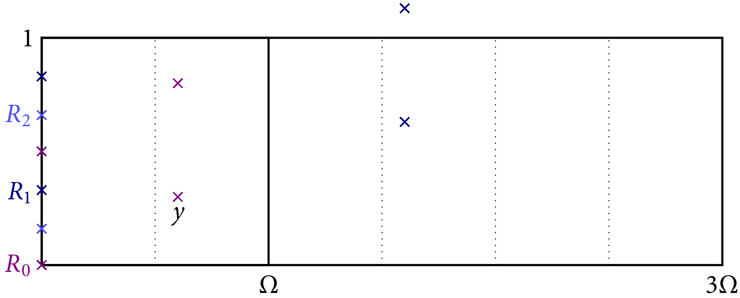
		Miller		Theta coordinates
		Doubling	Addition	One step
$g = 1$	d even	$1\mathbf{M} + 1\mathbf{S} + 1\mathbf{m}$	$1\mathbf{M} + 1\mathbf{m}$	$1\mathbf{M} + 2\mathbf{S} + 2\mathbf{m}$
	d odd	$2\mathbf{M} + 2\mathbf{S} + 1\mathbf{m}$	$2\mathbf{M} + 1\mathbf{m}$	
$g = 2$	Q degenerate + denominator elimination	$1\mathbf{M} + 1\mathbf{S} + 3\mathbf{m}$	$1\mathbf{M} + 3\mathbf{m}$	$3\mathbf{M} + 4\mathbf{S} + 4\mathbf{m}$
	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 $\mathbb{F}_{q^d}$).

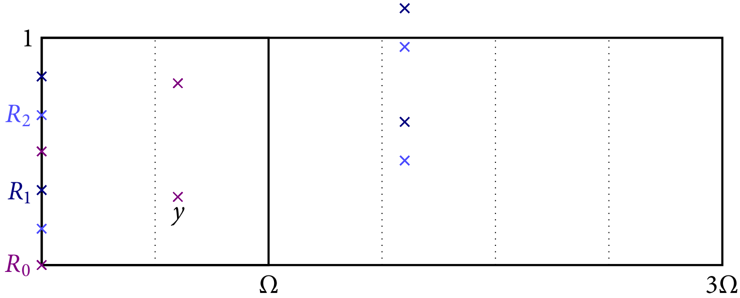
Explicit isogenies [LR10a]



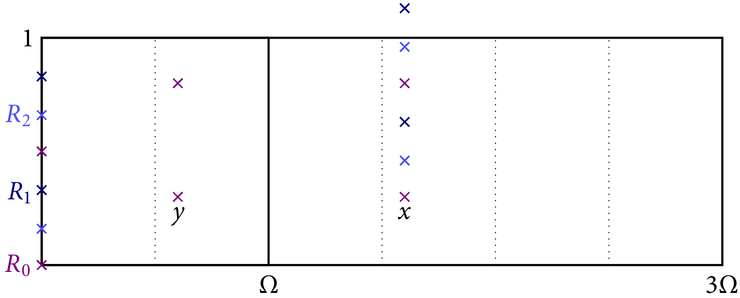
Explicit isogenies [LR10a]



Explicit isogenies [LR10a]



Explicit isogenies [LR10a]



Explicit isogenies [LR10a]

Explicit isogenies algorithm

- Compute the isogeny π from the knowledge of the kernel K.
- Only need to do $O(\#K)$ differential additions.

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).

[BGL09] Reinier Bröker, David Gruenewald, and Kristin Lauter. *Explicit CM-theory in dimension 2*. Oct. 2009. arXiv: 0910.1848. (Cit. on p. 20).

[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. 24).

[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. 24).

[LR10a] David Lubicz and Damien Robert. *Computing isogenies between abelian varieties*. Jan. 2010. arXiv: 1001.2016. (Cit. on pp. 28–32).

[LR10b] David Lubicz and Damien Robert. *Efficient pairing computation with theta functions*. Accepted at ANTS IX (Ninth Algorithmic Number Theory Symposium). Jan. 2010. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. (Cit. on p. 26).

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

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

[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).