Hardness of isogeny problems and equidistribution

j w/ B. Wesolowski

I

I) Isogeny problems

<u>Def</u> A <u>hash function</u> is a map $h : \{0,1\}^* \longrightarrow S$ where S finite set.

<u>Desirable properties</u>:

(1) h(random string) $\approx$ uniform distribution on S

(2) preimage resistance: there is no ~~polynomial time~~ algo ~~algorithm~~ to compute preimages in time $\mathrm{Poly}(\log \# S)$. Family $(h_i)_i$ $\# S_i \to \infty$

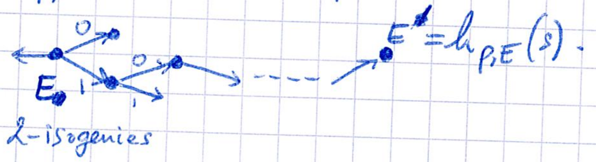
(3) Collision resistance: there is no algorithm in time $\mathrm{Poly}(\log \# S)$ that computes $s_1 \neq s_2 \in \{0,1\}^*$ ~~and outputs~~ such that $h(s_1) = h(s_2)$.

<u>CGL hash function</u>:

p prime. $S_p = \{\text{supersingular } E/\overline{\mathbb{F}}_p\}/\text{isom}$. $\# S_p \approx \frac{p}{12}$

$E_0 \in S$: $h_{p,E_0} : \{0,1\}^* \longrightarrow S_p$

$h_{p,E_0}(s)$:



walk on <u>2-isogeny graph</u> $\mathcal{G}_{p,2}$.

$\mathcal{G}_{p,\ell}$: vertices: S_p

edges: isogenies of degree ℓ

$h_{p,E}$(random string of length k) = end of non-backtracking random walk of length k.

<u>Thm</u> (Pizer) Random walks of length $\to \infty$ converge to proba$(E') \sim \frac{1}{\# \mathrm{Aut}(E')}$

adjacency operator $T_\ell \circlearrowright L^2(\mathcal{G}_{p,\ell})$ self-adjoint $\Rightarrow T_\ell \mathbb{1} = (\ell+1)\mathbb{1}$

on orthogonal $L^2_0(\mathcal{G}_{p,\ell}) = \mathbb{1}^\perp$, eigenvalues $|\lambda| \leq 2\sqrt{\ell}$

$$\Rightarrow \left(\frac{T_\ell}{\ell+1}\right)^k \cdot f \xrightarrow[k \to \infty]{} \left(\int f\right) \mathbb{1}.$$

Problem ℓ-Isog: Given $E, E' / \overline{\mathbb{F}}_p$ supersingular, find $E \xrightarrow{\text{path}} E'$ in $\mathcal{G}_{p,\ell}$.

<u>Problem: OneEnd</u>: Given $E / \overline{\mathbb{F}}_p$ supersingular, find $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.

Encoding of morphism isogeny φ? degree bound + algo for efficient evaluation of φ & $\hat{\varphi}$ on points.

$\longrightarrow$ degree, addition, composition, dual, trace, division

<u>Problem EndRing</u>: Given $E/\overline{\mathbb{F}}_p$ supersingular, find $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ basis of $\mathrm{End}(E)$.

properties of $\mathrm{End}(E)$: $\mathrm{tr}(\alpha) = \alpha + \hat{\alpha} \in \mathbb{Z}$ $\quad \mathrm{tr}(\alpha\hat{\beta})$ pos. def. $\quad \det(\mathrm{tr}(\alpha_i \hat{\alpha}_j)) = p^2$.

II) Reductions

Def A, B computational problems. $A \leq B$ "A reduces to B"
if there exists a probabilistic polynomial-time algorithm with access to an oracle $\mathcal{O}_B$ for B that solves A. (can call several times) $A \simeq B$ if $A \leq B$ and $B \leq A$.

$$\ell\text{-Isog} \underset{\substack{\text{GRH} \\ (\text{KLPT+W})}}{\simeq} \text{EndRing} \geq \text{OneEnd}$$

Best known: $\tilde{O}(\sqrt{p})$.

Thm (P.-Wesolowski) $\text{EndRing} \leq \text{OneEnd}$. ⚠ $\neq$ can compute all End if given one.

Algo 1 Input E

- $\Lambda \leftarrow \mathbb{Z}$
- repeat $\Lambda \leftarrow \Lambda + \mathbb{Z} \cdot \mathcal{O}_{\text{OneEnd}}(E)$
- until $\Lambda = \text{End}(E)$

trace bilinear form nondeg. on $B = \text{End}(E) \otimes \mathbb{Q}$
→ basis
→ discriminant

Problem $\mathcal{O}_{\text{OneEnd}}(E)$ could be constant.

Algo 2 Input E.

- $\Lambda \leftarrow \mathbb{Z}$
- repeat
  - $\varphi : E \to E'$ random 2-isogeny walk
  - $\alpha \leftarrow \hat{\varphi} \circ \mathcal{O}_{\text{OneEnd}}(E') \circ \varphi$
  - $\Lambda \leftarrow \Lambda + \mathbb{Z}\alpha$
- until $\Lambda = \text{End}(E)$

Problem $\mathcal{O}_{\text{OneEnd}}(E')$ could always lie in $\mathbb{Z} + N\,\text{End}(E') \Rightarrow$ all $\alpha \in \mathbb{Z} + N\,\text{End}(E)$ for some $N \in \mathbb{Z}_{\geq 2}$

Thm (P.-W.) "asymptotically, only obstruction"

A) $\forall M \geq 2$, distribution of $\mathbb{Z}\alpha \bmod M \xrightarrow[\text{length of walk} \to \infty]{}$ conjugacy-invariant distribution (speed depends on M)

B) Every order that is maximal at p and conj-invariant mod M $\forall M$ is of the form $\mathbb{Z} + N\,\text{End}(E)$.

Algo 3 idem Algo 2 ... until $\Lambda = \mathbb{Z} + N\,\text{End}(E)$ for some N (+ maximise at p)

- return $\mathbb{Z} + \frac{1}{N}(\Lambda / \mathbb{Z})$.

Problem Might not converge in polynomial time.

Algo 4 Input E

$\Lambda \leftarrow \mathbb{Z}$

repeat

- $\alpha \leftarrow \hat{\varphi}\, \mathcal{O}^{\mathrm{Om}}_{\mathrm{End}}(E')\, \varphi$ with random φ
- $\Lambda \leftarrow \Lambda + \mathbb{Z}\alpha$
- if Λ has full rank
  - $\Lambda \leftarrow p\text{-max}(\Lambda)$
  - update lazy factorization of $\mathrm{disc}(\Lambda)$ with $\mathrm{disc}(\alpha)$
  - $\beta \leftarrow \underset{\alpha\text{-scalar}}{\bullet}$ divided by all possible known factors of $\mathrm{disc}(\Lambda)$
  - $\Lambda \leftarrow \Lambda + \mathbb{Z}\beta$

until $\Lambda = \mathrm{End}(E)$

Thm (P-W): Algo 4 terminates in polynomial time.

IV) Equidistribution and modular forms

$\mathcal{O}_0 = \mathrm{End}(E_0)$

$$\begin{array}{ccc} \mathcal{G}_{p,\ell}^{\mathrm{End}/M} & \xrightarrow{\sim} & \bigsqcup_i \mathcal{G}_{\mathcal{O}_0,\ell}^{U_i} \\ \downarrow & & \downarrow \\ \mathcal{G}_{p,\ell} & \xrightarrow[\text{Deuring correspondence}]{\sim} & \mathcal{G}_{\mathcal{O}_0,\ell} \end{array}$$

• "augmented Deuring correspondence" general class of extra structure

vertices: {right $\mathcal{O}_0$-ideals}/equivalence

edges: ℓ-neighbours $I \underset{\ell}{\supseteq} J$.

$E \longmapsto \mathrm{Hom}(E_0, E)$

$E/E[I] \longleftarrow\!\mid\; I$

$\mathcal{G}^{U_i}_{\mathcal{O}_0,\ell} \longrightarrow \mathrm{Cay}\big((\mathbb{Z}/M\mathbb{Z})^{*}/H_i,\ \ell\big)$

orthogonal to pullbacks: $L^2_0(\mathcal{G}^{U_i}_{\mathcal{O}_0,\ell}) \subseteq L^2(\mathcal{G}^{U_i}_{\mathcal{O}_0,\ell}) \circlearrowleft T_\ell$ adjacency = Hecke op.

$L^2_0(\mathcal{G}^{U_i}_{\mathcal{O}_0,\ell}) \underset{T_\ell}{\hookrightarrow} S_2(pM)$ quaternionic automorphic forms

Jacquet-Langlands / Eichler

Bounds on eigenvalues $|a_\ell| \leq 2\sqrt{\ell}$ Shimura / Deligne

$\Rightarrow$ equidistribution theorem.