An efficient computation of the commutator pairing

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

[1]CÉLAR

[2]IRMAR, Université de Rennes 1

[3]Nancy Université, CNRS, Inria Nancy Grand Est

Octobre 2010, Réunion CHIC

Pairings and isogeny

Let $f : A \to B$ be an isogeny between two abelian varieties defined over an algebraically closed field k.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{f} & B & \longrightarrow & 0 \\ & & 0 & \longleftarrow & \hat{A} & \xleftarrow{\hat{f}} & \hat{B} & \longleftarrow & \hat{K} & \longleftarrow & 0 \end{array}$$

$\hat{K}$ is the Cartier dual of K. The isogeny f gives a pairing

$$e_f : K \times \hat{K} \to k$$

- Let $Q \in \hat{K}$. Q is a line bundle on B and $\hat{f}(Q) = f^* Q = 0$ so $f^* Q = (g_Q)$.
-
$$e_f(P, Q) = \frac{g_Q(x + P)}{g_Q(x)}$$

Pairings and isogeny

Let $f : A \to B$ be an isogeny between two abelian varieties defined over an algebraically closed field k.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & A & \xrightarrow{f} & B & \longrightarrow & 0 \\ & & 0 & \longleftarrow & \hat{A} & \xleftarrow{\hat{f}} & \hat{B} & \longleftarrow & \hat{K} & \longleftarrow & 0 \end{array}$$

$\hat{K}$ is the Cartier dual of K. The isogeny f gives a pairing

$$e_f : K \times \hat{K} \to k$$

- Let $Q \in \hat{K}$. Q is a line bundle on B and $\hat{f}(Q) = f^*Q = 0$ so $f^*Q = (g_Q)$.
- $$e_f(P, Q) = \frac{g_Q(x + P)}{g_Q(x)}$$

Reformulations

$$\begin{array}{ccc} f^*Q & \xrightarrow{\psi_Q} & \mathscr{O}_A \\ \Big\downarrow \psi_P & & \Big\| \, e_f(P,Q) \\ \tau_P^* f^*Q & \xrightarrow{\tau_P^*\psi_Q} & \tau_P^*\mathscr{O}_A \end{array}$$

(ψ_P is the normalized isomorphism.)

- $$e_f(P,Q) = \frac{g_Q(x+P)}{g_Q(x)}$$
  Since $(g_Q)^\ell = \ell(g_Q) = \ell f^*Q = f^*lQ = f^*(h_Q) = (h_Q \circ f)$, we see that $e_f(P,Q)^m = 1$.
- Since f^*Q is trivial, by Grothendieck descent theory Q is the quotient of $A \times \mathbb{A}^1$ by an action of K.
  $$g_x.(t,\lambda) = (t+x, g_x^0(t)(\lambda))$$
  where the cocycle g_x^0 is a character χ (Appell-Humbert). $e_f(P,Q) = \chi(P)$

Reformulations

$$\begin{array}{ccc} f^*Q & \xrightarrow{\psi_Q} & \mathscr{O}_A \\ \downarrow \psi_P & & \| \, e_f(P,Q) \\ \tau_P^* f^* Q & \xrightarrow{\tau_P^* \psi_Q} & \tau_P^* \mathscr{O}_A \end{array}$$

(ψ_P is the normalized isomorphism.)

- $$e_f(P,Q) = \frac{g_Q(x+P)}{g_Q(x)}$$

  Since $(g_Q)^\ell = \ell(g_Q) = \ell f^*Q = f^* lQ = f^*(h_Q) = (h_Q \circ f)$, we see that $e_f(P,Q)^m = 1$.
- Since f^*Q is trivial, by Grothendieck descent theory Q is the quotient of $A \times \mathbb{A}^1$ by an action of K.

  $$g_x.(t, \lambda) = (t + x, g_x^0(t)(\lambda))$$

  where the cocycle g_x^0 is a character χ (Appell-Humbert). $e_f(P,Q) = \chi(P)$

Reformulations

$$\begin{array}{ccc}
f^* Q & \xrightarrow{\psi_Q} & \mathscr{O}_A \\
\Big\downarrow \psi_P & & \Big\| \, e_f(P,Q) \\
\tau_P^* f^* Q & \xrightarrow{\tau_P^* \psi_Q} & \tau_P^* \mathscr{O}_A
\end{array}$$

(ψ_P is the normalized isomorphism.)

- $$e_f(P,Q) = \frac{g_Q(x+P)}{g_Q(x)}$$
  Since $(g_Q)^\ell = \ell(g_Q) = \ell f^* Q = f^* lQ = f^*(h_Q) = (h_Q \circ f)$, we see that $e_f(P,Q)^m = 1$.
- Since $f^* Q$ is trivial, by Grothendieck descent theory Q is the quotient of $A \times \mathbb{A}^1$ by an action of K.
  $$g_x.(t, \lambda) = (t + x, g_x^0(t)(\lambda))$$
  where the cocycle g_x^0 is a character χ (Appell-Humbert). $e_f(P,Q) = \chi(P)$

Pairings and polarization

- Let $\mathscr{L}$ be a line bundle on A. The polarization $f_{\mathscr{L}} : A \to \hat{A}$ is given by

$$x \mapsto \tau_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$$

- We note $K(\mathscr{L})$ the kernel of the polarization.
- We have $\hat{f}_{\mathscr{L}} = f_{\mathscr{L}}$ so $e_{\mathscr{L}}$ is defined on $K(\mathscr{L}) \times K(\mathscr{L})$.
- 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 :

$$1 \longrightarrow k^* \longrightarrow G(\mathscr{L}) \longrightarrow K(\mathscr{L}) \longrightarrow 0$$

The commutator pairing

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

$$\begin{array}{ccc} \mathscr{L} & \xrightarrow{\psi_P} & \tau_P^* \mathscr{L} \\ \downarrow{\scriptstyle \psi_Q} & & \downarrow{\scriptstyle \tau_P^* \psi_Q} \\ \tau_Q^* \mathscr{L} & \xrightarrow{\tau_Q^* \psi_P} & \tau_{P+Q}^* \mathscr{L} \end{array}$$

Let $g_P = (P, \psi_P) \in G(\mathscr{L})$ and $g_Q = (Q, \psi_Q) \in G(\mathscr{L})$.

$$e_{\mathscr{L}}(P,Q) = g_P g_Q g_P^{-1} g_Q^{-1}$$

The commutator pairing

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

$$\begin{array}{ccc} \mathscr{L} & \xrightarrow{\psi_P} & \tau_P^* \mathscr{L} \\ \downarrow{\scriptstyle \psi_Q} & & \downarrow{\scriptstyle \tau_P^* \psi_Q} \\ \tau_Q^* \mathscr{L} & \xrightarrow{\tau_Q^* \psi_P} & \tau_{P+Q}^* \mathscr{L} \end{array}$$

Let $g_P = (P, \psi_P) \in G(\mathscr{L})$ and $g_Q = (Q, \psi_Q) \in G(\mathscr{L})$.

$$e_{\mathscr{L}}(P,Q) = g_P g_Q g_P^{-1} g_Q^{-1}$$

The Weil pairing

Définition

Let $\mathscr{L}_0$ be a principal polarization on A. The Weil pairing e_ℓ is the pairing associated to the polarization

$$A \xrightarrow{[\ell]} A \xrightarrow{\mathscr{L}_0} \hat{A}$$

We have the following diagram :

$$\begin{CD} A @>f^*\mathscr{M}>> \hat{A} \\ @VfVV @AA\hat{f}A \\ B @>\mathscr{M}>> \hat{B} \end{CD}$$

This mean that $e_{[\ell]^*\mathscr{L}_0} = e_{\ell^2}$ and if $\ell P' = P$ and $\ell Q' = Q$ we have :

$$e_\ell(P,Q) = e_{[\ell]^*\mathscr{L}_0}(P',Q')^\ell$$

The Weil pairing

Définition

Let $\mathscr{L}_0$ be a principal polarization on A. The Weil pairing e_ℓ is the pairing associated to the polarization

$$A \xrightarrow{[\ell]} A \xrightarrow{\mathscr{L}_0} \hat{A}$$

We have the following diagram :

$$\begin{array}{ccc} A & \xrightarrow{f^* \mathscr{M}} & \hat{A} \\ \downarrow f & & \uparrow \hat{f} \\ B & \xrightarrow{\mathscr{M}} & \hat{B} \end{array}$$

This mean that $e_{[\ell]^* \mathscr{L}_0} = e_{\ell^2}$ and if $\ell P' = P$ and $\ell Q' = Q$ we have :

$$e_\ell(P, Q) = e_{[\ell]^* \mathscr{L}_0}(P', Q')^\ell$$

The extended commutator pairing

Let $(A, \mathscr{L})$ be a polarized abelian variety of degree n. There exist a theta structure Θ_n of level n such that the embedding $A \to \mathbf{P}^{n^g-1}$ is given by the theta functions $(\vartheta_i)_{i \in \mathcal{Z}_n}$. We suppose that $4|n$, and that $n \nmid \operatorname{char} k$.
Let ℓ be prime to n, $P, Q \in A[\ell]$. Let $P', Q' \in (A, [\ell]^* \mathscr{L})$ be such that $\ell P' = P$, $\ell Q' = Q$. We want to compute

$$e_{\mathscr{L},\ell}(P, Q) = e_{[\ell]^* \mathscr{L}}(P', Q')^\ell$$

The addition relations

Théorème

$$\Big[\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big[.\Big[\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big[=$$

$$\Big[\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big[.\Big[\sum_{t\in\mathcal{Z}_2}\chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big[. \quad (1)$$

$$where \quad A = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$\chi \in \hat{\mathcal{Z}}_2, i, j, k, l \in \mathcal{Z}_n$$

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

Computing the pairing using chain additions

0_A	P	$2P$	$\dots$	$\ell P = \lambda_P^0 0_A$
Q	$P+Q$	$2P+Q$	$\dots$	$\ell P + Q = \lambda_P^1 Q$
$2Q$	$P+2Q$			
$\dots$	$\dots$			
$\ell Q = \lambda_Q^0 0_A$	$P + \ell Q = \lambda_Q^1 P$			

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

Corollaire

By using a Montgomery ladder, we can compute $e_\ell(P,Q)$ with two fast addition chains of length ℓ, hence we need $O(\log(\ell))$ additions.

Computing the pairing using chain additions

0_A	P	$2P$	$\dots$	$\ell P = \lambda_P^0 0_A$
Q	$P+Q$	$2P+Q$	$\dots$	$\ell P + Q = \lambda_P^1 Q$
$2Q$	$P+2Q$			
$\dots$	$\dots$			
$\ell Q = \lambda_Q^0 0_A$	$P + \ell Q = \lambda_Q^1 P$			

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

Corollaire

By using a Montgomery ladder, we can compute $e_\ell(P,Q)$ with two fast addition chains of length ℓ, hence we need $O(\log(\ell))$ additions.

The Tate pairing

- If we change $P+Q$ by $\lambda(P+Q)$, $\ell P+Q$ is changed by λ^ℓ.
- Hence the half pairing

$$e(P,Q)=\frac{\lambda_P^1}{\lambda_P^0}\in k^*/(k^*)^\ell$$

Corollaire

We can compute the Tate pairing using half as many additions.

The Tate pairing

- If we change $P+Q$ by $\lambda(P+Q)$, $\ell P+Q$ is changed by λ^ℓ.
- Hence the half pairing

$$e(P,Q)=\frac{\lambda_P^1}{\lambda_P^0} \in k^*/(k^*)^\ell$$

Corollaire

We can compute the Tate pairing using half as many additions.

The Kummer surface

- If $n = 2$, we have fast chain addition law in genus 1 and 2 (Gaudry-Lubicz).
- The embedding given by the theta functions $(\vartheta_i)_{i \in \mathcal{Z}_2}$ is the embedding of the Kummer surface $K = A/\pm 1$.
  (And the homogeneous equations of the embedding are not given by Riemann equations but by some other equations from the addition relations).
- Since $P = -P$ and $Q = -Q$ in K, the pairing $e_\ell(P, Q)$ lives in $k^{*,\pm 1}$.
- e_ℓ is compatible with the $\mathbb{Z}$-structure on K and $k^{*,\pm 1}$.
- We represent a class $\{x, 1/x\} \in k^{*,\pm 1}$ by $x + 1/x \in k^*$. We want to compute the symmetric pairing :

$$e(P, Q) = e_\ell(P, Q) + e_\ell(-P, Q)$$

The Kummer surface

- If $n = 2$, we have fast chain addition law in genus 1 and 2 (Gaudry-Lubicz).
- The embedding given by the theta functions $(\vartheta_i)_{i \in \mathcal{Z}_2}$ is the embedding of the Kummer surface $K = A/\pm 1$.
  (And the homogeneous equations of the embedding are not given by Riemann equations but by some other equations from the addition relations).
- Since $P = -P$ and $Q = -Q$ in K, the pairing $e_\ell(P,Q)$ lives in $k^{*,\pm 1}$.
- e_ℓ is compatible with the $\mathbb{Z}$-structure on K and $k^{*,\pm 1}$.
- We represent a class $\{x, 1/x\} \in k^{*,\pm 1}$ by $x + 1/x \in k^*$. We want to compute the symmetric pairing :

$$e(P,Q) = e_\ell(P,Q) + e_\ell(-P,Q)$$

Addition law on the Kummer surface

- Once we have $P \pm Q$ we can use chain additions to compute the symmetric pairing.

Conjecture

If $\chi(i-j)=0$ *then :*

$$\Big[\sum_{t \in \mathcal{Z}_2} \chi(t)\vartheta_{j+t}(0)\vartheta_{i+t}(0) \Big[\neq 0 \qquad (2)$$

- This means that with the addition formulas we can compute

$$\vartheta_i(P+Q)\vartheta_i(P-Q)$$

$$\vartheta_i(P+Q)\vartheta_j(P-Q)+\vartheta_j(P+Q)\vartheta_i(P-Q)$$

- This is sufficient to write a projective system of degree 2 such that the roots are $(P+Q, P-Q)$ and $(P-Q, P+Q)$.

Addition law on the Kummer surface

- Once we have $P \pm Q$ we can use chain additions to compute the symmetric pairing.

Conjecture

If $\chi(i-j)=0$ *then :*

$$\Big[\sum_{t \in \mathcal{Z}_2} \chi(t)\vartheta_{j+t}(0)\vartheta_{i+t}(0) \Big[\neq 0 \qquad (2)$$

- This means that with the addition formulas we can compute

$$\vartheta_i(P+Q)\vartheta_i(P-Q)$$

$$\vartheta_i(P+Q)\vartheta_j(P-Q)+\vartheta_j(P+Q)\vartheta_i(P-Q)$$

- This is sufficient to write a projective system of degree 2 such that the roots are $(P+Q, P-Q)$ and $(P-Q, P+Q)$.

Direct computation of the symmetric pairing ($g = 1$ for the example)

- We want to compute

$$e_\ell(P,Q) = \frac{\vartheta_i(Q)(\vartheta_i(P+\ell Q)\vartheta_i(\ell P - Q) + \vartheta_i(P - \ell Q)\vartheta_i(\ell P + Q))}{\vartheta_i(P)\vartheta_i(\ell P + Q)\vartheta_i(\ell P - Q)}$$

- We can compute $a_0 = \vartheta_0(P+Q)\vartheta_0(P-Q)$, $a_1 = \vartheta_1(P+Q)\vartheta_1(P-Q)$, and $b = \vartheta_0(P+Q)\vartheta_1(P-Q) + \vartheta_1(P-Q)\vartheta_0(P+Q)$.
- Let t_1 and t_2 be the roots of $P = X^2 - bX + a_1 a_2$.
- Then $(t_1, a_1) = \vartheta_1(P+Q)(P-Q)$ and $(t_2, a_1) = \vartheta_1(P-Q)(P+Q)$.

$\Rightarrow$ This mean we can compute e_ℓ using a Montgomery ladder by working on $k[X]/P(X)$.

Direct computation of the symmetric pairing ($g=1$ for the example)

- We want to compute

$$e_\ell(P,Q) = \frac{\vartheta_i(Q)(\vartheta_i(P+\ell Q)\vartheta_i(\ell P - Q) + \vartheta_i(P-\ell Q)\vartheta_i(\ell P+Q))}{\vartheta_i(P)\vartheta_i(\ell P+Q)\vartheta_i(\ell P-Q)}$$

- We can compute $a_0 = \vartheta_0(P+Q)\vartheta_0(P-Q)$, $a_1 = \vartheta_1(P+Q)\vartheta_1(P-Q)$, and $b = \vartheta_0(P+Q)\vartheta_1(P-Q) + \vartheta_1(P-Q)\vartheta_0(P+Q)$.
- Let t_1 and t_2 be the roots of $P = X^2 - bX + a_1 a_2$.
- Then $(t_1, a_1) = \vartheta_1(P+Q)(P-Q)$ and $(t_2, a_1) = \vartheta_1(P-Q)(P+Q)$.

$\Rightarrow$ This mean we can compute e_ℓ using a Montgomery ladder by working on $k[X]/P(X)$.

Tate pairing on $k^{*,\pm 1}$

- We have the following formulas :

$$(x^\ell + \frac{1}{x^\ell})^2 = (x^{2\ell} + \frac{1}{x^{2\ell}}) + 2$$

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

$\Rightarrow$ We can also use a Montgomery ladder to compute the $\mathbb{Z}$-structure on $k^{*,\pm 1}$.

$\Rightarrow$ This allows us to compute directly the Tate pairing, or a one round tripartite Diffie-Hellman.