Pairings on abelian varieties and the Discrete Logarithm Problem

2014/05 — Ascona

David Lubicz, **Damien Robert**

Inria Bordeaux Sud-Ouest

Goal

- $A/\mathbb{F}_q$ is a principally polarized abelian variety of small dimension defined over a field of small characteristic and of size 256 bits;
- We want to attack the DLP on A;
- $\#A(\mathbb{F}_q)$ is divisible by a large prime ℓ;
- But there exists a small d such that $\ell \mid q^d - 1$ …

Outline

1. Pairings on abelian varieties
2. Miller's algorithm
3. Theta functions
4. Pairings with theta functions

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;
- In dimension $g \geqslant 4$, not every abelian variety is a Jacobian.

The dual Abelian variety

- We have $\hat{A}(\overline{k}) = \mathrm{Pic}^0(A)$;
- Let $\mathscr{L} \in \mathrm{Pic}^0(A)$, since $\mathscr{L}$ is algebraically equivalent to 0, $t_P^\star \mathscr{L} \otimes \mathscr{L}^{-1}$ is linearly equivalent to 0 for all $P \in A(\overline{k})$, so it corresponds to a function $g_{\mathscr{L},P}$;
- The application $\mathscr{L} \mapsto (A \times A \to \mathbb{G}_m,\ (P,Q) \mapsto g_{\mathscr{L},P}(Q)/g_{\mathscr{L},P}(0))$ gives a natural isomorphism $\mathrm{Pic}^0(A) \xrightarrow{\sim} \mathrm{Ext}^1(A, \mathbb{G}_m)$.

Dual isogeny

- Let $f: A \to B$ be a separable isogeny with kernel K between two abelian varieties defined over k;
- Applying the functor Ext to the short exact sequence

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

  gives the long sequence

$$\begin{tikzcd}
0 \arrow[r] & Hom(K,\mathbb{G}_m) \arrow[r] \arrow[d, equal] & Ext^1(B,\mathbb{G}_m) \arrow[r] \arrow[d, equal] & Ext^1(A,\mathbb{G}_m) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \hat{K} \arrow[r] & \hat{B} \arrow[r, "\hat{f}"] & \hat{A} \arrow[r] & 0
\end{tikzcd}$$

- $\hat{K}$ is then naturally identified with $\mathrm{Hom}(K,\mathbb{G}_m)$, the Cartier dual of K.

The Weil-Cartier pairing

- The isogeny f and its dual $\hat{f}$ fit into the diagram

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] & A \arrow[r, "f"] & B \arrow[r] & 0 \\ & 0 & \hat{A} \arrow[l] & \hat{B} \arrow[l, "\hat{f}"'] & \hat{K} \arrow[l] & 0 \arrow[l] \end{tikzcd}$$

- Since $\hat{K}$ is the Cartier dual of K we have a non degenerate pairing $e_f : K \times \hat{K} \to \mathbb{G}_m$;
- Unravelling the identification, we can compute the Weil-Cartier pairing as follows:
  1. If $Q \in \hat{K}(\bar{k})$, 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 $[\ell] : A \to A$

$$e_{W,\ell} : A[\ell] \times \hat{A}[\ell] \to \mu_\ell.$$

Reformulation

$$\begin{tikzcd}
f^*D_Q \arrow[r, "\psi_Q"] \arrow[d, "\psi_P"] & \mathcal{O}_A \arrow[d, equal, "e_f(P,Q)"] \\
\tau_P^* f^* D_Q \arrow[r, "\tau_P^*\psi_Q"] & \tau_P^*\mathcal{O}_A
\end{tikzcd}$$

(ψ_P is normalized via $A(P) \simeq A(0)$.)

- Since f^*D_Q is trivial, by descent theory D_Q is the quotient of $A \times \mathbb{A}^1$ by an action of K:
$$g_x.(t,\lambda) = (t+x, \chi_Q(x)\lambda)$$
where χ_Q is a character on K;
$$e_f(P,Q) = \chi_Q(P).$$

Polarizations

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

Definition (Weil pairing)

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

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

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

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

Definition (Embedding degree)

If A is defined over a finite field $\mathbb{F}_q$, the Weil pairing has image in $\mu_\ell(\overline{\mathbb{F}}_q) \subset \mathbb{F}_{q^d}^*$ where d is the embedding degree.

The commutator pairing

- In general for an ample line bundle $\mathscr{L}$, the polarization $\varphi_{\mathscr{L}}$ gives an isogeny

$$0 \longrightarrow K(\mathscr{L}) \longrightarrow A \longrightarrow \hat{A} \longrightarrow 0$$

  and thus a pairing

$$e_{\mathscr{L}} : K(\mathscr{L}) \times K(\mathscr{L}) \to \mathbb{G}_m.$$

- The following diagram is commutative up to a multiplication by $e_{\mathscr{L}}(P,Q)$:

$$\begin{tikzcd}
\mathscr{L} \arrow[r, "\psi_P"] \arrow[d, "\psi_Q"] & \tau_P^*\mathscr{L} \arrow[d, "\tau_P^*\psi_Q"] \\
\tau_Q^*\mathscr{L} \arrow[r, "\tau_Q^*\psi_P"] & \tau_{P+Q}^*\mathscr{L}
\end{tikzcd}$$

The commutator pairing

- The Theta group $G(\mathscr{L})$ is the group $\{(x, \psi_x)\}$ where $x \in K(\mathscr{L})$ and ψ_x is an isomorphism
$$\psi_x : \mathscr{L} \to \tau_x^* \mathscr{L}$$
The composition is given by $(y, \psi_y).(x, \psi_x) = (y + x, \tau_x^* \psi_y \circ \psi_x)$.
- $G(\mathscr{L})$ is an Heisenberg group:
$$0 \longrightarrow k^* \longrightarrow G(\mathscr{L}) \longrightarrow K(\mathscr{L}) \longrightarrow 0$$
- Let $g_P = (P, \psi_P) \in G(\mathscr{L})$ and $g_Q = (Q, \psi_Q) \in G(\mathscr{L})$,
$$e_{\mathscr{L}}(P, Q) = g_P g_Q g_P^{-1} g_Q^{-1};$$
- If $\psi : K(\mathscr{L}) \times K(\mathscr{L}) \to k^*$ is the 2-cocycle associated to $G(\mathscr{L})$, we also have
$$e_{\mathscr{L}}(P, Q) = \frac{\psi(P, Q)}{\psi(Q, P)}.$$

The Tate-Lichtenbaum-Frey-Rück pairing [FR94]

- If A is a principally polarised abelian variety over a p-adic field, the Tate pairing is a non degenerate pairing
$$H^1(G,A) \times A(k) \to \mathrm{Br}(k)$$
where G is the absolute Galois group and $\mathrm{Br}(k) = H^2(G, \overline{k}^*) \simeq \mathbb{Q}/\mathbb{Z} \simeq \mu$.
- Frey and Rück then reduces this pairing modulo p to obtain that on an abelian variety $A/\mathbb{F}_q$, there is a non degenerate pairing
$$e_T : A_0[\ell](\mathbb{F}_{q^d}) \times A(\mathbb{F}_q)/\ell A(\mathbb{F}_q) \to \mathbb{F}_{q^d}^*/\mathbb{F}_{q^d}^{*,\ell},$$
where d is the embedding degree and $A_0[\ell] = \{P \in A[\ell] \mid \pi P = [q]P\}$.
- To compute the pairing on a Jacobian $\mathrm{Jac}(C)$, they use a version of the Tate pairing given by Lichtenbaum using the exact sequence
$$1 \longrightarrow \mathrm{Princ}_{C_{\overline{k}}} \longrightarrow \mathrm{Div}^0_{C_{\overline{k}}} \longrightarrow \mathrm{Pic}^0_{C_{\overline{k}}} \longrightarrow 0$$
which gives the connection $\delta : H^1(G, \mathrm{Pic}^0_{C_{\overline{k}}}) \to H^2(G, \mathrm{Princ}_{C_{\overline{k}}})$ and a pairing
$$\begin{aligned} H^1(G, \mathrm{Pic}^0_{C_{\overline{k}}}) \times \mathrm{Pic}^0_C &\longrightarrow H^2(G, \mathbb{G}_m) \\ (\gamma, D) &\longmapsto (\sigma \mapsto (\delta(\gamma)(\sigma)(D))) \end{aligned}$$
- Thus $e_T(D_1, D_2) = f_{\ell, D_1}(D_2)$ where f_{ℓ, D_1} is a function with divisor ℓD_1.

Galois cohomology

- Let G be a finite group; the functor $M \mapsto M^G$ defined on G-modules is left exact but not right exact. This defines the cohomology groups $H^i(G,M)$;
- If G is the absolute Galois group of a field K, we will also note the cohomology groups as $H^i(K,M)$;
- If L/K is Galoisian, there is an inflation restriction exact sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), M(L)) \underset{\mathrm{inf}}{\longrightarrow} H^1(K,M) \underset{\mathrm{res}}{\longrightarrow} H^1(L,M)^{\mathrm{Gal}(L/K)} \longrightarrow H^2(Gal(L/K), M(L))$$

- If $k = \mathbb{F}_q$, one can use Tate's cohomology groups to show that $H^1(k,M) = M/(\pi-1)M$ and $\#H^1(k,M) = \#H^0(k,M) = \#M(k)$ (for a finitely generated module M).

Kummer exact sequence

- The exact sequence
$$1 \to \mu_\ell \to \overline{k}^* \to \overline{k}^* \to 1$$
induces a connecting map
$$\delta : \overline{k}^* / \overline{k}^{*,\ell} \simeq H^1(k, \mu_\ell)$$
(the isomorphism comes from Hilbert 90: $H^1(k, k^*) = 0$).
- Thus for a finite field $k = \mathbb{F}_q$
$$\mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*,\ell} \simeq H^1(\mathbb{F}_{q^d}, \mu_\ell) \simeq \mu_\ell(\mathbb{F}_{q^d});$$
- The isomorphism is given by the exponentiation $x \mapsto x^{\frac{q^d-1}{\ell}}$.

The Tate-Cartier pairing on abelian varieties over finite fields

- Let $f : A \to B$ be an isogeny with $\operatorname{Ker} f \subset A[\ell]$;
- From the exact sequence
$$0 \to \operatorname{Ker} f \to A \to B \to 0$$
we get from Galois cohomology a connecting morphism
$$\delta : A(\mathbb{F}_{q^d})/f(B(\mathbb{F}_{q^d})) \simeq H^1(\mathbb{F}_{q^d}, \operatorname{Ker} f)$$
(this is an isomorphism since $H^1(\mathbb{F}_{q^d}, A) = 0$ for an abelian variety over a finite field);
- Composing with the Weil-Cartier pairing, we get a bilinear application
$$\operatorname{Ker} \hat{f}(\mathbb{F}_{q^d}) \times A(\mathbb{F}_{q^d})/f(B(\mathbb{F}_{q^d})) \to H^1(\mathbb{F}_{q^d}, \mu_\ell) \simeq \mathbb{F}_{q^d}^*/\mathbb{F}_{q^d}^{*\,\ell} \simeq \mu_\ell;$$
- Explicitely, if $P \in \operatorname{Ker} \hat{f}(\mathbb{F}_{q^d})$ and $Q \in A(\mathbb{F}_{q^d})$ then the (reduced) Tate pairing is given by
$$e_T(P,Q) = e_W(\pi^d(Q_0) - Q_0, P)$$
where $Q_0 \in A$ is any point such that $Q = f(Q_0)$ and π is the Frobenius of $\mathbb{F}_q$;

The Tate-Cartier pairing on abelian varieties over finite fields

Theorem

The Tate pairing

$$\operatorname{Ker} \hat{f}(\mathbb{F}_{q^d}) \times A(\mathbb{F}_{q^d})/f(B(\mathbb{F}_{q^d})) \to H^1(\mathbb{F}_{q^d}, \mu_\ell) \simeq \mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*\,\ell} \simeq \mu_\ell$$

is non degenerate.

Proof.

We have canonically

$$\begin{aligned}\operatorname{Ker} \hat{f}(\mathbb{F}_{q^d}) &= \operatorname{Hom}(\operatorname{Ker} f, \mathbb{G}_m)^{\operatorname{Gal}(\overline{\mathbb{F}}_{q^d}/\mathbb{F}_{q^d})} \\ &= \operatorname{Hom}(\operatorname{Ker} f/(\pi^d - 1), \mathbb{F}_{q^d}^*) \\ &= \operatorname{Hom}(H^1(\mathbb{F}_{q^d}, \operatorname{Ker} f), \mathbb{F}_{q^d}^*)\end{aligned}$$

and

$$A(\mathbb{F}_{q^d})/f(B(\mathbb{F}_{q^d})) \simeq H^1(\mathbb{F}_{q^d}, \operatorname{Ker} f).$$

□

The Tate pairing on a principally polarised abelian variety

- Let $(A, \mathscr{L})$ be a principally polarised abelian variety; applying the theory to the isogeny $f = [\ell]$ yields the usual Tate pairing

$$A[\ell](\mathbb{F}_{q^d}) \times A(\mathbb{F}_{q^d})/\ell A(\mathbb{F}_{q^d}) \to \mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*\,\ell} \simeq \mu_\ell;$$

- If A is principally polarised over a finite field, the Weil-Cartier pairing associated to the isogeny $\pi^d - 1$ gives a non degenerate pairing

$$A(\mathbb{F}_{q^d}) \times \mathrm{Ker}(\widehat{\pi}^d - 1) \to \mathbb{G}_m$$

  where $\widehat{\pi}$ is the Verschiebung;
- Since $(\pi^d - 1)(\widehat{\pi}^d - 1) = q^d - \pi^d - \widehat{\pi}^d + 1$ we get by restriction a (possibly degenerate) pairing

$$A[\ell](\mathbb{F}_{q^d}) \times A[\ell](\mathbb{F}_{q^d}) \to \mu_\ell;$$

- From the definition above, this is a special case of the Tate pairing (restricted to a subgroup).

The Tate pairing on a principally polarised abelian variety

- Let $(A, \mathscr{L})$ be a principally polarised abelian variety; applying the theory to the isogeny $f = [\ell]$ yields the usual Tate pairing

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

- Over $\mathbb{F}_q$, if we note $G_1 = A[\ell](\mathbb{F}_q)$ of type $(\mathbb{Z}/\ell\mathbb{Z})^r$, because π is a Weil number there is a subgroup $G_2 \subset A[\ell]$ of type μ_ℓ^r;
- Let $g : A \rightarrow A/G_2$, and $f : A/G_2 \rightarrow \hat{A} \simeq A$ be the dual isogeny; then we get that the restriction of the Tate pairing to

$$G_2(\mathbb{F}_{q^d}) \times A(\mathbb{F}_q)/\ell A(\mathbb{F}_q) \rightarrow \mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*\,\ell}$$

  is non degenerate;
- If $A(\mathbb{F}_q)$ does not contain a point of ℓ^2-torsion, we get a pairing

$$G_2(\mathbb{F}_{q^d}) \times G_1(\mathbb{F}_q) \rightarrow \mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*\,\ell};$$

- Likewise, if $A(\mathbb{F}_{q^d})$ does not contain a point of ℓ^2-torsion, we get by considering the isogeny $A \rightarrow A/G_1$ a pairing

$$G_1(\mathbb{F}_q) \times G_2(\mathbb{F}_{q^d}) \rightarrow \mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*\,\ell}.$$

Pairings and the Discrete Logarithm Problem

- The Weil pairing was first used to transfer the DLP from an elliptic curve to $\mathbb{F}_{q^d}^*$ (the MOV attack [MOV91]);
- Unfortunately, to get a non degenerate pairing we need to work in the field of definition of the points of ℓ torsion which may be larger than $\mathbb{F}_{q^d}$;
- Frey and Rück then introduced the Tate pairing to alleviate this problem: we can always find a non degenerate pairing by working over $\mathbb{F}_{q^d}$;
- Moreover in the cryptographic case where $A(\mathbb{F}_q) = < P >$ is cyclic with order a large prime, it is straightforward to find a point $Q \in A(\mathbb{F}_{q^d})$ such that $e_T(P, Q) \neq 1$;
- Computing the Tate (and Weil pairing) on elliptic curves (and Jacobians) can be done using Miller's algorithm [Mil86];
- What about abelian varieties?

The Weil and Tate pairing on elliptic curves

- Let $E: y^2 = x^3 + ax + b$ be an elliptic curve over a field k ($\operatorname{char} k \neq 2, 3$, $4a^3 + 27b^2 \neq 0$.)
- Let $P, Q \in E[\ell]$ be points of ℓ-torsion; let $f_{\ell,P}$ be a function associated to the principal divisor $\ell(P) - \ell(0)$, and $f_{\ell,Q}$ to $\ell(Q) - \ell(0)$.
- The Weil pairing $e_{W,\ell}: E[\ell] \times E[\ell] \to \mu_\ell(\overline{k})$ is given by

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

- The Tate pairing is given by

$$\begin{array}{rcl} e_T \colon G_2(\mathbb{F}_{q^d}) \times E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_{q^d}^* / \mathbb{F}_{q^d}^{*\ \ell} \\ (P,Q) & \longmapsto & f_{\ell,P}((Q)-(0)) \end{array}.$$

  where

$$G_2(\mathbb{F}_{q^d}) = \{P \in E[\ell](\mathbb{F}_{q^d}) \mid \pi(P) = [q]P\}.$$

Miller's functions

- We need to compute the functions $f_{\ell,P}$ and $f_{\ell,Q}$. 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:

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

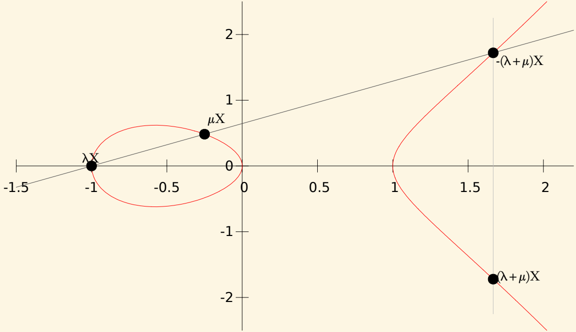
- We want to compute (for instance) $f_{\ell,P}((Q)-(0))$.

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
$$([\lambda]X) + ([\mu]X) - ([\lambda+\mu]X) - (0).$$
- 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
$$\mathfrak{f}_{\lambda,\mu,X} = \frac{y - \alpha(x - x_1) - y_1}{x + (x_1 + x_2) - \alpha^2}.$$

Miller's algorithm for elliptic curves

$$[\lambda]X = (x_1, y_1) \quad [\mu]X = (x_2, y_2)$$



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

Miller's algorithm for the Tate pairing on elliptic curves

Algorithm (Computing the Tate pairing)

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

Output: $e_T(P, Q)$.

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

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

Miller's algorithm on Jacobians

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

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

- A key ingredient for evaluating $f_P(D_Q)$ comes from Weil's 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

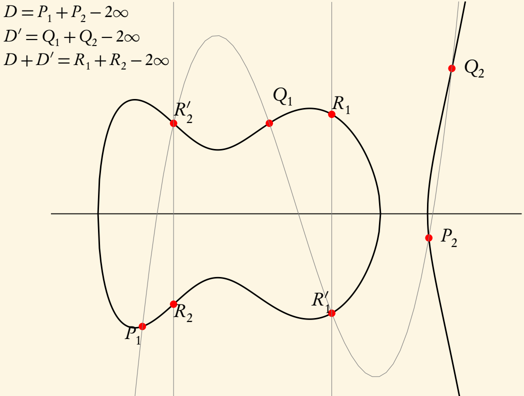
$$f_{D_1}(D_2) = f_{D_2}(D_1).$$

Miller's algorithm on Jacobians of genus 2 curves

- 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.



Cycles and Lang reciprocity

- Let (A,Θ) be a principally polarized abelian variety;
- To a degree 0 cycle $\sum n_i(P_i)$ on A, we can associate the divisor $\sum n_i t_{P_i}^* \Theta$ on A;
- The cycle $\sum n_i(P_i)$ corresponds to a trivial divisor iff $\sum n_i P_i = 0$ 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

$$f(D) = \prod f(P_i)^{n_i}.$$

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

Theorem (Lang [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

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

Polarised abelian varieties over $\mathbb{C}$

Definition

A complex abelian variety A of dimension g is isomorphic to a compact Lie group V/Λ with

- A complex vector space V of dimension g;
- A $\mathbb{Z}$-lattice Λ in V (of rank $2g$);

such that there exists an Hermitian form H on V with $E(\Lambda,\Lambda) \subset \mathbb{Z}$ where $E = \operatorname{Im} H$ is symplectic.

- Such an Hermitian form H is called a polarisation on A. Conversely, any symplectic form E on V such that $E(\Lambda,\Lambda) \subset \mathbb{Z}$ and $E(ix,iy) = E(x,y)$ for all $x,y \in V$ gives a polarisation H with $E = \operatorname{Im} H$.
- Over a symplectic basis of Λ, E is of the form.

$$\begin{pmatrix} 0 & D_\delta \\ -D_\delta & 0 \end{pmatrix}$$

  where D_δ is a diagonal positive integer matrix $\delta = (\delta_1, \delta_2, \ldots, \delta_g)$, with $\delta_1 \mid \delta_2 | \cdots \mid \delta_g$.
- The product $\prod \delta_i$ is the degree of the polarisation; H is a principal polarisation if this degree is 1.

Projective embeddings

Proposition

Let $\Phi : A = V/\Lambda \mapsto \mathbb{P}^{m-1}$ be a projective embedding. Then the linear functions f associated to this embedding are Λ-automorphics:

$$f(x+\lambda) = a(\lambda,x)f(x) \quad x \in V, \lambda \in \Lambda;$$

for a fixed automorphy factor a:

$$a(\lambda+\lambda',x) = a(\lambda, x+\lambda')a(\lambda',x).$$

Theorem (Appell-Humbert)

All automorphy factors are of the form

$$a(\lambda,x) = \pm e^{\pi(H(x,\lambda)+\frac{1}{2}H(\lambda,\lambda))}$$

for a polarisation H on A.

Theta functions

- Let (A, H_0) be a principally polarised abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ with $\Omega \in \mathfrak{H}_g$.
- The associated Riemann form on A is then given by $E_1(\Omega x_1 + x_2, \Omega y_1 + y_2) = {}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2$; equivalently the matrix of H_0 is $\operatorname{Im}\Omega^{-1}$.
- The Weil pairing on $A[\ell]$ corresponds to the symplectic form E on $\frac{1}{\ell}\Lambda/\Lambda$.
- All automorphic forms corresponding to a multiple $H = nH_0$ of H_0 come from the theta functions with characteristics:

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

- Automorphic property:

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

Remark

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

Theta functions of level n

- Define $\vartheta_i = \vartheta\left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix}\right](., \frac{\Omega}{n})$ for $i \in Z(\overline{n}) = \mathbb{Z}^g / n\mathbb{Z}^g$ and
- This is a basis of the automorphic functions for $H = nH_0$ (theta functions of level n);
- This is the unique basis such that in the projective coordinates:

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

  the translation by a point of n-torsion is normalized by

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

- $(\vartheta_i)_{i \in Z(\overline{n})} = \begin{cases} \text{coordinates system} & n \geqslant 3 \\ \text{coordinates on the Kummer variety } A/\pm 1 & n = 2 \end{cases}$
- $(\vartheta_i)_{i \in Z(\overline{n})}$: basis of the theta functions of level n
  $\Leftrightarrow A[n] = A_1[n] \oplus A_2[n]$: symplectic decomposition.
- Theta null point: $\vartheta_i(0)_{i \in Z(\overline{n})} =$ modular invariant.

Jacobians

- Let C be a curve of genus g;
- Let V be the dual of the space $V^* = \Omega^1(C, \mathbb{C})$ of holomorphic differentials of the first kind on C;
- Let $\Lambda \simeq H^1(C, \mathbb{Z}) \subset V$ be the set of periods (integration of differentials on loops);
- The intersection pairing gives a symplectic form E on Λ;
- Let H be the associated hermitian form on V;

$$H^*(w_1, w_2) = \int_C w_1 \wedge w_2;$$

- Then $(V/\Lambda, H)$ is a principally polarised abelian variety: the Jacobian of C.

Theorem (Torelli)

$\mathrm{Jac}\, C$ with the associated principal polarisation uniquely determines C.

Remark (Weil pairing)

In this setting, the Weil pairing can be seen as the intersection pairing on

$$\mathrm{Jac}\, C[\ell] \simeq \frac{1}{\ell} H_1(C, \mathbb{Z}) / H_1(C, \mathbb{Z}) \simeq H_1(C, \mathbb{Z}/\ell\mathbb{Z}).$$

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

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

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

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}.

Proof.

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

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

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

□

Three way addition in dimension 1 level 2

Algorithm

Input *The points* $x, y, z, X = y+z, Y = x+z, Z = x+y$;

Output $T = x+y+z$.

Return

$$T_0 = \frac{(aX_0 + bX_1)(Y_0Z_0 + Y_1Z_1)}{x_0(y_0z_0 + y_1z_1)} + \frac{(aX_0 - bX_1)(Y_0Z_0 - Y_1Z_1)}{x_0(y_0z_0 - y_1z_1)}$$

$$T_1 = \frac{(aX_0 + bX_1)(Y_0Z_0 + Y_1Z_1)}{x_1(y_0z_0 + y_1z_1)} - \frac{(aX_0 - bX_1)(Y_0Z_0 - Y_1Z_1)}{x_1(y_0z_0 - y_1z_1)}$$

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 allows 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;
- ☹ Three way additions and normal (or compatible) additions are quite cumbersome, is there a way to only use differential additions?

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

Using directly the formula for $f_{\ell,P}(z)$ we get that the Weil and Tate pairings are given by

$$e_{W,\ell}(P,Q) = \frac{\vartheta(z_Q + \ell z_P)\vartheta(0)}{\vartheta(z_Q)\vartheta(\ell z_P)} \frac{\vartheta(z_P)\vartheta(\ell z_Q)}{\vartheta(z_P + \ell z_Q)\vartheta(0)}$$

$$e_{T,\ell}(P,Q) = \frac{\vartheta(z_Q + \ell z_P)\vartheta(0)}{\vartheta(z_Q)\vartheta(\ell z_P)}$$

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

P and Q points of ℓ-torsion.

$$\begin{array}{ccccc}
z_0 & z_P & 2z_P & \dots & \ell z_P = \lambda_P^0 z_0 \\
z_Q & z_P \oplus z_Q & 2z_P + z_Q & \dots & \ell z_P + z_Q = \lambda_P^1 z_Q \\
2z_Q & z_P + 2z_Q & & & \\
\dots & \dots & & & \\
\ell Q = \lambda_Q^0 0_A & z_P + \ell z_Q = \lambda_Q^1 z_P & & &
\end{array}$$

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

Why does it work?

$$
\begin{array}{ccccc}
z_0 & \alpha z_P & \alpha^4(2z_P) & \dots & \alpha^{\ell^2}(\ell z_P) = \lambda'^0_P z_0 \\
\beta z_Q & \gamma(z_P \oplus z_Q) & \frac{\gamma^2\alpha^2}{\beta}(2z_P + z_Q) & \dots & \frac{\gamma^\ell \alpha^{\ell(\ell-1)}}{\beta^{\ell-1}}(\ell z_P + z_Q) = \lambda'^1_P \beta z_Q \\
\beta^4(2z_Q) & \frac{\gamma^2\beta^2}{\alpha}(z_P + 2z_Q) & & & \\
\dots & \dots & & & \\
\beta^{\ell^2}(\ell z_Q) = \lambda'^0_Q z_0 & \frac{\gamma^\ell \beta^{\ell(\ell-1)}}{\alpha^{\ell-1}}(z_P + \ell z_Q) = \lambda'^1_Q \alpha z_P & & &
\end{array}
$$

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 over 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:

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

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

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 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.
- 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.

Bibliography

P. Bruin. "The Tate pairing for abelian varieties over finite fields". In: *J. de theorie des nombres de Bordeaux* 23.2 (2011), pp. 323–328.

H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, eds. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xxxiv+808. ISBN: 978-1-58488-518-4; 1-58488-518-1.

G. Frey, M. Muller, and H.-G. Ruck. "The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems". In: *Information Theory, IEEE Transactions on* 45.5 (1999), pp. 1717–1719.

G. Frey and H.-G. Rück. "A remark concerning -divisibility and the discrete logarithm in the divisor class group of curves". In: *Mathematics of computation* 62.206 (1994), pp. 865–874 (cit. on p. 12).

T. Garefalakis. "The generalized Weil pairing and the discrete logarithm problem on elliptic curves". In: *LATIN 2002: Theoretical Informatics*. Springer, 2002, pp. 118–130.

F. Heß. "A note on the Tate pairing of curves over finite fields". In: *Archiv der Mathematik* 82.1 (2004), pp. 28–32.

S. Lang. "Reciprocity and Correspondences". In: *American Journal of Mathematics* 80.2 (1958), pp. 431–440 (cit. on p. 27).

D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: ed. by G. Hanrot, F. Morain, and E. Thomé. Vol. 6197. Lecture Notes in Comput. Sci. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Springer–Verlag, July 2010. 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 pp. 41, 42).

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. 36, 37).

A. Menezes, T. Okamoto, and S. Vanstone. "Reducing elliptic curve logarithms to logarithms in a finite field". In: *Proceedings of the twenty-third annual ACM symposium on Theory of computing*. ACM. 1991, p. 89 (cit. on p. 19).

V. Miller. "Short programs for functions on curves". In: *Unpublished manuscript* 97 (1986), pp. 101–102 (cit. on p. 19).

V. S. Miller. "The Weil Pairing, and Its Efficient Calculation". In: *J. Cryptology* 17.4 (2004), pp. 235–261. DOI: 10.1007/s00145-004-0315-8.

E. F. Schaefer. "A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field". In: *Computational aspects of algebraic curves* 13 (2005), pp. 1–12.