Isogeny-based cryptography: why, how, and the latest news

Chloe Martindale

University of Bristol

2nd June 2021

Isogeny-based cryptography: why?

- Based on hard problems believed to (still) be hard for quantum computers

Isogeny-based cryptography: why?

- Based on hard problems believed to (still) be hard for quantum computers
- Low memory requirements
  - Lowest of all post-quantum candidates (by far)
  - Smallest option similar size to classical ECC

Isogeny-based cryptography: why?

- Based on hard problems believed to (still) be hard for quantum computers
- Low memory requirements
  - Lowest of all post-quantum candidates (by far)
  - Smallest option similar size to classical ECC
- Made up of ECC subroutines $\rightsquigarrow$ quite compatible with current small-device implementations

Isogeny-based cryptography: why?

- Based on hard problems believed to (still) be hard for quantum computers
- Low memory requirements
  - Lowest of all post-quantum candidates (by far)
  - Smallest option similar size to classical ECC
- Made up of ECC subroutines $\rightsquigarrow$ quite compatible with current small-device implementations
- Rich mathematical structure $\rightsquigarrow$ most flexible* post-quantum applications.

Isogeny-based cryptography: why?

- Based on hard problems believed to (still) be hard for quantum computers
- Low memory requirements
  - Lowest of all post-quantum candidates (by far)
  - Smallest option similar size to classical ECC
- Made up of ECC subroutines $\rightsquigarrow$ quite compatible with current small-device implementations
- Rich mathematical structure $\rightsquigarrow$ most flexible* post-quantum applications. Since 2018:
  - Only pq non-interactive key exchange (c.f. Diffie-Hellman)
  - Two different signature schemes
  - Oblivious pseudorandom functions
  - Threshold schemes
  - ElGamal-style message encryption
  - ...

Isogeny-based cryptography: why not?

- Newest of all pq schemes $\rightsquigarrow$ less confidence in security.
  - Oldest practical idea “still standing” is from 2011.

Isogeny-based cryptography: why not?

- Newest of all pq schemes $\rightsquigarrow$ less confidence in security.
  - Oldest practical idea “still standing” is from 2011.
- Rich mathematical structure $\rightsquigarrow$ many attack avenues, maybe not all explored.

Isogeny-based cryptography: why not?

- Newest of all pq schemes $\rightsquigarrow$ less confidence in security.
  - Oldest practical idea "still standing" is from 2011.
- Rich mathematical structure $\rightsquigarrow$ many attack avenues, maybe not all explored.
- Lowest memory, most flexible Hard Problem admits a subexponential quantum attack, the complexity of which is still an active research topic.
  - Difficult to make concrete parameter choices.

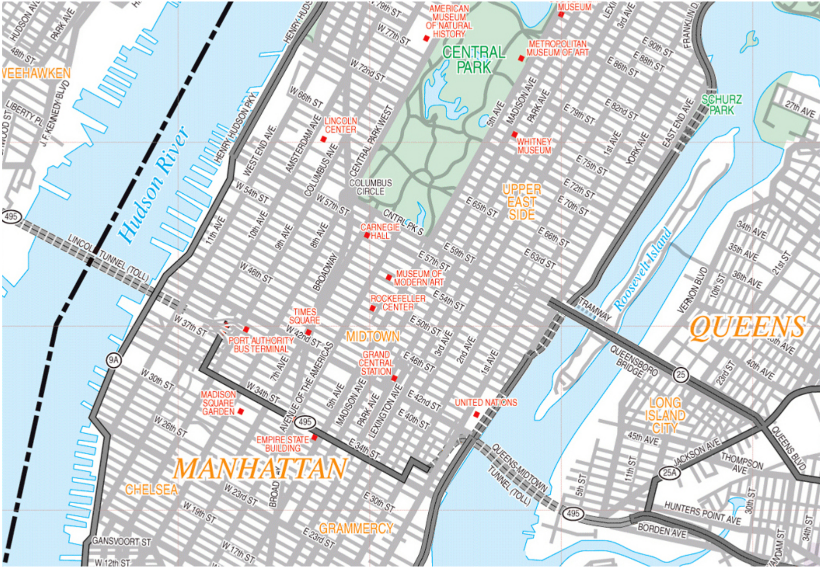
Isogeny-based cryptography: why not?

- Newest of all pq schemes $\rightsquigarrow$ less confidence in security.
  - Oldest practical idea "still standing" is from 2011.
- Rich mathematical structure $\rightsquigarrow$ many attack avenues, maybe not all explored.
- Lowest memory, most flexible Hard Problem admits a subexponential quantum attack, the complexity of which is still an active research topic.
  - Difficult to make concrete parameter choices.
- Slow: Fastest key encapsulation is $\approx \times 25$ slower than ECC or the fastest pq option (lattices).

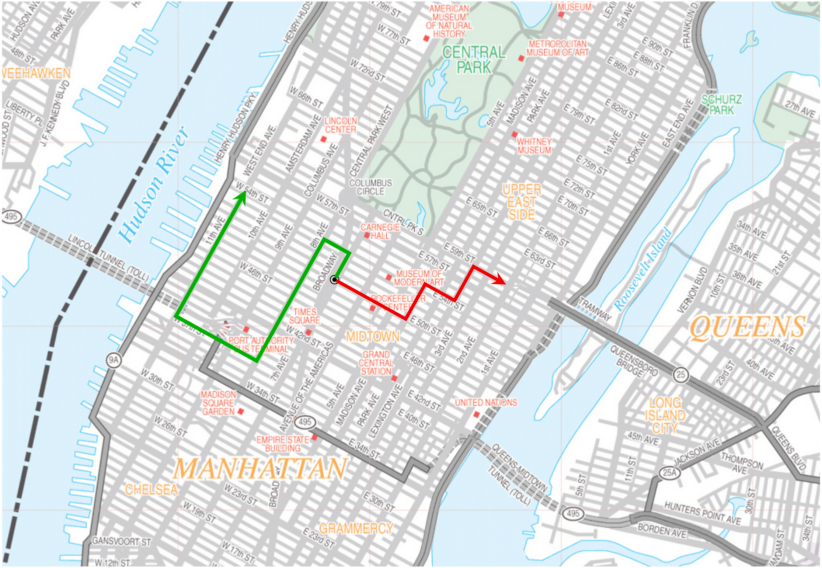
Isogeny-based cryptography: how?

- Hard Problems in isogeny-based cryptography are (mostly) based on elliptic curves.
- On a high level, this can be abstracted away…

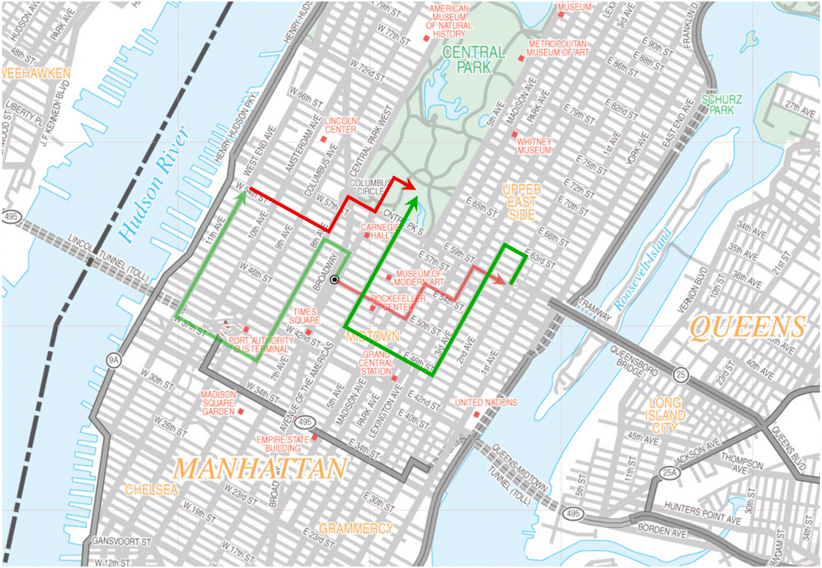
Graph walking Diffie–Hellman?



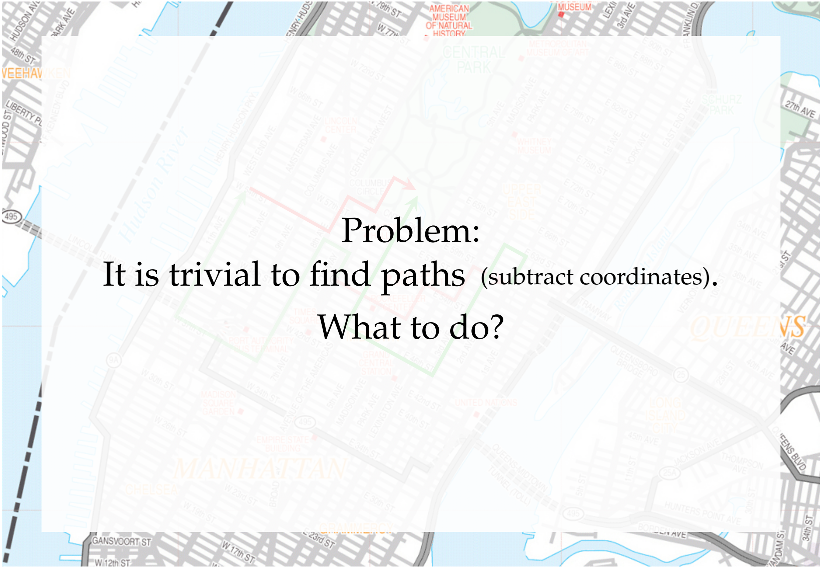
Graph walking Diffie–Hellman?



Graph walking Diffie–Hellman?



Graph walking Diffie–Hellman?



Problem:

It is trivial to find paths (subtract coordinates).

What to do?

Big picture

- Isogenies are a source of exponentially-sized graphs.

Big picture

- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.

Big picture

- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.

Big picture

- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
- No known efficient algorithms to recover paths from endpoints.

Big picture

- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
- No known efficient algorithms to recover paths from endpoints.
- Enough structure to navigate the graph meaningfully.
  That is: some *well-behaved* 'directions' to describe paths. More later.

Big picture

- Isogenies are a source of exponentially-sized graphs.
- We can walk efficiently on these graphs.
- Fast mixing: short paths to (almost) all nodes.
- No known efficient algorithms to recover paths from endpoints.
- Enough structure to navigate the graph meaningfully.
  That is: some *well-behaved* ‘directions’ to describe paths. More later.

It is easy to construct graphs that satisfy *almost* all of these — not enough for crypto!

Ex: CSIDH (Castryck-Lange-M.-Panny-Renes '18)

Traditionally, Diffie-Hellman works in a group G via the map

$$\begin{array}{rcl} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x. \end{array}$$

Ex: CSIDH (Castryck-Lange-M.-Panny-Renes '18)

Traditionally, Diffie-Hellman works in a group G via the map

$$\begin{array}{ccc} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x. \end{array}$$

Shor's algorithm quantumly computes x from g^x in any group in polynomial time.

Ex: CSIDH (Castryck-Lange-M.-Panny-Renes '18)

Traditionally, Diffie-Hellman works in a group G via the map

$$\begin{array}{rcl} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x. \end{array}$$

Shor's algorithm quantumly computes x from g^x in any group in polynomial time.

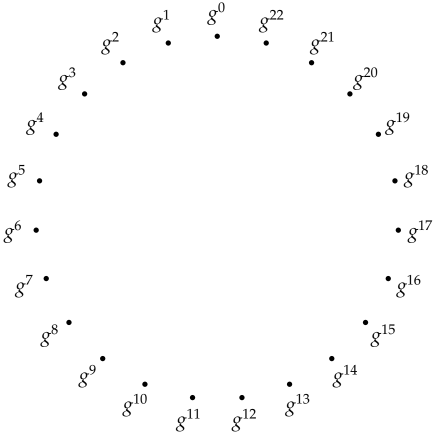
$\rightsquigarrow$ Idea:

Replace exponentiation on the group G by a group action of a group H on a set S:

$$H \times S \to S.$$

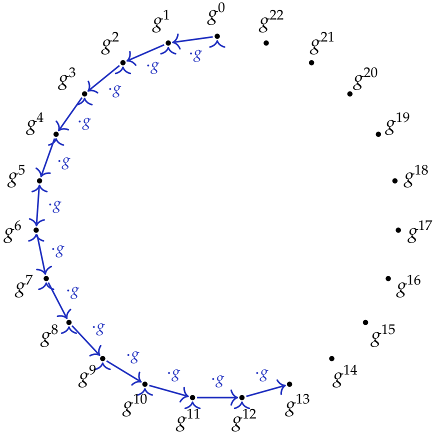
Square-and-multiply

Suppose $G \cong \mathbb{Z}/23$ and that Alice computes g^{13}.



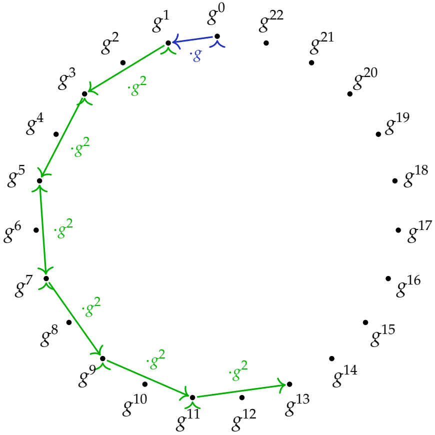
Square-and-multiply

Suppose $G \cong \mathbb{Z}/23$ and that Alice computes g^{13}.



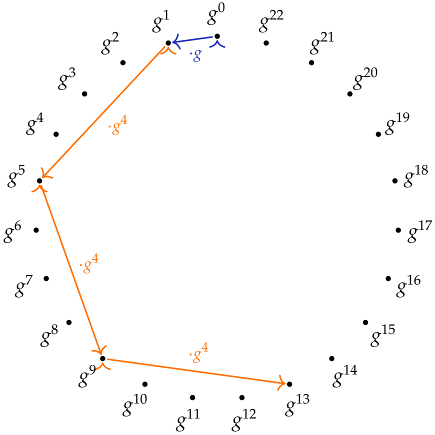
Square-and-multiply

Suppose $G \cong \mathbb{Z}/23$ and that Alice computes g^{13}.



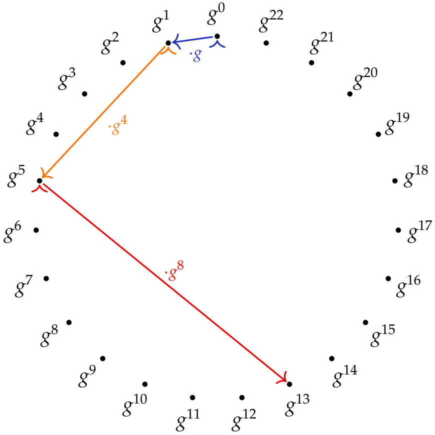
Square-and-multiply

Suppose $G \cong \mathbb{Z}/23$ and that Alice computes g^{13}.

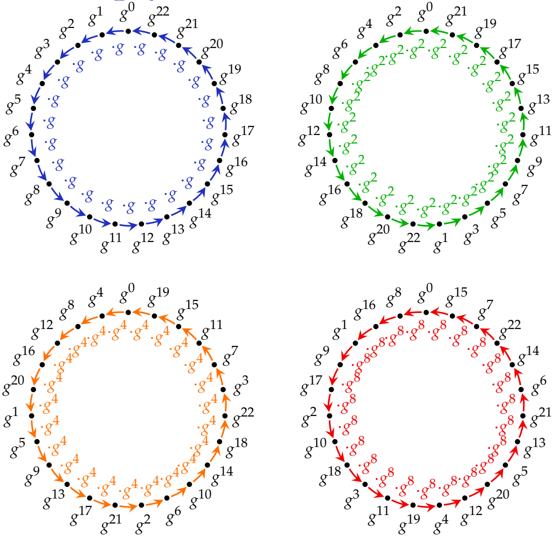


Square-and-multiply

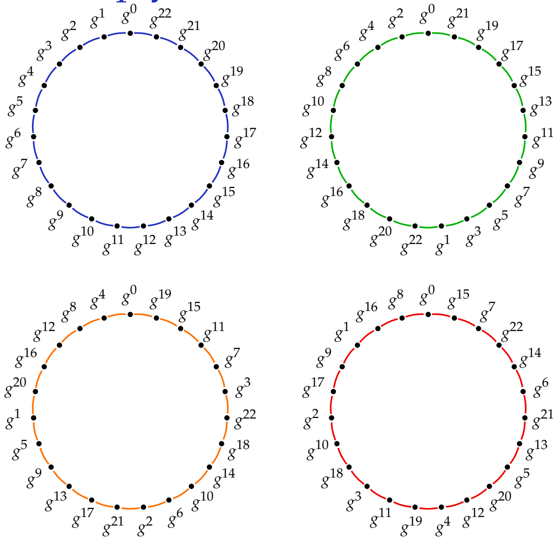
Suppose $G \cong \mathbb{Z}/23$ and that Alice computes g^{13}.



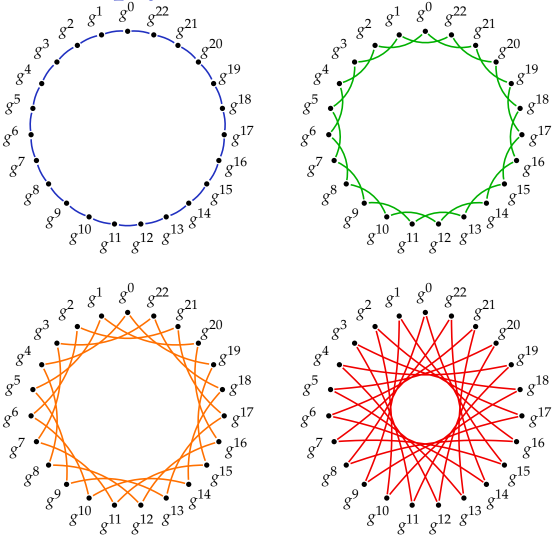
Square-and-multiply



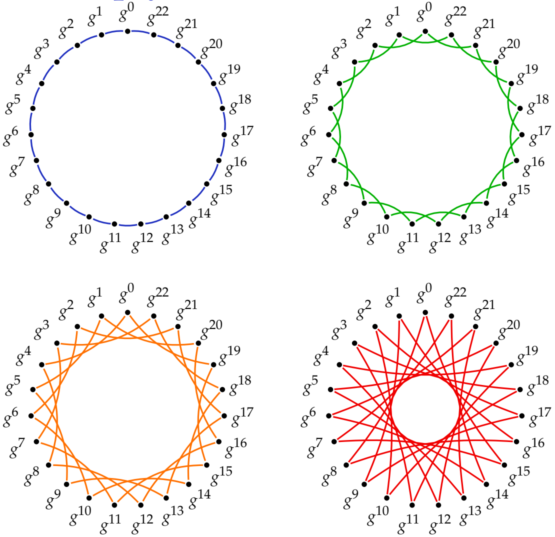
Square-and-multiply



Square-and-multiply

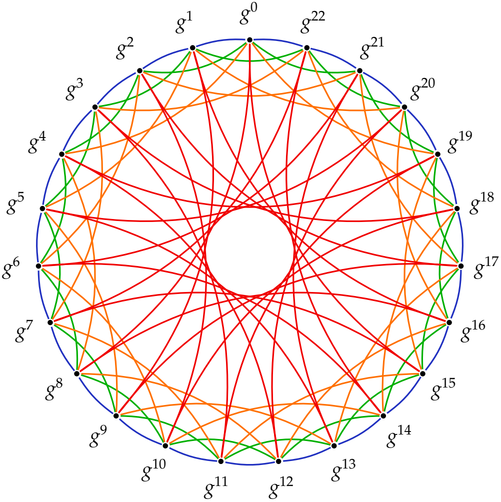


Square-and-multiply

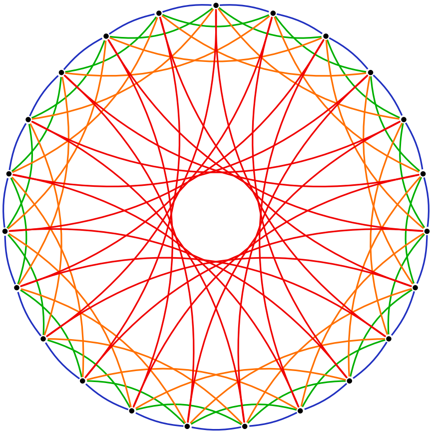


Cycles are compatible: [right, then left] = [left, then right], etc.

Union of cycles: rapid mixing

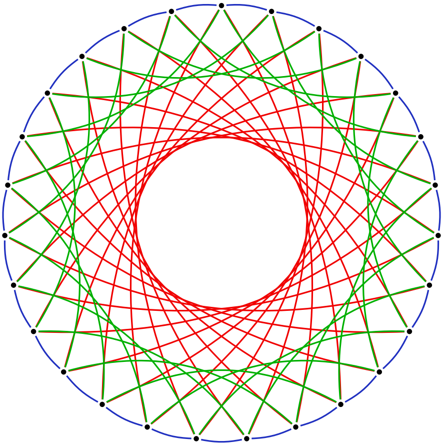


Union of cycles: rapid mixing

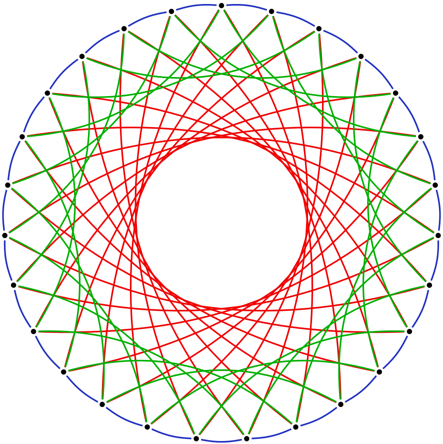


CSIDH: Nodes are now elliptic curves and edges are isogenies.

Graphs of elliptic curves

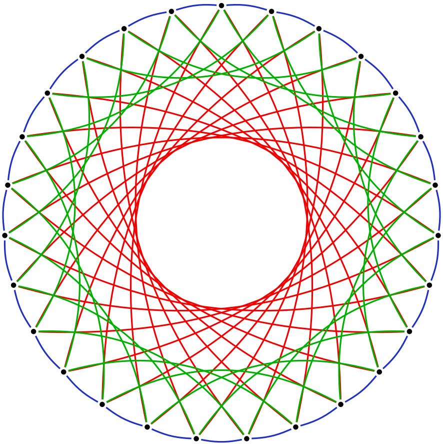


Graphs of elliptic curves



Nodes: Supersingular curves $E_A\colon y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.

Graphs of elliptic curves



Nodes: Supersingular curves $E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.
Edges: 3-, 5-, and 7-isogenies.

Quantumifying Exponentiation

- We want to replace the exponentiation map

$$\begin{array}{rcl} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x \end{array}$$

by a group action on a set.

Quantumifying Exponentiation

- We want to replace the exponentiation map

$$\begin{array}{ccc} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x \end{array}$$

  by a group action on a set.
- Replace G by the set S of supersingular elliptic curves $E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.

Quantumifying Exponentiation

- We want to replace the exponentiation map

$$\begin{array}{ccc} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x \end{array}$$

  by a group action on a set.
- Replace G by the set S of supersingular elliptic curves $E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.
- Replace $\mathbb{Z}$ by a commutative group H.

Quantumifying Exponentiation

- We want to replace the exponentiation map

$$\begin{array}{ccc} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x \end{array}$$

  by a group action on a set.
- Replace G by the set S of supersingular elliptic curves $E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.
- Replace $\mathbb{Z}$ by a commutative group H.
- The action of a well-chosen $\mathfrak{l} \in H$ on S moves the elliptic curves one step around one of the cycles.

$$\begin{array}{ccc} H \times S & \to & S \\ (\mathfrak{l}_3, E) & \mapsto & \mathfrak{l}_3 * E. \end{array}$$

Quantumifying Exponentiation

- We want to replace the exponentiation map

$$\begin{array}{ccc} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x \end{array}$$

  by a group action on a set.
- Replace G by the set S of supersingular elliptic curves $E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.
- Replace $\mathbb{Z}$ by a commutative group H.
- The action of a well-chosen $\mathfrak{l} \in H$ on S moves the elliptic curves one step around one of the cycles.

$$\begin{array}{ccc} H \times S & \to & S \\ (\mathfrak{l}_5, E) & \mapsto & \mathfrak{l}_5 * E. \end{array}$$

Quantumifying Exponentiation

- We want to replace the exponentiation map

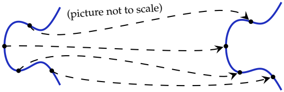
$$\begin{array}{ccc} \mathbb{Z} \times G & \to & G \\ (x, g) & \mapsto & g^x \end{array}$$

  by a group action on a set.
- Replace G by the set S of supersingular elliptic curves $E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.
- Replace $\mathbb{Z}$ by a commutative group H.
- The action of a well-chosen $\mathfrak{l} \in H$ on S moves the elliptic curves one step around one of the cycles.

$$\begin{array}{ccc} H \times S & \to & S \\ (\mathfrak{l}_7, E) & \mapsto & \mathfrak{l}_7 * E. \end{array}$$

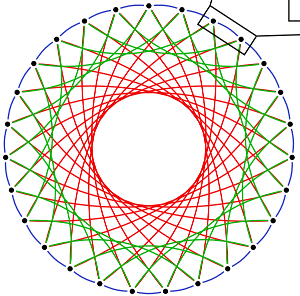
Graphs of elliptic curves

A 3-isogeny



$$E_{51}\colon y^2 = x^3 + 51x^2 + x \longrightarrow E_9\colon y^2 = x^3 + 9x^2 + x$$

$$(x, y) \longmapsto \left(\frac{97x^3 - 183x^2 + x}{x^2 - 183x + 97},\; y \cdot \frac{133x^3 + 154x^2 - 5x + 97}{-x^3 + 65x^2 + 128x - 133} \right)$$



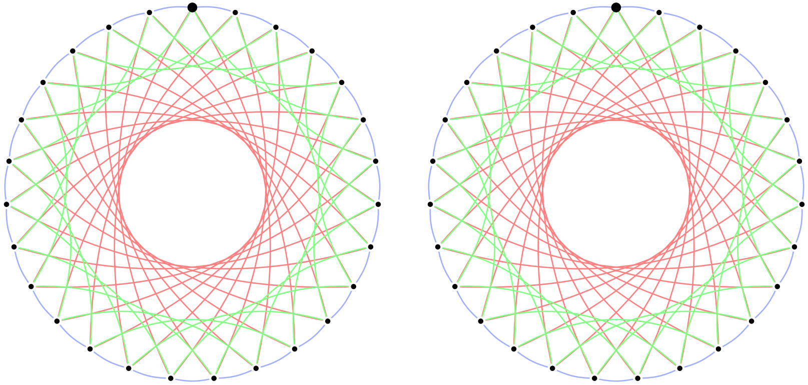
Diffie and Hellman go to the CSIDH

Alice

$[\mathfrak{l}_3, \mathfrak{l}_7{}^{-1}, \mathfrak{l}_3, \mathfrak{l}_5{}^{-1}]$

Bob

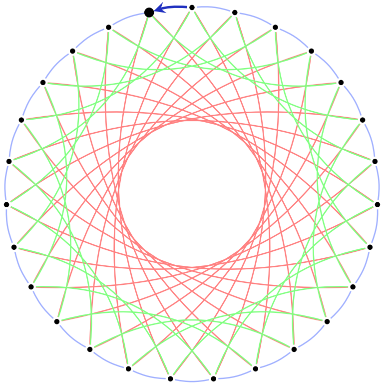
$[\mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3{}^{-1}, \mathfrak{l}_5]$



Diffie and Hellman go to the CSIDH

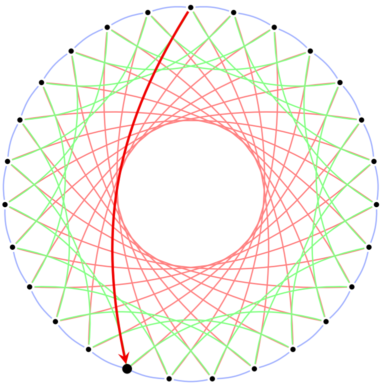
Alice

$[\mathfrak{l}_3, \mathfrak{l}_7^{-1}, \mathfrak{l}_3, \mathfrak{l}_5^{-1}]$
$\uparrow$



Bob

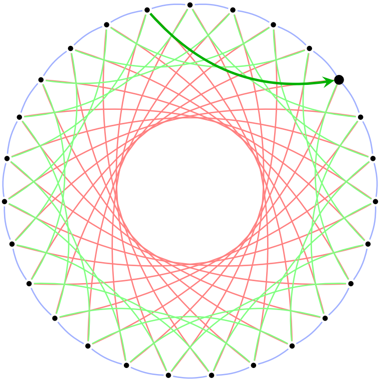
$[\mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3^{-1}, \mathfrak{l}_5]$
$\uparrow$



Diffie and Hellman go to the CSIDH

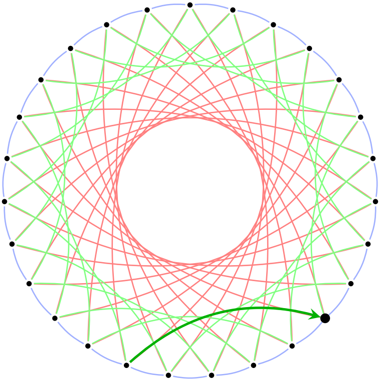
Alice

$[\mathfrak{l}_3, \underset{\uparrow}{\mathfrak{l}_7}^{-1}, \mathfrak{l}_3, \mathfrak{l}_5^{-1}]$



Bob

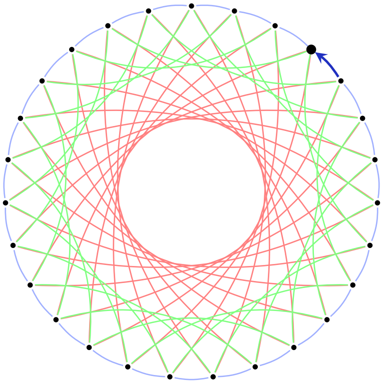
$[\mathfrak{l}_5, \underset{\uparrow}{\mathfrak{l}_7}, \mathfrak{l}_3^{-1}, \mathfrak{l}_5]$



Diffie and Hellman go to the CSIDH

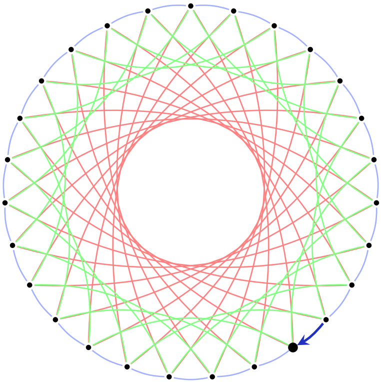
Alice

$$[\mathfrak{l}_3, \mathfrak{l}_7{}^{-1}, \underset{\uparrow}{\mathfrak{l}_3}, \mathfrak{l}_5{}^{-1}]$$



Bob

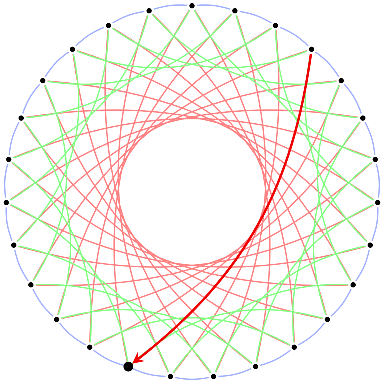
$$[\mathfrak{l}_5, \mathfrak{l}_7, \underset{\uparrow}{\mathfrak{l}_3{}^{-1}}, \mathfrak{l}_5]$$



Diffie and Hellman go to the CSIDH

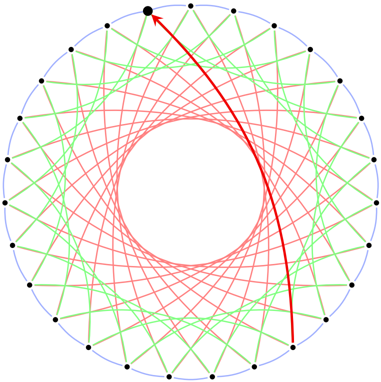
Alice

$[\mathfrak{l}_3, \mathfrak{l}_7{}^{-1}, \mathfrak{l}_3, \underset{\uparrow}{\mathfrak{l}_5{}^{-1}}]$



Bob

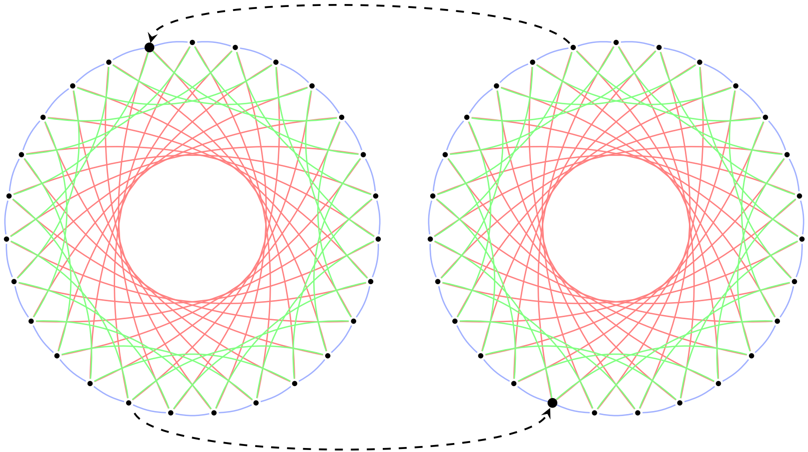
$[\mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3{}^{-1}, \underset{\uparrow}{\mathfrak{l}_5}]$



Diffie and Hellman go to the CSIDH

Alice
$[\mathfrak{l}_3, \mathfrak{l}_7{}^{-1}, \mathfrak{l}_3, \mathfrak{l}_5{}^{-1}]$

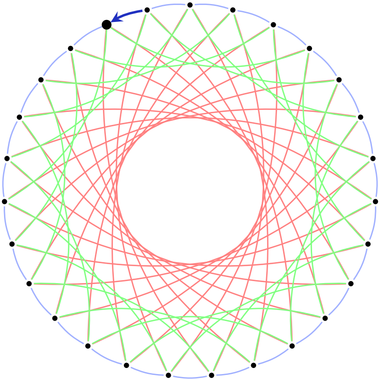
Bob
$[\mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3{}^{-1}, \mathfrak{l}_5]$



Diffie and Hellman go to the CSIDH

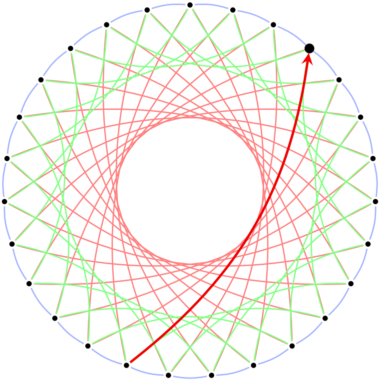
Alice

$[\mathfrak{l}_3, \mathfrak{l}_7{}^{-1}, \mathfrak{l}_3, \mathfrak{l}_5{}^{-1}]$
$\uparrow$



Bob

$[\mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3{}^{-1}, \mathfrak{l}_5]$
$\uparrow$



Diffie and Hellman go to the CSIDH

Alice

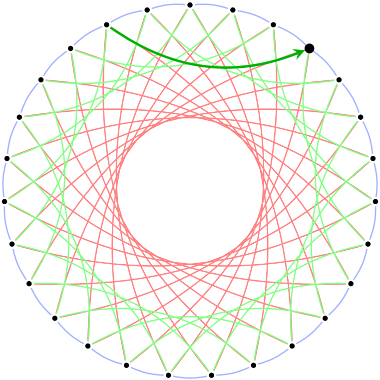
$[\mathfrak{l}_3, \mathfrak{l}_7^{-1}, \mathfrak{l}_3, \mathfrak{l}_5^{-1}]$

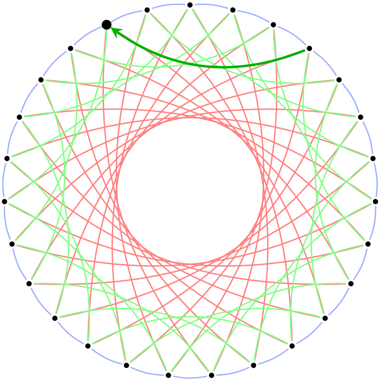
$\uparrow$

Bob

$[\mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3^{-1}, \mathfrak{l}_5]$

$\uparrow$

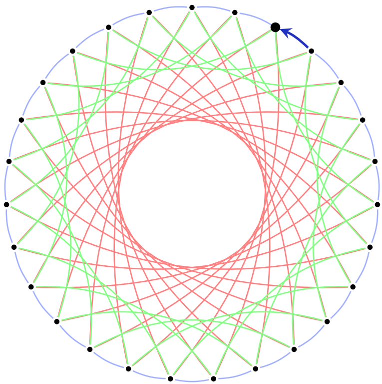




Diffie and Hellman go to the CSIDH

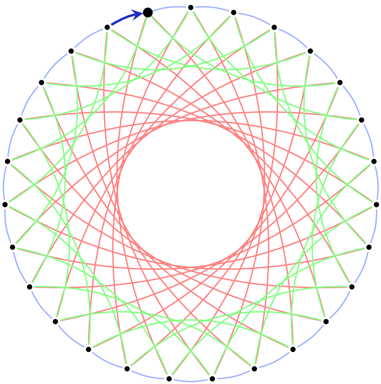
Alice

$[\mathfrak{l}_3, \mathfrak{l}_7{}^{-1}, \underset{\uparrow}{\mathfrak{l}_3}, \mathfrak{l}_5{}^{-1}]$



Bob

$[\mathfrak{l}_5, \mathfrak{l}_7, \underset{\uparrow}{\mathfrak{l}_3{}^{-1}}, \mathfrak{l}_5]$



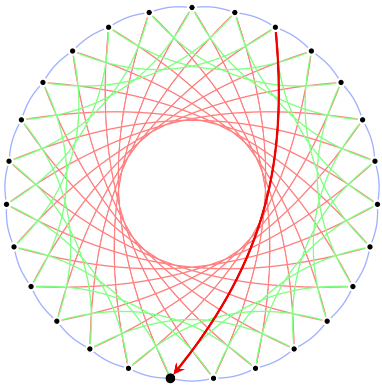
Diffie and Hellman go to the CSIDH

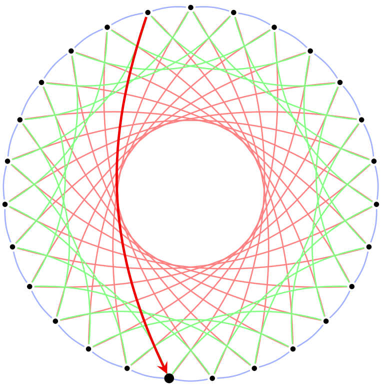
Alice

$[\mathfrak{l}_3, \mathfrak{l}_7{}^{-1}, \mathfrak{l}_3, \underset{\uparrow}{\mathfrak{l}_5{}^{-1}}]$

Bob

$[\mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3{}^{-1}, \underset{\uparrow}{\mathfrak{l}_5}]$





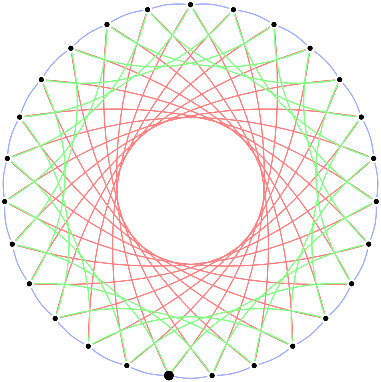
Diffie and Hellman go to the CSIDH

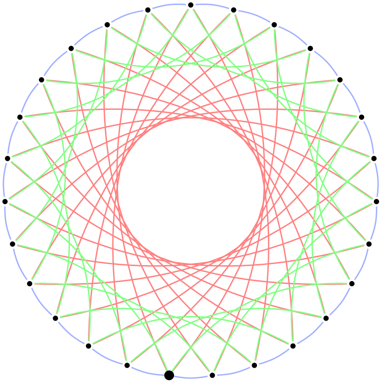
Alice

$[\mathfrak{l}_3, \mathfrak{l}_7{}^{-1}, \mathfrak{l}_3, \mathfrak{l}_5{}^{-1}]$

Bob

$[\mathfrak{l}_5, \mathfrak{l}_7, \mathfrak{l}_3{}^{-1}, \mathfrak{l}_5]$





Ex: CSI-FiSh (S '06, D-G '18, Beullens-Kleinjung-Vercauteren '19)

Identification scheme from $H \times S \to S$:

Prover		**Public**		**Verifier**
		$E \in S, \mathfrak{l}_i \in H$		
$s_i \leftarrow \$ \, \mathbb{Z}$				
$\mathsf{sk} = \prod \mathfrak{l}_i^{s_i}$,				
$\mathsf{pk} = \mathsf{sk} * E$	$\xrightarrow{\mathsf{pk}}$	pk		
				$c \leftarrow \$ \, \{0, 1\}$
$t_i \leftarrow \$ \, \mathbb{Z}$	$\xleftarrow{c}$			
$\mathsf{esk} = \prod \mathfrak{l}_i^{t_i}$,				
$\mathsf{epk}_1 = \mathsf{esk} * E$,				
$\mathsf{epk}_2 = \mathsf{esk} \cdot \mathsf{sk}^{-c}$		$\xrightarrow{\mathsf{pk}, \mathsf{epk}_1, \mathsf{epk}_2}$		check:
				$\mathsf{epk}_1 = \mathsf{epk}_2 * ([\mathsf{sk}^c] * E)$.

After k challenges c, an imposter succeeds with prob 2^{-k}.

Ex: SQISign (De Feo-Kohel-Leroux-Petit-Wesolowski '20)

Hard Problem in CSIDH, CSI-FiSh, etc:
Given elliptic curves E and $E' \in S$, find $\mathfrak{a} \in H$ such that
$\mathfrak{a} * E = E'$.

Ex: SQISign (De Feo-Kohel-Leroux-Petit-Wesolowski '20)

Hard Problem in CSIDH, CSI-FiSh, etc:
Given elliptic curves E and $E' \in S$, find an isogeny* $E \to E'$
(*rational map + group homomorphism)

Ex: SQISign (De Feo-Kohel-Leroux-Petit-Wesolowski '20)

Hard Problem in CSIDH, CSI-FiSh, etc:
Given elliptic curves E and $E' \in S$, find an isogeny* $E \to E'$
(*rational map + group homomorphism)

SQISign is a newer signature scheme based on this idea:

Ex: SQISign (De Feo-Kohel-Leroux-Petit-Wesolowski '20)

Hard Problem in CSIDH, CSI-FiSh, etc:
Given elliptic curves E and $E' \in S$, find an isogeny* $E \to E'$
(*rational map + group homomorphism)

SQISign is a newer signature scheme based on this idea:

$$\begin{tikzcd} E \arrow[d] \\ E_{\text{pk}} \end{tikzcd}$$

public, secret, ephemeral secret, public challenge, public proof

Ex: SQISign (De Feo-Kohel-Leroux-Petit-Wesolowski '20)

Hard Problem in CSIDH, CSI-FiSh, etc:
Given elliptic curves E and $E' \in S$, find an isogeny* $E \to E'$
(*rational map + group homomorphism)

SQISign is a newer signature scheme based on this idea:

$$\begin{tikzcd} E \arrow[r] \arrow[d] & E_{\text{epk}} \\ E_{\text{pk}} & \end{tikzcd}$$

public, secret, ephemeral secret, public challenge, public proof

Ex: SQISign (De Feo-Kohel-Leroux-Petit-Wesolowski '20)

Hard Problem in CSIDH, CSI-FiSh, etc:

Given elliptic curves E and $E' \in S$, find an isogeny* $E \to E'$

(*rational map + group homomorphism)

SQISign is a newer signature scheme based on this idea:

$$\begin{tikzcd} E \arrow[r] \arrow[d] & E_{\mathrm{epk}} \arrow[d] \\ E_{\mathrm{pk}} & E_{\mathrm{ver}} \end{tikzcd}$$

public, secret, ephemeral secret, public challenge, public proof

Ex: SQISign (De Feo-Kohel-Leroux-Petit-Wesolowski '20)

Hard Problem in CSIDH, CSI-FiSh, etc:
Given elliptic curves E and $E' \in S$, find an isogeny* $E \to E'$
(*rational map + group homomorphism)

SQISign is a newer signature scheme based on this idea:

$$\begin{tikzcd}
E \arrow[r] \arrow[d] & E_{\mathrm{epk}} \arrow[d] \\
E_{\mathrm{pk}} \arrow[r] & E_{\mathrm{ver}}
\end{tikzcd}$$

public, secret, ephemeral secret, public challenge, public proof

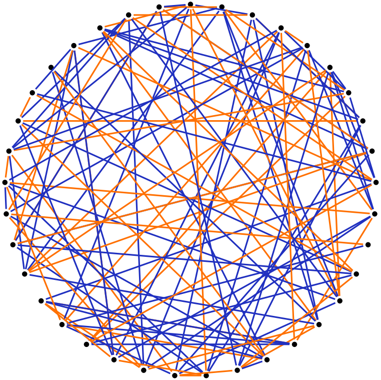
Ex: SIDH (De Feo-Plut-Jao '11) / SIKE (NIST Round 3 alternate)

Main idea: Graph-walking Diffie-Hellman on this graph:

Ex: SIDH (De Feo-Plut-Jao '11) / SIKE (NIST Round 3 alternate)

Main idea: Graph-walking Diffie-Hellman on this graph:

- **Vertices**: isomorphism classes of elliptic curves.
- **Edges**: 2- and 3-isogenies of elliptic curves (up to $\cong$).



2 and 3-isogenies of elliptic curves over $\mathbb{F}_{431^2}$

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in CSIDH, CSI-FiSh, SQISign etc:
Given elliptic curves E and $E' \in S$,
find an isogeny $E \to E'$.

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

- '16 Active attack on SIDH (Galbrait-Petit-Shani-Ti)

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

- '16 Active attack on SIDH (Galbrait-Petit-Shani-Ti)
- '17 Poly-time attack on overstretched parameters (Petit)

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

- '16 Active attack on SIDH (Galbrait-Petit-Shani-Ti)
- '17 Poly-time attack on overstretched parameters (Petit)
- '21 Poly-time attack on SIDH group key exchange (Us)

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

> Hard Problem in SIDH/SIKE:
> Given elliptic curves E and $E' \in S$,
> and given some info about an isogeny $E \to E'$,
> find an isogeny $E \to E'$.

- '16 Active attack on SIDH (Galbrait-Petit-Shani-Ti)
- '17 Poly-time attack on overstretched parameters (Petit)
- '21 Poly-time attack on SIDH group key exchange (Us)
- '21 Poly-time attack on SIDH-based OPRF (Basso-Kutas-Merz-Petit-Sanso)

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

Parameters:

- Let Alice and Bob's path lengths be A and B.
- In SIKE: $A \approx B \approx \frac{1}{2}\log(p)$.

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

Parameters:

- Let Alice and Bob's path lengths be A and B.
- In SIKE: $A \approx B \approx \frac{1}{2}\log(p)$.

Results:

- Petit '17: poly-time attack when $B > 4A > \log(p)$.

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

Parameters:

- Let Alice and Bob's path lengths be A and B.
- In SIKE: $A \approx B \approx \frac{1}{2}\log(p)$.

Results:

- Petit '17: poly-time attack when $B > 4A > \log(p)$.
- New attack:
  - Poly-time when $B > \log(p) + A$ or $B > \frac{1}{2}\log(p) + 2A$.

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

Parameters:

- Let Alice and Bob's path lengths be A and B.
- In SIKE: $A \approx B \approx \frac{1}{2}\log(p)$.

Results:

- Petit '17: poly-time attack when $B > 4A > \log(p)$.
- New attack:
  - Poly-time when $B > \log(p) + A$ or $B > \frac{1}{2}\log(p) + 2A$.
  - Improves on best known attack when $B > \frac{1}{2}\log(p)$.

A new result (De Quehen-Kutas-Leonardi-M.-Panny-Petit-Stange)

Hard Problem in SIDH/SIKE:
Given elliptic curves E and $E' \in S$,
and given some info about an isogeny $E \to E'$,
find an isogeny $E \to E'$.

Parameters:

- Let Alice and Bob's path lengths be A and B.
- In SIKE: $A \approx B \approx \frac{1}{2}\log(p)$.

Results:

- Petit '17: poly-time attack when $B > 4A > \log(p)$.
- New attack:
  - Poly-time when $B > \log(p) + A$ or $B > \frac{1}{2}\log(p) + 2A$.
  - Improves on best known attack when $B > \frac{1}{2}\log(p)$.
  - Backdoor primes and starting curves.

Summary and overview

- SIKE '11 KEM. Best-studied, in NIST, fast, small-ish, torsion-point attacks most likely attack avenue.

Summary and overview

- SIKE '11 KEM. Best-studied, in NIST, fast, small-ish, torsion-point attacks most likely attack avenue.
- CSIDH '18 Key exchange. Small, many applications (c.f. group actions), fast-ish, known quantum attack needs further study, other attack avenues non-obvious.

Summary and overview

- SIKE '11 KEM. Best-studied, in NIST, fast, small-ish, torsion-point attacks most likely attack avenue.
- CSIDH '18 Key exchange. Small, many applications (c.f. group actions), fast-ish, known quantum attack needs further study, other attack avenues non-obvious.
- CSI-FiSh '19 Digital signature. Small-ish, flexible, fast-ish, known quantum attack needs further study.

Summary and overview

- SIKE '11 KEM. Best-studied, in NIST, fast, small-ish, torsion-point attacks most likely attack avenue.
- CSIDH '18 Key exchange. Small, many applications (c.f. group actions), fast-ish, known quantum attack needs further study, other attack avenues non-obvious.
- CSI-FiSh '19 Digital signature. Small-ish, flexible, fast-ish, known quantum attack needs further study.
- SQISign '20 Digital signature. Small, slow, clean security assumption, no known attack avenues.

Thank you!