# Making and breaking post-quantum cryptography from elliptic curves

Chloe Martindale

University of Bristol

29th November 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 |
|---|---|---|
| $a \xleftarrow{\text{random}} \{0 \ldots p-1\}$ | | $b \xleftarrow{\text{random}} \{0 \ldots p-1\}$ |
| $g^a$ | $g^a \rightarrow$, $\leftarrow g^b$ | $g^b$ |
| $s := (g^b)^a$ | | $s := (g^a)^b$ |

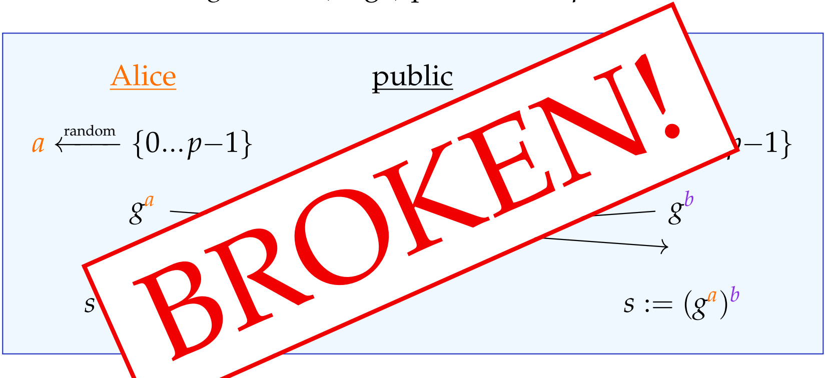
The Discrete Logarithm Problem, finding $a$ given $g$ and $g^a$, should be hard[1] in $\langle g \rangle$.

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

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

# 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 set $S$ of specially chosen elliptic curves $/\mathbb{F}_q$.

# 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.
- Replace $G$ by a set $S$ of specially chosen elliptic curves $/\mathbb{F}_q$.
- Replace $\mathbb{Z}$ by a commutative group $H$ that acts freely and transitively on $S$ via surjective morphisms (isogenies):

$$\begin{array}{rcl} H \times S & \to & S \\ (\alpha, E) & \mapsto & \alpha * E := \alpha(E) \end{array}$$

# Couveignes-Rostovstev-Stolbunov key exchange

Public parameters:

- a finite set $S$ (of specially chosen elliptic curves $/\mathbb{F}_q$),
- an element $E \in S$,
- a group $H$ that acts freely and transitively on $S$ via $*$.

| Alice | public | Bob |
| --- | --- | --- |
| $\alpha \xleftarrow{\text{random}} H$ | | $\beta \xleftarrow{\text{random}} H$ |
| $\alpha * E$ | $\alpha * E \longrightarrow$ Bob; $\beta * E \longrightarrow$ Alice | $\beta * E$ |
| $s := \alpha * (\beta * E)$ | | $s := \beta * (\alpha * E)$ |

Finding $\alpha$ 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.

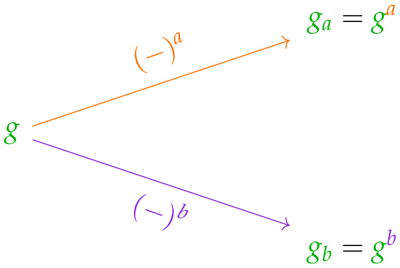
2018 Castryck, Lange, M., Panny, Renes propose CSIDH.

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


[ˈsiːˌsaɪd]

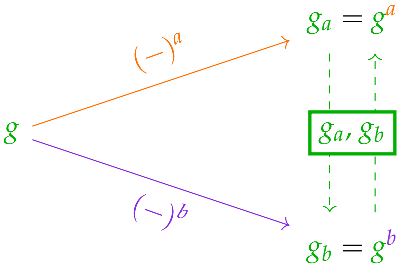
# Evolution of key exchange

**Diffie-Hellman**




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

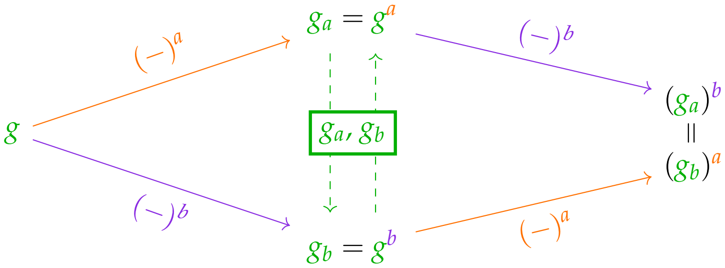
# Diffie-Hellman




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

# Evolution of key exchange

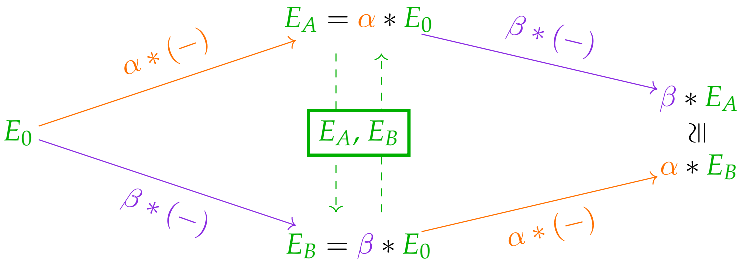
## Diffie-Hellman




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

# Evolution of key exchange

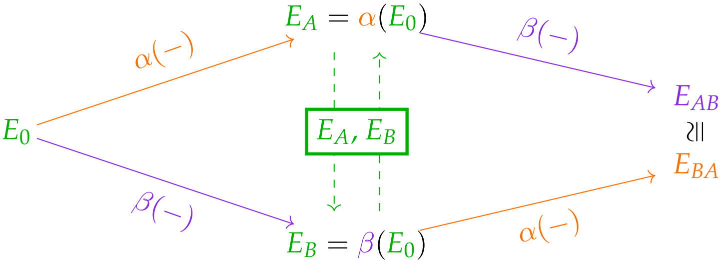
## CRS or CSIDH




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

# Evolution of key exchange

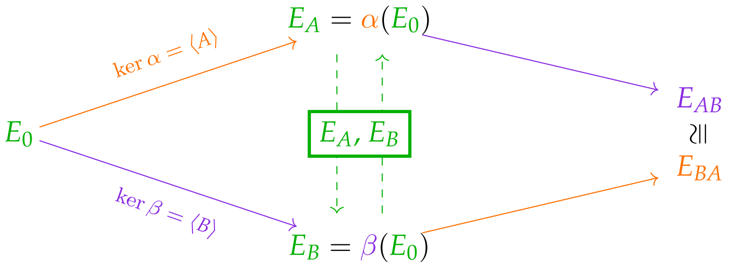
## From CRS to SIDH




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

# Evolution of key exchange

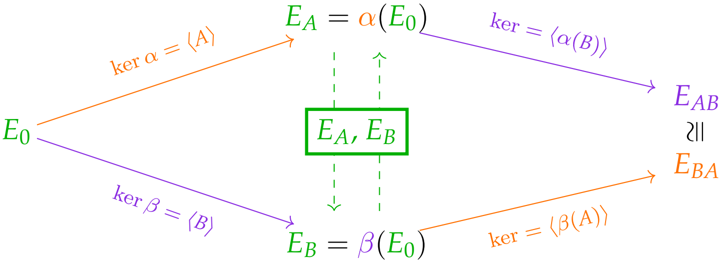
## From CRS to SIDH




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

# Evolution of key exchange

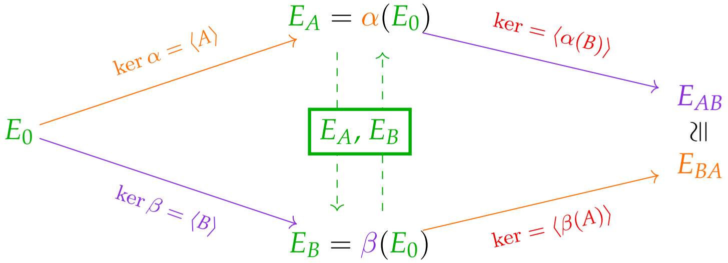
## From CRS to SIDH




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

# Evolution of key exchange

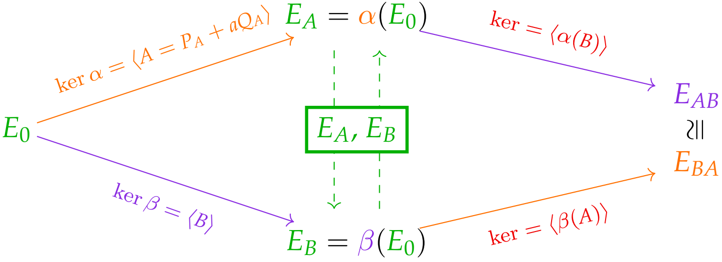
## From CRS to SIDH




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

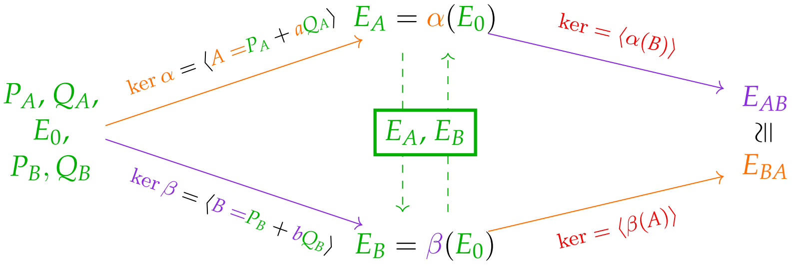
# Evolution of key exchange

## From CRS to SIDH



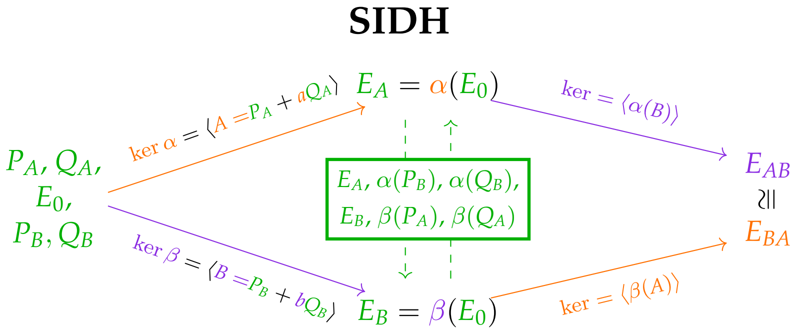

Colour code: Public, Alice's secret, Bob's secret, ?!

## From CRS to SIDH




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

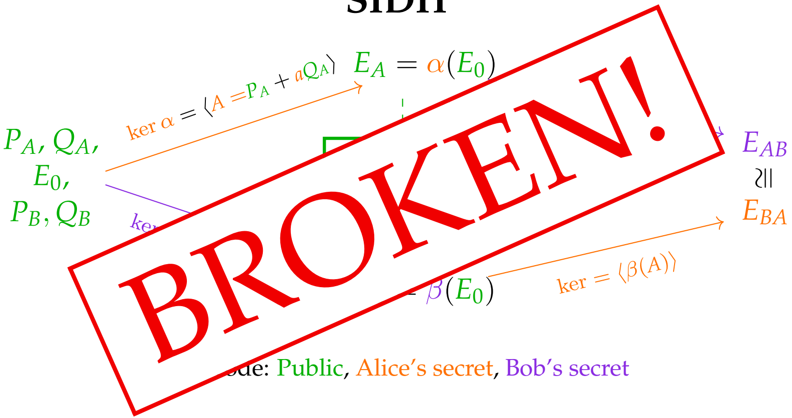
# Evolution of key exchange




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

# Evolution of key exchange

## SIDH



# 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 $\alpha$ 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 $\alpha$ 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.

# Summary of hard problems

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

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$. (modulo technical restrictions)*

*Details for the elliptic curve lovers:

$p$ a large prime; $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$ supersingular; $\deg(\alpha)$, $N$ public large smooth coprime integers; points $P_B$, $Q_B$ chosen such that $\langle P_B, Q_B \rangle = E_0[N]$.

# 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
- Panny and Pope implement MM attack; Wesolowski independently discovers direct recovery method

# Technical interlude

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$ . (modulo technical restrictions)*

# Technical interlude

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$ or $\ker(\alpha)$. (modulo technical restrictions)*

# Technical interlude

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$ or $\ker(\alpha)$. (modulo technical restrictions)*

- The set of points on an elliptic curve forms a group.

# Technical interlude

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B, Q_B$ on $E_0$ and $\alpha(P_B), \alpha(Q_B)$, compute $\alpha$ or $\ker(\alpha)$. (modulo technical restrictions)*

- The set of points on an elliptic curve forms a group.
- $E_A[N]$ = set of points of order dividing $N$.

# Technical interlude

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$ or $\ker(\alpha)$. (modulo technical restrictions)*

- The set of points on an elliptic curve forms a group.
- $E_A[N]$ = set of points of order dividing $N$.
- $^* \rightsquigarrow E_A[N] = \langle \alpha(P_B), \alpha(Q_B) \rangle$.

# Technical interlude

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$ or $\ker(\alpha)$. (modulo technical restrictions)*

- The set of points on an elliptic curve forms a group.
- $E_A[N]$ = set of points of order dividing $N$.
- $^* \rightsquigarrow E_A[N] = \langle \alpha(P_B), \alpha(Q_B) \rangle$.
- If $\deg(\theta : E_A \to E_A) = N$, then $\ker(\theta) \subseteq E_A[N]$.

# Technical interlude

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$ or $\ker(\alpha)$. (modulo technical restrictions)*

- The set of points on an elliptic curve forms a group.
- $E_A[N]$ = set of points of order dividing $N$.
- $^* \rightsquigarrow E_A[N] = \langle \alpha(P_B), \alpha(Q_B) \rangle$.
- If $\deg(\theta : E_A \to E_A) = N$, then $\ker(\theta) \subseteq E_A[N]$.
- Every isogeny (e.g. $\alpha : E_0 \to E_A$) has a dual isogeny (e.g. $\widehat{\alpha} : E_A \to E_0$)

# Technical interlude

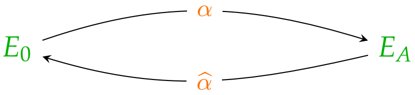
There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$ or $\ker(\alpha)$. (modulo technical restrictions)*

- The set of points on an elliptic curve forms a group.
- $E_A[N]$ = set of points of order dividing $N$.
- $^* \rightsquigarrow E_A[N] = \langle \alpha(P_B), \alpha(Q_B) \rangle$.
- If $\deg(\theta : E_A \to E_A) = N$, then $\ker(\theta) \subseteq E_A[N]$.
- Every isogeny (e.g. $\alpha : E_0 \to E_A$) has a dual isogeny (e.g. $\widehat{\alpha} : E_A \to E_0$)

$\rightsquigarrow$ Petit's idea: Construct $\theta : E_A \to E_A$ such that $\ker(\widehat{\alpha}) \subseteq \ker(\theta)$.

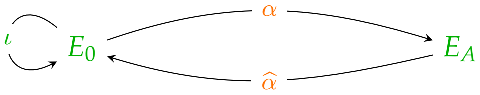
# Petit's trick: torsion points to isogenies

Finding the secret isogeny $\alpha$ of known degree.



# Petit's trick: torsion points to isogenies

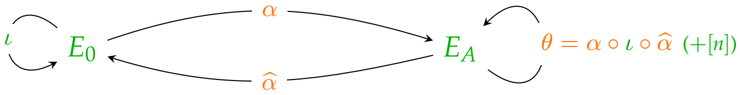
Finding the secret isogeny $\alpha$ of known degree.




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

# Petit's trick: torsion points to isogenies

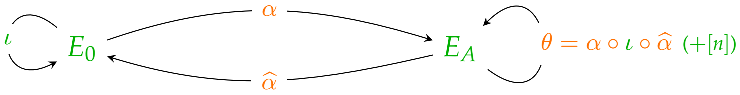
Finding the secret isogeny $\alpha$ of known degree.




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

# Petit's trick: torsion points to isogenies

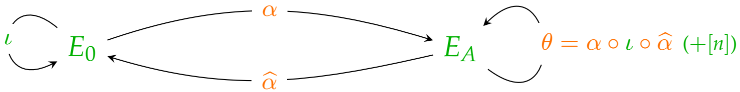
Finding the secret isogeny $\alpha$ of known degree.




- 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

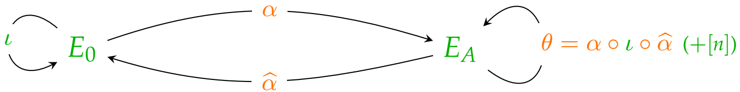
Finding the secret isogeny $\alpha$ of known degree.




- 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

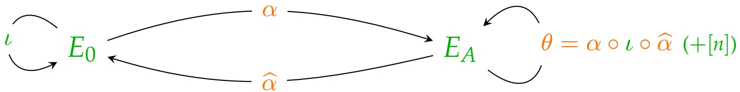
Finding the secret isogeny $\alpha$ of known degree.




- 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 $\iota, n$ such that $\deg(\theta) = N$, then can completely determine $\theta$, and $\alpha$, in polynomial-time.

# Petit's trick: torsion points to isogenies

Finding the secret isogeny $\alpha$ 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 $\iota, n$ such that $\deg(\theta) = N$, then can completely determine $\theta$, and $\alpha$, in polynomial-time.
- Restriction # 2 rules out SIKE parameters, where $N \approx \deg(\alpha)$ (and $p \approx N \cdot \deg \alpha$).

# Enter Kani

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$. (modulo technical restrictions)*

# Enter Kani

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$. (modulo technical restrictions)*

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

# Enter Kani

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$. (modulo technical restrictions)*

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

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

# Enter Kani

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$. (modulo technical restrictions)*

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

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

# Enter Kani

There are public elliptic curves $E_0$ and $E_A$, and a secret isogeny $\alpha : E_0 \to E_A$. Given the points $P_B$, $Q_B$ on $E_0$ and $\alpha(P_B)$, $\alpha(Q_B)$, compute $\alpha$. (modulo technical restrictions)*

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

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

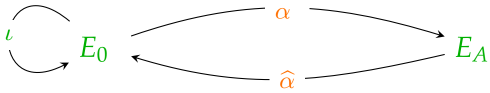
- Constructs $E_1$, $E_2$ such that there exists a (structure-preserving) isogeny

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

  of the right degree, $N^2$.
- Petit's trick then applies.

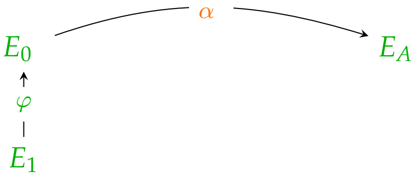
# Recovering the secret

Finding the secret isogeny $\alpha$ of known degree.



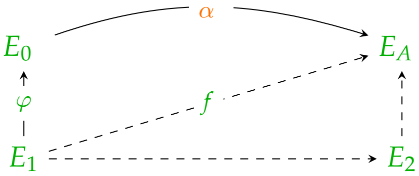
# Recovering the secret

Finding the secret isogeny $\alpha$ of known degree.



# Recovering the secret

Finding the secret isogeny $\alpha$ of known degree.




Kani's theorem constructs the above such that

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

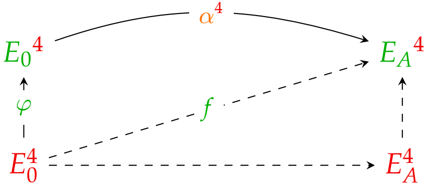
is a structure preserving isogeny of degree $N^2$, and

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

$\rightsquigarrow$ can compute $\Phi$ and read off secret $\alpha$!

# Recovering the secret with Robert's trick

Finding the secret isogeny $\alpha$ of known degree.




constructs the above such that

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

is a structure preserving isogeny of degree $N^2$, and

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

$\rightsquigarrow$ can compute $\Phi$ and read off secret $\alpha$!

# 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.)
  - Cryptanalysis ongoing effort

# 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.)
  - Cryptanalysis ongoing effort
- Constructive applications?
  - FESTA: New PKE. Fast and small as SIKE was?
  - SQISignHD: Small, fast signatures with clean security reduction.
  - VDF-like construction.
  - 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.)
  - Cryptanalysis ongoing effort
- Constructive applications?
  - FESTA: New PKE. Fast and small as SIKE was?
  - SQISignHD: Small, fast signatures with clean security reduction.
  - VDF-like construction.
  - Work in progress with Maino and Robert $\rightsquigarrow$ computing genus 2 cyclic isogenies.

Thank you!