Constructing Smooth-Degree Isogenies in Isogeny-Based Cryptography

Yu-Hsuan Huang (黃右萱)
Advisor: Rong-Jaye Chen (陳榮傑)
Institute of Computer Science and Engineering

Elliptic curve. Given some base field $\mathbb{F}$, an elliptic curve E is a smooth algebraic (planar) curve of degree 3. Assuming characteristic $p > 3$, the curve could be specified be Weierstrass equation, $y^2 = x^3 + ax + b$. We write $E/\mathbb{F}$ to emphasize $a, b \in \mathbb{F}$.

Isogenies. Given curves $E_0/\mathbb{F}, E_1/\mathbb{F}$, a (separable) isogeny ϕ of degree d is a surjective group homomorphism in closure $E_0(\bar{\mathbb{F}}) \to E_1(\bar{\mathbb{F}})$ with kenel size d. For $\mathbb{K} \leq \bar{\mathbb{F}}$, ϕ is said $\mathbb{K}$-rational if $\ker\phi$ is stabilized by $\mathsf{Gal}(\bar{\mathbb{F}}/\mathbb{K})$ action.

Powersmoothness. Powersmoothness of an isogeny ϕ indicates that prime factors of its degree $\deg\phi = p_1 \dots p_n$ are small, i.e. $\ell_i \leq s$ for all i and some prescribed s. The question we ask here is, "how do we construct smooth-degree isogenies." More importantly, how to do it fast? Two particular cases to consider: (1) when $\ker\phi = \langle Q_1, \dots, Q_n\rangle$ are given, and (2) when endomorphism rings $\mathsf{End}(E_i)$ are given.

Isogeny Strategies

SIDH and CSIDH both need to...

- Consider primes $\ell_1, \dots, \ell_n$ and curve E.
- Sample $P \in E$ with $\mathsf{ord}(P) = \ell_1 \dots \ell_n$.
- Iteratively construct isogenies $\{\phi_i\}_{1\leq i\leq n}$ that
  - $E = E_0 \xrightarrow{\phi_n} E_1 \xrightarrow{\phi_{n-1}} \dots \xrightarrow{\phi_1} E_n$
  - $\ker\phi_i := \langle R_i\rangle, \quad R_i := \ell_1 \dots \ell_{i-1}\phi_{i+1} \dots \phi_n(R)$

Note that $\ell_i\phi_j = \phi_j\ell_i$ for each i, j. Therefore the *isogeny strategies* kick in. (HLKA19) An (canonical) isogeny strategy is a recursively defined graph embedded in the 2D plane.

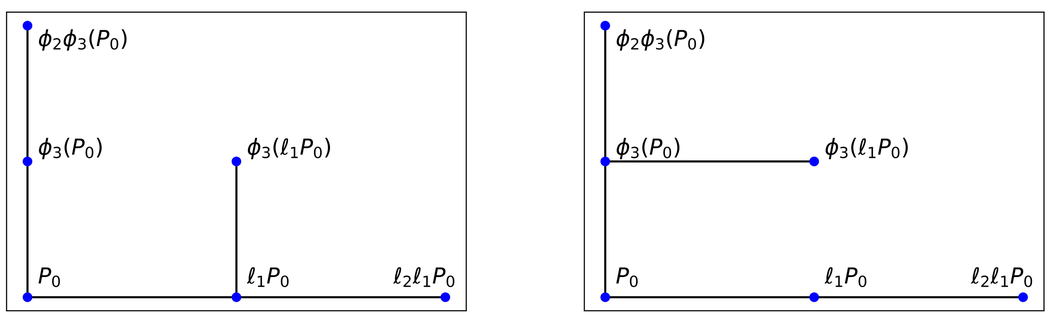

Fig. 1: $(T_1\#T_1)\#T_1$ versus $T_1\#(T_1\#T_1)$

Use a *measure* $\mathcal{M} = (\{\ell_1, \dots, \ell_n\}, h, v)$ as cost models, where horizontal costs $h(\ell_i)$ and vertical costs $v(\ell_i)$ specify the costs of multiplication by ℓ_i and *evaluating* an ℓ_i isogeny respectively. For measure $\mathcal{M}$, strategy S, write $\mathcal{M}(S)$ as total cost of S.

Isogeny Strategy Problem. Given a measure $\mathcal{M}$, find a strategy that minimizes $\mathcal{M}(S)$.

Our contributions. For isogeny measure $\mathcal{M} = (\{\ell_1, \dots, \ell_n\}, h, v)$ write $\mathcal{M}[i:j] = (\{\ell_i, \dots, \ell_j\}, h, v)$ and $\mathsf{Opt}(\mathcal{M}) = \min_S \mathcal{M}(S)$. We show that there is a Knuth-Yao's quadrangle inequality in optimal substrategies, i.e. for $1 \leq b \leq c \leq n$

$$\mathsf{Opt}(\mathcal{M}) + \mathsf{Opt}(\mathcal{M}[b:c]) \geq \mathsf{Opt}(\mathcal{M}[1:c]) + \mathsf{Opt}(\mathcal{M}[b:n]).$$

Consequently, for K_{ij} being the optimal transition point, we can prove that $K_{i+1,j} \leq K_{ij} \leq K_{i,j-1}$ and obtain the following asymptotic improvements.

- For $\ell_1 = \dots = \ell_n$, $\tilde{O}(n^2) \to \tilde{O}(n)$.
- For general case, $\tilde{O}(n^3) \to \tilde{O}(n^2)$.
- For B-batch SIMBA variant, $\tilde{O}(n^3{+}?) \to \tilde{O}(n^2B)$.

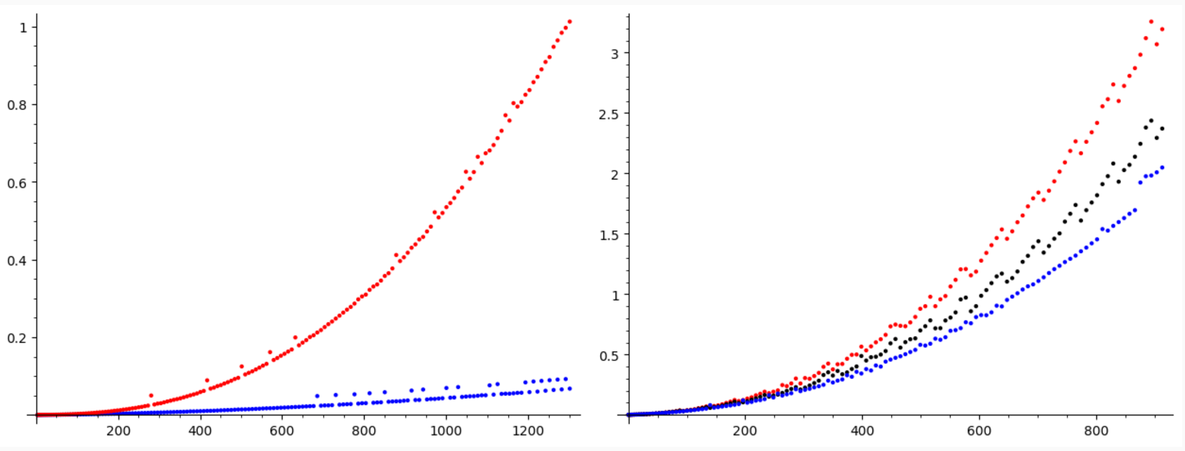

Fig. 2: General case and SIMBA variant improvements

Quaternion Isogeny

Theorem (Duering's correspondence). There's a bijective correspondence between

$$\{j(E) : E/\bar{\mathbb{F}}_p \text{ is supersingular}\}/\mathsf{Gal}(\mathbb{F}_p) \leftrightarrow \{\text{maximal orders } \mathcal{O} \subseteq B_{p,\infty}\},$$

where $B_{p,\infty}$ is a quaternion $\mathbb{Q}$-algebra ramified at $\{p, \infty\}$.

KLPT(KLPT14). Given a curve E and an endomorphism ideal $\mathcal{I} \lhd \mathsf{End}(E)$ there is a heuristic polynomial-time algorithm constructing $\mathcal{J} \cong \mathcal{I}$ of powersmooth or primepower norm.

Ideal evaluation. Using KLPT, there is a (heristic polynomial-time) reduction (PL17) that finds an ℓ-isogeny $\phi : E_0 \to E$ with small ℓ given the endomorphism ring $\mathsf{End}(E)$ for some prescribed E_0 illustrated as follows.

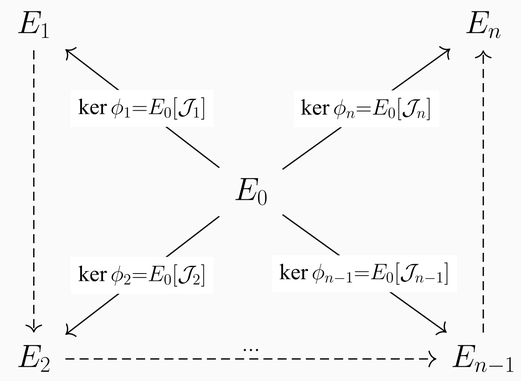

Fig. 3: Finding an ℓ-isogeny path

Here, for any $\mathcal{J} = \mathcal{J}_i$ of powersmooth norm $\ell_1^{e_1} \dots \ell_n^{e_n}$, we want to compute $\phi : E_0 \to E_0/E_0[\mathcal{J}]$. This require us to successively quotient away $K_i = E_0[\mathcal{J}] \cap E_0[\ell^{e_i}]$ for each i by constructing $\psi_i : E'_{i-1} \to E'_i := E'_{i-1}/\psi_{i-1} \dots \psi_1(K_i)$ where $E'_0 = E_0$.

Major issue. We have $K_i \subseteq E_0[\ell_i^{e_i}] \subseteq E_0(\mathbb{F}_{p^{2k_i}})$ where $k_i \leq \ell_i^{e_i}$ is (polynomially) large, but in fact $\pi_{p^2}(K_i) = K_i$, meaning that each ψ_i is $\mathbb{F}_{p^2}$-rational. Thus we need to lift ψ_j to $\mathbb{F}_{p^{2k_i}}$-rational, which is computational expensive.

Our contributions. In order to deal with the above issue, we could either (i) minimize the powersmooth bound $\ell_i^{e_i} \leq s$ while executing KLPT's algorithm or (ii) minimize the computational combinatorially in later phase. For (i), in KLPT we need to solve x_i, y_i, z_i for the following (relaxed) systems

$$x_1^2 + x_2^2 = NS_1 - p(x_3^2 + x_4^2)$$
$$y_1^2 + y_2^2 = \frac{S_2 - p\left((\lambda z_3 + Ny_3)^2 + (\lambda z_4 + Ny_4)^2\right)}{N^2} =: \tau.$$

Fix x_i, y_i, λ as parameters of the system, we want $\tau, NS_1 - p(x_3^2 + d_4)^2 > 0$ while making the powersmooth bound of S_1S_2 small. We convert this into explicit insntances of the *closest vector problem*, ((PS) has similar observation but their lattice were not explicitly provided.) i.e. minimize $(\lambda z_3 + Ny_3)^2 + (\lambda z_4 + Ny_4)^2$ in the following latices,

$$\underbrace{\begin{pmatrix} z_3 & z_4 & N & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 4 \end{pmatrix}\begin{pmatrix} y_3 \\ y_4 \\ k_1 \\ k_2 \\ k_3 \end{pmatrix} = \begin{pmatrix} \tau_2 \\ \lambda z_3 \\ \lambda z_4 \end{pmatrix}}_{\text{for } S_1=1 \mod 4}; \quad \underbrace{\begin{pmatrix} z_3 & z_4 & N & 0 & 0 \\ 1 & 0 & 0 & 4 & 0 \\ 0 & 1 & 0 & 0 & 4 \end{pmatrix}\begin{pmatrix} y_3 \\ y_4 \\ k_1 \\ k_2 \\ k_3 \end{pmatrix} = \begin{pmatrix} \tau_2 \\ (\pm 1 - \lambda z_3)N^{-1} \mod 4 \\ (\pm 1 - \lambda z_4)N^{-1} \mod 4 \end{pmatrix}}_{\text{for } S_1=3 \mod 4}$$

where $\tau_2 = \frac{S_2 - p\lambda^2(z_3+z_4)}{N}(2\lambda p)^{-1} \mod N$. In experiments, we obtain $\mathsf{n}(\mathcal{J})/\log_2(p) \approx 5.45$ and $\mathsf{psmooth}(\mathcal{J})/\log_2(p) \approx 4.37$ for $\lambda_4(\mathcal{I}) \approx \tilde{O}(p)$. For (ii), we model the lifting cost. Write $m_i = \ell_i^{e_i}$ for short. To lift ψ_j to $\mathbb{F}_{p^{2k_i}}$-rational, $\mathsf{cost}(k_i) = m_jk_i$. To lift $P \in E_0$, from $\mathbb{F}_{p^{2k_j}} \hookrightarrow \mathbb{F}_{p^{2k_i}}$, $\mathsf{cost}(k_jk_i) = \mathsf{constant} \cdot k_ik_j$. Two heuristics kick in...

- Reasonable to require $m_jk_i < m_ik_j$ by sorting $\{\ell_i\}_i$.
- For $j < i, i'$, if $k_{i'}|k_i$, there are two choices as follows, we use linear programming to decide the optimal.
  - Lift ϕ_j to both $\mathbb{F}_{p^{2k_{i'}}}$ and $\mathbb{F}_{p^{2k_i}}$.
  - Lift ϕ_j to $\mathbb{F}_{p^{2k_i}}$ and lift $K_{i'}$ from $\mathbb{F}_{p^{2k_{i'}}} \hookrightarrow \mathbb{F}_{p^{2k_i}}$.

Our best heuristic ourperforms the "vanilla" version by at least 2 times faster. Overall, our implementation outperforms related work (Ray18) by at least 7 times faster.

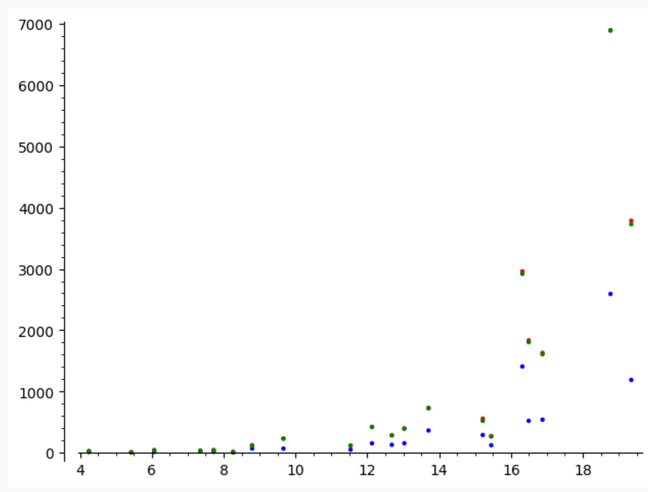

Fig. 4: Compare running time of different kinds of evaluation

References

[HLKA19] Aaron Hutchinson, Jason T LeGrow, Brian Koziel, and Reza Azarderakhsh, *Further optimizations of csidh: A systematic approach to efficient strategies, permutations, and bound vectors.*, IACR Cryptol. ePrint Arch. **2019** (2019), 1121.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol, *On the quaternion ℓ-isogeny path problem*, LMS Journal of Computation and Mathematics **17** (2014), no. A, 418–432.

[PL17] Christophe Petit and Kristin E Lauter, *Hard and easy problems for supersingular isogeny graphs.*, IACR Cryptol. ePrint Arch. **2017** (2017), 962.

[PS] C Petit and S Smith, *An improvement to the quaternion analogue of the l-isogeny problem*.

[Ray18] Dimitrij Ray, *Constructing the deuring correspondence with applications to supersingular isogeny-based cryptography*.