Infinitesimal pairings and CSIDH

2024/01/23 — Journées PQ TLS, Paris

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

Pairings in isogeny based cryptography

- [CSV2020]: Tate pairing to attack isogeny-DDH;
  Genus theory describes the characters $\chi : \mathrm{Cl}(O) \to \pm 1$, and the Tate pairing can be used to compute $\chi(\mathfrak{a})$;
- [CHVW2022]: Weil pairing to compute $\chi(\mathfrak{a})$;
- [CHMMvBV2023]: Generalised Tate pairing to attack the class group action;
  $\Rightarrow$Applies when Δ_O has a large enough smooth factor

- This talk: CSIDH
- Infinitesimal pairings
- Work in progress (Euphemism for "I don't know how to compute anything")
- More questions than answers…

The Weil-Cartier pairing

- If $\gamma \in \mathrm{End}(E)$ of norm d, non degenerate pairing

$$e_\gamma : E[\gamma] \times E[\hat{\gamma}] \to \mu_d.$$

- Primitively oriented elliptic curve: O quadratic imaginary order of discriminant $\Delta = \Delta_O < 0$;
- Special case $\gamma = \alpha := \sqrt{\Delta}$;
- $E[\alpha]$ is cyclic (the orientation is primitive);
- $E[\hat{\alpha}] = E[\alpha]$ ($\hat{\alpha} = \overline{\alpha} = -\alpha$);

$\Rightarrow$ $e_\alpha : E[\alpha] \times E[\alpha] \to \mu_\Delta$ is a non degenerate self pairing of order Δ.

- $e_\alpha(P, Q) = e_\Delta(P, Q')$ for $\alpha(Q') = Q$

Application 1: reconstructing an isogeny [CHMMvBV2023]

- $\phi : E_A \to E_B$ unknown oriented isogeny of known degree n;
- $\phi(E_A[\gamma]) = E_B[\gamma]$
- $\gamma = [\ell]$: e_ℓ gives constraints on $\phi \mid E_A[\ell]$;
- γ cyclic: via the Weil pairing e_γ, recover the action of ϕ on $E_A[\hat{\gamma}]$ from the action on $E_A[\gamma]$.

- Special case: $\gamma = \alpha$;
- $e_\alpha(\phi(P), \phi(P)) = e_\alpha(P, P)^n$;
- If $Q \in E_B[\alpha]$ such that $e_\alpha(Q, Q) = e_\alpha(P, P)$, then $\phi(P) = c.Q$ with $c^2 = n$ modulo Δ;

$\Rightarrow$ Recover $\phi(P)$ up to a "sign" μ ($\mu^2 = 1$ modulo Δ)

- If $\Delta > n$ this is enough to recover ϕ (Kani+Zarhin+Banff/Bristol workshop)

Application 2: genus theory

- If $\ell \mid \Delta$ odd prime, character χ_ℓ on $\mathrm{Cl}(O)$:

$$\chi_\ell([\mathfrak{a}]) = \left(\frac{N(\mathfrak{a})}{\ell}\right) \in \{\pm 1\}$$

- Special formulas for $\ell = 2$;
- There is exactly one non trivial relation between the characters.

- $\phi_{\mathfrak{a}} : E_A \to E_B = \mathfrak{a} \cdot E_A$
- $U_A = \{e_\alpha(P,P)^{\Delta/\ell} \mid P \in E_A[\alpha]\} = \{\zeta_A^{i^2} \mid i \in \{1, \dots, \Delta\}\}$,
  $U_B = \{e_\alpha(Q,Q)^{\Delta/\ell} \mid Q \in E_B[\alpha]\} = \{\zeta_B^{i^2} \mid i \in \{1, \dots, \Delta\}\} = \{\zeta_A^{N(\mathfrak{a})i^2} \mid i \in \{1, \dots, \Delta\}\}$;
- $\chi_\ell([\mathfrak{a}]) = 1 \Leftrightarrow U_A = U_B$,
  $\chi_\ell([\mathfrak{a}]) = -1 \Leftrightarrow U_A \cap U_B = \{1\}$.

- $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{b}'][\mathfrak{a}']$, DDH: check if $[\mathfrak{a}] = [\mathfrak{a}']$ ($\Leftrightarrow [\mathfrak{b}] = [\mathfrak{b}']$)?
- Genus check: $\chi_\ell([\mathfrak{a}]) = \chi_\ell([\mathfrak{a}'])$ for all $\ell \mid \Delta$?

Generalised Tate pairings

- If $m \mid \Delta$, e_α induces a non degenerate pairing (the generalised Tate pairing)

$$E[\alpha, m] \times E[\alpha]/mE[\alpha] \to \mu_m$$

- If $P = \frac{\Delta}{m} P' \in E[\alpha, m]$ and $Q = mQ' \in E[\alpha]/mE[\alpha]$,

$$e_\alpha(P, Q) = e_m(P, \hat{\alpha}(Q')) = e_\alpha(P', Q)^{\frac{\Delta}{m}} = e_\Delta(P', \hat{\alpha}(Q'))^{\frac{\Delta}{m}}$$

- $P \in E[\alpha] \mapsto e_\alpha(\frac{\Delta}{m} P, P)$ induces a self pairing of order m on $E[\alpha, m]$;
- Allows to restrict to the smooth part of Δ.

- Usual Tate pairing: $\alpha = \pi - 1$;
- Generalised Tate-Cartier pairing: if $\psi_2 \circ \sigma_1 = \sigma_2 \circ \psi_1$, $e_{\sigma_1} : A_1[\sigma_1] \times A_2[\hat{\sigma}_1] \to \mathbb{G}_m$ induces

$$A_1[\sigma_1, \psi_1] \times \hat{A}_2[\hat{\sigma}_1]/\hat{\psi}_2(\hat{B}_2[\hat{\sigma}_2]) \to \mathbb{G}_m$$

and $e_{\sigma_1}(P_1, Q_2) = e_{\psi_1}(P_1, \hat{\sigma}_2 Q')$ where $\hat{\psi}_2 Q' = Q$.

CSIDH

- In CSIDH/CSURF: $E/\mathbb{F}_p$ supersingular elliptic curve
- $\Delta = -4p$ or $\Delta = -p$;
- Needs $\ell = p$ to get meaningful information
- Infinitesimal Weil pairing: $e_p : E[p] \times E[p] \to \mu_p$
- $\alpha = \pi$ is the Frobenius
- Infinitesimal self pairing: e_π on $E[\pi]$ with values in μ_p
- $e_\pi(P, Q) = e_p(P, Q')$ where $\pi(Q') = Q$.

- E/k supersingular curve, k perfect of characteristic p
- $E[\pi] = \{(X : Y : Z) \in E \mid (X^p : Y^p : Z^p) = (0 : 1 : 0)\} \simeq \alpha_p = \operatorname{Spec} k[X]/X^p$
- $E[p] = \left\{(X : Y : Z) \in E \mid (X^{p^2} : Y^{p^2} : Z^{p^2}) = (0 : 1 : 0)\right\} \simeq I_{1,1}$
  the unique autodual non split extension of α_p by itself
- $\mu_p = \operatorname{Spec} k[X]/(X^p - 1)$

Dieudonné theory

- Dieudonné ring: $A = W(k)\{F, V\}$ with $VF = FV = p, F\lambda = \lambda^\sigma F, \lambda V = V\lambda^\sigma$ (σ Frobenius on $W(k)$)
- Anti-equivalence of category $G \mapsto \mathbb{D}(G)$ from finite (flat) commutative group schemes of p-primary degree to left A-modules of finite $W(k)$-length
- F corresponds to the Frobenius on G and V to the Verschiebung
- Functorial in k
- If $p.G = 0$ then $\mathbb{D}(G)$ is a $k\{F, V\}$-module;
- Extends to p-divisible groups: anti-equivalence between p-divisible groups G of height n and free left A-modules of rank n

- Composing with duality we get a covariant theory but which permutes the role of F and V

Examples

- If G/k of order p, $\mathbb{D}(G)$ is a k-vector space of dimension 1 with some action by F and V
- $\mathbb{D}(\mathbb{Z}/p\mathbb{Z})$: $F = 1, V = 0$
- $\mathbb{D}(\mu_p)$: $F = 0, V = 1$
- $\mathbb{D}(\alpha_p)$: $F = 0, V = 0$

- If E/k is an elliptic curve, $E(p)$ is a p-divisible group of height 2, $\mathbb{D}(E(p))$ is a free $W(k)$-module of rank 2
- If E/k is ordinary, $E(p) = E_{etale}(p) \times E_{mult}(p)$,

$$\mathbb{D}(E(p)) = \mathbb{D}(E_{etale}(p)) \oplus \mathbb{D}(E_{mult}(p))$$

$$F = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, V = \begin{pmatrix} \mu & 0 \\ 0 & \lambda \end{pmatrix}$$

  λ, μ the two eigenvalues, λ invertible modulo p
- If E/k is supersingular,

$$F = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$$

  and $V = -F$ on $\mathbb{D}(E[p])$.

Duality [Oda 1969], [Berthelot, Breen, Messing 1979]

- Duality behaves as expected for the p-divisible group $A(p)$ of an abelian variety A/k: we have a canonical (functorial) isomorphism

$$A^\vee(p) \simeq A(p)^\vee$$

- Duality behaves as expected for Dieudonné theory:

$$\mathbb{D}(G^\vee) \simeq \mathbb{D}(G)^\vee$$

$\Rightarrow$ Pairing: $\mathbb{D}(A(p)) \times \mathbb{D}(A^\vee(p)) \to \mathbb{D}(\mathbb{G}_m)$

- Weil pairing: $e_p : A[p] \times A^\vee[p] \to \mu_p$
- If A is principally polarised:

$$e_p : \mathbb{D}(A[p]) \times \mathbb{D}(A[p]) \to \mathbb{D}(\mu_p)$$

Infinitesimal self pairing for supersingular elliptic curves

- Frobenius filtration: $0 \to E[\hat{\pi}] \to E[p] \to E[\pi] \to 0$ induces

$$0 \to \mathbb{D}(E[\pi]) \simeq \mathbb{D}(\alpha_p) \to \mathbb{D}(E[p]) \to \mathbb{D}(E[\hat{\pi}]) \simeq \mathbb{D}(\alpha_p) \to 0$$

- On a compatible symplectic basis $(e_1, e_2), e_1 \in \mathbb{D}(E[\pi])$:

$$F \mid \mathbb{D}(E[p]) = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$$

  with $e_p(e_1, e_2) = 1 \in \mathbb{D}(\mu_p)$

- Since $F(e_2/c) = e_1$,

$$e_\pi(e_1, e_1) = e_p(e_1, e_2/c) = 1/c$$

Infinitesimal pairings for CSIDH

1. Find a symplectic basis e_1, e_2 of $\mathbb{D}(E[p])$
2. Compute the action of F on this basis
3. Recover e_π

⇒ Recover $\chi_p(\mathfrak{a})$ given only the domain and codomain of $\phi_\mathfrak{a}$

⇒ If $\phi_\mathfrak{a} : E_A \to E_B$ unknown isogeny of known degree n, embed $\phi_\mathfrak{a}$ into a purely inseparable isogeny in higher dimension

- ???[1]
- Profit!

[1] No reason to believe that an inseparable isogeny can be computed in time faster than $O(p^C)$; the Frobenius seems to be a special case

De Rham cohomology

- [Oda 1969]: canonical isomorphisms

$$\mathbb{D}(A[p]) \simeq H^1_{DR}(A), \mathbb{D}(A[\pi]) \simeq H^0(A, \Omega^1_{A/k}), \mathbb{D}(A[\hat{\pi}]) \simeq H^1(A, O_A)$$

- De Rham cohomology: hypercohomology of the De Rham complex
- The Frobenius filtration

$$0 \to A[\hat{\pi}] \to A[p] \to A[\pi] \to 0$$

corresponds to the Hodge filtration

$$0 \to H^0(A, \Omega^0_{A/k}) \to H^1_{DR}(A) \to H^1(A, O_A) \to 0$$

⇒ e_p is a pairing on $H^1_{DR}(A)$

- If $A = \mathrm{Jac}(C), H^1_{DR}(A) = H^1_{DR}(C), H^1(A, O_A) = H^1(C, O_C) = H^0(C, K_C)$.
- Cup product: $H^1_{DR}(C) \times H^1_{DR}(C) \to H^2_{DR}(C) \simeq^{Trace} k$
- [Coleman]: e_p is the cup product pairing

De Rham cohomology of an elliptic curve

- $H^1_{DR}(E) \simeq H^1_{DR}(E \backslash 0_E) \simeq H^0(\Omega(20_E)) = \langle dx/y, xdx/y \rangle$ ([Katz 1972] via log differentials) = Differentials with a pole of order ≤ 2 at infinity
- $e_p(dx/y, xdx/y) = 1$;
- For $E/\mathbb{F}_p$ supersingular: π induces from e_p a non degenerate pairing e_π on $H^0(E, \Omega_{E/k}) = \langle dx/y \rangle$;
- If $F(xdx/y) = cdx/y$,

$$e_\pi(dx/y, dx/y) = 1/c.$$

- To compute e_π, we just need to know the action of F on xdx/y
- This c depends on the curve equation $y^2 = x^3 + ax + b$;
- The change of variable $(x, y) \mapsto (x', y') = (u^2 x, u^3 y)$ gives $dx'/y' = 1/u \cdot dx/y$, $x'dx'/y' = u \cdot xdx/y$, so $c' = u^2 \cdot c$, and $e_\pi(dx'/y', dx'/y') = \frac{1}{u^2 c} = \frac{1}{u^2} e_\pi(dx/y, dx/y)$.
- Kedlaya's algorithm: $O(p)$, Harvey: $O(\sqrt{p})$

  (their algorithm actually computes the action of F on the Monsky-Vashnitzer cohomology which reduces modulo p to the De Rham cohomology)

De Rham cohomology of an elliptic curve: the ordinary case

- $E/\mathbb{F}_q$ ordinary
- $A[p] = A[\pi] \oplus A[\hat{\pi}]$, $A[\hat{\pi}]$ étale and $A[\pi]$ multiplicative
- The Hodge filtration splits
- $H^1_{DR}(E) = H^0(E, \Omega^1_E) \oplus H^1(E, O_E) = \langle dx/y, xdx/y \rangle$
- $\langle dx/y \rangle \simeq \mathbb{D}(E[\pi]) \simeq H^0(E, \Omega^1_E)$
- $\langle xdx/y \rangle \simeq \mathbb{D}(E[\hat{\pi}]) \simeq H^1(E, O_E)$

Applications of the infinitesimal self pairing

- $\phi_{\mathfrak{a}} : E_A \to E_B$ unknown CSIDH isogeny of known degree n
- Compute e_π on E_A and E_B
- Recover the action on differentials: $\phi_{\mathfrak{a}}^* dx_B/y_B = \lambda dx_A/y_A$ (up to a sign)
- Solve a differential equation to recover the action of $\phi_{\mathfrak{a}}$ on the formal group up to precision $N < p$ [BMSS2008]

Deformations for CSIDH

- The action on differentials is only defined up to a sign
- Kodaira-Spencer: $H^0(E, \mathrm{Sym}^2\,\Omega^1_{E/k}) \simeq \Omega^1_{\mathcal{A}_1,E}$
- The square of a differential determines a deformation to $k[\epsilon]/(\epsilon^2)$;
- Concretely: $j'/j = -E_6/E_4$ is a modular form of weight two and for a deformation $\widetilde{E}/k[\varepsilon]$, $j(\tilde(E)) = j(E) + j'(E)\epsilon$

- Using e_π, given a deformation $\widetilde{E}_A$ of E_A to $k[\epsilon]/\epsilon^2$, we can compute the codomain $\widetilde{E}_B$ knowing only $\deg \phi_{\mathfrak{a}}$;
- The CSIDH action carries additional information on the deformations!

More on deformations

- $\mathbb{D}(A(p)) = H^1_{crys}(A, W(k))$ = hypercohomology of the De Rham-Witt complex [Deligne-Illusie] = $H^1_{DR}(\widetilde{A}/W(k))$ for any lift $\widetilde{A}/W(k)$ of A/k (this is a crystal for the crystalline topology)
- Serre-Tate: deforming A/k = deforming $A(p)/k$
- Grothendieck-Messing: deforming a p-divisible group G/k = deforming $\mathbb{D}(G)/k$ = deforming/lifting its Hodge filtration
- If $\widetilde{A}/R$ is a lift of A/k, the Hodge filtration on $\mathbb{D}(A(p))/R$ is the Hodge filtration on $\widetilde{A}$ (it does lift the Hodge filtration of A/k).

- If $E/\mathbb{F}_p$ supersingular, it lifts canonically to $\widetilde{E}/\mathbb{Z}_p$, and an oriented CSIDH isogeny lifts
- Since $\widetilde{E}/\mathbb{Z}_p$ has supersingular reduction, the Weil pairing on $\mathbb{D}(\widetilde{E}(p))/\mathbb{Z}_p$ induces a self pairing on $\mathbb{D}(\widetilde{E}(p))/F\mathbb{D}(\widetilde{E}(p))$!

Revisiting anomalous curves

- If $E/\mathbb{F}_p$ is an ordinary elliptic curve, $\mathbb{D}(\hat{E}[\hat{\pi}]) \simeq H^0(E, \Omega^1_{E/k})$ is explicitly given by $D_P \in \hat{E}[\hat{\pi}] \mapsto df_P/f_P$ where f_P is any function in $k(E)$ with divisor pD_P.
- The map $P \in E[p]_{etale} = E[\hat{\pi}] \mapsto (P) - (0_E) \in \hat{E}[\hat{\pi}] \mapsto df_P/f_P \in H^0(E, \Omega^1_{E/k})$ efficiently transfers the DLP to a (trivial) DLP on differentials (Semaev).
- Smart: uses the p-adic elliptic logarithm on a non canonical lift to $\mathbb{Z}_p/p^2\mathbb{Z}_p$ instead.
- Canonical lift: the unique lift whose associated filtration is stable under Frobenius; p-adic elliptic logarithm: isomorphism of the formal Lie group of the elliptic curve with $\hat{G}_a$.
- Belding: uses the Weil pairing to a (non trivial) deformation to $\mathbb{F}_p[\epsilon]$.
- Voloch: uses p-descent.

- **In summary:** The Dieudonné functor, which replaces the algebraic group structure $E[p]$ with differential linear data $\mathbb{D}(E[p]) \simeq H^1_{DR}(E)$ or $\mathbb{D}(E(p)) \simeq H^1_{crys}(E, \mathbb{Z}_p)$, underlies these various anomalous DLP attacks.
- Can we find an "anomalous" attack on CSIDH?