Multiprime Strategies for Serial Evaluations of eSIDH-Like Isogenies

12^{th} July 2023

Jason LeGrow   Brian Koziel   Reza Azarderakhsh

VIRGINIA TECH

Commonwealth Cyber Initiative
SOUTHWEST VIRGINIA

Diffie-Hellman Key Establishment

The goal: Alice and Bob have a public conversation, and leave with a shared secret.

Diffie-Hellman Key Establishment

The goal: Alice and Bob have a public conversation, and leave with a shared secret.
Diffie and Hellman proposed: choose $G = \langle g \rangle$ of prime order p and do:

$$\begin{array}{ccc}
x \xleftarrow{\$} \{0, 1, \ldots, p-1\} & & y \xleftarrow{\$} \{0, 1, \ldots, p-1\} \\
X \leftarrow g^x & & Y \leftarrow g^y \\
& \xrightarrow{\quad X \quad} & \\
& \xleftarrow[\quad Y \quad]{} & \\
K_A \leftarrow Y^x & & K_B \leftarrow X^y
\end{array}$$

Diffie-Hellman Key Establishment

The goal: Alice and Bob have a public conversation, and leave with a shared secret. Diffie and Hellman proposed: choose $G = \langle g \rangle$ of prime order p and do:

Alice		Bob
$x \xleftarrow{\$} \{0, 1, \ldots, p-1\}$		$y \xleftarrow{\$} \{0, 1, \ldots, p-1\}$
$X \leftarrow g^x$		$Y \leftarrow g^y$
	$\xrightarrow{\quad X \quad}$	
	$\xleftarrow[\quad Y \quad]{}$	
$K_A \leftarrow Y^x$		$K_B \leftarrow X^y$

Correctness: We have $K_A = Y^x = g^{xy} = X^y = K_B$.

Diffie-Hellman Key Establishment

The goal: Alice and Bob have a public conversation, and leave with a shared secret.
Diffie and Hellman proposed: choose $G = \langle g \rangle$ of prime order p and do:

$$x \xleftarrow{\$} \{0, 1, \ldots, p-1\} \qquad\qquad y \xleftarrow{\$} \{0, 1, \ldots, p-1\}$$
$$X \leftarrow g^x \qquad\qquad Y \leftarrow g^y$$

$$\xrightarrow{\quad X \quad}$$

$$\xleftarrow[\quad Y \quad]{}$$

$$K_A \leftarrow Y^x \qquad\qquad K_B \leftarrow X^y$$

Correctness: We have $K_A = Y^x = g^{xy} = X^y = K_B$.

Security: In the quantum setting, **completely broken** by Shor's algorithm. We need new primitives.

Elliptic Curves

For my purposes, an **elliptic curve** is a set of the form

$$E_C/k = \{(x, y) \in \overline{k}^2 : y^2 = x^3 + Cx^2 + x\} \sqcup \{\infty\}$$

for some $C \in k \setminus \{2, -2\}$. This is **Montgomery form**, and C is the **Montgomery coefficient.**

Elliptic Curves

For my purposes, an **elliptic curve** is a set of the form

$$E_C/k = \{(x, y) \in \overline{k}^2 \,:\, y^2 = x^3 + Cx^2 + x\} \sqcup \{\infty\}$$

for some $C \in k \backslash \{2, -2\}$. This is **Montgomery form**, and C is the **Montgomery coefficient.**

I will also care about the k-rational points of a curve:

$$E_C(k) = \{(x, y) \in k^2 \,:\, y^2 = x^3 + Cx^2 + x\} \sqcup \{\infty\}.$$

Elliptic Curves and the Group Law

Here's (the real points of) an elliptic curve:

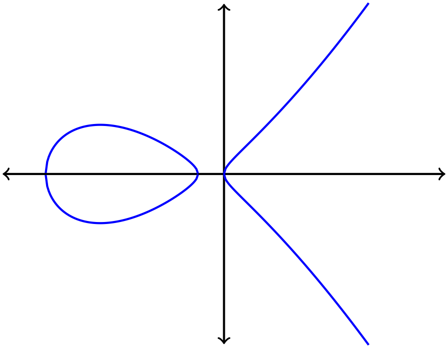


Figure: The curve $E_3/\mathbb{R}\colon y^2 = x^3 + 3x^2 + x$.

Elliptic Curves and the Group Law

Every elliptic curve is also a group, using the chord and tangent law.

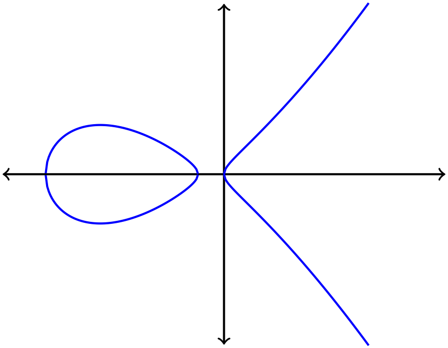


Figure: The curve $E_3/\mathbb{R}\colon y^2 = x^3 + 3x^2 + x$.

Elliptic Curves and the Group Law

Every elliptic curve is also a group, using the chord and tangent law.

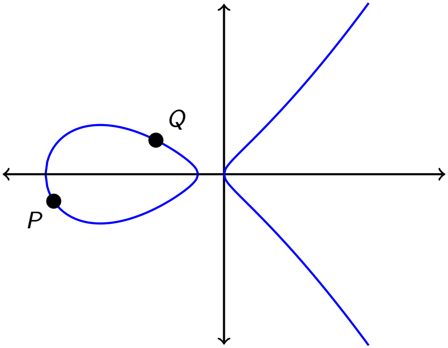


Figure: The curve $E_3/\mathbb{R}\colon\ y^2 = x^3 + 3x^2 + x$.

Elliptic Curves and the Group Law

Every elliptic curve is also a group, using the chord and tangent law.

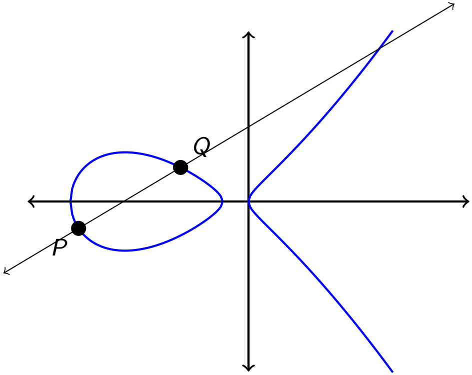


Figure: The curve $E_3/\mathbb{R}\colon y^2 = x^3 + 3x^2 + x$.

Elliptic Curves and the Group Law

Every elliptic curve is also a group, using the chord and tangent law.

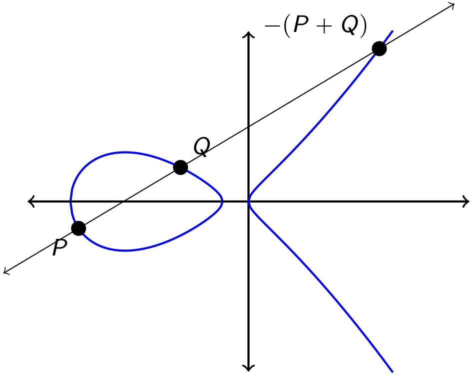


Figure: The curve $E_3/\mathbb{R}\colon y^2 = x^3 + 3x^2 + x$.

Elliptic Curves and the Group Law

Every elliptic curve is also a group, using the chord and tangent law.

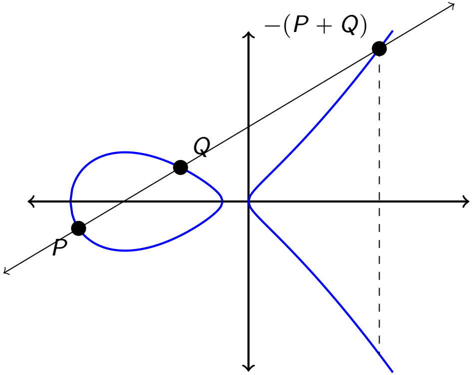


Figure: The curve $E_3/\mathbb{R}$: $y^2 = x^3 + 3x^2 + x$.

Elliptic Curves and the Group Law

Every elliptic curve is also a group, using the chord and tangent law.

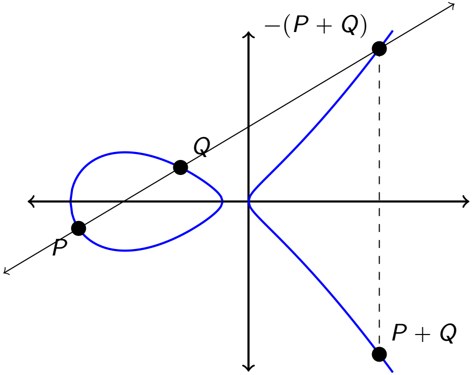


Figure: The curve $E_3/\mathbb{R}\colon y^2 = x^3 + 3x^2 + x$.

Elliptic Curves and the Group Law

With this group operation in mind, I define the m-**torsion subgroup** of an elliptic curve as

$$E[m] = \{P \in E : [m]P = \infty\}.$$

(here $[m]$ is the multiplication-by-m map).

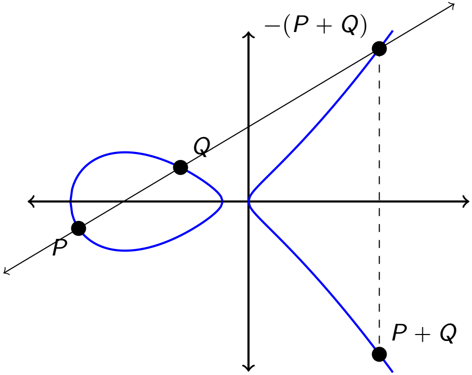


Figure: The curve $E_3/\mathbb{R}$: $y^2 = x^3 + 3x^2 + x$.

Ordinary and Supersingular Elliptic Curves

Elliptic curves come in two flavours: **ordinary** and **supersingular**.

Ordinary and Supersingular Elliptic Curves

Elliptic curves come in two flavours: **ordinary** and **supersingular**. There are many equivalent definitions that differentiate these cases; for us, we care about:

- $E/\mathbb{F}_{p^r}$ is supersingular iff $p|(p^r + 1 - |E(\mathbb{F}_{p^r})|)$

Ordinary and Supersingular Elliptic Curves

Elliptic curves come in two flavours: **ordinary** and **supersingular**. There are many equivalent definitions that differentiate these cases; for us, we care about:

- $E/\mathbb{F}_{p^r}$ is supersingular iff $p | (p^r + 1 - |E(\mathbb{F}_{p^r})|)$
- $E/\mathbb{F}_{p^r}$ is supersingular iff $\mathrm{End}(E)$ is non-commutative.

Ordinary and Supersingular Elliptic Curves

Elliptic curves come in two flavours: **ordinary** and **supersingular**. There are many equivalent definitions that differentiate these cases; for us, we care about:

- $E/\mathbb{F}_{p^r}$ is supersingular iff $p|(p^r + 1 - |E(\mathbb{F}_{p^r})|)$
- $E/\mathbb{F}_{p^r}$ is supersingular iff $\mathrm{End}(E)$ is non-commutative.

Fact: If E/k is supersingular and char $k = p$, then E is defined over $\mathbb{F}_{p^2}$.

Ordinary and Supersingular Elliptic Curves

Elliptic curves come in two flavours: **ordinary** and **supersingular**. There are many equivalent definitions that differentiate these cases; for us, we care about:

- $E/\mathbb{F}_{p^r}$ is supersingular iff $p|(p^r + 1 - |E(\mathbb{F}_{p^r})|)$
- $E/\mathbb{F}_{p^r}$ is supersingular iff $\mathrm{End}(E)$ is non-commutative.

Fact: If E/k is supersingular and char $k = p$, then E is defined over $\mathbb{F}_{p^2}$.

In classical cryptography, supersingular elliptic curves are not used as platform groups for Diffie-Hellman, since the discrete logarithm problem can be solved on such curves in subexponential time.

Isogenies

An **isogeny** between two elliptic curves is a function $\psi\colon E \to E'$ which is simultaneously a group homomorphism and a morphism of varieties.

Isogenies

An **isogeny** between two elliptic curves is a function $\psi\colon E \to E'$ which is simultaneously a group homomorphism and a morphism of varieties.
I will only care about isogenies whose degree is coprime to char k; such an isogeny is **separable** and is defined up to isomorphism by its **kernel**

$$\ker \psi = \{P \in E \ : \ \psi(P) = \infty\}.$$

Isogenies

An **isogeny** between two elliptic curves is a function $\psi\colon E \to E'$ which is simultaneously a group homomorphism and a morphism of varieties.
I will only care about isogenies whose degree is coprime to char k; such an isogeny is **separable** and is defined up to isomorphism by its **kernel**

$$\ker\psi = \{P \in E \; : \; \psi(P) = \infty\}.$$

Given a description of $\ker\psi$, we can compute E' and $\psi(P)$ for any $P \in E$ in time polynomial in $\deg\psi$ using **Vélu's formulas.**

Isogenies

An **isogeny** between two elliptic curves is a function $\psi\colon E \to E'$ which is simultaneously a group homomorphism and a morphism of varieties.
I will only care about isogenies whose degree is coprime to char k; such an isogeny is **separable** and is defined up to isomorphism by its **kernel**

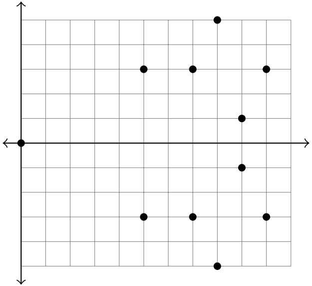
$$\ker\psi = \{P \in E \;:\; \psi(P) = \infty\}.$$

Given a description of $\ker\psi$, we can compute E' and $\psi(P)$ for any $P \in E$ in time polynomial in $\deg\psi$ using **Vélu's formulas.** We will write $E' = E/\ker\psi$.

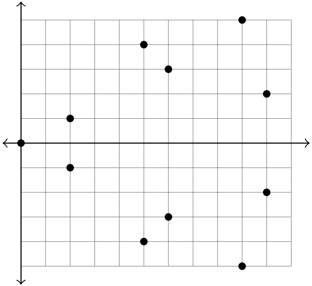
Example: An Isogeny

These curves are related by the isogeny

$$\psi(x,y) = \left(\frac{3x^3+x^2+x}{x^2+x+3},\; y\frac{4x^3-5x^2-3}{x^3-4x^2-2x-4}\right)$$



$E_0/\mathbb{F}_{11} : y^2 = x^3 + x$

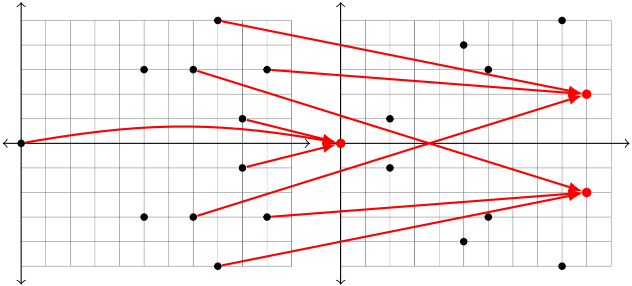


$E_6/\mathbb{F}_{11} : y^2 = x^3 + 6x^2 + x$

Example: An Isogeny

These curves are related by the isogeny

$$\psi(x,y) = \left(\frac{3x^3 + x^2 + x}{x^2 + x + 3}, \; y\frac{4x^3 - 5x^2 - 3}{x^3 - 4x^2 - 2x - 4} \right)$$



$E_0/\mathbb{F}_{11} : y^2 = x^3 + x$ $E_6/\mathbb{F}_{11} : y^2 = x^3 + 6x^2 + x$

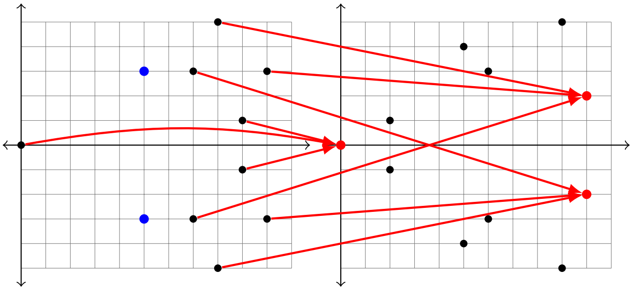
Example: An Isogeny

These curves are related by the isogeny

$$\psi(x,y) = \left(\frac{3x^3+x^2+x}{x^2+x+3},\ y\,\frac{4x^3-5x^2-3}{x^3-4x^2-2x-4}\right)$$

We have $\deg\psi = 3$, so as you expect it is a 3-to-1 map. Its kernel is

$$\ker\psi = \{\infty, (5,3), (5,8)\} = \langle(5,3)\rangle\,.$$



$E_0/\mathbb{F}_{11} : y^2 = x^3 + x$ $E_6/\mathbb{F}_{11} : y^2 = x^3 + 6x^2 + x$

SIDH: Protocol Description

Global parameters:

- A prime $p = \ell_A^{e_A} \ell_B^{e_B} - 1$ for small primes $\ell_A \neq \ell_B$;
- A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $|E(\mathbb{F}_{p^2})| = (p+1)^2$; and,
- Torsion bases $\{P_A, Q_A\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_A^{e_A}]$, $\{P_B, Q_B\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_B^{e_B}]$.

SIDH: Protocol Description

Global parameters:

- A prime $p = \ell_A^{e_A}\ell_B^{e_B} - 1$ for small primes $\ell_A \neq \ell_B$;
- A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $|E(\mathbb{F}_{p^2})| = (p+1)^2$; and,
- **Torsion bases $\{P_A, Q_A\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_A^{e_A}]$, $\{P_B, Q_B\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_B^{e_B}]$.**

We can show that

$$
\begin{aligned}
E[\ell_A^{e_A}], E[\ell_B^{e_B}] &\subseteq E(\mathbb{F}_{p^2}) \\
E[\ell_A^{e_A}] &\cong \mathbb{Z}_{\ell_A^{e_A}} \oplus \mathbb{Z}_{\ell_A^{e_A}} \\
E[\ell_B^{e_B}] &\cong \mathbb{Z}_{\ell_B^{e_B}} \oplus \mathbb{Z}_{\ell_B^{e_B}}
\end{aligned}
$$

SIDH: Protocol Description

Global parameters:

- A prime $p = \ell_A^{e_A}\ell_B^{e_B} - 1$ for small primes $\ell_A \neq \ell_B$;
- A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $|E(\mathbb{F}_{p^2})| = (p+1)^2$; and,
- **Torsion bases $\{P_A, Q_A\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_A^{e_A}]$, $\{P_B, Q_B\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_B^{e_B}]$.**

We can show that

$$E[\ell_A^{e_A}], E[\ell_B^{e_B}] \subseteq E(\mathbb{F}_{p^2})$$

$$E[\ell_A^{e_A}] \cong \mathbb{Z}_{\ell_A^{e_A}} \oplus \mathbb{Z}_{\ell_A^{e_A}}$$

$$E[\ell_B^{e_B}] \cong \mathbb{Z}_{\ell_B^{e_B}} \oplus \mathbb{Z}_{\ell_B^{e_B}}$$

This only works because E is supersingular and because of the special form of p.

SIDH: Protocol Description

Global parameters:

- A prime $p = \ell_A^{e_A}\ell_B^{e_B} - 1$ for small primes $\ell_A \neq \ell_B$;
- A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $|E(\mathbb{F}_{p^2})| = (p+1)^2$; and,
- Torsion bases $\{P_A, Q_A\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_A^{e_A}]$, $\{P_B, Q_B\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_B^{e_B}]$.

$$x \xleftarrow{\$} \{0, 1, \ldots, \ell_A^{e_A} - 1\} \qquad\qquad y \xleftarrow{\$} \{0, 1, \ldots, \ell_B^{e_B} - 1\}$$

$$\ker\psi_A = \langle P_A + xQ_A\rangle \qquad\qquad \ker\psi_B = \langle P_B + yQ_B\rangle$$

$$\xrightarrow{X = (E_A = E/\ker\psi_A, \psi_A(P_B), \psi_A(Q_B))}$$

$$\xleftarrow[Y = (E_B = E/\ker\psi_B, \psi_B(P_A), \psi_B(Q_A))]{}$$

$$K_A \leftarrow \quad E_B/\langle\psi_B(P_A) + x\psi_B(Q_A)\rangle \qquad\qquad K_B \leftarrow \quad E_A/\langle\psi_A(P_B) + y\psi_A(Q_B)\rangle$$

SIDH: Protocol Description

Global parameters:

- A prime $p = \ell_A^{e_A}\ell_B^{e_B} - 1$ for small primes $\ell_A \neq \ell_B$;
- A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $|E(\mathbb{F}_{p^2})| = (p+1)^2$; and,
- Torsion bases $\{P_A, Q_A\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_A^{e_A}]$, $\{P_B, Q_B\} \subseteq E(\mathbb{F}_{p^2})$ for $E[\ell_B^{e_B}]$.

$$x \xleftarrow{\$} \{0, 1, \ldots, \ell_A^{e_A} - 1\} \qquad\qquad y \xleftarrow{\$} \{0, 1, \ldots, \ell_B^{e_B} - 1\}$$

$$\ker \psi_A = \langle P_A + xQ_A \rangle \qquad\qquad \ker \psi_B = \langle P_B + yQ_B \rangle$$

$$\xrightarrow{X = (E_A = E/\ker\psi_A, \psi_A(P_B), \psi_A(Q_B))}$$

$$\xleftarrow[Y = (E_B = E/\ker\psi_B, \psi_B(P_A), \psi_B(Q_A))]{}$$

$$K_A \leftarrow j(E_B/\langle \psi_B(P_A) + x\psi_B(Q_A)\rangle) \qquad\qquad K_B \leftarrow j(E_A/\langle \psi_A(P_B) + y\psi_A(Q_B)\rangle)$$

SIDH: Computing the Required Isogenies

Let's think about ψ_A; it has degree $\ell_A^{e_A}$, and we know its kernel is $\langle P_A + xQ_A \rangle$.

SIDH: Computing the Required Isogenies

Let's think about ψ_A; it has degree $\ell_A^{e_A}$, and we know its kernel is $\langle P_A + xQ_A \rangle$.

It decomposes as

$$\psi_A = \psi_{A,e_A} \circ \psi_{A,e_{A-1}} \circ \cdots \circ \psi_{A,1}$$

whose kernels are given by

$$\ker \psi_{A,i} = \langle \overbrace{[\ell_A^{e_A - i}] \cdot \psi_{A,i-1} \circ \cdots \circ \psi_{A,1}(P_A + xQ_A)}^{Q_{A,i}} \rangle$$

SIDH: Computing the Required Isogenies

Let's think about ψ_A; it has degree $\ell_A^{e_A}$, and we know its kernel is $\langle P_A + xQ_A \rangle$.

It decomposes as

$$\psi_A = \psi_{A,e_A} \circ \psi_{A,e_{A-1}} \circ \cdots \circ \psi_{A,1}$$

whose kernels are given by

$$\ker \psi_{A,i} = \langle \overbrace{[\ell_A^{e_A - i}] \cdot \psi_{A,i-1} \circ \cdots \circ \psi_{A,1}(P_A + xQ_A)}^{Q_{A,i}} \rangle$$

Running SIDH quickly $\iff$ finding the $Q_{A,i}$ quickly.

A Common Thread: Strategies

- There is an obvious way for Alice to compute her $Q_{A,i}$:
  - Set $R_A = P_A + xQ_A$
  - In the i^{th} round:
    - Compute $Q_{A,i} = [\ell_A^{e_A - i}]R_A$
    - Update $R_A \leftarrow \psi_{A,i}(R_A)$

A Common Thread: Strategies

- There is an obvious way for Alice to compute her $Q_{A,i}$:
  - Set $R_A = P_A + xQ_A$
  - In the i^{th} round:
    - Compute $Q_{A,i} = [\ell_A^{e_A - i}]R_A$
    - Update $R_A \leftarrow \psi_{A,i}(R_A)$
- We can represent this pictorially:
  - Vertices $\iff$ Points on curves
  - Horizontal edges $\iff$ $[\ell_A]$
  - Vertical edges $\iff$ ℓ_A-isogeny

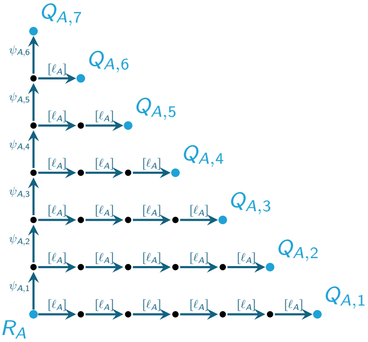


Figure: Some illustrations with $e_A = 7$.

A Common Thread: Strategies

- There is an obvious way for Alice to compute her $Q_{A,i}$:
  - Set $R_A = P_A + xQ_A$
  - In the i^{th} round:
    - Compute $Q_{A,i} = [\ell_A^{e_A - i}]R_A$
    - Update $R_A \leftarrow \psi_{A,i}(R_A)$
- We can represent this pictorially:
  - Vertices $\iff$ Points on curves
  - Horizontal edges $\iff$ $[\ell_A]$
  - Vertical edges $\iff$ ℓ_A-isogeny
- There are some "unused edges":

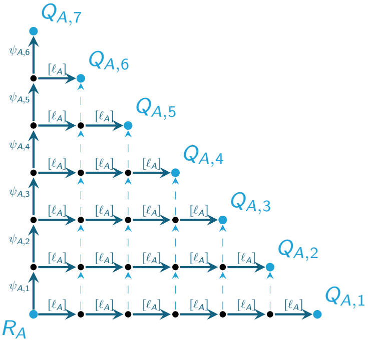


Figure: Some illustrations with $e_A = 7$.

A Common Thread: Strategies

- Let's forget about the obvious algorithm for a minute

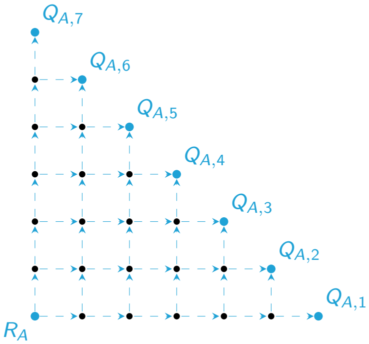


Figure: Some illustrations with $e_A = 7$.

A Common Thread: Strategies

- Let's forget about the obvious algorithm for a minute
- Any **Steiner arborescence** with root R_A and terminals $\{Q_{A,1}, \ldots, Q_{A,e_A}\}$ gives us an algorithm by following its edges from bottom to top, left to right.
  (A Steiner arborescence in G with root r and terminals T is a connected subgraph of G that contains a path from r to each element of T, and has no undirected cycles).

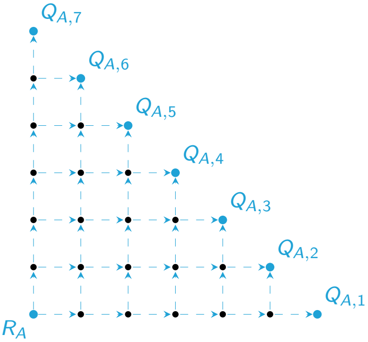


Figure: Some illustrations with $e_A = 7$.

A Common Thread: Strategies

- Let's forget about the obvious algorithm for a minute
- Any **Steiner arborescence** with root R_A and terminals $\{Q_{A,1}, \ldots, Q_{A,e_A}\}$ gives us an algorithm by following its edges from bottom to top, left to right.
- We call such an arborescence a **strategy**. Here's one:

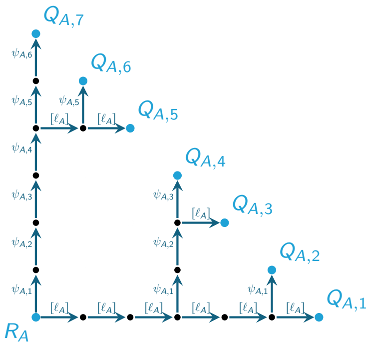


Figure: Some illustrations with $e_A = 7$.

Optimal Strategies

How do we choose the strategy to use?

Optimal Strategies

How do we choose the strategy to use? We want the one that will run the fastest.

Optimal Strategies

How do we choose the strategy to use? We want the one that will run the fastest.

Each edge corresponds to a known algorithm (scalar multiplication or isogeny evaluation) whose "cost" we can measure. The total cost of the algorithm is the sum of the edge costs.

Optimal Strategies

How do we choose the strategy to use? We want the one that will run the fastest.

Each edge corresponds to a known algorithm (scalar multiplication or isogeny evaluation) whose "cost" we can measure. The total cost of the algorithm is the sum of the edge costs.

Cycle count

+ Corresponds "directly" to running time
- Algorithm must be implemented first!
- Platform-dependent

Field multiplication count

+ Can "read off" from algorithm description
- Clock time depends on field arithmetic speed $\Longrightarrow$ hard to compare across fields

Optimal Strategies

How do we choose the strategy to use? We want the one that will run the fastest.

Each edge corresponds to a known algorithm (scalar multiplication or isogeny evaluation) whose "cost" we can measure. The total cost of the algorithm is the sum of the edge costs.

Cycle count

+ Corresponds "directly" to running time
− Algorithm must be implemented first!
− Platform-dependent

Field multiplication count

+ Can "read off" from algorithm description
− Clock time depends on field arithmetic speed $\Longrightarrow$ hard to compare across fields

For `SIKEp434` (*i.e.*, for the prime $p = 2^{216}3^{137} - 1$):

- Multiplication by 3 takes 2965 cycles/11 field multiplications
- 3-isogeny evaluation takes 1478 cycles/5.6 field multiplications

Strategies in Weighted Graphs for SIDH

We can redraw the graph so that it better depicts the algorithm's cost; in this drawing, the total length of solid edges is (a proxy for) running time:

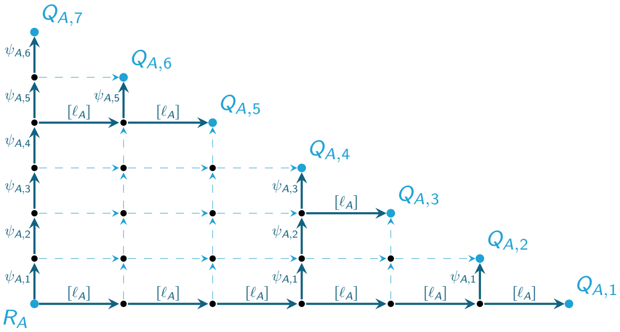


Figure: A weighted strategy for $\ell_A = 3$ and $e_A = 7$.

Strategies in Weighted Graphs for SIDH

We can redraw the graph so that it better depicts the algorithm's cost; in this drawing, the total length of solid edges is (a proxy for) running time:

For the cost model (11,5.6) from before, this strategy is optimal.

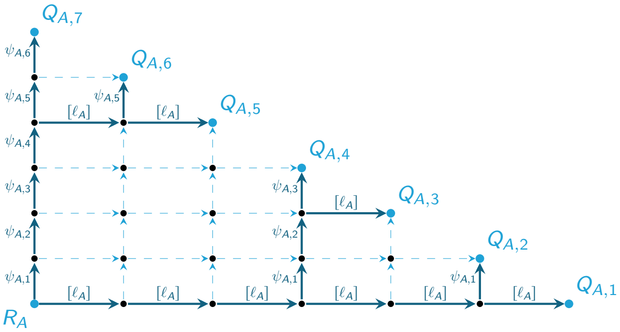


Figure: A weighted strategy for $\ell_A = 3$ and $e_A = 7$.

Strategies in Weighted Graphs for SIDH

We can redraw the graph so that it better depicts the algorithm's cost; in this drawing, the total length of solid edges is (a proxy for) running time:

For the cost model (11,5.6) from before, this strategy is optimal.

De Feo–Jao–Plût (2011) construct optimal strategies for SIDH using a recursive decomposition/dynamic programming technique.

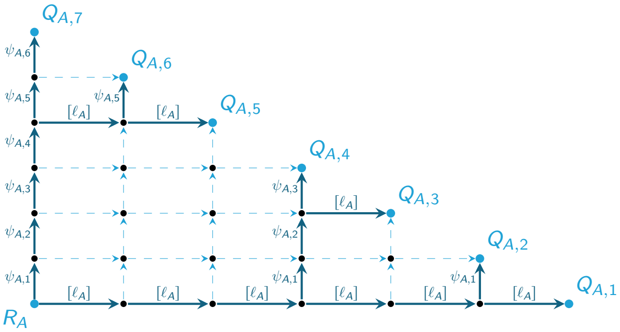


Figure: A weighted strategy for $\ell_A = 3$ and $e_A = 7$.

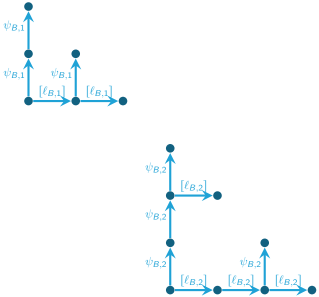
eSIDH

In Extended SIDH (eSIDH), Bob uses isogenies of non-prime-power degree $\ell_{B,1}^{e_{B,1}} \cdots \ell_{B,m}^{e_{B,m}}$.

eSIDH

In Extended SIDH (eSIDH), Bob uses isogenies of non-prime-power degree $\ell_{B,1}^{e_{B,1}} \cdots \ell_{B,m}^{e_{B,m}}$.

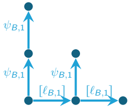
In the first round, Bob computes m isogenies using m different strategies—this saves a lot of edges!



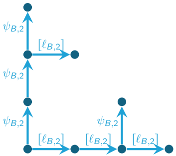
eSIDH

In Extended SIDH (eSIDH), Bob uses isogenies of non-prime-power degree $\ell_{B,1}^{e_{B,1}} \cdots \ell_{B,m}^{e_{B,m}}$.

In the first round, Bob computes m isogenies using m different strategies—this saves a lot of edges!



But each "small" strategy requires a torsion basis to construct the root... So in the *second* round, these must be constructed using costly scalar multiplications.



Multiprime Strategies in Serial eSIDH

Note that if $E[\ell_{B,1}^{e_{B,1}}] = \langle P_1, Q_1 \rangle$ and $E[\ell_{B,2}^{e_{B,2}}] = \langle P_2, Q_2 \rangle$ then for any β_1, β_2 there exists an integer β^* such that

$$\underbrace{\langle P_1 + \beta_1 Q_1, P_2 + \beta_2 Q_2 \rangle}_{\text{Bob does this in eSIDH}} = \underbrace{\langle P_1 + P_2 + \beta(Q_1 + Q_2) \rangle}_{\text{Bob could do this instead}}$$

Multiprime Strategies in Serial eSIDH

Note that if $E[\ell_{B,1}^{e_{B,1}}] = \langle P_1, Q_1 \rangle$ and $E[\ell_{B,2}^{e_{B,2}}] = \langle P_2, Q_2 \rangle$ then for any β_1, β_2 there exists an integer β^* such that

$$\underbrace{\langle P_1 + \beta_1 Q_1, P_2 + \beta_2 Q_2 \rangle}_{\text{Bob does this in eSIDH}} = \underbrace{\langle P_1 + P_2 + \beta(Q_1 + Q_2) \rangle}_{\text{Bob could do this instead}}$$

Righthand side needs a *single* strategy of size $e_{B,1} + e_{B,2}$, where different edges use different primes ($\ell_{B,1}$ or $\ell_{B,2}$).

Multiprime Strategies in Serial eSIDH

Note that if $E[\ell_{B,1}^{e_{B,1}}] = \langle P_1, Q_1 \rangle$ and $E[\ell_{B,2}^{e_{B,2}}] = \langle P_2, Q_2 \rangle$ then for any β_1, β_2 there exists an integer β^* such that

$$\underbrace{\langle P_1 + \beta_1 Q_1, P_2 + \beta_2 Q_2 \rangle}_{\text{Bob does this in eSIDH}} = \underbrace{\langle P_1 + P_2 + \beta(Q_1 + Q_2) \rangle}_{\text{Bob could do this instead}}$$

Righthand side needs a *single* strategy of size $e_{B,1} + e_{B,2}$, where different edges use different primes ($\ell_{B,1}$ or $\ell_{B,2}$).

Interestingly: I don't have to do all $\ell_{B,2}$ edges and then all $\ell_{B,1}$ edges; I can interweave them—**multiprime** strategies.

Multiprime Strategies in Serial eSIDH

Note that if $E[\ell_{B,1}^{e_{B,1}}] = \langle P_1, Q_1 \rangle$ and $E[\ell_{B,2}^{e_{B,2}}] = \langle P_2, Q_2 \rangle$ then for any β_1, β_2 there exists an integer β^* such that

$$\underbrace{\langle P_1 + \beta_1 Q_1, P_2 + \beta_2 Q_2 \rangle}_{\text{Bob does this in eSIDH}} = \underbrace{\langle P_1 + P_2 + \beta(Q_1 + Q_2) \rangle}_{\text{Bob could do this instead}}$$

Righthand side needs a *single* strategy of size $e_{B,1} + e_{B,2}$, where different edges use different primes ($\ell_{B,1}$ or $\ell_{B,2}$).

Interestingly: I don't have to do all $\ell_{B,2}$ edges and then all $\ell_{B,1}$ edges; I can interweave them—**multiprime** strategies.

I don't just need to optimize the strategy, but the **permutation** too.

On the (Permutation, Strategy) Problem

The dream: an algorithm $\vec{\ell} \mapsto (\Sigma, S)$ of minimal cost.

On the (Permutation, Strategy) Problem

The dream: an algorithm $\vec{\ell} \mapsto (\Sigma, S)$ of minimal cost.

The reality: for fixed $\vec{\ell}$,

- Given Σ, we can find the optimal S (dynamic programming *à la* De Feo-Jao-Plût);
- Given S, we can find the optimal Σ (linear programming);
- Stochastic search yields (Σ, S) which improves upon the state-of-the-art.

Optimizing the Permutation

Let the cost model be $(\vec{\mu}, \vec{\iota})$ (for multiplication and isogeny evaluation, respectively).

Optimizing the Permutation

Let the cost model be $(\vec{\mu}, \vec{\iota})$ (for multiplication and isogeny evaluation, respectively).

We construct a matrix $C_{S,\vec{\mu},\vec{\iota}}$ such that $\left\langle C_{S,\vec{\mu},\vec{\iota}}, \Sigma \right\rangle_F$ is the cost of the algorithm.

Optimizing the Permutation

Let the cost model be $(\vec{\mu}, \vec{\iota})$ (for multiplication and isogeny evaluation, respectively).

We construct a matrix $C_{S,\vec{\mu},\vec{\iota}}$ such that $\left\langle C_{S,\vec{\mu},\vec{\iota}}, \Sigma \right\rangle_F$ is the cost of the algorithm.

Thus we get the program

$$\begin{array}{rc} \text{Minimize} & \langle C_{S,\vec{\mu},\vec{\iota}}, \Sigma \rangle_F \\ \text{Subject to} & \Sigma \mathbb{1} = \mathbb{1} \\ & \mathbb{1}^T \Sigma = \mathbb{1}^T \\ & \Sigma \geqslant 0 \\ & \Sigma \in \mathbb{Z}^{n \times n} \end{array}$$

Optimizing the Permutation

Let the cost model be $(\vec{\mu}, \vec{\iota})$ (for multiplication and isogeny evaluation, respectively).

We construct a matrix $C_{S,\vec{\mu},\vec{\iota}}$ such that $\left\langle C_{S,\vec{\mu},\vec{\iota}}, \Sigma \right\rangle_F$ is the cost of the algorithm.

Thus we get the program

$$\begin{array}{rc} \text{Minimize} & \langle C_{S,\vec{\mu},\vec{\iota}}, \Sigma \rangle_F \\ \text{Subject to} & \Sigma \mathbb{1} = \mathbb{1} \\ & \mathbb{1}^T \Sigma = \mathbb{1}^T \\ & \Sigma \geqslant 0 \\ & \Sigma \in \mathbb{Z}^{n \times n} \end{array}$$

We can drop $\Sigma \in \mathbb{Z}^{n \times n}$ because the feasible polytope is integral. Then solve an LP for Σ.

eSIDH Timing Estimates

Scheme	Operation	Timings (Mcycles)		Improvement
		Split Prime	Multiprime	
$p_{443} = 2^{222}3^{73}5^{45} - 1$				
eSIDH	Bob R1	7.44	7.75	-4.03%
	Bob R2	**7.00**	**6.47**	**8.24%**
eSIKE	Keygen	7.43	7.74	-4.01%
	Decap	**13.71**	**13.17**	**4.10%**
$p_{765} = 2^{391}3^{119}5^{81} - 1$				
eSIDH	Bob R1	27.14	28.37	-4.34%
	Bob R2	**25.56**	**23.90**	**6.96%**
eSIKE	Keygen	27.14	28.39	-4.42%
	Decap	**50.47**	**48.83**	**3.36%**

Table: eSIDH/eSIKE timing results on Intel i7-8650u processor.