Making and breaking post-quantum cryptography from elliptic curves

Chloe Martindale

University of Bristol

17th April 2023

Recall: Diffie–Hellman key exchange '76

Public parameters:

- a finite group G (typically $\mathbb{F}_q^*$ or $E(\mathbb{F}_q)$)
- an element $g \in G$ of (large) prime order p

Alice	public	Bob
$a \xleftarrow{\text{random}} \{0 \ldots p-1\}$		$b \xleftarrow{\text{random}} \{0 \ldots p-1\}$
g^a	$\longrightarrow$ g^a / g^b $\longleftarrow$	g^b
$s := (g^b)^a$		$s := (g^a)^b$

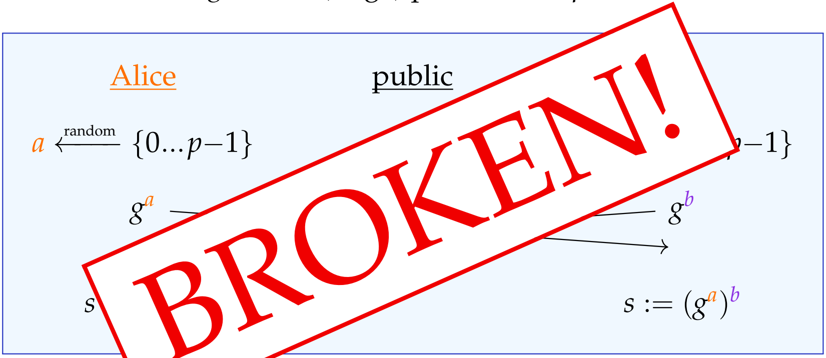
The Discrete Logarithm Problem, finding a given g and g^a, should be hard[1] in $\langle g \rangle$.

[1] Complexity (at least) subexponential in $\log(p)$.

Recall: Diffie–Hellman key exchange ‘76

Public parameters:

- a finite group G (typically $\mathbb{F}_q^*$ or $E(\mathbb{F}_q)$)
- an element $g \in G$ of (large) prime order p



The Discre[illegible] Logarithm Problem, finding a given g and g^a, should be hard[1] in $\langle g \rangle$.

[1]Complexity (at least) subexponential in $\log(p)$.

Quantumifying Exponentiation

- Couveignes '97, Rostovtsev, Stolbunov '04: Idea to replace the Discrete Logarithm Problem: replace exponentiation

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

by a group action on a set.

Quantumifying Exponentiation

- Couveignes '97, Rostovtsev, Stolbunov '04: Idea to replace the Discrete Logarithm Problem: replace exponentiation

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

  by a group action on a set.
- Replace G by a (sub)set S of the elliptic curves $E/\mathbb{F}_q$ with commutative $\mathrm{End}(E) = \mathcal{O}$.

Quantumifying Exponentiation

- Couveignes '97, Rostovtsev, Stolbunov '04: Idea to replace the Discrete Logarithm Problem: replace exponentiation

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

  by a group action on a set.
- Replace G by a (sub)set S of the elliptic curves $E/\mathbb{F}_q$ with commutative $\mathrm{End}(E) = \mathcal{O}$.
- Replace $\mathbb{Z}$ by $\mathrm{cl}(\mathcal{O})$; this acts freely and transitively on S via isogenies:

$$\begin{array}{ccc} \mathrm{cl}(\mathcal{O}) \times S & \to & S \\ (\alpha, E) & \mapsto & \alpha * E := \alpha(E) \end{array}$$

Couveignes-Rostovstev-Stolbunov key exchange

Public parameters:

- the finite set S (of some $E/\mathbb{F}_q$ with $\mathrm{End}(E) = \mathcal{O}$),
- an element $E \in S$,
- the group $\mathrm{cl}(\mathcal{O})$; acts on S via $*$.

Alice	public	Bob
$\alpha \xleftarrow{\text{random}} \mathrm{cl}(\mathcal{O})$		$\beta \xleftarrow{\text{random}} \mathrm{cl}(\mathcal{O})$
$\alpha * E$	$\alpha * E \rightarrow$ / $\leftarrow \beta * E$	$\beta * E$
$s := \alpha * (\beta * E)$		$s := \beta * (\alpha * E)$

Finding α given E and $\alpha * E$, should be hard.[2]

[2] Complexity (at least) subexponential in $\log(\#S)$.

From CRS to CSIDH

1997 Couveignes proposes the now-CRS scheme.

- Uses ordinary elliptic curves/$\mathbb{F}_p$ with same end ring.
- Paper is rejected and forgotten.

2004 Rostovstev, Stolbunov rediscover now-CRS scheme.

- Best known quantum and classical attacks are exponential.

2005 Kuperberg: quantum subexponential attack for the dihedral hidden subgroup problem.

2010 Childs, Jao, Soukharev apply Kuperberg to CRS.

- Secure parameters $\rightsquigarrow$ key exchange of 20 minutes.

2011 Jao, De Feo propose SIDH [more to come!].

2017 De Feo, Kieffer, Smith use modular curves to do a CRS key exchange in 8 minutes.

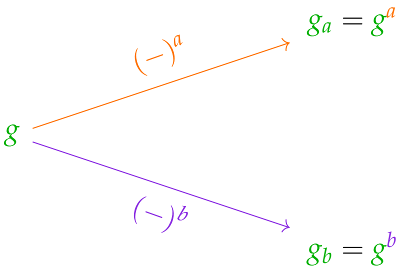
2018 Castryck, Lange, M., Panny, Renes propose CSIDH.

- CRS but with supersingular elliptic curves $/\mathbb{F}_p$.
- p constructed to make scheme efficient.
- Key exchange runs in 60ms.

[ˈsiːˌsaɪd]

Evolution of key exchange

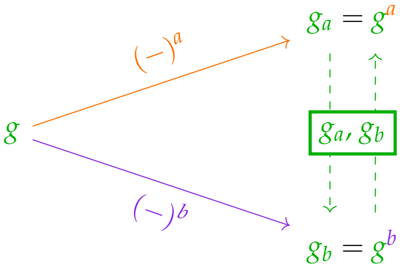
Diffie-Hellman



Colour code: Public, Alice's secret, Bob's secret

Evolution of key exchange

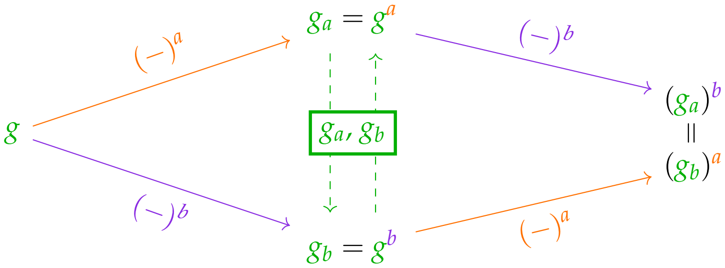
Diffie-Hellman



Colour code: Public, Alice's secret, Bob's secret

Evolution of key exchange

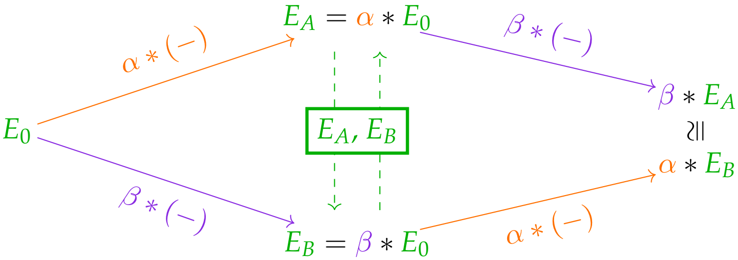
Diffie-Hellman



Colour code: Public, Alice's secret, Bob's secret

Evolution of key exchange

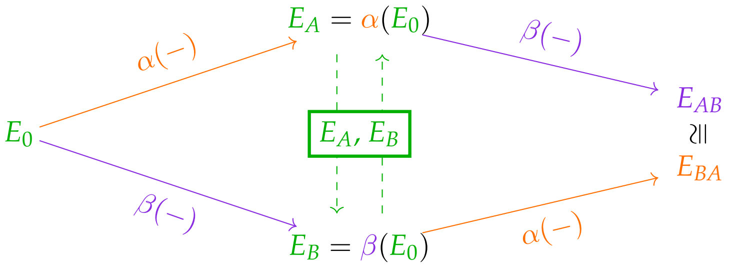
CRS or CSIDH



Colour code: Public, Alice's secret, Bob's secret

Evolution of key exchange

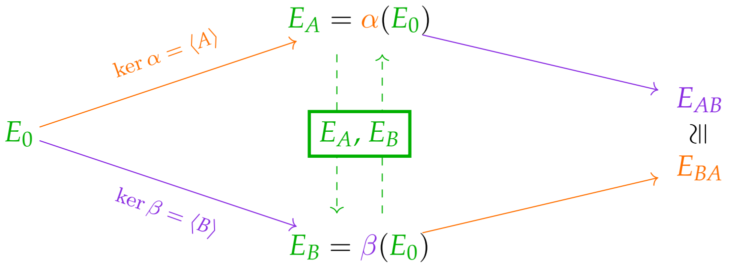
From CRS to SIDH



Colour code: Public, Alice's secret, Bob's secret

Evolution of key exchange

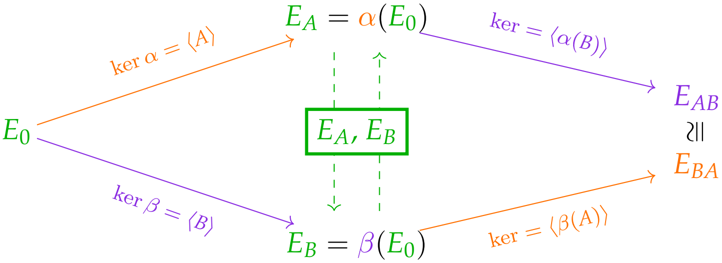
From CRS to SIDH



Colour code: Public, Alice's secret, Bob's secret

Evolution of key exchange

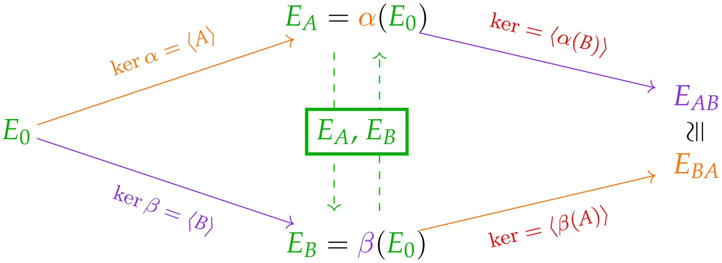
From CRS to SIDH



Colour code: Public, Alice's secret, Bob's secret

Evolution of key exchange

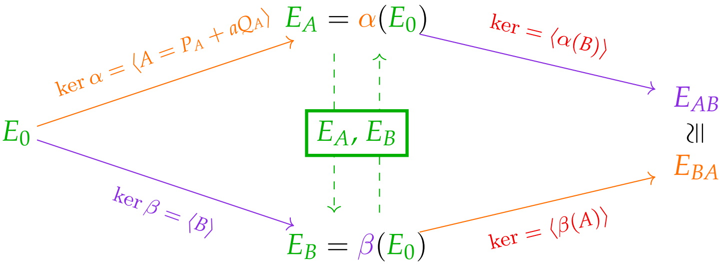
From CRS to SIDH



Colour code: Public, Alice's secret, Bob's secret, ?!

Evolution of key exchange

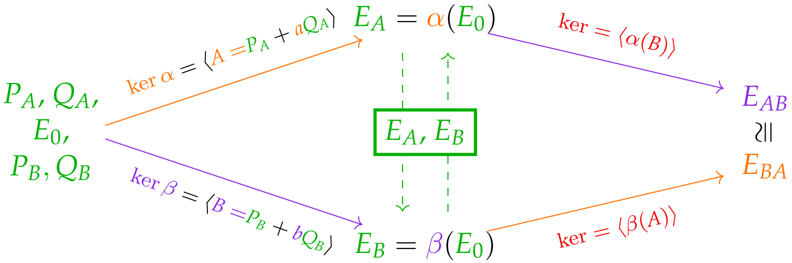
From CRS to SIDH



Colour code: Public, Alice's secret, Bob's secret, ?!

Evolution of key exchange

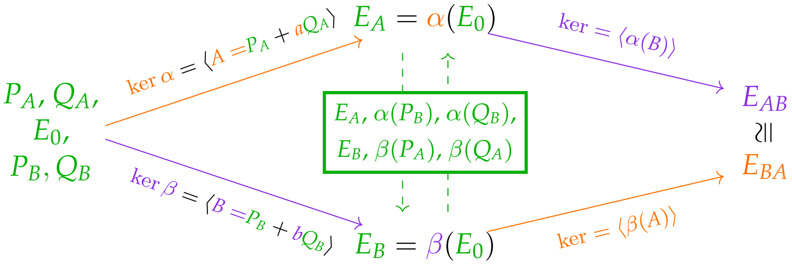
From CRS to SIDH



Colour code: Public, Alice's secret, Bob's secret, ?!

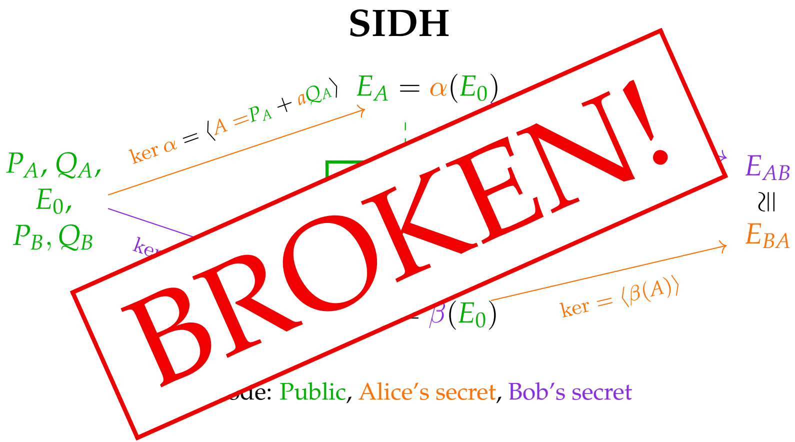
Evolution of key exchange

SIDH



Colour code: Public, Alice's secret, Bob's secret

Evolution of key exchange



Summary of hard problems

- Diffie-Hellman – The Discrete Logarithm Problem, finding a given g and g^a.

Summary of hard problems

- Diffie-Hellman – The Discrete Logarithm Problem, finding a given g and g^a.
- CRS / CSIDH – Finding α given E and $\alpha * E$.

Summary of hard problems

- Diffie-Hellman – The Discrete Logarithm Problem, finding a given g and g^a.
- CRS / CSIDH – Finding α given E and $\alpha * E$.
- All isogeny-based schemes – Given elliptic curves E_0 and E_A, compute an isogeny $\alpha : E_0 \rightarrow E_A$ if it exists.

Summary of hard problems

- Diffie-Hellman – The Discrete Logarithm Problem, finding a given g and g^a.
- CRS / CSIDH – Finding α given E and $\alpha * E$.
- All isogeny-based schemes – Given elliptic curves E_0 and E_A, compute an isogeny $\alpha : E_0 \to E_A$ if it exists.
- SIDH –

Let p be a large prime and N, M large smooth prime integers. Given public supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$, the existence of a secret isogeny $\alpha : E_0 \to E_A$ of degree M, and the action of α on $E_0[N]$, compute α.

History of the SIDH problem

2011 Problem introduced by De Feo, Jao, and Plut

2016 Galbraith, Petit, Shani, Ti give active attack

2017 Petit gives passive attack on some parameter sets

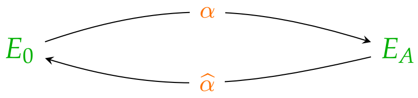
2020 de Quehen, Kutas, Leonardi, M., Panny, Petit, Stange give passive attack on more parameter sets

2022 Castryck-Decru and Maino-M. give passive attack on SIKE parameter sets; Robert extends to all parameter sets

- CD and MM attack is subexponential in most cases
- CD attack polynomial-time when $\mathrm{End}(E_0)$ known
- Robert attack polynomial-time in all cases

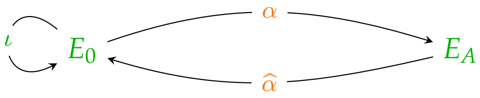
Petit's trick: torsion points to isogenies

Finding the secret isogeny α of known degree.



Petit's trick: torsion points to isogenies

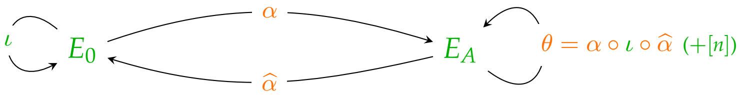
Finding the secret isogeny α of known degree.



- Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.

Petit's trick: torsion points to isogenies

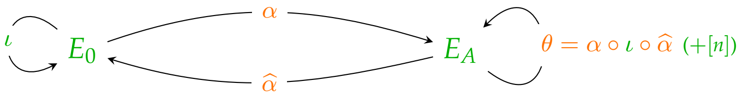
Finding the secret isogeny α of known degree.



- Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.

Petit's trick: torsion points to isogenies

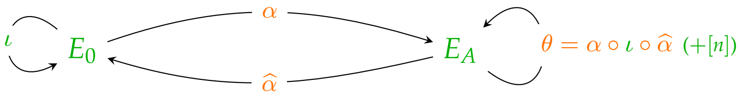
Finding the secret isogeny α of known degree.



- Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.
- Know $\alpha(E_0[N])$ (and $\widehat{\alpha}(E_A[N])$) from public torsion points.

Petit's trick: torsion points to isogenies

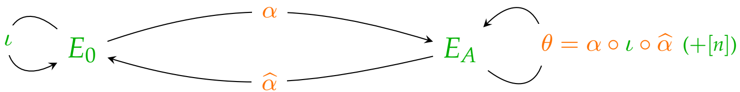
Finding the secret isogeny α of known degree.



- Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.
- Know $\alpha(E_0[N])$ (and $\widehat{\alpha}(E_A[N])$) from public torsion points.
- Know $\deg(\theta) = \deg(\alpha)^2 \deg(\iota) + n^2$.

Petit's trick: torsion points to isogenies

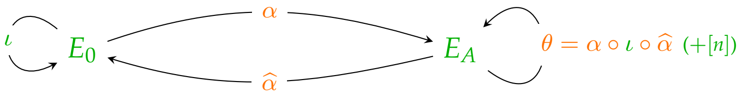
Finding the secret isogeny α of known degree.



- Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.
- Know $\alpha(E_0[N])$ (and $\widehat{\alpha}(E_A[N])$) from public torsion points.
- Know $\deg(\theta) = \deg(\alpha)^2 \deg(\iota) + n^2$.
- Restriction # 2: If there exist ι, n such that $\deg(\theta) = N$, then can completely determine θ, and α, in polynomial-time.

Petit's trick: torsion points to isogenies

Finding the secret isogeny α of known degree.



- Restriction # 1: Assume we can choose $\iota : E_0 \to E_0$.
- Know $\alpha(E_0[N])$ (and $\widehat{\alpha}(E_A[N])$) from public torsion points.
- Know $\deg(\theta) = \deg(\alpha)^2 \deg(\iota) + n^2$.
- Restriction # 2: If there exist ι, n such that $\deg(\theta) = N$, then can completely determine θ, and α, in polynomial-time.
- Restriction # 2 rules out SIKE parameters, where $N \approx \deg(\alpha)$ and $p \approx N \cdot \deg \alpha$.

Enter Kani

Let p be a large prime and N, M large smooth prime integers. Given public supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$, the existence of a secret isogeny $\alpha : E_0 \to E_A$ of degree M, and the action of α on $E_0[N]$, compute α.

Enter Kani

Let p be a large prime and N, M large smooth prime integers. Given public supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$, the existence of a secret isogeny $\alpha : E_0 \to E_A$ of degree M, and the action of α on $E_0[N]$, compute α.

Problem:

Not enough choices $\theta : E_A \to E_A$.

'No θ of degree N.'

Enter Kani

Let p be a large prime and N, M large smooth prime integers. Given public supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$, the existence of a secret isogeny $\alpha : E_0 \to E_A$ of degree M, and the action of α on $E_0[N]$, compute α.

Problem:
Not enough choices $\theta : E_A \to E_A$.
'No θ of degree N.'

Solution? $\theta : E_0 \times E_A \to E_0 \times E_A$?
$\rightsquigarrow$ still not enough.

Enter Kani

Let p be a large prime and N, M large smooth prime integers. Given public supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$, the existence of a secret isogeny $\alpha : E_0 \to E_A$ of degree M, and the action of α on $E_0[N]$, compute α.

Problem:
Not enough choices $\theta : E_A \to E_A$.
'No θ of degree N.'

Solution? $\theta : E_0 \times E_A \to E_0 \times E_A$?
$\rightsquigarrow$ still not enough. But!

Enter Kani

Let p be a large prime and N, M large smooth prime integers. Given public supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$, the existence of a secret isogeny $\alpha : E_0 \to E_A$ of degree M, and the action of α on $E_0[N]$, compute α.

Problem:
Not enough choices $\theta : E_A \to E_A$.
'No θ of degree N.'

Solution? $\theta : E_0 \times E_A \to E_0 \times E_A$?
$\rightsquigarrow$ still not enough. But! Kani's theorem:

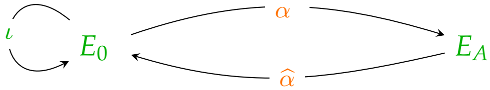
- Constructs E_1, E_2 such that there exists a (N, N)-isogeny

$$E_1 \times E_A \to E_0 \times E_2.$$

- Petit's trick then applies.

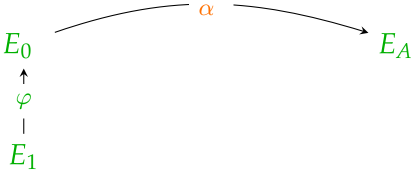
Recovering the secret

Finding the secret isogeny α of known degree.



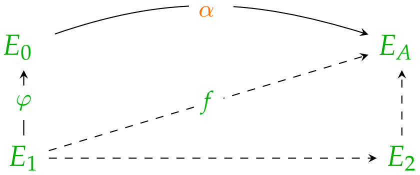
Recovering the secret

Finding the secret isogeny α of known degree.



Recovering the secret

Finding the secret isogeny α of known degree.



Kani's theorem constructs the above such that

$$\Phi = \begin{pmatrix} \varphi & -\widehat{\alpha} \\ * & * \end{pmatrix} : E_1 \times E_A \to E_0 \times E_2$$

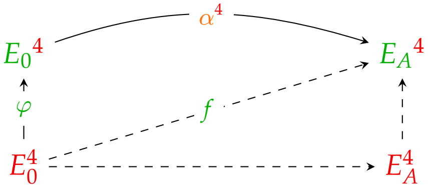
is a (N, N)-isogeny, and

$$\ker(\Phi) = \{(\deg(\alpha)P, f(P)) : P \in E_1[N]\}$$

$\rightsquigarrow$ can compute Φ and read off secret α!

Recovering the secret with Robert's trick

Finding the secret isogeny α of known degree.



constructs the above such that

$$\Phi = \begin{pmatrix} \varphi & -\widehat{\alpha}^4 \\ * & * \end{pmatrix} : E_0 \times E_A \to E_0 \times E_A$$

is a (N, N)-isogeny, and

$$\ker(\Phi) \text{ is known}$$

$\rightsquigarrow$ can compute Φ and read off secret α!

What next?

- Fouotsa, Moriya, and Petit proposed mitigations
  - Masks either torsion point images or isogeny degrees
  - The mitigations make SIKE/SIDH unusably slow and big
  - For advanced protocols may still be a good option (c.f. Basso's OPRF, threshold schemes, etc.)

What next?

- Fouotsa, Moriya, and Petit proposed mitigations
  - Masks either torsion point images or isogeny degrees
  - The mitigations make SIKE/SIDH unusably slow and big
  - For advanced protocols may still be a good option
    (c.f. Basso's OPRF, threshold schemes, etc.)
- Constructive applications?
  - Work in progress with Maino and Robert
    $\rightsquigarrow$ computing genus 2 cyclic isogenies.

What next?

- Fouotsa, Moriya, and Petit proposed mitigations
  - Masks either torsion point images or isogeny degrees
  - The mitigations make SIKE/SIDH unusably slow and big
  - For advanced protocols may still be a good option (c.f. Basso's OPRF, threshold schemes, etc.)
- Constructive applications?
  - Work in progress with Maino and Robert $\rightsquigarrow$ computing genus 2 cyclic isogenies.

Thank you!