A faster way to the CSIDH

Indocrypt 2018, New Delhi

Michael Meyer[1,2] Steffen Reith[1]

11.12.2018

[1]University of Applied Sciences Wiesbaden, Germany

[2]University of Würzburg, Germany

A faster way to the CSIDH

Our paper is about implementation aspects of CSIDH:

- Faster isogeny computations by combining Montgomery and Twisted Edwards isogeny formulas
- Reducing computational effort for point multiplications
- Preliminary ideas for constant-time implementations

Isogenies

- Let $\mathbb{F}_q$ be a finite field with $q = p^k$, p prime.
- Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.

Isogenies

- Let $\mathbb{F}_q$ be a finite field with $q = p^k$, p prime.
- Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.

Definition

An isogeny between E_1 and E_2 is a non-constant morphism φ, such that $\varphi(\mathcal{O}_1) = \mathcal{O}_2$.

Isogenies

- Let $\mathbb{F}_q$ be a finite field with $q = p^k$, p prime.
- Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.

Definition

An isogeny between E_1 and E_2 is a non-constant morphism φ, such that $\varphi(\mathcal{O}_1) = \mathcal{O}_2$.

- Isogenies are group homomorphisms.

Isogenies

- Let $\mathbb{F}_q$ be a finite field with $q = p^k$, p prime.
- Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.

Definition

An isogeny between E_1 and E_2 is a non-constant morphism φ, such that $\varphi(\mathcal{O}_1) = \mathcal{O}_2$.

- Isogenies are group homomorphisms.
- For every finite subgroup $G \subset E_1$, there exists an (up to isomorphisms) unique elliptic curve E_2 and a separable isogeny $\varphi : E_1 \to E_2$ such that $ker(\varphi) = G$. ($\to$ Vélu's formulas)

Isogenies

- Let $\mathbb{F}_q$ be a finite field with $q = p^k$, p prime.
- Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.

Definition

An isogeny between E_1 and E_2 is a non-constant morphism φ, such that $\varphi(\mathcal{O}_1) = \mathcal{O}_2$.

- Isogenies are group homomorphisms.
- For every finite subgroup $G \subset E_1$, there exists an (up to isomorphisms) unique elliptic curve E_2 and a separable isogeny $\varphi : E_1 \to E_2$ such that $ker(\varphi) = G$. ($\to$ Vélu's formulas)
- If φ is separable, then $\#ker(\varphi) = deg(\varphi)$ is the degree of φ.

Isogenies

- Let $\mathbb{F}_q$ be a finite field with $q = p^k$, p prime.
- Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$.

Definition

An isogeny between E_1 and E_2 is a non-constant morphism φ, such that $\varphi(\mathcal{O}_1) = \mathcal{O}_2$.

- Isogenies are group homomorphisms.
- For every finite subgroup $G \subset E_1$, there exists an (up to isomorphisms) unique elliptic curve E_2 and a separable isogeny $\varphi : E_1 \to E_2$ such that $ker(\varphi) = G$. ($\to$ Vélu's formulas)
- If φ is separable, then $\#ker(\varphi) = deg(\varphi)$ is the degree of φ.
- For every degree-ℓ isogeny $\varphi : E_1 \to E_2$, there exists a dual isogeny $\hat{\varphi} : E_2 \to E_1$ of degree ℓ, such that $\hat{\varphi} \circ \varphi = [\ell]$.

SIDH

- Diffie-Hellman-style key exchange
- Works with supersingular elliptic curves over $\mathbb{F}_{p^2}$.
- Can be represented by random walks in isogeny graphs.

SIDH

- Diffie-Hellman-style key exchange
- Works with supersingular elliptic curves over $\mathbb{F}_{p^2}$.
- Can be represented by random walks in isogeny graphs.

Definition

An ℓ-isogeny graph is a graph with

- vertices representing isomorphic elliptic curves over $\mathbb{F}_q$
- undirected edges representing isogenies of degree ℓ (and their dual isogenies)

SIDH

- Diffie-Hellman-style key exchange
- Works with supersingular elliptic curves over $\mathbb{F}_{p^2}$.
- Can be represented by random walks in isogeny graphs.

Definition

An ℓ-isogeny graph is a graph with

- vertices representing isomorphic elliptic curves over $\mathbb{F}_q$
- undirected edges representing isogenies of degree ℓ (and their dual isogenies)

- Alice and Bob perform a random walk of length e_A resp. e_B through the ℓ_A- resp. ℓ_B-isogeny graph.

SIDH

- Diffie-Hellman-style key exchange
- Works with supersingular elliptic curves over $\mathbb{F}_{p^2}$.
- Can be represented by random walks in isogeny graphs.

Definition

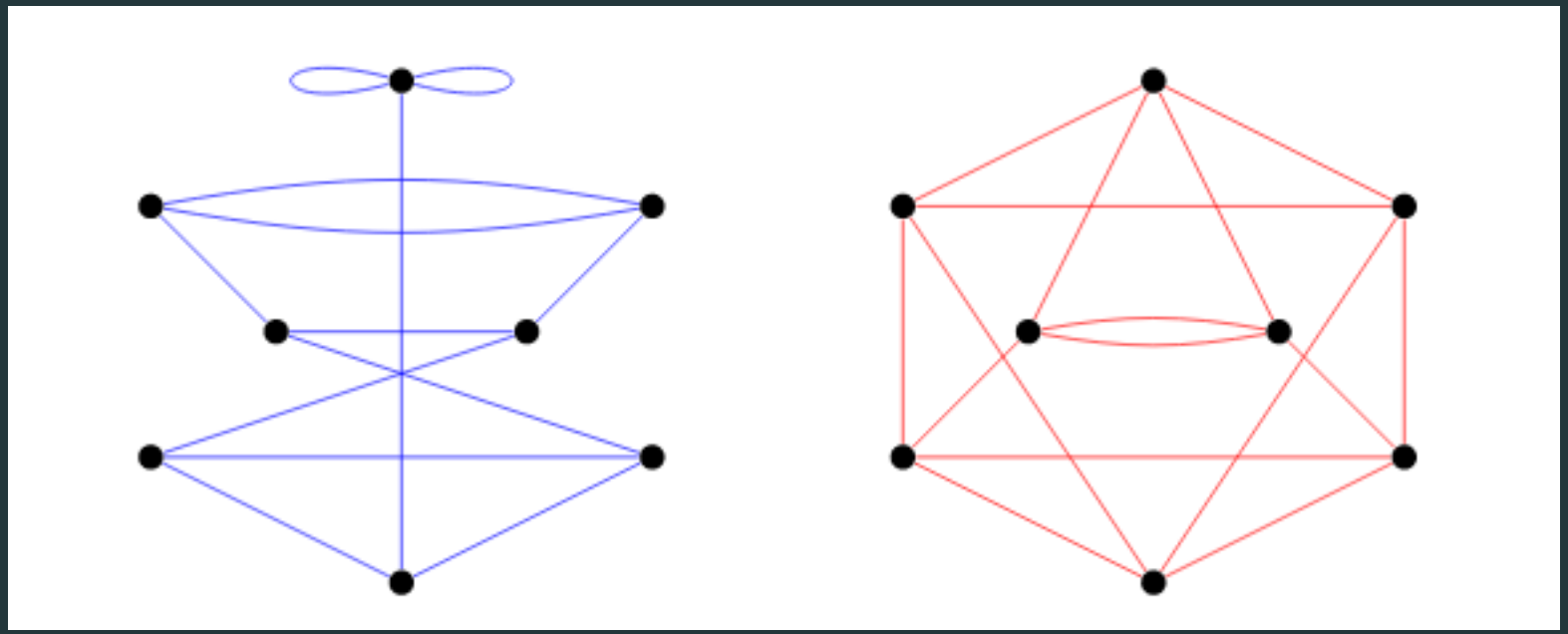
An ℓ-isogeny graph is a graph with

- vertices representing isomorphic elliptic curves over $\mathbb{F}_q$
- undirected edges representing isogenies of degree ℓ (and their dual isogenies)

- Alice and Bob perform a random walk of length e_A resp. e_B through the ℓ_A- resp. ℓ_B-isogeny graph.
- Secret: Isogeny of degree $\ell_A^{e_A}$ resp. $\ell_B^{e_B}$, determined by suitable kernel generator points.

SIDH

Toy example for 2- and 3-isogeny graphs over $\mathbb{F}_{97^2}$ by Luca De Feo[1]:



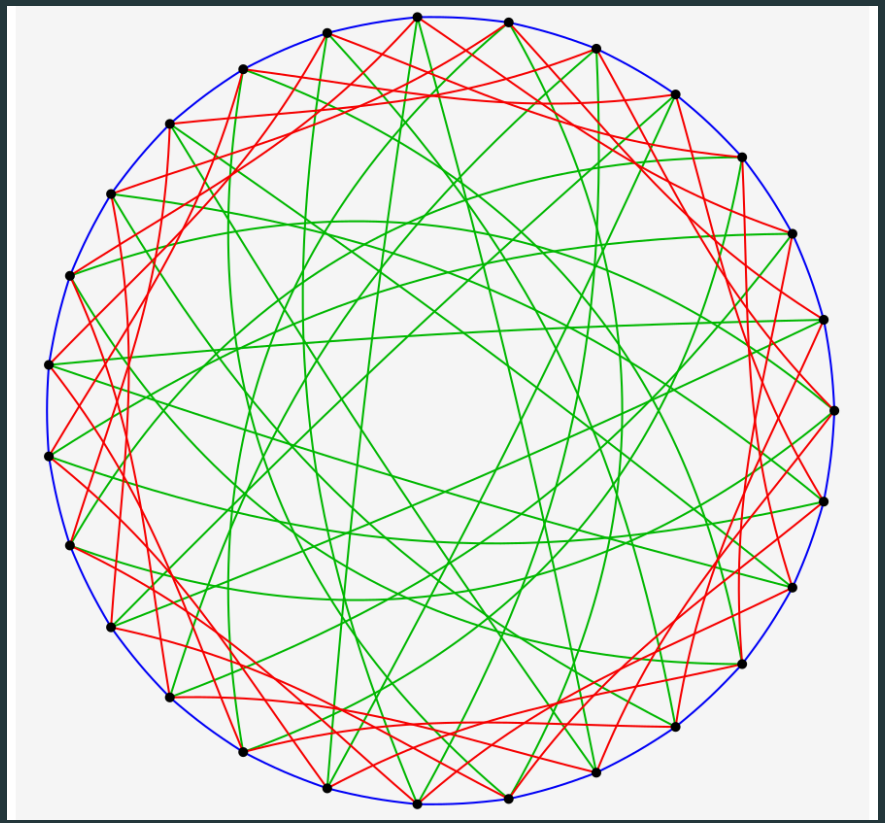
[1] Luca De Feo, *Lecture notes: Mathematics of Isogeny Based Cryptography*, https://arxiv.org/abs/1711.04062

CSIDH

- Introduced in May 2018 by Castryck, Lange, Martindale, Panny, and Renes.
- Diffie-Hellman-style key exchange
- Works with supersingular elliptic curves over $\mathbb{F}_p$.
- Isogeny graphs now consist of circles.
- Uses the union of supersingular ℓ_i-isogeny graphs for different ℓ_i.

CSIDH

Toy example for $\mathbb{F}_{419}$ by Castryck, Lange, Martindale, Panny, Renes[2], using 3- (blue), 5- (green), and 7-isogenies (red):



[2] Castryck, Lange, Martindale, Panny, Renes, *CSIDH: An Efficient Post-Quantum Commutative Group Action*, ASIACRYPT 2018

CSIDH

Setting

- Choose n small distinct odd primes $\ell_1, ..., \ell_n$, such that $p = 4 \cdot \ell_1 \cdot ... \cdot \ell_n - 1$ is prime.

CSIDH

Setting

- Choose n small distinct odd primes $\ell_1, ..., \ell_n$, such that $p = 4 \cdot \ell_1 \cdot ... \cdot \ell_n - 1$ is prime.
- Choose a supersingular elliptic curve E in Montgomery form over $\mathbb{F}_p$.

CSIDH

Setting

- Choose n small distinct odd primes $\ell_1, ..., \ell_n$, such that $p = 4 \cdot \ell_1 \cdot ... \cdot \ell_n - 1$ is prime.
- Choose a supersingular elliptic curve E in Montgomery form over $\mathbb{F}_p$.
- We now have $\#E(\mathbb{F}_p) = p + 1 = 4 \cdot \ell_1 \cdot ... \cdot \ell_n$.

CSIDH

Setting

- Choose n small distinct odd primes $\ell_1, ..., \ell_n$, such that $p = 4 \cdot \ell_1 \cdot ... \cdot \ell_n - 1$ is prime.
- Choose a supersingular elliptic curve E in Montgomery form over $\mathbb{F}_p$.
- We now have $\#E(\mathbb{F}_p) = p + 1 = 4 \cdot \ell_1 \cdot ... \cdot \ell_n$.

  $\Rightarrow E(\mathbb{F}_p)$ contains points of orders $4, \ell_1, ..., \ell_n$.

CSIDH

Setting

- Choose n small distinct odd primes $\ell_1, ..., \ell_n$, such that $p = 4 \cdot \ell_1 \cdot ... \cdot \ell_n - 1$ is prime.
- Choose a supersingular elliptic curve E in Montgomery form over $\mathbb{F}_p$.
- We now have $\#E(\mathbb{F}_p) = p + 1 = 4 \cdot \ell_1 \cdot ... \cdot \ell_n$.

  $\Rightarrow E(\mathbb{F}_p)$ contains points of orders $4, \ell_1, ..., \ell_n$.

  $\Rightarrow$ We can compute ℓ_i-isogenies via Vélu-type formulas.

CSIDH

Setting

- Choose n small distinct odd primes $\ell_1, ..., \ell_n$, such that $p = 4 \cdot \ell_1 \cdot ... \cdot \ell_n - 1$ is prime.
- Choose a supersingular elliptic curve E in Montgomery form over $\mathbb{F}_p$.
- We now have $\#E(\mathbb{F}_p) = p + 1 = 4 \cdot \ell_1 \cdot ... \cdot \ell_n$.

  $\Rightarrow E(\mathbb{F}_p)$ contains points of orders $4, \ell_1, ..., \ell_n$.

  $\Rightarrow$ We can compute ℓ_i-isogenies via Vélu-type formulas.
- Secret: tuple of integers $(e_1, ..., e_n)$ sampled from an interval $[-B, B]$

CSIDH

Setting

- Choose n small distinct odd primes $\ell_1, ..., \ell_n$, such that $p = 4 \cdot \ell_1 \cdot ... \cdot \ell_n - 1$ is prime.
- Choose a supersingular elliptic curve E in Montgomery form over $\mathbb{F}_p$.
- We now have $\#E(\mathbb{F}_p) = p + 1 = 4 \cdot \ell_1 \cdot ... \cdot \ell_n$.

  $\Rightarrow E(\mathbb{F}_p)$ contains points of orders $4, \ell_1, ..., \ell_n$.

  $\Rightarrow$ We can compute ℓ_i-isogenies via Vélu-type formulas.
- Secret: tuple of integers $(e_1, ..., e_n)$ sampled from an interval $[-B, B]$

  $\Rightarrow$ Go $|e_i|$ steps in direction $sign(e_i)$ through the ℓ_i-isogeny graph.

How to compute isogenies?

Costello, Hisil (2017)

Let K be a point of order $\ell = 2d + 1$ on a Montgomery curve $E : by^2 = x^3 + ax^2 + x$.

Computation of the coordinate map of the unique (up to compositions by isomorphisms) ℓ-isogeny $\varphi : E \to E'$ with $ker(\varphi) = \langle K \rangle$:

$$\varphi : (x, y) \mapsto (f(x), y \cdot f'(x)),$$

where

$$f(x) = x \cdot \prod_{i=1}^{d} \left(\frac{x \cdot x_{[i]K} - 1}{x - x_{[i]K}} \right)^2,$$

and $f'(x)$ is its derivative. Curve parameters a' and b' of E': $a' = (6\sigma - 6\tilde{\sigma} + a) \cdot \pi^2$ and $b' = b \cdot \pi^2$, where we define $\sigma = \sum_{i=1}^{d} x_{[i]K}$, $\tilde{\sigma} = \sum_{i=1}^{d} 1/x_{[i]K}$, and $\pi = \prod_{i=1}^{d} x_{[i]K}$.

Point evaluation

We work with XZ-only projective Montgomery coordinates: Write $(X_i : Z_i) = (x_{[i]K} : 1)$ for $i = 1, ..., d$, $(X : Z) = (x_P : 1)$ for the point P, at which the isogeny should be evaluated, and $(X' : Z')$ for the result. Then

$$X' = X \cdot \left(\prod_{i=1}^{d} \left[(X - Z)(X_i + Z_i) + (X + Z)(X_i - Z_i) \right] \right)^2, \quad \text{and}$$

$$Z' = Z \cdot \left(\prod_{i=1}^{d} \left[(X - Z)(X_i + Z_i) - (X + Z)(X_i - Z_i) \right] \right)^2.$$

Image curve computation

Computing $a' = (6\sigma - 6\tilde{\sigma} + a) \cdot \pi^2$ and $b' = b \cdot \pi^2$, where we have $\sigma = \sum_{i=1}^{d} x_{[i]K}$, $\tilde{\sigma} = \sum_{i=1}^{d} 1/x_{[i]K}$, and $\pi = \prod_{i=1}^{d} x_{[i]K}$ is not really efficient.

Image curve computation

Computing $a' = (6\sigma - 6\tilde{\sigma} + a) \cdot \pi^2$ and $b' = b \cdot \pi^2$, where we have $\sigma = \sum_{i=1}^{d} x_{[i]K}$, $\tilde{\sigma} = \sum_{i=1}^{d} 1/x_{[i]K}$, and $\pi = \prod_{i=1}^{d} x_{[i]K}$ is not really efficient.

Our idea:

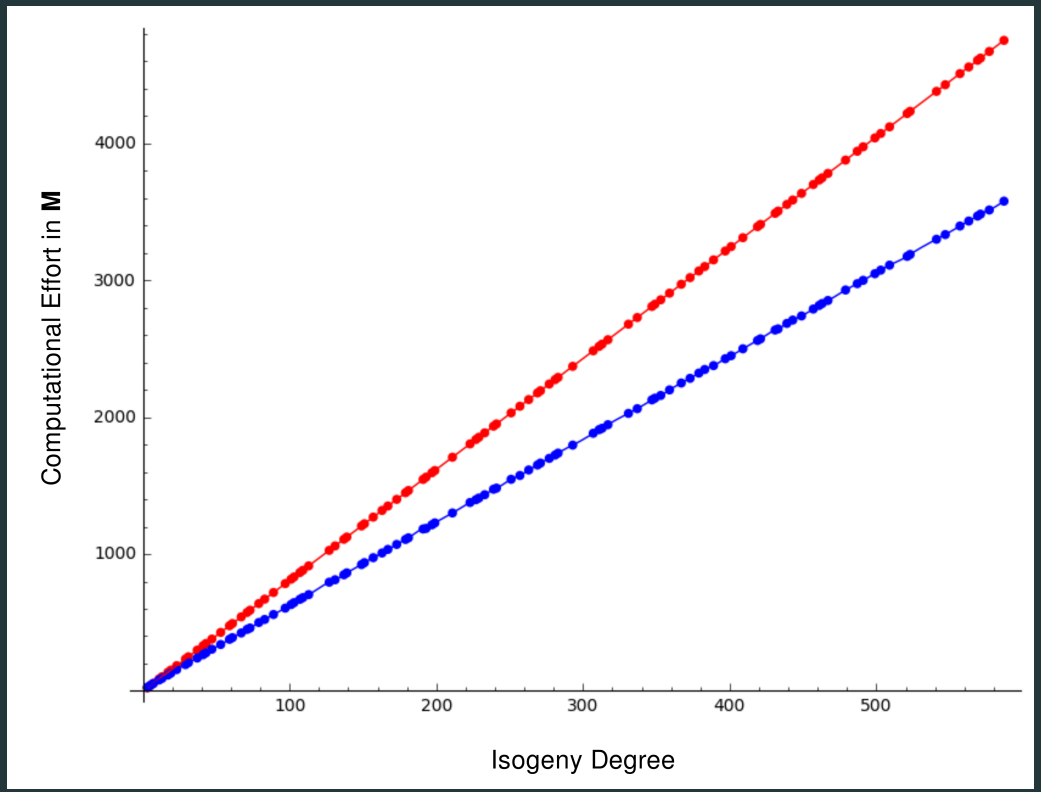
Switch to a birationally equivalent twisted Edwards curve for the image curve computation, and use isogeny formulas of Moody and Shumow (2011) (switching costs only a few additions):

$$a'_E = a^{\ell}_E \cdot \pi_Z^8, \quad \text{and} \quad d'_E = d^{\ell}_E \cdot \pi_Y^8,$$

where $\pi_Y = \prod_{i=1}^{d} Y_i^E$, and $\pi_Z = \prod_{i=1}^{d} Z_i^E$.
Switch back to Montgomery form afterwards by
$(A' : C') = (2(a'_E + d'_E) : a'_E - d'_E)$

Isogeny computations

Comparison: our approach (blue) and (optimized) implementation by Castryck et al. (red)



CSIDH algorithm

Algorithm 1: Evaluating the class group action.

Input : $A \in \mathbb{F}_p$ and a list of integers $(e_1, ..., e_n)$.
Output: A' such that $[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_A = E_{A'}$.

1 **while** some $e_i \neq 0$ **do**
2 Sample a random $x \in \mathbb{F}_p$.
3 Set $s \leftarrow +1$ if $x^3 + Ax^2 + x$ is a square in $\mathbb{F}_p$, else $s \leftarrow -1$.
4 Let $S = \{i \mid sign(e_i) = s\}$.
5 **if** $S = \emptyset$ **then**
6 Go to line 2.
7 $P = (x : 1)$, $k \leftarrow \prod_{i \in S} \ell_i$, $P \leftarrow [(p+1)/k]P$.
8 **foreach** $i \in S$ **do**
9 $K \leftarrow [k/\ell_i]P$.
10 **if** $K \neq \infty$ **then**
11 Compute a degree-ℓ_i isogeny $\varphi : E_A \rightarrow E_{A'}$ with $ker(\varphi) = \langle K \rangle$.
12 $A \leftarrow A'$, $P \leftarrow \varphi(P)$, $k \leftarrow k/\ell_i$, $e_i \leftarrow e_i - s$.

Implementation results

We plugged our optimizations into the implementation of Castryck et. al for a comparison of the running time of one class group action evaluation (averaged over 10 000 runs on an Intel Core i7-6500 Skylake processor running Ubuntu 16.04 LTS):

	Clock Cycles $\times 10^6$	Speed-up Factor
Castryck et al.	138.6	-
Isogeny Optimization	118.2	1.173
Combination of all Optimizations	103.9	1.334

CSIDH

Advantages

- Small key sizes: 64 bytes for conjectured NIST security level 1
- Validation of public keys is possible (and efficient): check if the corresponding curve parameter defines a supersingular curve.

  $\Rightarrow$ static-static key exchange possible

CSIDH

Advantages

- Small key sizes: 64 bytes for conjectured NIST security level 1
- Validation of public keys is possible (and efficient): check if the corresponding curve parameter defines a supersingular curve.

  $\Rightarrow$ static-static key exchange possible

Disadvantages

- Significantly slower than SIDH and other post-quantum primitives
- More analysis on the (quantum) security is necessary

Future work

- Protected constant-time implementations
- Further optimizations and speed-ups
- Analysis of the quantum security of CSIDH
- Hardware implementations
- ...

Mentioned references

- W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, *CSIDH: An Efficient Post-Quantum Commutative Group Action*, ASIACRYPT 2018.
- C. Costello, H. Hisil, *A simple and compact algorithm for SIDH with arbitrary degree isogenies*, ASIACRYPT 2017.
- D. Moody, D. Shumow. *Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves*, Mathematics of Computation, 85(300), 1929-1951, 2016.
- L. De Feo, *Lecture notes: Mathematics of Isogeny Based Cryptography*, https://arxiv.org/abs/1711.04062, 2017.

Thank you for the attention!

Questions?