Computing optimal pairings on abelian varieties with theta functions

06/06/2013 — AGCT

David Lubicz, **Damien Robert**

June 6, 2013

Outline

The Weil pairing on elliptic curves

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

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

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

Definition (Embedding degree)

The embedding degree d is the smallest number thus that $\ell \mid q^d - 1$; $\mathbb{F}_{q^d}$ is then the smallest extension containing $\mu_\ell(\overline{k})$.

The Tate pairing on elliptic curves over $\mathbb{F}_q$

Definition

The Tate pairing is a non degenerate (on the right) bilinear application given by

$$\begin{array}{rcl} e_T : E_0[\ell] \times E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*\ \ell} \\ (P,Q) & \longmapsto & f_P((Q)-(0)) \end{array}.$$

where

$$E_0[\ell] = \{P \in E[\ell](\mathbb{F}_{q^d}) \mid \pi(P) = [q]P\}.$$

- On $\mathbb{F}_{q^d}$, the Tate pairing is a non degenerate pairing

$$e_T : E[\ell](\mathbb{F}_{q^d}) \times E(\mathbb{F}_{q^d})/\ell E(\mathbb{F}_{q^d}) \rightarrow \mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*\ \ell} \simeq \mu_\ell;$$

- We normalise the Tate pairing by going to the power of $(q^d - 1)/\ell$.

Miller's functions

- 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:

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

- We want to compute (for instance) $f_{\ell,P}((Q)-(0))$.

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

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

Pairings on Jacobians

- Let C be a curve of genus g;
- Let $P \in \mathrm{Jac}(C)[\ell]$ and D_P a divisor of degree 0 on C representing P;
- By definition of $\mathrm{Jac}(C)$, ℓD_P corresponds to a principal divisor (f_P) on C;
- The same formulas as for elliptic curve define the Weil and Tate pairings:

$$e_W(P,Q) = f_P(D_Q)/f_Q(D_P)$$
$$e_T(P,Q) = f_P(D_Q).$$

Pairings on Jacobians

- Let C be a curve of genus g;
- Let $P \in \mathrm{Jac}(C)[\ell]$ and D_P a divisor of degree 0 on C representing P;
- By definition of $\mathrm{Jac}(C)$, ℓD_P corresponds to a principal divisor (f_P) on C;
- The same formulas as for elliptic curve define the Weil and Tate pairings:

$$e_W(P,Q) = f_P(D_Q)/f_Q(D_P)$$
$$e_T(P,Q) = f_P(D_Q).$$

- A key ingredient for evaluating $f_P(D_Q)$ comes from Weil reciprocity theorem.

Theorem (Weil)

Let D_1 and D_2 be two divisors with disjoint support linearly equivalent to (0) on a smooth curve C. Then

$$f_{D_1}(D_2) = f_{D_2}(D_1).$$

Pairings on Jacobians

- Let C be a curve of genus g;
- Let $P \in \mathrm{Jac}(C)[\ell]$ and D_P a divisor of degree 0 on C representing P;
- By definition of $\mathrm{Jac}(C)$, ℓD_P corresponds to a principal divisor (f_P) on C;
- The same formulas as for elliptic curve define the Weil and Tate pairings:

$$e_W(P,Q) = f_P(D_Q)/f_Q(D_P)$$
$$e_T(P,Q) = f_P(D_Q).$$

- The extension of Miller's algorithm to Jacobians is "straightforward";
- For instance if $g=2$, the function $f_{\lambda,\mu,P}$ is of the form

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

where l is of degree 3.

Abelian varieties

Definition

An Abelian variety is a complete connected group variety over a base field k.

Example

- Elliptic curves= Abelian varieties of dimension 1;
- If C is a (projective smooth absolutely irreducible) curve of genus g, its Jacobian is an abelian variety of dimension g;
- In dimension $g \geqslant 4$, not every abelian variety is a Jacobian.

Isogenies and pairings

Let $f: A \rightarrow B$ be a separable isogeny with kernel K between two abelian varieties defined over k:

$$0 \longrightarrow K \longrightarrow A \xrightarrow{f} B \longrightarrow 0$$

$$0 \longleftarrow \hat{A} \xleftarrow{\hat{f}} \hat{B} \longleftarrow \hat{K} \longleftarrow 0$$

- $\hat{K}$ is the Cartier dual of K, and we have a non degenerate pairing $e_f: K \times \hat{K} \rightarrow \overline{k}^*$:
  1. If $Q \in \hat{K}(\overline{k})$, Q defines a divisor D_Q on B;
  2. $\hat{f}(Q) = 0$ means that $f^* D_Q$ is equal to a principal divisor (g_Q) on A;
  3. $e_f(P, Q) = g_Q(x)/g_Q(x+P)$. (This last function being constant in its definition domain).
- The Weil pairing $e_{W,\ell}$ is the pairing associated to the isogeny $[\ell]: A \rightarrow A$.

Polarisations

If $\mathscr{L}$ is an ample line bundle, the polarisation $\varphi_{\mathscr{L}}$ is a morphism $A \to \widehat{A}, x \mapsto t_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$.

Definition

Let $\mathscr{L}$ be a principal polarization on A. The (polarized) Weil pairing $e_{W,\mathscr{L},\ell}$ is the pairing

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

associated to the polarization $\mathscr{L}^\ell$:

$$A \xrightarrow{[\ell]} A \xrightarrow{\mathscr{L}} \hat{A}$$

The Tate pairings on abelian varieties over finite fields

- From the exact sequence

$$0 \to A[\ell](\overline{\mathbb{F}}_{q^d}) \to A(\overline{\mathbb{F}}_{q^d}) \to^{[\ell]} A(\overline{\mathbb{F}}_{q^d}) \to 0$$

  we get from Galois cohomology a connecting morphism

$$\delta : A(\mathbb{F}_{q^d})/\ell A(\mathbb{F}_{q^d}) \to H^1(\mathrm{Gal}(\overline{\mathbb{F}}_{q^d}/\mathbb{F}_{q^d}), A[\ell]);$$

- Composing with the Weil pairing, we get a bilinear application

$$A[\ell](\mathbb{F}_{q^d}) \times A(\mathbb{F}_{q^d})/\ell A(\mathbb{F}_{q^d}) \to H^1(\mathrm{Gal}(\overline{\mathbb{F}}_{q^d}/\mathbb{F}_{q^d}), \mu_\ell) \simeq \mathbb{F}^*_{q^d}/{\mathbb{F}^*_{q^d}}^{\ell} \simeq \mu_\ell$$

  where the last isomorphism comes from the Kummer sequence

$$1 \to \mu_\ell \to \overline{\mathbb{F}}^*_{q^d} \to \overline{\mathbb{F}}^*_{q^d} \to 1$$

  and Hilbert 90;

- Explicitely, if $P \in A[\ell](\mathbb{F}_{q^d})$ and $Q \in A(\mathbb{F}_{q^d})$ then the (reduced) Tate pairing is given by

$$e_T(P,Q) = e_W(P, \pi(Q_0) - Q_0)$$

  where Q_0 is any point such that $Q = [\ell]Q_0$ and π is the Frobenius of $\mathbb{F}_{q^d}$.

Cycles and Lang reciprocity

- Let $(A, \mathscr{L})$ be a principally polarized abelian variety;
- To a degree 0 cycle $\sum(P_i)$ on A, we can associate the line bundle $\otimes t_{P_i}^* \mathscr{L}$ on A;
- The cycle $\sum(P_i)$ corresponds to a trivial line bundle iff $\sum P_i = 0$ in A;
- If f is a function on A and $D = \sum(P_i)$ a cycle whose support does not contain a zero or pole of f, we let

$$f(D) = \prod f(P_i).$$

(In the following, when we write $f(D)$ we will always assume that we are in this situation.)

Theorem ([Lan58])

Let D_1 and D_2 be two cycles equivalent to 0, and f_{D_1} and f_{D_2} be the corresponding functions on A. Then

$$f_{D_1}(D_2) = f_{D_2}(D_1)$$

The Weil and Tate pairings on abelian varieties

Theorem

Let $P,Q \in A[\ell]$. Let D_P and D_Q be two cycles equivalent to $(P)-(0)$ and $(Q)-(0)$. The Weil pairing is given by

$$e_W(P,Q) = \frac{f_{\ell D_P}(D_Q)}{f_{\ell D_Q}(D_P)}.$$

Theorem

Let $P \in A[\ell](\mathbb{F}_{q^d})$ and $Q \in A(\mathbb{F}_{q^d})$, and let D_P and D_Q be two cycles equivalent to $(P)-(0)$ and $(Q)-(0)$. The (non reduced) Tate pairing is given by

$$e_T(P,Q) = f_{\ell D_P}(D_Q).$$

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.
- 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.
- Supersingular abelian varieties can have larger embedding degree than supersingular elliptic curves.
- Over a Jacobian, we can use twists even if they are not coming from twists of the underlying curve.

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 commutator 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 associated Riemann form 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

- The theta functions of level n give a system of projective coordinates:

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

- If $n=2$, we get (in the generic case) an embedding of the Kummer variety $A/\pm 1$.

Remark

Working on level n mean we take a n-th power of the principal polarisation. So in the following we will compute the n-th power of the usual Weil and Tate pairings.

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: differential addition in dimension 1 and in level 2

Algorithm

Input $z_P = (x_0, x_1)$, $z_Q = (y_0, y_1)$ *and* $z_{P-Q} = (z_0, z_1)$ *with* $z_0 z_1 \neq 0$;
$z_0 = (a, b)$ *and* $A = 2(a^2 + b^2)$, $B = 2(a^2 - b^2)$.

Output $z_{P+Q} = (t_0, t_1)$.

1. $t'_0 = (x_0^2 + x_1^2)(y_0^2 + y_2^2)/A$
2. $t'_1 = (x_0^2 - x_1^2)(y_0^2 - y_1^2)/B$
3. $t_0 = (t'_0 + t'_1)/z_0$
4. $t_1 = (t'_0 - t'_1)/z_1$

Return (t_0, t_1)

Miller functions with theta coordinates

Proposition (Lubicz-R. [LR13])

- *For $P \in A$ we note z_P a lift to $\mathbb{C}^g$. We call P a projective point and z_P an affine point (because we describe them via their projective, resp affine, theta coordinates);*
- *We have (up to a constant)*

$$f_{\lambda,P}(z) = \frac{\vartheta(z)}{\vartheta(z+\lambda z_P)} \left(\frac{\vartheta(z+z_P)}{\vartheta(z)} \right)^{\lambda};$$

- *So (up to a constant)*

$$\mathfrak{f}_{\lambda,\mu,P}(z) = \frac{\vartheta(z+\lambda z_P)\vartheta(z+\mu z_P)}{\vartheta(z)\vartheta(z+(\lambda+\mu)z_P)}.$$

Three way addition

Proposition (Lubicz-R. [LR13])

From the affine points z_P, z_Q, z_R, z_{P+Q}, z_{P+R} and z_{Q+R} one can compute the affine point z_{P+Q+R}.
(In level 2, the proposition is only valid for "generic" points).

Proof.

We can compute the three way addition using a generalised version of Riemann's relations:

$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{i+t}(z_{P+Q+R})\vartheta_{j+t}(z_P)\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{k+t}(z_Q)\vartheta_{l+t}(z_R)\Big)=$$

$$\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{-i'+t}(z_0)\vartheta_{j'+t}(z_{Q+R})\Big).\Big(\sum_{t\in Z(\overline{2})}\chi(t)\vartheta_{k'+t}(z_{P+R})\vartheta_{l'+t}(z_{P+Q})\Big).$$

□

Computing the Miller function $f_{\lambda,\mu,P}((Q)-(0))$

Algorithm

Input λP, μP and Q;

Output $f_{\lambda,\mu,P}((Q)-(0))$

1. *Compute $(\lambda+\mu)P$, $Q+\lambda P$, $Q+\mu P$ using normal additions and take any affine lifts $z_{(\lambda+\mu)P}$, $z_{Q+\lambda P}$ and $z_{Q+\mu P}$;*
2. *Use a three way addition to compute $z_{Q+(\lambda+\mu)P}$;*

Return

$$f_{\lambda,\mu,P}((Q)-(0)) = \frac{\vartheta(z_Q+\lambda z_P)\vartheta(z_Q+\mu z_P)}{\vartheta(z_Q)\vartheta(z_Q+(\lambda+\mu)z_P)} \cdot \frac{\vartheta((\lambda+\mu)z_P)\vartheta(z_P)}{\vartheta(\lambda z_P)\vartheta(\mu z_P)}.$$

Lemma

The result does not depend on the choice of affine lifts in Step 2.

- ☺ This allow us to evaluate the Weil and Tate pairings and derived pairings;
- ☹ Not possible *a priori* to apply this algorithm in level 2.

The Tate pairing with Miller's functions and theta coordinates

- Let $P \in A[\ell](\mathbb{F}_{q^d})$ and $Q \in A(\mathbb{F}_{q^d})$; choose any lift z_P, z_Q and z_{P+Q}.
- The algorithm loop over the binary expansion of ℓ, and at each step does a doubling step, and if necessary an addition step.

Given	$z_{\lambda P}, z_{\lambda P+Q}$;
Doubling	Compute $z_{2\lambda P}, z_{2\lambda P+Q}$ using two differential additions;
Addition	Compute $(2\lambda+1)P$ and take an arbitrary lift $z_{(2\lambda+1)P}$. Use a three way addition to compute $z_{(2\lambda+1)P+Q}$.

- At the end we have computed affine points $z_{\ell P}$ and $z_{\ell P+Q}$. Evaluating the Miller function then gives exactly the quotient of the projective factors between $z_{\ell P}, z_0$ and $z_{\ell P+Q}, z_Q$.

☺ Described this way can be extended to level 2 by using compatible additions;

☹ Can we get rid of three way additions?

The Weil and Tate pairing with theta coordinates (Lubicz-R. [LR10])

P and Q points of ℓ-torsion.

z_0	z_P	$2z_P$	$\dots$	$\ell z_P = \lambda_P^0 z_0$
z_Q	$z_P \oplus z_Q$	$2z_P + z_Q$	$\dots$	$\ell z_P + z_Q = \lambda_P^1 z_Q$
$2z_Q$	$z_P + 2z_Q$			
$\dots$	$\dots$			
$\ell Q = \lambda_Q^0 0_A$	$z_P + \ell z_Q = \lambda_Q^1 z_P$			

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

Ate pairing

- Let $P \in G_2 = A[\ell] \bigcap \mathrm{Ker}(\pi_q - [q])$ and $Q \in G_1 = A[\ell] \bigcap \mathrm{Ker}(\pi_q - 1)$; $\lambda \equiv q \mod \ell$.
- In projective coordinates, we have $\pi_q^d(P+Q) = \lambda^d P + Q = P + Q$;
- Of course, in affine coordinates, $\pi_q^d(z_{P+Q}) \neq \lambda^d z_P + z_Q$.
- But if $\pi_q(z_{P+Q}) = C * (\lambda z_P + z_Q)$, then C is exactly the (non reduced) ate pairing (up to a renormalisation)!

Algorithm (Computing the ate pairing)

Input $P \in G_2$, $Q \in G_1$;

1. *Compute* $z_Q + \lambda z_P$, λz_P *using differential additions;*
2. *Find the projective factors* C_1 *and* C_0 *such that* $z_Q + \lambda z_P = C_1 * \pi(z_{P+Q})$ *and* $\lambda z_P = C_0 * \pi(z_P)$ *respectively;*

Return $(C_1/C_0)^{\frac{q^d-1}{\ell}}$.

Optimal ate pairing

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

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

  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 $c_i \approx \ell^{1/\varphi(d)}$.

Optimal ate pairing with theta functions

Algorithm (Computing the optimal ate pairing)

Input $\pi_q(P)=[q]P$, $\pi_q(Q)=Q$, $\lambda=m\ell=\sum c_i q^i$;

1. *Compute the* $z_Q+c_i z_P$ *and* $c_i z_P$;
2. *Apply Frobeniuses to obtain the* $z_Q+c_i q^i z_P$, $c_i q^i z_P$;
3. *Compute* $c_i q^i z_P \oplus \sum_j c_j q^j z_P$ *(up to a constant) and then do a three way addition to compute* $z_Q+c_i q^i z_P+\sum_j c_j q^j z_P$ *(up to the same constant);*
4. *Recurse until we get* $\lambda z_P = C_0 * z_P$ *and* $z_Q+\lambda z_P = C_1 * z_Q$;

Return $(C_1/C_0)^{\frac{q^d-1}{\ell}}$.

One step of the pairing computation

Algorithm (A step of the Miller loop with differential additions)

Input $nP=(x_n,z_n)$; $(n+1)P=(x_{n+1},z_{n+1})$, $(n+1)P+Q=(x'_{n+1},z'_{n+1})$.

Output $2nP=(x_{2n},z_{2n})$; $(2n+1)P=(x_{2n+1},z_{2n+1})$; $(2n+1)P+Q=(x'_{2n+1},z'_{2n+1})$.

1. $\alpha=(x_n^2+z_n^2)$; $\beta=\frac{A}{B}(x_n^2-z_n^2)$.
2. $X_n=\alpha^2$; $X_{n+1}=\alpha(x_{n+1}^2+z_{n+1}^2)$; $X'_{n+1}=\alpha({x'}_{n+1}^2+{z'}_{n+1}^2)$;
3. $Z_n=\beta(x_n^2-z_n^2)$; $Z_{n+1}=\beta(x_{n+1}^2-z_{n+1}^2)$; $Z'_{n+1}=\beta({x'}_{n+1}^2+{z'}_{n+1}^2)$;
4. $x_{2n}=X_n+Z_n$; $x_{2n+1}=(X_{n+1}+Z_{n+1})/x_P$; $x'_{2n+1}=(X'_{n+1}+Z'_{n+1})/x_Q$;
5. $z_{2n}=\frac{a}{b}(X_n-Z_n)$; $z_{2n+1}=(X_{n+1}-Z_{n+1})/z_p$; $z'_{2n+1}=(X'_{n+1}-Z'_{n+1})/z_Q$;

Return (x_{2n},z_{2n}); (x_{2n+1},z_{2n+1}); (x'_{2n+1},z'_{2n+1}).

Weil and Tate pairing over $\mathbb{F}_{q^d}$

$g=1$	$4\mathbf{M}+2\mathbf{m}+8\mathbf{S}+3\mathrm{m}_0$
$g=2$	$8\mathbf{M}+6\mathbf{m}+16\mathbf{S}+9\mathrm{m}_0$

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

Operations in $\mathbb{F}_q$: M: multiplication, S: square, m multiplication by a coordinate of P or Q, m_0 multiplication by a theta constant;

Mixed operations in $\mathbb{F}_q$ and $\mathbb{F}_{q^d}$: M, m and m_0;

Operations in $\mathbb{F}_{q^d}$: $\mathbf{M}$, $\mathbf{m}$ and $\mathbf{S}$.

Remark

- *Doubling step for a Miller loop with Edwards coordinates:* $9\mathbf{M}+7\mathbf{S}+2\mathrm{m}_0$;
- *Just doubling a point in Mumford projective coordinates using the fastest algorithm [Lan05]:* $33\mathbf{M}+7\mathbf{S}+1\mathrm{m}_0$;
- *Asymptotically the final exponentiation is more expensive than Miller's loop, so the Weil's pairing is faster than the Tate's pairing!*

Tate pairing

$g=1$	$1\mathbf{m}+2\mathbf{S}+2\mathrm{M}+2M+1m+6S+3m_0$
$g=2$	$3\mathbf{m}+4\mathbf{S}+4\mathrm{M}+4M+3m+12S+9m_0$

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

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

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

Ate and optimal ate pairings

$g=1$	$4\mathbf{M}+1\mathbf{m}+8\mathbf{S}+1\mathrm{m}+3\mathrm{m}_0$
$g=2$	$8\mathbf{M}+3\mathbf{m}+16\mathbf{S}+3\mathrm{m}+9\mathrm{m}_0$

Ate pairing with theta coordinates, $P\in G_2, Q\in G_1$ (one step)

Remark

Using affine Mumford coordinates in dimension 2, the hyperelliptic ate pairing costs [Gra+07]:

Doubling $1\mathbf{I}+29\mathbf{M}+9\mathbf{S}+7\mathrm{M}$

Addition $1\mathbf{I}+29\mathbf{M}+5\mathbf{S}+7\mathrm{M}$

(where $\mathbf{I}$ *denotes the cost of an affine inversion in* $\mathbb{F}_{q^d}$*).*

Bibliography

R. Granger, F. Hess, R. Oyono, N. Thériault, and F. Vercauteren. "Ate pairing on hyperelliptic curves". In: *Advances in cryptology—EUROCRYPT 2007*. Vol. 4515. Lecture Notes in Comput. Sci. Berlin: Springer, 2007, pp. 430–447 (cit. on p. 32).

S. Lang. "Reciprocity and Correspondences". In: *American Journal of Mathematics* 80.2 (1958), pp. 431–440 (cit. on p. 14).

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. 30).

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. 25).

D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". Mar. 2013. Url: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192 (cit. on pp. 21, 22).