Cryptology, elliptic curves and number theory

Damien Robert

LFANT Team, IMB & Inria Bordeaux Sud-Ouest

08/03/2011 (Bordeaux)

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 [KAF+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 order n. Let $x \in \mathbb{N}$ and $h = g^x$. The discrete logarithm $\log_g(h)$ is x.

- Exponentiation: $O(\log n)$. DLP?
- If $n = \prod p_i^{e_i}$ then the DLP $\log_g(h)$ is reduced to several DLP $\log_{g_i}(\cdot)$ where g_i if of order p_i (CRT+Hensel lemma). Thus the cost of the DLP depends on the largest prime divisor of n.
- Generic method to solve the DLP: let $u = [\sqrt{n}]$, and compute the intersection of $\{h, hg^{-1}, \ldots, hg^{-u}\}$ and $\{g^u, g^{2u}, g^{3u}, \ldots\}$. Cost: $\widetilde{O}(\sqrt{n})$ (Baby steps, giant steps).
- Reduce memory consumption by doing a random walk $g^{a_i} h^{b_i}$ until a collision is found (Pollard-ρ).
- If G is of prime order p, the DLP costs $\widetilde{O}(\sqrt{p})$ (in a generic group).

Key exchange

Protocol [Diffie-Hellman Key Exchange]

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

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

Zero knowledge

- Alice knowns $a \in \mathbb{Z}/n\mathbb{Z}$. Publish $p = g^a$.
- Alice sends $q = g^r$ to Bob, $\quad r \in \mathbb{Z}$ random.
- Bob either:
  - Asks r to Alice and checks that $q = g^r$.
  - Asks $r + a$ to Alice and checks that $qp = g^{r+a}$.

Public key cryptography

- Cyclic group of prime order $G = \langle g \rangle$.
- Alice: secret key a, public key $p = g^a$.

Asymetric encryption

- Encrypting $m \in G$: Bob sends g^r, $s = m p^r$, $\quad r \in \mathbb{Z}$ random.
- Decryption: $m = s / {g^r}^a$.

Signature [$G = \mathbb{F}_p^*$]

- Signing m: Alice sends g^r, $s = (m - a g^r)/r$. $\quad r \in \mathbb{Z}$ random.
- Verification: Bob checks that $g^m = p^{g^r} g^{rs}$.

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 [GPSW06].

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 elliptic curves.

Pairing-based cryptography

Tripartite Diffie–Helman

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

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

Example (Identity-based cryptography)

- Master key: (P, sP), s. $\quad s \in \mathbb{N}, P \in G_1$.
- Derived key: Q, sQ. $\quad Q \in G_1$.
- Encryption, $m \in G_2$: $m' = m \oplus e(Q, sP)^r$, rP. $\quad r \in \mathbb{N}$.
- Decryption: $m = m' \oplus e(sQ, rP)$.

Which groups to use?

- The DLP costs $\widetilde{O}(\sqrt{p})$ in a generic group.
- $G = \mathbb{Z}/p\mathbb{Z}$: DLP is trivial.
- $G = \mathbb{F}_p^*$: sub-exponential attacks.

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

$\Rightarrow$ We also want efficient pairings.

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.

Pairings on abelian varieties

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

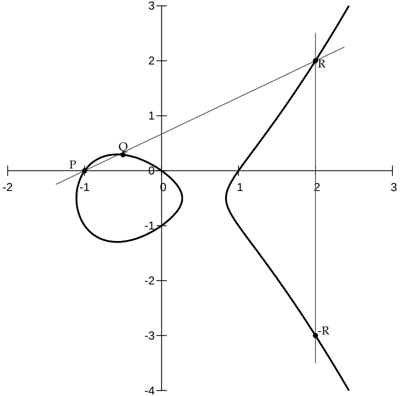
$$e_W : A[\ell] \times A[\ell] \rightarrow \mu_\ell \subset \mathbb{F}_{q^k}^*.$$

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. $(\deg f = 2g+1)$

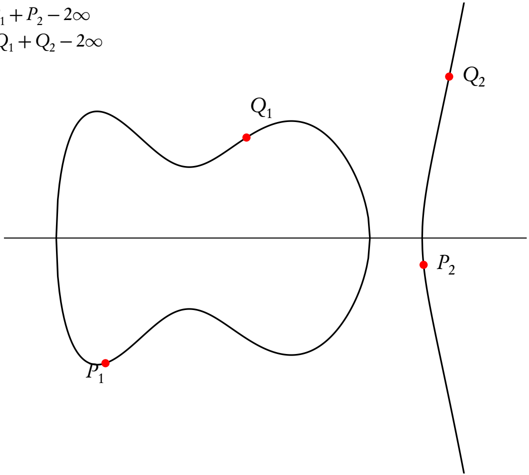
- Divisor: formal sum $D = \sum n_i P_i$, $P_i \in C(\overline{k})$.
  $\deg D = \sum n_i$.
- Principal divisor: $\sum_{P \in C(\overline{k})} v_P(f).P$; $f \in \overline{k}(C)$.
- Jacobian of C = Divisors of degree 0 modulo principal divisors
  + Galois action
  = Abelian variety of dimension g.
- Divisor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

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

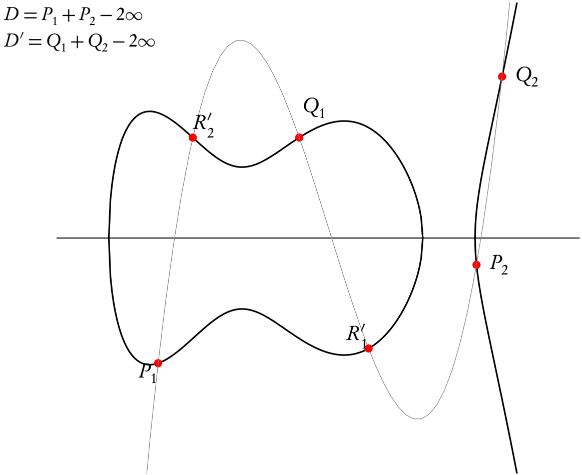
- Mumford coordinates: $D = (u, v) \Rightarrow u = \prod (x - x_i),\ v(x_i) = y_i$.
- Cantor algorithm: addition law.

Example of the addition law in genus 2

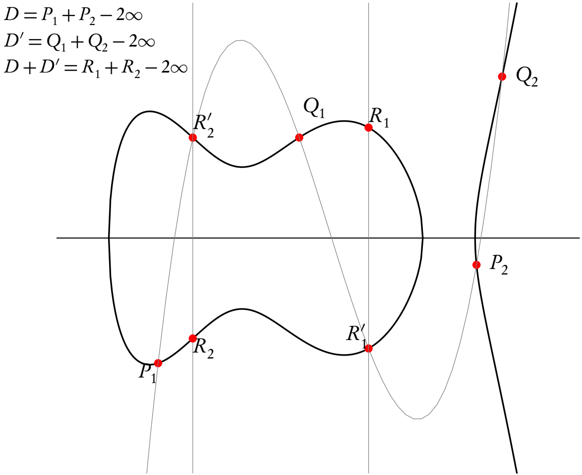
$D = P_1 + P_2 - 2\infty$
$D' = Q_1 + Q_2 - 2\infty$



Example of the addition law in genus 2



Example of the addition law in genus 2



Complex abelian varieties

- Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$, where $\Omega \in \mathscr{H}_g(\mathbb{C})$ the Siegel upper half space.
- An elliptic curve over $\mathbb{C}$ is a torus $\mathbb{C}/\Lambda$, where Λ is a lattice.
- The isomorphism $E \to \mathbb{C}/\Lambda$ is given by $P \mapsto \int_0^P dx/y$, Λ is the image of $H_1(E, \mathbb{Z})$.
- Let $\mathscr{E}_{2k}(\Lambda) = \sum_{w \in \Lambda^*} w^{-2k}$ be the Eisenstein series of weight $2k$, and

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{w \in \Lambda^*} \frac{1}{(z-w)^2} - \frac{1}{w^2}.$$

  Then $\mathbb{C}/\Lambda \to E, z \mapsto (\wp(z), \wp'(z))$ is an isomorphism, where $E : y^2 = 4x^3 - 60\mathscr{E}_4(\Lambda) - 140\mathscr{E}_6(\Lambda)$.

Modular function

- A lattice $\Lambda \subset \mathbb{C}$ can be uniquely represented as $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$, where τ is in the Poincarré half-plane $\mathfrak{H}$.
- There is a bijection between $\mathfrak{H}/\Gamma(1)$ and the set of isomorphic elliptic curves, where $\Gamma(1) = \mathrm{Sl}_2(\mathbb{Z})/\{\pm 1\}$ and the action is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \tau = \frac{a\tau + b}{c\tau + d}.$$

- Let $X(1)$ be the compatification of $\mathfrak{H}/\Gamma(1)$ (constructed by adding the cusps to $\mathfrak{H}$). It is an analytic space, and the j-function gives an isomorphism between $X(1)$ and $\mathbb{P}^1_{\mathbb{C}}$.
- The (meromorphic) k-forms on $X(1)$ corresponds to modular functions of weight $2k$:

$$f\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} . \tau \right) = (c\tau + d)^{2k} f(\tau).$$

Security of abelian varieties

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

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 $g \leqslant 4$.

Security of abelian varieties

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

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 $g \leqslant 4$.

Choosing an elliptic curve

1. One can choose a random elliptic curve E over $\mathbb{F}_q$, and check that $\#E(\mathbb{F}_q)$ is divisible by a large prime number.
2. Let $\chi_\pi(X) = X^2 - tX + q$ be the characteristic polynomial of the Frobenius. Then $\#E(\mathbb{F}_q) = \chi_\pi(1)$.
   (Reminder: the characteristic polynomial of an endomorphism α is the unique polynomial χ_α such that for all $n \in \mathbb{N}$ $\chi_\alpha(n) = \deg(\alpha - n\,\mathrm{Id})$. It is also the characteristic polynomial of α acting on the Tate module $T_\ell(E)$ for $\ell \nmid q$.)
3. Hasse: $|t| \leqslant 2\sqrt{q}$.
   (Comes from the fact that $\deg$ is a positive quadratic form).
4. We need an efficient algorithm to find the trace t.

Schoof algorithm

- Let $E : y^2 = x^3 + ax + b$ defined over $\mathbb{F}_q$ (of characteristic > 3).
- The idea to count the points on E is to compute $t \mod \ell$ for a lot of small primes ℓ, and then use the CRT to find back ℓ.
- We will need $O(\log q)$ primes of size $O(\log q)$.
- For each small prime $\ell \geqslant 3$, we can construct a division polynomial ψ_ℓ of degree $(\ell^2 - 1)/2$ such that $P \in E[\ell]$ if and only if $\psi_\ell(x_P) = 0$.
- We can then work over the algebra $A = \mathbb{F}_q[x, y]/(y^2 - ax - b, \psi_\ell(x))$, to recover $t \mod \ell$. This costs $O(\log(q) + \ell)$ operations in A, each costing $O(\ell^2 \log(q))$, so in total $O(\log q^4)$.
- We recover t in time $O(\log q^5)$.
- Can we improve this algorithm? We need to work on subgroups of the ℓ-torsion.

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).

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

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

- Generalized to abelian varieties by Cosset, Lubicz, R.

Modular polynomials

Definition

- Modular polynomial $\varphi_n(x,y) \in \mathbb{Z}[x,y]$: $\varphi_n(x,y)=0 \Leftrightarrow x=j(E)$ 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 $\varphi_n(j(E),.) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- Atkins and Elkies ameliorations to Schoof algorithm:
  1. Compute $\varphi_\ell(X,j(E))$ and checks if there is a rational root j'.
  2. Compute the factor $g_\ell(X)$ of $\psi_\ell(X)$ corresponding to the isogeny $E \to E'$.
  3. Compute the action of π on the algebra $B=\mathbb{F}_q[x,y]/(y^2-ax-b, g_\ell(X))$.

The total complexity is $O(\log q^4)$.

Other 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.

Point counting in small characteristic

- Let $E/\mathbb{F}_q$ be an ordinary elliptic curve. There exists a unique lift $\mathscr{E}$ of E on $\mathbb{Q}_q$ such that $\mathrm{End}(E) \simeq \mathrm{End}(\mathscr{E})$. $\mathscr{E}$ is called the canonical lift of E, and moreover we have

$$\varphi_p(j_{\mathscr{E}}, \sigma j_{\mathscr{E}}) = 0,$$

  where σ is the lift of the (small) Frobenius on $\mathbb{Q}_q$.
- The idea of Satoh's algorithm is that the cycle: $\mathscr{E} \mapsto \mathscr{E}^{\sigma} \mapsto \mathscr{E}^{\sigma^2} \ldots \mapsto \mathscr{E}^{\sigma^n}$ lift the Frobenius if $q = p^n$.
- In fact it suffices to compute the action of $\mathscr{E} \mapsto \mathscr{E}^{\sigma}$ on the differentials given by $\gamma \in \mathbb{Q}_q$. Since the action on the differentials on $\mathscr{E}^{\sigma} \mapsto \mathscr{E}^{\sigma^2}$ is given by γ^{σ}, we deduce that the norm of γ is an eigenvector of the Frobenius.
- The cost is $O(n^2)$.
- Hard to extend to other curves $\Rightarrow$ Kedlaya algorithm: choose any lift, and compute the action of the Frobenius on the Monsky–Washnitzer cohomology.

Complex multiplication

- Another idea to choose a good elliptic curve is to fix a prescribed number of point and generate a curves with this number.
- This is indispensable for pairings applications where we want to control the embedding degree (otherwise it is of order q with a random curve).
- If $E/\mathbb{F}_q$ is an ordinary elliptic curve, $\mathrm{End}(E)$ is an order in $\mathbb{Q}(\pi)$ containing $\mathbb{Z}[\pi,\overline{\pi}]$. The endomorphism ring of an elliptic curve is a finer invariant than its number of points.
- If $\mathcal{O}_K$ is the maximal order of an imaginary quadratic field K, then there are h_K class of complex elliptic curves E such that $\mathrm{End}(E) = \mathcal{O}_K$, where h_K is the class number of K.
- The algorithm of complex multiplication computes the class polynomial of degree h_K: $H_K = \prod (X - j(E))$ where the product goes over each complex elliptic curve with complex multiplication by $\mathcal{O}_K$.

The theory of complex multiplication

- If $E/\mathbb{C}$ as complex multiplication by $\mathcal{O}_K$, then $K(j(E))$ is the Hilbert class field of K. Adjoining the x coordinates of the points of torsion gives the maximal abelian extension of K (and adjoining all the points of torsion give the maximal abelian extension of the Hilbert class field).
- $H_K \in \mathbb{Z}[X]$ and is the minimal polynomial of $j(E)$ over K. In particular $j(E)$ is an algebraic integer.

Example

$Q(\sqrt{-163})$ is principal, so $j\left(\frac{1+\sqrt{-163}}{2}\right) \in \mathbb{Z}$. Moreover $j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \ldots$ with $q = e^{2\pi i \tau}$. When we substitute $\tau = \frac{1+\sqrt{-163}}{2}$ we find that $q = -e^{-\pi\sqrt{163}} \approx -3.809.10^{-18}$ is very small. Such $e^{\pi\sqrt{163}}$ is almost an integer, and indeed we compute

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007\ldots.$$

Applications

- Since the j-invariant give the field of moduli (and even the field of definition), if p splits completely in $K(j(E))$, E reduces to $\mathbb{F}_p$.
- For such a p, the polynomial H_K splits completely in $\mathbb{F}_p$, and its roots corresponds to the j-invariant of elliptic curves E defined over $\mathbb{F}_p$ such that $\mathrm{End}(E) = \mathcal{O}_K$.

Complex abelian varieties

- Let $A = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$ be a complex abelian variety.
- The theta functions with characteristic give a lot of analytic (quasi periodic) functions on $\mathbb{C}^g$.

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

Quasi-periodicity:

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

- Projective coordinates:

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

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

Theta functions of level n

- Translation by a point of n-torsion:

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

- $(\vartheta_i)_{i\in Z(\overline{n})}$: basis of the theta functions of level n
  $\Leftrightarrow A[n]=A_1[n]\oplus A_2[n]$: 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.

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

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

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

The Weil and Tate pairing with theta coordinates [LR10]

P and Q points of ℓ-torsion.

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

- $e_{W,\ell}(P,Q) = \frac{\lambda_P^1 \lambda_Q^0}{\lambda_P^0 \lambda_Q^1}$.
  If $P = \Omega x_1 + x_2$ and $Q = \Omega y_1 + y_2$, then $e_{W,\ell}(P,Q) = e^{-2\pi i \ell ({}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2)}$.
- $e_{T,\ell}(P,Q) = \frac{\lambda_P^1}{\lambda_P^0}$.

Duplication formula

$$\vartheta\begin{bmatrix}0\\ \frac{i}{n}\end{bmatrix}(z_1+z_2,\frac{\Omega}{n})\vartheta\begin{bmatrix}0\\ \frac{j}{n}\end{bmatrix}(z_1-z_2,\frac{\Omega}{n})=\sum_{t\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}\vartheta\begin{bmatrix}\frac{t}{2}\\ \frac{i+j}{2n}\end{bmatrix}(2z_1,2\frac{\Omega}{n})\vartheta\begin{bmatrix}\frac{t}{2}\\ \frac{i-j}{2n}\end{bmatrix}(2z_2,2\frac{\Omega}{n})$$

$$\vartheta\begin{bmatrix}\chi/2\\ i/(2n)\end{bmatrix}(2z_1,2\frac{\Omega}{n})\vartheta\begin{bmatrix}\chi/2\\ j/(2n)\end{bmatrix}(2z_2,2\frac{\Omega}{n})= \frac{1}{2^g}\sum_{t\in\frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g}e^{-2i\pi\,{}^t\chi\cdot t}\vartheta\begin{bmatrix}2\chi\\ \frac{i+j}{2n}+t\end{bmatrix}(z_1+z_2,\frac{\Omega}{n})\vartheta\begin{bmatrix}0\\ \frac{i-j}{2n}+t\end{bmatrix}(z_1-z_2,\frac{\Omega}{n}).$$

- The duplication formula give a modular polynomial for 2-isogenies on any abelian variety $\Rightarrow$ point counting in characteristic 2 by computing the canonical lift.
- The elliptic curves $E_n: y^2=x(x-a_n^2)(x-b_n^2)$ converges over $\mathbb{Q}_{2^k}$ to the canonical lift of $(E_0)_{\mathbb{F}_{2^k}}$ [Mes01], where $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ satisfy the Arithmetic Geometric Mean:

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

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

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. 8).

[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. 8).

[GPSW06] 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).

[Jou04] A. Joux. "A one round protocol for tripartite Diffie–Hellman". In: *Journal of Cryptology* 17.4 (2004), pp. 263–276 (cit. on p. 8).

[KAF+10] T. Kleinjung, K. Aoki, J. Franke, et al. "Factorization of a 768-bit RSA modulus". In: (2010) (cit. on p. 4).

[LR10] D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: *Algorithmic Number Theory*. Lecture Notes in Comput. Sci. 6197 (July 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 (cit. on p. 34).

[Mes01] J.-F. Mestre. *Lettre à Gaudry et Harley*. 2001. URL: http://www.math.jussieu.fr/mestre (cit. on p. 35).

[SW05] A. Sahai and B. Waters. "Fuzzy identity-based encryption". In: *Advances in Cryptology–EUROCRYPT 2005* (2005), pp. 457–473 (cit. on p. 8).

[Ver01] E. Verheul. "Self-blindable credential certificates from the Weil pairing". In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 533–551 (cit. on p. 8).