



CSIDH: An Efficient Post-Quantum Commutative Group Action

Wouter Castryck¹ Tanja Lange² Chloe Martindale²
Lorenz Panny² Joost Renes³

¹KU Leuven ²TU Eindhoven ³Radboud Universiteit

Brisbane, 6 December 2018

A tropical sunset scene with palm trees and the ocean. The sun is low on the horizon, casting a golden glow over the water and silhouetting the palm trees. A white box with a black border contains the phonetic transcription ['siː,saɪd].

['siː,saɪd]

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

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**: ~ 35 ms per operation. (Skylake i5 w/ TurboBoost)

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 ms** per operation. (Skylake i5 w/ TurboBoost)
- ▶ **Clean** mathematical structure: a true **group action**.
(No noise, no auxiliary points, no compromises.)

Why CSIDH?

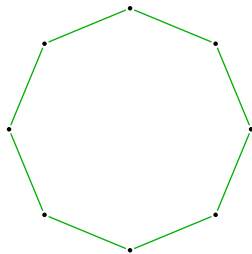
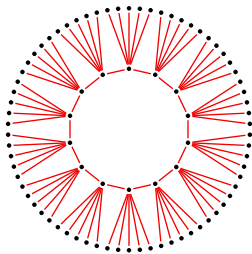
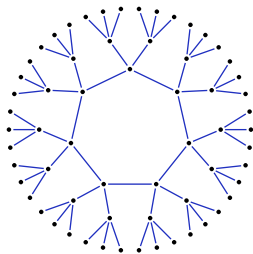
- ▶ Drop-in **post-quantum replacement** for (EC)DH.
- ▶ **Non-interactive key exchange** (full **public-key validation**); previously only slow solutions post-quantumly.
- ▶ **Small keys**: **64 bytes** at conjectured AES-128 security level
- ▶ Competitive **speed**: ~ 35 ms per operation. (Skylake 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 .

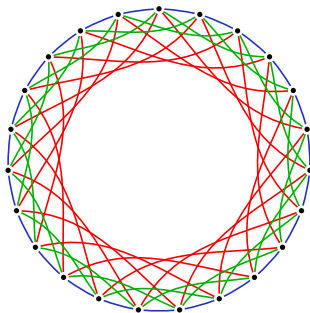
Components look something like this:



Ordinary isogeny graphs (cycles)

Nodes: Ordinary elliptic curves defined over k up to \cong_k .

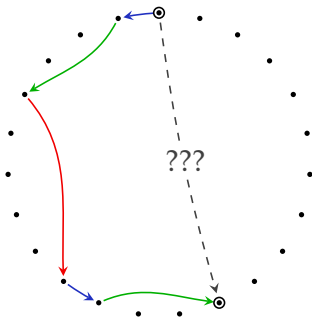
Edges: 3-, 5-, and 7-isogenies defined over k up to \cong_k .



Ordinary isogeny graphs (cycles)

Nodes: Ordinary elliptic curves defined over k up to \cong_k .

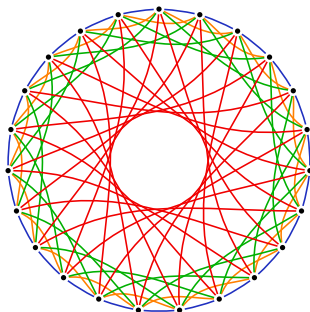
Edges: 3-, 5-, and 7-isogenies defined over k up to \cong_k .



Easy: Compute a random path, output the final node.

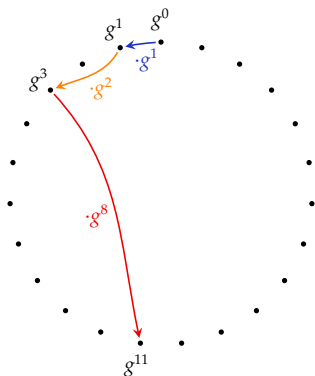
Hard problem: Find a path between two given nodes.

Alice vs. Eve



Intuition: Combining edges from **different cycles** allows taking **shortcuts** to remote parts of the graph!

Alice vs. Eve



Intuition: Combining edges from **different cycles** allows taking **shortcuts** to remote parts of the graph!

cf. **Square-&-Multiply**: Alice gets an advantage over Eve.

Point counting

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**.

**A crypto conference is
never complete without**

_____.



**A crypto conference is
never complete without**

_____.



**Citing personal
communication.**



Pictures: <https://github.com/CardsAgainstCryptography>

**A crypto conference is
never complete without**

**Citing personal
communication.**

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



Pictures: <https://github.com/CardsAgainstCryptography>

**A crypto conference is
never complete without**

**Citing personal
communication.**

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



Pictures: <https://github.com/CardsAgainstCryptography>

Supersingular isogeny graphs

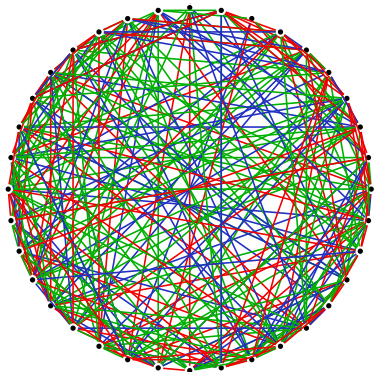
Nodes: Supersingular elliptic curves defined over k up to \cong_k .

Edges: 3-, 5-, and 7-isogenies defined over k up to \cong_k .

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 .

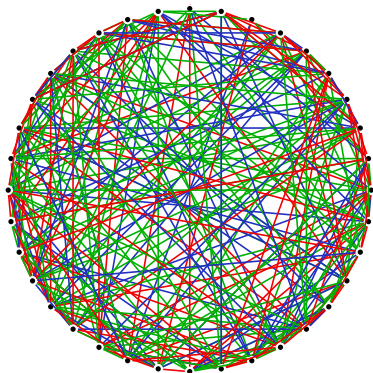


$$k = \mathbb{F}_{419^2} \text{ (same as } \overline{\mathbb{F}}_{419}\text{)}$$

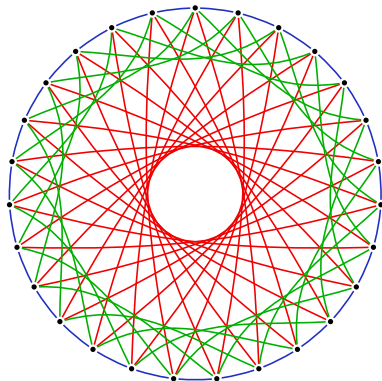
Supersingular isogeny graphs

Nodes: Supersingular elliptic curves defined over k up to \cong_k .

Edges: 3-, 5-, and 7-isogenies defined over k up to \cong_k .



$$k = \mathbb{F}_{4192} \text{ (same as } \overline{\mathbb{F}}_{419}\text{)}$$



$$k = \mathbb{F}_{419}$$

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 $\#E(\mathbb{F}_p) = p + 1$.

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**.

Reminder

The class group action is defined as follows:

► **Inputs:**

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

► **Output:**

The elliptic curve $[\mathfrak{a}]E$.

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

Reminder

The class group action is defined as follows:

► **Inputs:**

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

► **Output:**

The elliptic curve $[\mathfrak{a}]E$.

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

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

\implies **Complexity** of computing with $E[\mathfrak{a}]$ is **exponential**... ☹

CSIDH in one cslide (terrible pun totally intended)


CSIDH in one cslide (terrible pun totally intended)

1.
 - ▶ Choose some small odd primes ℓ_1, \dots, ℓ_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 ℓ_1, \dots, ℓ_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 $K = \{[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \mid (e_1, \dots, e_n) \text{ is 'short'}\} \subseteq \text{cl}(\mathcal{O})$.

CSIDH in one cslide (terrible pun totally intended)

- ▶ Choose some small odd primes ℓ_1, \dots, ℓ_n .
 - ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
 - ▶ Let $X = \{\text{supersingular } y^2 = x^3 + Ax^2 + x \text{ defined over } \mathbb{F}_p\}$.
- ▶ 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 $K = \{[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \mid (e_1, \dots, e_n) \text{ is 'short'}\} \subseteq \text{cl}(\mathcal{O})$.
- ▶  magic math happens!*

* see next slides

CSIDH in one cslide (terrible pun totally intended)

- ▶ Choose some small odd primes ℓ_1, \dots, ℓ_n .
 - ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
 - ▶ Let $X = \{\text{supersingular } y^2 = x^3 + Ax^2 + x \text{ defined over } \mathbb{F}_p\}$.
- ▶ 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 $K = \{[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \mid (e_1, \dots, e_n) \text{ is 'short'}\} \subseteq \text{cl}(\mathcal{O})$.
- ▶  magic math happens!*
- ▶ $\text{cl}(\mathcal{O})$ 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 $\mathfrak{l}_i \cdot \overline{\mathfrak{l}}_i$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$.
 \implies We can use all ℓ_i we started with (generally: about 1/2).

Magic (base field arithmetic)

- ▶ All the ideals $\ell_i \mathcal{O}$ split as $\mathfrak{l}_i \cdot \overline{\mathfrak{l}}_i$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$.
 \implies We can use all ℓ_i we started with (generally: about 1/2).
- ▶ The subgroup corresponding to \mathfrak{l}_i is $E[\mathfrak{l}_i] = E(\mathbb{F}_p)[\ell_i]$.
(Note that $\ker(\pi - 1)$ is just the \mathbb{F}_p -rational points!)

Magic (base field arithmetic)

- ▶ All the ideals $\ell_i \mathcal{O}$ split as $\mathfrak{l}_i \cdot \overline{\mathfrak{l}}_i$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$.
 \implies We can use all ℓ_i we started with (generally: about 1/2).
- ▶ The subgroup corresponding to \mathfrak{l}_i is $E[\mathfrak{l}_i] = E(\mathbb{F}_p)[\ell_i]$.
(Note that $\ker(\pi - 1)$ is just the \mathbb{F}_p -rational points!)
- ▶ The subgroup corresponding to $\overline{\mathfrak{l}}_i$ is

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

Magic (base field arithmetic)

- ▶ All the ideals $\ell_i \mathcal{O}$ split as $\mathfrak{l}_i \cdot \bar{\mathfrak{l}}_i$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$.
 \implies We can use all ℓ_i we started with (generally: about 1/2).
- ▶ The subgroup corresponding to \mathfrak{l}_i is $E[\mathfrak{l}_i] = E(\mathbb{F}_p)[\ell_i]$.
(Note that $\ker(\pi - 1)$ is just the \mathbb{F}_p -rational points!)
- ▶ The subgroup corresponding to $\bar{\mathfrak{l}}_i$ is

$$E[\bar{\mathfrak{l}}_i] = \{P \in E[\ell_i] \mid \pi(P) = -P\}.$$

For Montgomery curves,

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

Magic (base field arithmetic)

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

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

- ▶ The subgroup corresponding to $\bar{\mathfrak{l}}_i$ is

$$E[\bar{\mathfrak{l}}_i] = \{P \in E[\ell_i] \mid \pi(P) = -P\}.$$

For Montgomery curves,

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

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

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.

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 $A \in \mathbb{F}_p$.
 \rightsquigarrow Tiny keys.

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.

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 $A \in \mathbb{F}_p$.
 \rightsquigarrow 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 $O(\sqrt[4]{p})$. [Delfs–Galbraith]

Security

Classical:

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

Quantum:

- ▶ **Hidden-shift** algorithms: **Subexponential** complexity.

Security

Classical:

- ▶ **Meet-in-the-middle** variants: Time $O(\sqrt[4]{p})$. [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 ≈ 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 ≈ 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 ≈ 6 times slower.)
- ▶ More **security** analysis
- ▶ More **applications**
- ▶ [Your paper here!]



Questions?

[CSIDH] <https://ia.cr/2018/383>

[BS] <https://ia.cr/2018/537>

[BLMP] <https://ia.cr/2018/1059>

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.

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

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