CSIDH: An Efficient Post-Quantum Commutative Group Action

Wouter Castryck\textsuperscript{1} Tanja Lange\textsuperscript{2} Chloe Martindale\textsuperscript{2} Lorenz Panny\textsuperscript{2} Joost Renes\textsuperscript{3}

\textsuperscript{1}KU Leuven \textsuperscript{2}TU Eindhoven \textsuperscript{3}Radboud Universiteit

Brisbane, 6 December 2018
Why CSIDH?

► Drop-in post-quantum replacement for (EC)DH.
Why CSIDH?

- Drop-in post-quantum replacement for (EC)DH.
- Non-interactive key exchange (full public-key validation); previously only slow solutions post-quantumly.
Why CSIDH?

- Drop-in post-quantum replacement for (EC)DH.
- Non-interactive key exchange (full public-key validation); previously only slow solutions post-quantumly.
- Small keys: 64 bytes at conjectured AES-128 security level.

https://csidh.isogeny.org
Why CSIDH?

- Drop-in post-quantum replacement for (EC)DH.
- Non-interactive key exchange (full public-key validation); previously only slow solutions post-quantumly.
- Small keys: 64 bytes at conjectured AES-128 security level
- Competitive speed: \(\sim 35\text{ ms} \) per operation. (Skylake i5 w/ TurboBoost)

https://csidh.isogeny.org
Why CSIDH?

▶ Drop-in post-quantum replacement for (EC)DH.
▶ Non-interactive key exchange (full public-key validation); previously only slow solutions post-quantumly.
▶ Small keys: 64 bytes at conjectured AES-128 security level
▶ Competitive speed: $\sim 35\text{ ms} \text{ per operation.}$ (Skylake i5 w/ TurboBoost)

▶ Clean mathematical structure: a true group action. (No noise, no auxiliary points, no compromises.)
Why CSIDH?

- Drop-in post-quantum replacement for (EC)DH.
- Non-interactive key exchange (full public-key validation); previously only slow solutions post-quantumly.

- Small keys: 64 bytes at conjectured AES-128 security level
- Competitive speed: $\sim 35\text{ ms}$ per operation. (Skylake i5 w/ TurboBoost)

- Clean mathematical structure: a true group action. (No noise, no auxiliary points, no compromises.)

- By the way: not ‘better’ or ‘worse’ than SIDH. It’s simply different and likely to be useful for different applications.
Ordinary isogeny graphs

Nodes: Ordinary elliptic curves defined over $k$ up to $\cong_k$.
Edges: 3-, 5-, and 7-isogenies defined over $k$ up to $\cong_k$.

Components look something like this:
Ordinary isogeny graphs (cycles)

Nodes: Ordinary elliptic curves defined over \( k \) up to \( \cong_k \).
Edges: \( 3-, 5-, \) and \( 7- \)-isogenies defined over \( k \) up to \( \cong_k \).
Ordinary isogeny graphs (cycles)

Nodes: Ordinary elliptic curves defined over $k$ up to $\cong_k$.
Edges: 3-, 5-, and 7-isogenies defined over $k$ up to $\cong_k$.

Easy: Compute a random path, output the final node.
Hard problem: Find a path between two given nodes.
Intuition: Combining edges from different cycles allows taking shortcuts to remote parts of the graph!
**Intuition**: Combining edges from different cycles allows taking shortcuts to remote parts of the graph!

cf. **Square-&-Multiply**: Alice gets an advantage over Eve.
De Feo–Kieffer–Smith want an ordinary curve $E/ \mathbb{F}_q$ with many small primes $\ell \mid E(\mathbb{F}_q)$.

This seems difficult.
I've been experimenting with supersingular curves in this context, because they have all the properties Kieffer was looking for. Are there any security issues with using supersingular curves? Hope I did not overlook anything stupid here!

— an anonymous CSIDH coauthor

A crypto conference is never complete without ______.
A crypto conference is never complete without _______.

Citing personal communication.

Pictures: https://github.com/CardsAgainstCryptography
I’ve been experimenting with supersingular curves in this context, because they have all the properties Kieffer was looking for.
Are there any security issues with using supersingular curves?
Hope I did not overlook anything stupid here!

— an anonymous CSIDH coauthor
I’ve been experimenting with supersingular curves in this context, because they have all the properties Kieffer was looking for. Are there any security issues with using supersingular curves? Hope I did not overlook anything stupid here! — an anonymous CSIDH coauthor

Wouter, you are a genius! — me
Supersingular isogeny graphs

Nodes: Supersingular elliptic curves defined over $k$ up to $\cong_k$.
Edges: 3-, 5-, and 7-isogenies defined over $k$ up to $\cong_k$. 

https://csidh.isogeny.org
Supersingular isogeny graphs

Nodes: Supersingular elliptic curves defined over $k$ up to $\cong_k$.
Edges: 3-, 5-, and 7-isogenies defined over $k$ up to $\cong_k$.

$k = \mathbb{F}_{419^2}$ (same as $\overline{\mathbb{F}}_{419}$)

https://csidh.isogeny.org
Supersingular isogeny graphs

Nodes: Supersingular elliptic curves defined over $k$ up to $\cong_k$.
Edges: 3-, 5-, and 7-isogenies defined over $k$ up to $\cong_k$.

$k = \mathbb{F}_{419^2}$ (same as $\mathbb{F}_{419}$)

$k = \mathbb{F}_{419}$
Supersingular isogeny graphs

**Theorem.** The $\mathbb{F}_p$-rational endomorphism ring of an elliptic curve defined over $\mathbb{F}_p$ is an imaginary quadratic order.
Supersingular isogeny graphs

**Theorem.** The $\mathbb{F}_p$-rational endomorphism ring of an elliptic curve defined over $\mathbb{F}_p$ is an **imaginary quadratic order**.

...even in the supersingular case!
Supersingular isogeny graphs

**Theorem.** The $\mathbb{F}_p$-rational endomorphism ring of an elliptic curve defined over $\mathbb{F}_p$ is an **imaginary quadratic order**.

...even in the supersingular case!

**Theorem/fact/definition.** Let $p > 3$. An elliptic curve $E$ over $\mathbb{F}_p$ is **supersingular** if and only if $\#E(\mathbb{F}_p) = p + 1$. 

https://csidh.isogeny.org
Supersingular isogeny graphs

Theorem. The $\mathbb{F}_p$-rational endomorphism ring of an elliptic curve defined over $\mathbb{F}_p$ is an imaginary quadratic order.

...even in the supersingular case!

Theorem/fact/definition. Let $p > 3$. An elliptic curve $E$ over $\mathbb{F}_p$ is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$.

$\implies$ We can simply craft a curve with a good number of points.
The class group action is defined as follows:

- **Inputs:**
  An elliptic curve $E$ with $\mathbb{F}_q$-endomorphism ring $\mathcal{O}$, an ideal $a \subseteq \mathcal{O}$ of prime norm $\ell$.

- **Output:**
  The elliptic curve $[a]E$.

1. Compute the subgroup $E[a] = \bigcap_{\alpha \in a} \ker \alpha$ killed by $a$.
2. Compute an $\ell$-isogeny $E \longrightarrow E'$ with kernel $E[a]$.
3. Output $E'$. 

Typically $E[a]$ is only defined over $\mathbb{F}_q^m$ for $m \approx \ell$.

Complexity of computing with $E[a]$ is exponential.
The class group action is defined as follows:

- **Inputs:**
  An elliptic curve $E$ with $\mathbb{F}_q$-endomorphism ring $\mathcal{O}$, an ideal $a \subseteq \mathcal{O}$ of prime norm $\ell$.

- **Output:**
  The elliptic curve $[a]E$.

1. Compute the subgroup $E[a] = \bigcap_{\alpha \in a} \ker \alpha$ killed by $a$.
2. Compute an $\ell$-isogeny $E \rightarrow E'$ with kernel $E[a]$.
3. Output $E'$.

Typically $E[a]$ is only defined over $\mathbb{F}_{q^m}$ for $m \approx \ell$.

⇒ **Complexity** of computing with $E[a]$ is exponential... 😥
1. Choose some small odd primes $\ell_1, \ldots, \ell_n$.
2. Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
3. Let $X = \{\text{supersingular } y^2 = x^3 + Ax^2 + x \text{ defined over } \mathbb{F}_p\}$.
4. All curves in $X$ have $\mathbb{F}_p$-endomorphism ring $O = \mathbb{Z}[\sqrt{-p}]$.
5. Define the ideals $\mathfrak{l}_i = (\ell_i, \pi - 1)$ of $O$.
6. Let $K = \{[\mathfrak{l}_1 \cdots \mathfrak{l}_n] | (e_1, \ldots, e_n) \text{ is 'short'}\} \subseteq \text{cl}(O)$.
7. magic math happens!
8. $\text{cl}(O)$ acts on $X$ and the action of $K$ is very efficient!
CSIDH in one cslide (terrible pun totally intended)

1. ▶ Choose some small odd primes \( \ell_1, \ldots, \ell_n \).
   ▶ Make sure \( p = 4 \cdot \ell_1 \cdots \ell_n - 1 \) is prime.
   ▶ Let \( X = \{ \text{supersingular } y^2 = x^3 + Ax^2 + x \text{ defined over } \mathbb{F}_p \} \).
CSIDH in one cslide (terrible pun totally intended)

1. ▶ Choose some small odd primes $\ell_1, \ldots, \ell_n$.
   ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
   ▶ Let $X = \{\text{supersingular } y^2 = x^3 + Ax^2 + x \text{ defined over } \mathbb{F}_p\}$.

2. ▶ All curves in $X$ have $\mathbb{F}_p$-endomorphism ring $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.
   Define the ideals $I_i = (\ell_i, \pi - 1)$ of $\mathcal{O}$.
   ▶ Let $K = \{[I_1^{e_1} \cdots I_n^{e_n}] \mid (e_1, \ldots, e_n) \text{ is ‘short’}\} \subseteq \mathrm{cl}(\mathcal{O})$. 

https://csidh.isogeny.org
CSIDH in one cslide (terrible pun totally intended)

1. ▶ Choose some small odd primes \( \ell_1, \ldots, \ell_n \).
   ▶ Make sure \( p = 4 \cdot \ell_1 \cdots \ell_n - 1 \) is prime.
   ▶ Let \( X = \{ \text{supersingular } y^2 = x^3 + Ax^2 + x \text{ defined over } \mathbb{F}_p \} \).

2. ▶ All curves in \( X \) have \( \mathbb{F}_p \)-endomorphism ring \( \mathcal{O} = \mathbb{Z}[\sqrt{-p}] \).
   Define the ideals \( \mathfrak{l}_i = (\ell_i, \pi - 1) \) of \( \mathcal{O} \).
   ▶ Let \( K = \{ [\ell_1^{e_1} \cdots \ell_n^{e_n}] \mid (e_1, \ldots, e_n) \text{ is ‘short’} \} \subseteq \text{cl}(\mathcal{O}) \).

3.  
   ̂ magie math happens!*  

   * see next slides
CSIDH in one cslide (terrible pun totally intended)

1. ▶ Choose some small odd primes \( \ell_1, \ldots, \ell_n \).
   ▶ Make sure \( p = 4 \cdot \ell_1 \cdots \ell_n - 1 \) is prime.
   ▶ Let \( X = \{ \text{supersingular } y^2 = x^3 + Ax^2 + x \text{ defined over } \mathbb{F}_p \} \).

2. ▶ All curves in \( X \) have \( \mathbb{F}_p \)-endomorphism ring \( \mathcal{O} = \mathbb{Z}[\sqrt{-p}] \).
   Define the ideals \( \mathfrak{l}_i = (\ell_i, \pi - 1) \) of \( \mathcal{O} \).
   ▶ Let \( K = \{ [\ell_1^{e_1} \cdots \ell_n^{e_n}] \mid (e_1, \ldots, e_n) \text{ is 'short'} \} \subseteq \text{cl}(\mathcal{O}) \).

3. ✨ magie math happens!*

4. ▶ \( \text{cl}(\mathcal{O}) \) acts on \( X \) and the action of \( K \) is very efficient!

* see next slides
Magic (base field arithmetic)

- All the ideals $\ell_i \mathcal{O}$ split as $\ell_i \cdot \overline{\ell_i}$ where $\ell_i = (\ell_i, \pi - 1)$.

  $\Rightarrow$ We can use all $\ell_i$ we started with (generally: about 1/2).
Magic (base field arithmetic)

- All the ideals $\ell_i \mathcal{O}$ split as $\ell_i \cdot \overline{\ell_i}$ where $\ell_i = (\ell_i, \pi - 1)$. 
  $\implies$ We can use all $\ell_i$ we started with (generally: about $1/2$).

- The subgroup corresponding to $\ell_i$ is $E[\ell_i] = E(\mathbb{F}_p)[\ell_i]$. 
  (Note that $\ker(\pi - 1)$ is just the $\mathbb{F}_p$-rational points!)

https://csidh.isogeny.org
Magic (base field arithmetic)

- All the ideals $\ell_i \mathcal{O}$ split as $\ell_i \cdot \overline{\ell_i}$ where $\ell_i = (\ell_i, \pi - 1)$.
  \[ \implies \text{We can use all } \ell_i \text{ we started with} \quad (\text{generally: about } 1/2). \]

- The subgroup corresponding to $\ell_i$ is $E[\ell_i] = E(\mathbb{F}_p)[\ell_i]$.
  (Note that $\ker(\pi - 1)$ is just the $\mathbb{F}_p$-rational points!)

- The subgroup corresponding to $\overline{\ell_i}$ is
  \[ E[\overline{\ell_i}] = \{ P \in E[\ell_i] \mid \pi(P) = -P \}. \]
All the ideals $\ell_i \mathcal{O}$ split as $\ell_i \cdot \overline{\ell_i}$ where $\ell_i = (\ell_i, \pi - 1)$.

We can use all $\ell_i$ we started with (generally: about 1/2).

The subgroup corresponding to $\ell_i$ is $E[\ell_i] = E(\mathbb{F}_p)[\ell_i]$.

(Note that $\ker(\pi - 1)$ is just the $\mathbb{F}_p$-rational points!)

The subgroup corresponding to $\overline{\ell_i}$ is

$$E[\overline{\ell_i}] = \{ P \in E[\ell_i] \mid \pi(P) = -P \}.$$  

For Montgomery curves,

$$E[\overline{\ell_i}] = \{(x, y) \in E[\ell_i] \mid x \in \mathbb{F}_p; y \notin \mathbb{F}_p \} \cup \{\infty\}.$$
All the ideals $\ell_i\mathcal{O}$ split as $\ell_i \cdot \overline{\ell_i}$ where $\ell_i = (\ell_i, \pi - 1)$.

$\implies$ We can use all $\ell_i$ we started with (generally: about 1/2).

The subgroup corresponding to $\ell_i$ is $E[\ell_i] = E(\mathbb{F}_p)[\ell_i]$.

(Note that $\ker(\pi - 1)$ is just the $\mathbb{F}_p$-rational points!)

The subgroup corresponding to $\overline{\ell_i}$ is

$$E[\overline{\ell_i}] = \{ P \in E[\ell_i] \mid \pi(P) = -P \}.$$ 

For Montgomery curves,

$$E[\overline{\ell_i}] = \{ (x, y) \in E[\ell_i] \mid x \in \mathbb{F}_p; y \notin \mathbb{F}_p \} \cup \{ \infty \}.$$ 

$\implies$ With $x$-only arithmetic everything can be done over $\mathbb{F}_p$. 

https://csidh.isogeny.org
Magic (public keys)

**Theorem.** For $p > 3$ and $p \equiv 3 \pmod{8}$, a supersingular elliptic curve over $\mathbb{F}_p$ can be written in the form

$$E_A : y^2 = x^3 + Ax^2 + x$$

if and only if the $\mathbb{F}_p$-rational endomorphism ring of $E$ is $\mathbb{Z}[\sqrt{-p}]$. Moreover, in that case, $A \in \mathbb{F}_p$ is unique.
Theorem. For $p > 3$ and $p \equiv 3 \pmod{8}$, a supersingular elliptic curve over $\mathbb{F}_p$ can be written in the form

$$E_A : y^2 = x^3 + Ax^2 + x$$

if and only if the $\mathbb{F}_p$-rational endomorphism ring of $E$ is $\mathbb{Z}[\sqrt{-p}]$. Moreover, in that case, $A \in \mathbb{F}_p$ is unique.

- Public keys are represented by a single coefficient $A \in \mathbb{F}_p$.
  Tiny keys.
Theorem. For $p > 3$ and $p \equiv 3 \pmod{8}$, a supersingular elliptic curve over $\mathbb{F}_p$ can be written in the form

$$E_A : y^2 = x^3 + Ax^2 + x$$

if and only if the $\mathbb{F}_p$-rational endomorphism ring of $E$ is $\mathbb{Z}[\sqrt{-p}]$. Moreover, in that case, $A \in \mathbb{F}_p$ is unique.

- Public keys are represented by a single coefficient $A \in \mathbb{F}_p$. Tiny keys.
- Public-key validation:
  Check that $E_A$ is supersingular, i.e., has $p + 1$ points.
  Easy Monte-Carlo algorithm: Pick random $P$ on $E_A$ and check $[p+1]P = \infty$.
  This algorithm has a negligible chance $8/\sqrt{p} + o(1)$ of false positives.
  We actually use a variant that proves that $E_A$ has $p + 1$ points.
**Magic (public keys)**

**Theorem.** For $p > 3$ and $p \equiv 3 \pmod{8}$, a supersingular elliptic curve over $\mathbb{F}_p$ can be written in the form

$$E_A : y^2 = x^3 + Ax^2 + x$$

if and only if the $\mathbb{F}_p$-rational endomorphism ring of $E$ is $\mathbb{Z}[\sqrt{-p}]$. Moreover, in that case, $A \in \mathbb{F}_p$ is unique.

- Public keys are represented by a single coefficient $A \in \mathbb{F}_p$.
  - Tiny keys.

- Public-key validation:
  - Check that $E_A$ is supersingular, i.e., has $p + 1$ points.
    - Easy Monte-Carlo algorithm: Pick random $P$ on $E_A$ and check $[p+1]P = \infty$.
    - This algorithm has a negligible chance $8/\sqrt{p} + o(1)$ of false positives.
    - We actually use a variant that proves that $E_A$ has $p + 1$ points.

- About $\sqrt{p}$ of all $A \in \mathbb{F}_p$ are valid keys.
Security

Classical:

- **Meet-in-the-middle variants**: Time $O\left(\sqrt[4]{p}\right)$. [Delfs–Galbraith]
Security

Classical:
- Meet-in-the-middle variants: Time $O(4\sqrt{p})$. [Delfs–Galbraith]

Quantum:
- Hidden-shift algorithms: Subexponential complexity.
Security

Classical:
- **Meet-in-the-middle** variants: Time $O\left(\sqrt[4]{p}\right)$. [Delfs–Galbraith]

Quantum:
- **Hidden-shift** algorithms: **Subexponential** complexity.
  - Literature contains mostly asymptotics.
  - **Time-space trade-off**: Fastest variants need huge memory.
  - [BS] ignores much of the cost. **No need to panic!**
CSIDH-512

Sizes:
- Private keys: 32 bytes.
- Public keys: 64 bytes.
CSIDH-512

Sizes:

- **Private keys**: 32 bytes.
- **Public keys**: 64 bytes.

Performance:

- **Wall-clock time**: 35 ms per operation.
- **Clock cycles** (Skylake): about $10^8$ per operation.
- **Memory usage** (x86_64): about 4 kilobytes.
CSIDH-512

Sizes:

- Private keys: 32 bytes.
- Public keys: 64 bytes.

Performance:

- Wall-clock time: 35 ms per operation.
- Clock cycles (Skylake): about $10^8$ per operation.
- Memory usage (x86_64): about 4 kilobytes.

Security:

- Classical: at least 128 bits.
CSIDH-512

Sizes:

- **Private keys**: 32 bytes.
- **Public keys**: 64 bytes.

Performance:

- **Wall-clock time**: 35 ms per operation.
- **Clock cycles** (Skylake): about $10^8$ per operation.
- **Memory usage** (x86_64): about 4 kilobytes.

Security:

- **Classical**: at least 128 bits.
- **Quantum**: complicated. AFAWK it reaches NIST level 1.
  
  [BS] says $2^{32.5}$ queries; [BLMP] estimates $\approx 2^{81}$ quantum gates using millions of qubits.
Work in progress & future work

- Fast and constant-time implementation
  (Quick ‘n’ slightly dirty version based on [BLMP] is ≈ 6 times slower.)
Work in progress & future work

- **Fast and constant-time implementation**
  (Quick ‘n’ slightly dirty version based on [BLMP] is $\approx 6$ times slower.)

- More **security** analysis
Work in progress & future work

- **Fast** and **constant-time** implementation
  (Quick ‘n’ slightly dirty version based on [BLMP] is \( \approx 6 \) times slower.)

- More **security** analysis

- More **applications**
Work in progress & future work

- **Fast** and **constant-time** implementation
  (Quick ‘n’ slightly dirty version based on [BLMP] is \(\approx 6\) times slower.)

- More **security** analysis

- More **applications**

- [Your paper here!]
SIDH vs. CSIDH

CSIDH = SIDH?
SIDH vs. CSIDH

\[ \text{CSIDH} = \text{SIDH} + \text{C} \]
SIDH vs. CSIDH

Sizes and times are for (conjectured) NIST level 1. SIDH parameters are more conservative.

<table>
<thead>
<tr>
<th></th>
<th>SIDH</th>
<th>CSIDH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time per key exchange</td>
<td>≈ 10 ms</td>
<td>≈ 70 ms</td>
</tr>
<tr>
<td>Public keys</td>
<td>378 b</td>
<td>64 b</td>
</tr>
<tr>
<td>Public key compression</td>
<td>222 b (∼ 15 ms)</td>
<td>n/a</td>
</tr>
<tr>
<td>Constant-time slowdown</td>
<td>≈ 1</td>
<td>≈ 6 (quick ‘n’ dirty)</td>
</tr>
<tr>
<td>In the NIST not-a-competition</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Maturity</td>
<td>7 years</td>
<td>7 months</td>
</tr>
<tr>
<td>Classical security</td>
<td>$p^{1/4}$</td>
<td>$p^{1/4}$</td>
</tr>
<tr>
<td>Quantum security</td>
<td>$p^{1/6}$</td>
<td>$L_p[1/2]$</td>
</tr>
<tr>
<td>Key size scaling</td>
<td>linear</td>
<td>quadratic</td>
</tr>
<tr>
<td>Chosen-ciphertext security (KEM)</td>
<td>generic transform</td>
<td>built-in</td>
</tr>
<tr>
<td>Non-interactive key exchange</td>
<td>slow</td>
<td>built-in</td>
</tr>
<tr>
<td>Signatures (now)</td>
<td>seconds</td>
<td>snail speed</td>
</tr>
<tr>
<td>Signatures (future?)</td>
<td>still seconds?</td>
<td>seconds</td>
</tr>
</tbody>
</table>

(slide mostly stolen from Chloe Martindale, who mostly stole it from Luca De Feo)