Computing optimal pairings on abelian varieties with theta functions

David Lubicz[1,2], **Damien Robert**[3]

[1]CÉLAR

[2]IRMAR, Université de Rennes 1

[3]Microsoft Research

30/09/2011 (IMB, Bordeaux)

Outline

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).

Usage in public key cryptography

- Asymetric encryption;
- Signature;
- Zero-knowledge.

Example (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 $e : G_1 \times G_1 \to G_2$.

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.

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

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.
- Elliptic curves or Jacobian of hyperelliptic curves of genus 2 over $\mathbb{F}_q$: best attack is the generic attack except for some particular cases.
- Abelian variety: better attack (still exponential) when the dimension g is greater than 2. Subexponential attack when g is greater than $\log q$.
- Abelian varieties give the only known examples of secure cryptographic pairings.

The Weil pairing on elliptic curves

- Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over k $(\operatorname{car} k \neq 2,3)$.
- Let $P, Q \in E[\ell]$ be points of ℓ-torsion.
- Let f_P be a function associated to the principal divisor $\ell(P-0)$, and f_Q to $\ell(Q-0)$. We define:

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

- The application $e_{W,\ell} : E[\ell] \times E[\ell] \to \mu_\ell(\overline{k})$ is a non degenerate pairing: the Weil pairing.

Computing the Weil pairing

- We need to compute the functions f_P and f_Q. More generally, we define the Miller's functions:

Definition

Let $\lambda \in \mathbb{N}$ and $X \in E[\ell]$, we define $f_{\lambda,X} \in k(E)$ to be a function thus that:

$$(f_{\lambda,X}) = \lambda(X) - ([\lambda]X) - (\lambda - 1)(0).$$

Miller's algorithm

- The key idea in Miller's algorithm is that

$$f_{\lambda+\mu,X} = f_{\lambda,X} f_{\mu,X} \mathfrak{f}_{\lambda,\mu,X}$$

where $\mathfrak{f}_{\lambda,\mu,X}$ is a function associated to the divisor

$$([\lambda+\mu]X) - ([\lambda]X) - ([\mu]X) + (0).$$

- We can compute $\mathfrak{f}_{\lambda,\mu,X}$ using the addition law in E: if $[\lambda]X = (x_1, y_1)$ and $[\mu]X = (x_2, y_2)$ and $\alpha = (y_1 - y_2)/(x_1 - x_2)$, we have

$$\mathfrak{f}_{\lambda,\mu,X} = \frac{y - \alpha(x - x_1) - y_1}{x + (x_1 + x_2) - \alpha^2}.$$

Tate pairing

Definition

- Let $E/\mathbb{F}_q$ be an elliptic curve of cardinal divisible by ℓ. Let d be the smallest number thus that $\ell \mid q^d - 1$: we call d the embedding degree. $\mathbb{F}_{q^d}$ is constructed from $\mathbb{F}_q$ by adjoining all the ℓ-th root of unity.
- The Tate pairing is a non degenerate bilinear application given by

$$\begin{array}{rcl} e_T\colon E(\mathbb{F}_{q^d})/\ell E(\mathbb{F}_{q^d}) \times E[\ell](\mathbb{F}_q) & \longrightarrow & \mathbb{F}^*_{q^d}/\mathbb{F}^{*\,\ell}_{q^d} \\ (P,Q) & \longmapsto & f_Q((P)-(0)) \end{array}.$$

- If $\ell^2 \nmid E(\mathbb{F}_{q^d})$ then $E(\mathbb{F}_{q^d})/\ell E(\mathbb{F}_{q^d}) \simeq E[\ell](\mathbb{F}_{q^d})$.
- We normalise the Tate pairing by going to the power of $(q^d-1)/\ell$.
- This final exponentiation allows to save some computations. For instance if $d = 2d'$ is even, we can suppose that $P = (x_2, y_2)$ with $x_2 \in E(\mathbb{F}_{q^{d'}})$. Then the denominators of $\mathfrak{f}_{\lambda,\mu,Q}$ are ℓ-th powers and are killed by the final exponentiation.

Miller's algorithm

Computing the Tate pairing

Input: $\ell \in \mathbb{N}$, $Q = (x_1, y_1) \in E[\ell](\mathbb{F}_q)$, $P = (x_2, y_2) \in E(\mathbb{F}_{q^d})$.

Output: $e_T(P, Q)$.

- Compute the binary decomposition: $\ell := \sum_{i=0}^{I} b_i 2^i$. Let $T = Q, f_1 = 1, f_2 = 1$.
- For i in $[I..0]$ compute
  - α, the slope of the tangent of E at T.
  - $T = 2T$. $T = (x_3, y_3)$.
  - $f_1 = f_1^2(y_2 - \alpha(x_2 - x_3) - y_3)$, $f_2 = f_2^2(x_2 + (x_1 + x_3) - \alpha^2)$.
  - If $b_i = 1$, then compute
    - α, the slope of the line going through Q and T.
    - $T = T + Q$. $T = (x_3, y_3)$.
    - $f_1 = f_1^2(y_2 - \alpha(x_2 - x_3) - y_3)$, $f_2 = f_2(x_2 + (x_1 + x_3) - \alpha^2)$.
- Return

$$\left(\frac{f_1}{f_2}\right)^{\frac{q^d-1}{\ell}}.$$

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.

Pairing on abelian varieties

- Let $Q \in \widehat{A}[\ell]$. By definition of the dual abelian variety, Q is a divisor of degree 0 on A such that $[\ell]^* Q$ is principal. Let $g_Q \in k(A)$ be a function associated to $[\ell]^* Q$.
- We can then define the Weil pairing:

$$\begin{array}{rcl} e_{W,\ell} : A[\ell] \times \widehat{A}[\ell] & \longrightarrow & \mu_\ell(\overline{k}) \\ (P,Q) & \longmapsto & \dfrac{g_Q(x+P)}{g_Q(x)} \end{array}.$$

  (This last function being constant in its definition domain).
- Likewise, we can extend the Tate pairing to abelian varieties.

Pairings and polarizations

- If Θ is an ample divisor, the polarisation φ_Θ is a morphism $A \to \widehat{A}, x \mapsto t_x^*\Theta - \Theta$.
- We can then compose the Weil and Tate pairings with φ_Θ:

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

- More explicitly, if f_P and f_Q are the functions associated to the principal divisors $\ell t_P^*\Theta - \ell\Theta$ and $\ell t_Q^*\Theta - \ell\Theta$ we have

$$e_{W,\Theta,\ell}(P,Q) = \frac{f_Q(P-0)}{f_P(Q-0)}.$$

Remark

If Θ corresponds to the ample line bundle $\mathscr{L}$, $e_{W,\Theta,\ell}$ corresponds to the commutator pairing $e_{\mathscr{L}^\ell}$.

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 elliptic curves have a too small embedding degree. [RS09] says that for the current security parameters, optimal supersingular abelian varieties of small dimension are of dimension 4.
- 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.

Computing pairings on abelian varieties

- If J is the Jacobian of an hyperelliptic curve H of genus g, it is easy to extend Miller's algorithm to compute the Tate and Weil pairing on J with Mumford coordinates.
- For instance if $g = 2$, the function $f_{\lambda,\mu,Q}$ is of the form

$$\frac{y - l(x)}{(x - x_1)(x - x_2)}$$

  where l is of degree 3.
- What about more general abelian varieties? We don't have Mumford coordinates.

Complex abelian variety

- A complex abelian variety is of the form $A = V/\Lambda$ where V is a $\mathbb{C}$-vector space and Λ a lattice, with a polarization (actually an ample line bundle) $\mathscr{L}$ on it.
- The Chern class of $\mathscr{L}$ corresponds to a symplectic real form E on V such that $E(ix, iy) = E(x, y)$ and $E(\Lambda, \Lambda) \subset \mathbb{Z}$.
- The pairing $e_{\mathscr{L}}$ is then given by $\exp(2i\pi E(\cdot, \cdot))$.
- A principal polarization on A corresponds to a decomposition $\Lambda = \Omega\mathbb{Z}^g + \mathbb{Z}^g$ with $\Omega \in \mathfrak{H}_g$ the Siegel space.
- The corresponding polarization on A is then given by $E(\Omega x_1 + x_2, \Omega y_1 + y_2) = {}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2$.

Theta coordinates on abelian varieties

- Every abelian variety (over an algebraically closed field) can be described by theta coordinates of level $n > 2$ even. (The level n encodes information about the n-torsion).
- The theta coordinates of level 2 on A describe the Kummer variety of A.
- For instance if $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ is an abelian variety over $\mathbb{C}$, the theta coordinates on A come from the theta functions with characteristic:

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

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

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

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

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 $x_3 z_3 \neq 0$.
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 $(x' : z')$.

Cost of the arithmetic with low level theta functions (car $k \neq 2$)

	Mumford	Level 2	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 coordinates
Doubling	$5M+4S+1m_0$	$3M+6S+3m_0$	$3M+5S$
Mixed Addition			$7M+6S+1m_0$

Multiplication cost in genus 1 (one step).

The Weil and Tate pairing with theta coordinates

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

Why does it works?

$$
\begin{array}{ccccc}
0_A & \alpha P & \alpha^4(2P) & \dots & \alpha^{\ell^2}(\ell P) = \lambda'^0_P 0_A \\
\beta Q & \gamma(P \oplus Q) & \frac{\gamma^2\alpha^2}{\beta}(2P+Q) & \dots & \frac{\gamma^\ell \alpha^{\ell(\ell-1)}}{\beta^{\ell-1}}(\ell P + Q) = \lambda'^1_P \beta Q \\
\beta^4(2Q) & \frac{\gamma^2\beta^2}{\alpha}(P+2Q) & & & \\
\dots & \dots & & & \\
\beta^{\ell^2}(\ell Q) = \lambda'^0_Q 0_A & \frac{\gamma^\ell \beta^{\ell(\ell-1)}}{\alpha^{\ell-1}}(P+\ell Q) = \lambda'^1_Q \alpha P & & &
\end{array}
$$

We then have

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

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

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

The case $n=2$

- If $n=2$ we work over the Kummer variety K, so $e(P,Q) \in \overline{k}^{*,\pm 1}$.
- We represent a class $x \in \overline{k}^{*,\pm 1}$ by $x+1/x \in \overline{k}^{*}$. We want to compute the symmetric pairing

$$e_s(P,Q) = e(P,Q) + e(-P,Q).$$

- From $\pm P$ and $\pm Q$ we can compute $\{\pm(P+Q), \pm(P-Q)\}$ (need a square root), and from these points the symmetric pairing.
- e_s is compatible with the $\mathbb{Z}$-structure on K and $\overline{k}^{*,\pm 1}$.
- The $\mathbb{Z}$-structure on $\overline{k}^{*,\pm}$ can be computed as follow:

$$(x^{\ell_1+\ell_2} + \frac{1}{x^{\ell_1+\ell_2}}) + (x^{\ell_1-\ell_2} + \frac{1}{x^{\ell_1-\ell_2}}) = (x^{\ell_1} + \frac{1}{x^{\ell_1}})(x^{\ell_2} + \frac{1}{x^{\ell_2}})$$

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 + d even	$1\mathbf{M}+1\mathbf{S}+3\mathbf{m}$	$1\mathbf{M}+3\mathbf{m}$	$3\mathbf{M}+4\mathbf{S}+4\mathbf{m}$
	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 $\mathbb{F}_{q^d}$).

Ate pairing

- Let $G_1 = E[\ell] \bigcap \mathrm{Ker}(\pi_q - 1)$ and $G_2 = E[\ell] \bigcap \mathrm{Ker}(\pi_q - [q])$.
- We have $f_{ab,Q} = f_{a,Q}^b f_{b,[a]Q}$.
- Let $P \in G_1$ and $Q \in G_2$ we have $f_{a,[q]Q}(P) = f_{a,Q}(P)^q$.
- Let $\lambda \equiv q \mod \ell$. Let $m = (\lambda^d - 1)/\ell$. We then have

$$\begin{aligned} e_T(P,Q)^m &= f_{\lambda^d,Q}(P)^{(q^d-1)/\ell} \\ &= \left(f_{\lambda,Q}(P)^{\lambda^{d-1}} f_{\lambda,[q]Q}(P)^{\lambda^{d-2}} \dots f_{\lambda,[q^{d-1}]Q}(P) \right)^{(q^d-1)/\ell} \\ &= \left(f_{\lambda,Q}(P)^{\sum \lambda^{d-1-i} q^i} \right)^{(q^d-1)/\ell} \end{aligned}$$

Definition

Let $\lambda \equiv q \mod \ell$, the (reduced) ate pairing is defined by

$$a_\lambda : G_1 \times G_2 \to \mu_\ell, (P,Q) \mapsto f_{\lambda,Q}(P)^{(q^d-1)/\ell}.$$

It is non degenerate if $\ell^2 \nmid (\lambda^k - 1)$.

Optimal ate

- Let $\lambda = m\ell = \sum c_i q^i$ be a multiple of ℓ with small coefficients c_i. $(\ell \nmid m)$
- The pairing

$$\begin{aligned} a_\lambda \colon G_1 \times G_2 &\longrightarrow \mu_\ell \\ (P,Q) &\longmapsto \left(\prod_i f_{c_i,Q}(P)^{q^i} \prod_i f_{\sum_{j>i} c_j q^j, c_i q^i, Q}(P) \right)^{(q^d-1)/\ell} \end{aligned}$$

is non degenerate when $mdq^{d-1} \not\equiv (q^d-1)/r \sum_i i c_i q^{i-1} \mod \ell$.

- Since $\varphi_d(q) = 0 \mod \ell$ we look at powers $q, q^2, \ldots, q^{\varphi(d)-1}$.
- We can expect to find λ such that $c_i \approx \ell^{1/\varphi(d)}$.

Ate pairing with theta functions

- Let $P \in G_1$ and $Q \in G_2$.
- In projective coordinates, we have $\pi_q^d(P \oplus Q) = P \oplus \lambda^d Q = P \oplus Q$.
- Unfortunately, in affine coordinates, $\pi_q^d(P+Q) \neq P + \lambda^d Q$.
- But if $\pi_q(P+Q) = C * (P+\lambda Q)$, then C is exactly the (non reduced) ate pairing!

Miller functions with theta coordinates

- We have
$$f_{\mu,Q}(P) = \frac{\vartheta(Q)}{\vartheta(P+\mu Q)} \left(\frac{\vartheta(P+Q)}{\vartheta(P)}\right)^{\mu}.$$
- So
$$\mathfrak{f}_{\lambda,\mu,Q}(P) = \frac{\vartheta(P+\lambda Q)\vartheta(P+\mu Q)}{\vartheta(P)\vartheta(P+(\lambda+\mu)Q)}.$$
- We can compute this function using a generalised version of Riemann's relations:

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

Optimal ate with theta functions

1. **Input:** $\pi_q(P) = P$, $\pi_q(Q) = q * Q$, $\lambda = m\ell = \sum c_i q^i$.
2. Compute the $P + c_i Q$ and $c_i Q$.
3. Apply Frobeniuses to obtain the $P + c_i q^i Q$, $c_i q^i Q$.
4. Compute $c_i q^i Q + c_j q^j Q$ (up to a constant) and then use the extended Riemann relations to compute $P + c_i q^i Q + c_j q^j Q$ (up to the same constant).
5. Recurse until we get $\lambda Q = C_0 * Q$ and $P + \lambda Q = C_1 * P$.
6. **Return** $(C_1/C_0)^{\frac{q^d-1}{\ell}}$.

The case $n = 2$

- Computing $c_i q^i Q \pm c_j q^j Q$ requires a square root (very costly).
- And we need to recognize $c_i q^i Q + c_j q^j Q$ from $c_i q^i Q - c_j q^j Q$.
- We will use compatible additions: if we know x, y, z and $x+z$, $y+z$, we can compute $x+y$ without a square root.
- We apply the compatible additions with $x = c_i q^i Q$, $y = c_j q^j Q$ and $z = P$.

Compatible additions

- Recall that we know x, y, z and $x+z$, $y+z$.
- From it we can compute $(x+z)\pm(y+z)=\{x+y+2z, x-y\}$ and of course $x\pm y$. Then $x+y$ is the element in $\{x+y, x-y\}$ not appearing in the preceding set.
- Since we can distinguish $x+y$ from $x-y$ we can compute them without a square root.

The compatible addition algorithm in dimension 1

1. **Input:** x, y, $xz = x+z$, $yz = y+z$.
2. Computing $x \pm y$:

$$\alpha = (y_0^2 + y_1^2)(x_0^2 + y_0^2)A', \beta = (y_0^2 - y_1^2)(x_0^2 - y_0^2)B'$$
$$\lambda_{00} = (\alpha+\beta), \lambda_{11} = (\alpha-\beta)$$
$$\lambda_{01} := 2y_0y_1x_0x_1/ab.$$

3. Computing $(x+z) \pm (y+z)$:

$$\alpha' = (yz_0^2 + yz_1^2)(xz_0^2 + yz_0^2)A', \beta' = (yz_0^2 - yz_1^2)(xz_0^2 - yz_0^2)B'$$
$$\lambda'_{00} = \alpha' + \beta', \lambda'_{11} = \alpha' - \beta'$$
$$\lambda'_{01} = 2yz_0yz_1xz_0xz_1/ab.$$

4. **Return** $x+y = [\lambda_{00}(\lambda_{11}\lambda'_{00} - \lambda'_{11}\lambda_{00}), -2\lambda_{11}(\lambda'_{01}\lambda_{00} - \lambda_{01}\lambda'_{00})]$.

Perspectives

- Characteristic 2 case (especially for supersingular abelian varieties of characteristic 2).
- Optimized implementations (FPGA, ...).
- Look at special points (degenerate divisors, ...).

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. 5).

[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. 5).

[GPS+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 (cit. on p. 5).

[Jou04] A. Joux. "A one round protocol for tripartite Diffie–Hellman". In: *Journal of Cryptology* 17.4 (2004), pp. 263–276 (cit. on p. 5).

[RS09] K. Rubin and A. Silverberg. "Using abelian varieties to improve pairing-based cryptography". In: *Journal of Cryptology* 22.3 (2009), pp. 330–364 (cit. on p. 16).

[SW05] A. Sahai and B. Waters. "Fuzzy identity-based encryption". In: *Advances in Cryptology–EUROCRYPT 2005* (2005), pp. 457–473 (cit. on p. 5).

[Ver01] E. Verheul. "Self-blindable credential certificates from the Weil pairing". In: *Advances in Cryptology—ASIACRYPT 2001* (2001), pp. 533–551 (cit. on p. 5).