SIKE不再

Lorenz Panny

Academia Sinica

Taipei, 15 December 2022

What's this all about?

- 2011: David Jao & Luca De Feo come up with something now known as "Supersingular-Isogeny Diffie–Hellman".

What's this all about?

- 2011: David Jao & Luca De Feo come up with something now known as "Supersingular-Isogeny Diffie–Hellman".
- 2020$-\varepsilon$: Semi-surprisingly, this stuff is still not broken.

— me, at ECC 2019

What's this all about?

- 2011: David Jao & Luca De Feo come up with something now known as "Supersingular-Isogeny Diffie–Hellman".
- 2020$-\varepsilon$: Semi-surprisingly, this stuff is still not broken.

— me, at ECC 2019

- 2022: Never mind, it *is* broken.

SIKE @ NISTPQC

- A version of SIDH called SIKE was submitted to NISTPQC.

SIKE @ NISTPQC

- A version of SIDH called SIKE was submitted to NISTPQC.
- *Zero* attack improvements for several years.

SIKE @ NISTPQC

- A version of SIDH called SIKE was submitted to NISTPQC.
- *Zero* attack improvements for several years.
- Security estimates actually increased with new analysis.
  Jaques–Schanck: Quantum attack scales much worse than originally claimed.
  Several works: Classical attack is costlier in practice than asymptotics suggest.

SIKE @ NISTPQC

- A version of SIDH called SIKE was submitted to NISTPQC.
- *Zero* attack improvements for several years.
- Security estimates actually increased with new analysis.
  Jaques–Schanck: Quantum attack scales much worse than originally claimed.
  Several works: Classical attack is costlier in practice than asymptotics suggest.
- Bounty for breaking toy "$IKE" instances: 5k + 50k USD.
  2021-08-28: Udovenko–Vitto claimed the 5k with a large brute-force computation.

SIKE @ NISTPQC

- A version of SIDH called SIKE was submitted to NISTPQC.
- *Zero* attack improvements for several years.
- Security estimates actually increased with new analysis.
  Jaques–Schanck: Quantum attack scales much worse than originally claimed.
  Several works: Classical attack is costlier in practice than asymptotics suggest.
- Bounty for breaking toy "$IKE" instances: 5k + 50k USD.
  2021-08-28: Udovenko–Vitto claimed the 5k with a large brute-force computation.
- SIKE remained an alternate candidate through round 3!

SIKE @ NISTPQC

- A version of SIDH called SIKE was submitted to NISTPQC.
- *Zero* attack improvements for several years.
- Security estimates actually increased with new analysis.
  Jaques–Schanck: Quantum attack scales much worse than originally claimed.
  Several works: Classical attack is costlier in practice than asymptotics suggest.
- Bounty for breaking toy "$IKE" instances: 5k + 50k USD.
  2021-08-28: Udovenko–Vitto claimed the 5k with a large brute-force computation.
- SIKE remained an alternate candidate through round 3!

- 2022-07-30: Castryck–Decru *destroye* SIDH. [ePrint 2022/975]
  Original Magma attack code breaks SIKEp751 in < 21 hours on a single laptop core.
  Subsequent SageMath implementation (Pope–Oudompheng–...) takes < 2 hours.

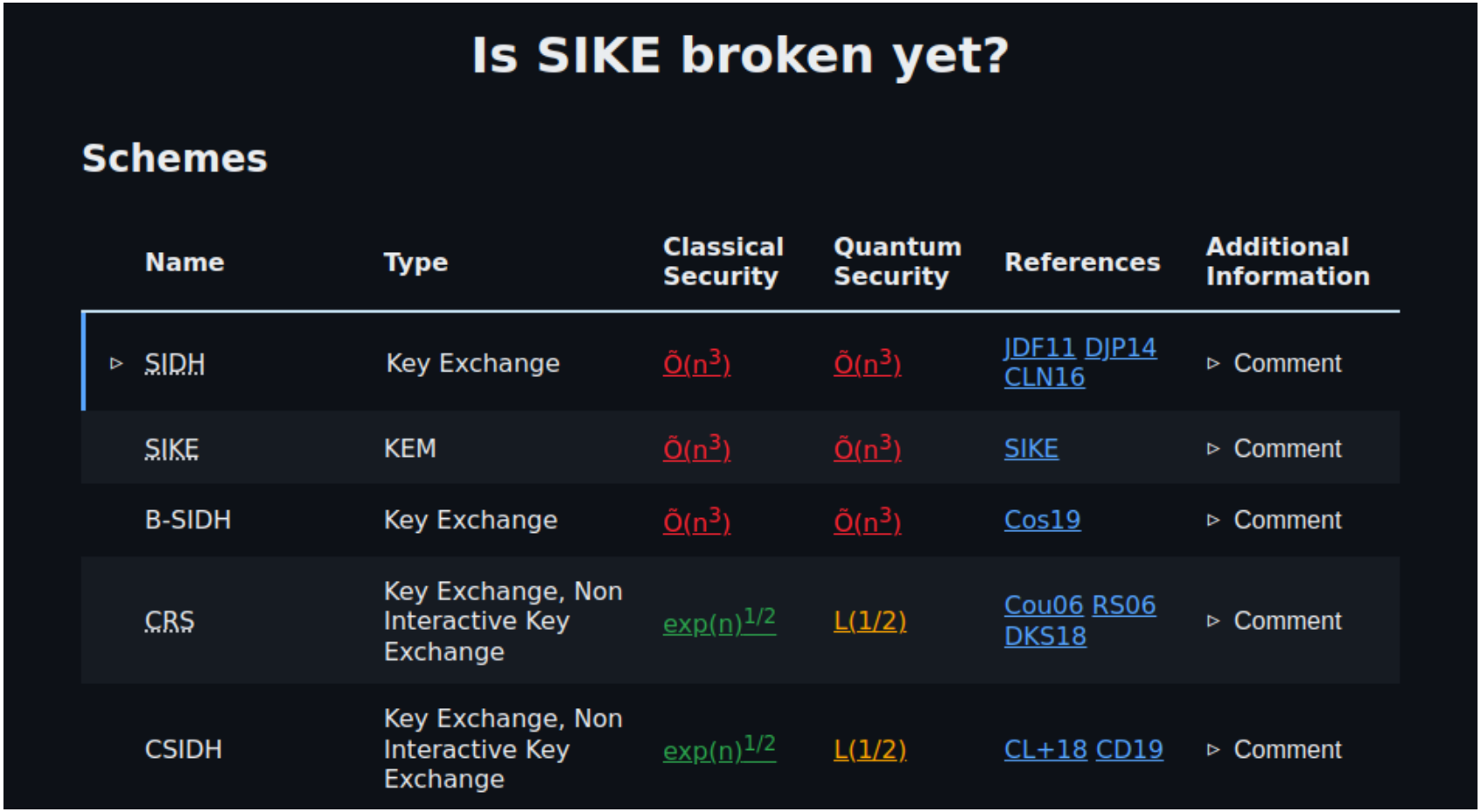
SIKE @ NISTPQC

- A version of SIDH called SIKE was submitted to NISTPQC.
- *Zero* attack improvements for several years.
- Security estimates actually increased with new analysis.
  Jaques–Schanck: Quantum attack scales much worse than originally claimed.
  Several works: Classical attack is costlier in practice than asymptotics suggest.
- Bounty for breaking toy "$IKE" instances: 5k + 50k USD.
  2021-08-28: Udovenko–Vitto claimed the 5k with a large brute-force computation.
- SIKE remained an alternate candidate through round 3!

- 2022-07-30: Castryck–Decru *destroye* SIDH. [ePrint 2022/975]
  Original Magma attack code breaks SIKEp751 in < 21 hours on a single laptop core.
  Subsequent SageMath implementation (Pope–Oudompheng–...) takes < 2 hours.
- The attack relies on extremely cool mathematics.

The fallout

https://issikebrokenyet.github.io/

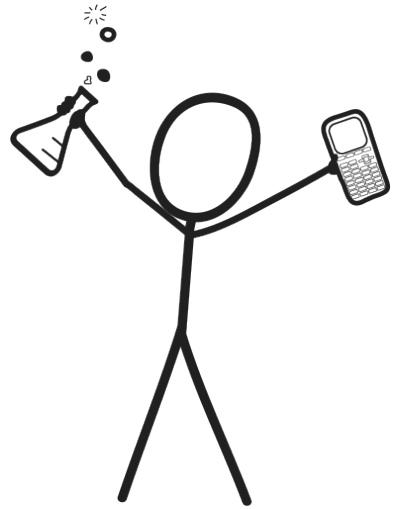


Is SIKE broken yet?

Schemes

Name	Type	Classical Security	Quantum Security	References	Additional Information
▹ SIDH	Key Exchange	$\tilde{O}(n^3)$	$\tilde{O}(n^3)$	JDF11 DJP14 CLN16	▹ Comment
SIKE	KEM	$\tilde{O}(n^3)$	$\tilde{O}(n^3)$	SIKE	▹ Comment
B-SIDH	Key Exchange	$\tilde{O}(n^3)$	$\tilde{O}(n^3)$	Cos19	▹ Comment
CRS	Key Exchange, Non Interactive Key Exchange	$\exp(n)^{1/2}$	L(1/2)	Cou06 RS06 DKS18	▹ Comment
CSIDH	Key Exchange, Non Interactive Key Exchange	$\exp(n)^{1/2}$	L(1/2)	CL+18 CD19	▹ Comment

Stand back!



We’re going to do math.

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$ that is:

- a group homomorphism.
- given by rational functions.

The degree of a separable* isogeny is the size of its kernel.

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$ that is:

- a group homomorphism.
- given by rational functions.

The degree of a separable* isogeny is the size of its kernel.

Example #1: For each $m \neq 0$, the multiplication-by-m map

$$[m] : E \to E$$

is a degree-m^2 isogeny. If $m \neq 0$ in the base field, its kernel is

$$E[m] \cong \mathbb{Z}/m \times \mathbb{Z}/m.$$

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$ that is:

- a group homomorphism.
- given by rational functions.

The degree of a separable* isogeny is the size of its kernel.

Example #2: For any a and b, the map $\iota : (x, y) \mapsto (-x, \sqrt{-1} \cdot y)$ defines a degree-1 isogeny of the elliptic curves

$$\{y^2 = x^3 + ax + b\} \longrightarrow \{y^2 = x^3 + ax - b\}.$$

It is an isomorphism; its kernel is $\{\infty\}$.

Isogenies

An isogeny of elliptic curves is a non-zero map $E \to E'$ that is:

- a group homomorphism.
- given by rational functions.

The degree of a separable* isogeny is the size of its kernel.

Example #3: $(x, y) \mapsto \left(\frac{x^3-4x^2+30x-12}{(x-2)^2}, \frac{x^3-6x^2-14x+35}{(x-2)^3} \cdot y \right)$ defines a degree-3 isogeny of the elliptic curves

$$\{y^2 = x^3 + x\} \longrightarrow \{y^2 = x^3 - 3x + 3\}$$

over $\mathbb{F}_{71}$. Its kernel is $\{(2, 9), (2, -9), \infty\}$.

The dual isogeny

Isogenies come in pairs.

Each isogeny $\varphi\colon E \to E'$ has a unique dual isogeny $\widehat{\varphi}\colon E' \to E$ characterized by $\widehat{\varphi} \circ \varphi = [\deg \varphi]$ and $\varphi \circ \widehat{\varphi} = [\deg \varphi]$.

The dual isogeny

Isogenies come in pairs.

Each isogeny $\varphi\colon E \to E'$ has a unique dual isogeny $\widehat{\varphi}\colon E' \to E$ characterized by $\widehat{\varphi} \circ \varphi = [\deg \varphi]$ and $\varphi \circ \widehat{\varphi} = [\deg \varphi]$.

- Computing the dual is practically always efficient.

Isogeny kernels

For any finite subgroup G of E, there exists a unique[1] separable isogeny $\varphi_G : E \to E'$ with kernel G.

The curve E' is denoted by E/G. (cf. quotient groups)

[1] (up to isomorphism of E')

Isogeny kernels

For any finite subgroup G of E, there exists a unique[1] separable isogeny $\varphi_G : E \to E'$ with kernel G.

The curve E' is denoted by E/G. (cf. quotient groups)

Vélu '71:
Formulas for computing E/G and evaluating φ_G at a point.

[1] (up to isomorphism of E')

Let’s talk about SIDH

Let's talk about ~~SIDH~~ the minimum set of knowledge about SIDH required to understand how to break it

SIDH: Bob's key-recovery problem

Fixed public data:

- Some large prime $p = 2^a 3^b - 1$.
- A particular starting curve E_0 defined over $\mathbb{F}_{p^2}$.
- Two points P_0, Q_0 on E_0 such that $E_0[2^a] = \langle P_0 \rangle + \langle Q_0 \rangle$.
  (In other words: a basis of the 2^a-torsion on E_0.)

SIDH: Bob's key-recovery problem

Fixed public data:

- Some large prime $p = 2^a 3^b - 1$.
- A particular starting curve E_0 defined over $\mathbb{F}_{p^2}$.
- Two points P_0, Q_0 on E_0 such that $E_0[2^a] = \langle P_0 \rangle + \langle Q_0 \rangle$.
  (In other words: a basis of the 2^a-torsion on E_0.)

Bob's *secret* key:

- An isogeny $\varphi : E_0 \to E$ of degree 3^b.

SIDH: Bob's key-recovery problem

Fixed public data:

- Some large prime $p = 2^a 3^b - 1$.
- A particular starting curve E_0 defined over $\mathbb{F}_{p^2}$.
- Two points P_0, Q_0 on E_0 such that $E_0[2^a] = \langle P_0 \rangle + \langle Q_0 \rangle$.
  (In other words: a basis of the 2^a-torsion on E_0.)

Bob's *secret* key:

- An isogeny $\varphi : E_0 \to E$ of degree 3^b.

Bob's public key:

- The codomain curve E.
- The images $P = \varphi(P_0)$ and $Q = \varphi(Q_0)$ of P_0, Q_0.

Extending φ to the 2^a-torsion!

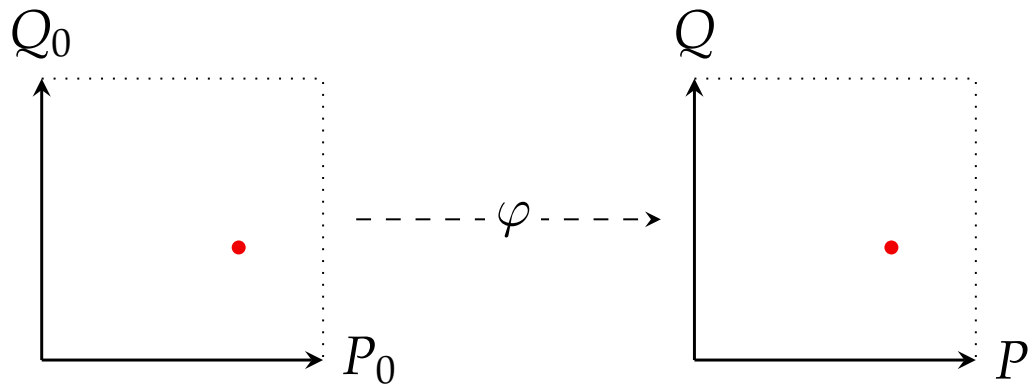
Recall:

- Given P_0, Q_0 and $P = \varphi(P_0)$ and $Q = \varphi(Q_0)$.
- The map φ is a group homomorphism.

Extending φ to the 2^a-torsion!

Recall:

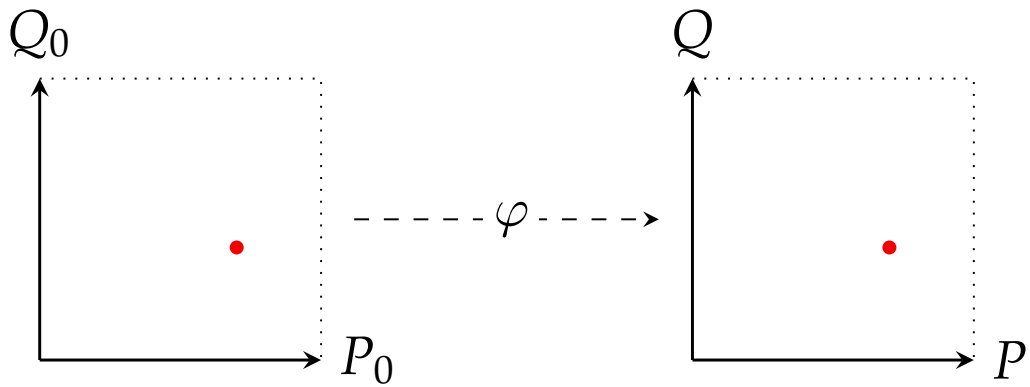
- Given P_0, Q_0 and $P = \varphi(P_0)$ and $Q = \varphi(Q_0)$.
- The map φ is a group homomorphism.



Extending φ to the 2^a-torsion!

Recall:

- Given P_0, Q_0 and $P = \varphi(P_0)$ and $Q = \varphi(Q_0)$.
- The map φ is a group homomorphism.



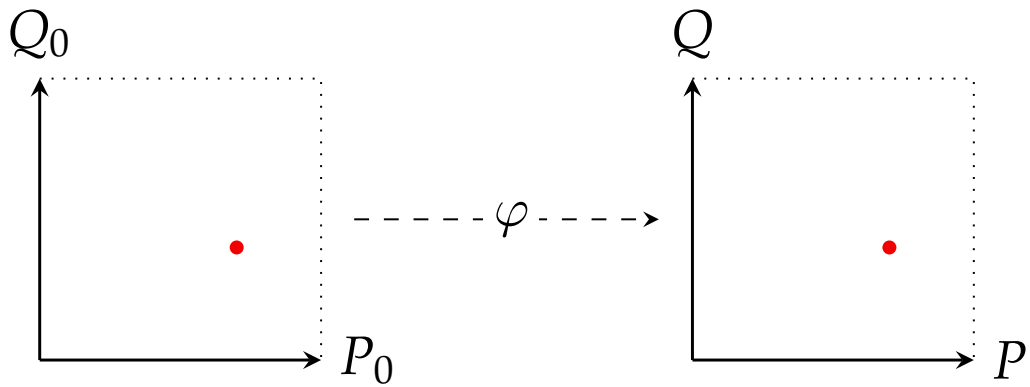
Evaluating φ at an arbitrary point $T \in E_0[2^a]$:

1. Decompose $T = [u]P_0 + [v]Q_0$ with $u, v \in \mathbb{Z}$.
   This is a DLP-like computation, which is easy because 2^a is smooth!
2. Output $[u]P + [v]Q$.

Extending φ to the 2^a-torsion!

Recall:

- Given P_0, Q_0 and $P = \varphi(P_0)$ and $Q = \varphi(Q_0)$.
- The map φ is a group homomorphism.



Evaluating φ at an arbitrary point $T \in E_0[2^a]$:

1. Decompose $T = [u]P_0 + [v]Q_0$ with $u, v \in \mathbb{Z}$.
   This is a DLP-like computation, which is easy because 2^a is smooth!
2. Output $[u]P + [v]Q$.

$\Longrightarrow$ Effectively "have" the *restriction* $\varphi|_{E_0[2^a]}$ to the 2^a-torsion.

Extending φ to the 3^b-torsion??

Suppose we could evaluate φ on the 3^b-torsion.

Extending φ to the 3^b-torsion??

Suppose we could evaluate φ on the 3^b-torsion.

Then, can simply compute $\ker \widehat{\varphi} = \varphi(E_0[3^b])$ (two evaluations) to find $\widehat{\varphi}$ and hence φ.

Proof: Exercise :-)

Extending φ to the 3^b-torsion??

Suppose we could evaluate φ on the 3^b-torsion.

Then, can simply compute $\ker \widehat{\varphi} = \varphi(E_0[3^b])$ (two evaluations) to find $\widehat{\varphi}$ and hence φ. Proof: Exercise :-)

Group theory says no: There's an isomorphism of groups

$$E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2^a)^2 \times (\mathbb{Z}/3^b)^2 .$$

Extending φ to the 3^b-torsion??

Suppose we could evaluate φ on the 3^b-torsion.

Then, can simply compute $\ker \widehat{\varphi} = \varphi(E_0[3^b])$ (two evaluations) to find $\widehat{\varphi}$ and hence φ. Proof: Exercise :-)

Group theory says no: There's an isomorphism of groups

$$E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2^a)^2 \times (\mathbb{Z}/3^b)^2 .$$

$\Longrightarrow$ can't learn anything about 3^b from 2^a using groups alone.

Attack idea: Interpolation?

- Recall: Isogenies are rational maps.
  We know enough input-output pairs to determine the map.

$\rightsquigarrow$ Rational-function interpolation?

Attack idea: Interpolation?

- Recall: Isogenies are rational maps.
  We know enough input-output pairs to determine the map.

$\rightsquigarrow$ Rational-function interpolation?

$\therefore$ ...the polynomials are of exponential degree $\approx \sqrt{p}$.

$\rightsquigarrow$ can't even write down the result without decomposing into a sequence of smaller-degree maps.

Attack idea: Interpolation?

- Recall: Isogenies are rational maps.
  We know enough input-output pairs to determine the map.

$\rightsquigarrow$ Rational-function interpolation?

$\therefore$ ...the polynomials are of exponential degree $\approx \sqrt{p}$.

$\rightsquigarrow$ can't even write down the result without decomposing into a sequence of smaller-degree maps.

- No known algorithms for interpolating and decomposing at the same time.
  - Also unlikely to exist...

The attack

Gluing elliptic curves

Main tool:

Computing isogenies of *products* of elliptic curves

Gluing elliptic curves

Main tool:

Computing isogenies of *products* of elliptic curves

- The product $E \times E'$ is an abelian *surface*.
  Compare: A product of two lines is a plane!

Gluing elliptic curves

Main tool:

Computing isogenies of *products* of elliptic curves

- The product $E \times E'$ is an abelian *surface*.
  Compare: A product of two lines is a plane!
- Similar to elliptic curves in many ways:
  - Points form an abelian group.
  - Similar group structure, but more components.
  - Can define isogenies from kernel subgroups.

Gluing elliptic curves

Main tool:

Computing isogenies of *products* of elliptic curves

- The product $E \times E'$ is an abelian *surface*.
  Compare: A product of two lines is a plane!
- Similar to elliptic curves in many ways:
  - Points form an abelian group.
  - Similar group structure, but more components.
  - Can define isogenies from kernel subgroups.
- Computing with surfaces explicitly is possible, but painful.
  Everyone works with Jacobians of genus-2 curves instead.

Splitting abelian surfaces

Fact:

Almost all abelian surfaces are *not products*.

Splitting abelian surfaces

Fact:

Almost all abelian surfaces are *not products*.

$\Longrightarrow$ Generic isogenies from $E \times E'$ will almost never lead to another product $E'' \times E'''$.

Splitting abelian surfaces

Fact:

Almost all abelian surfaces are *not products*.

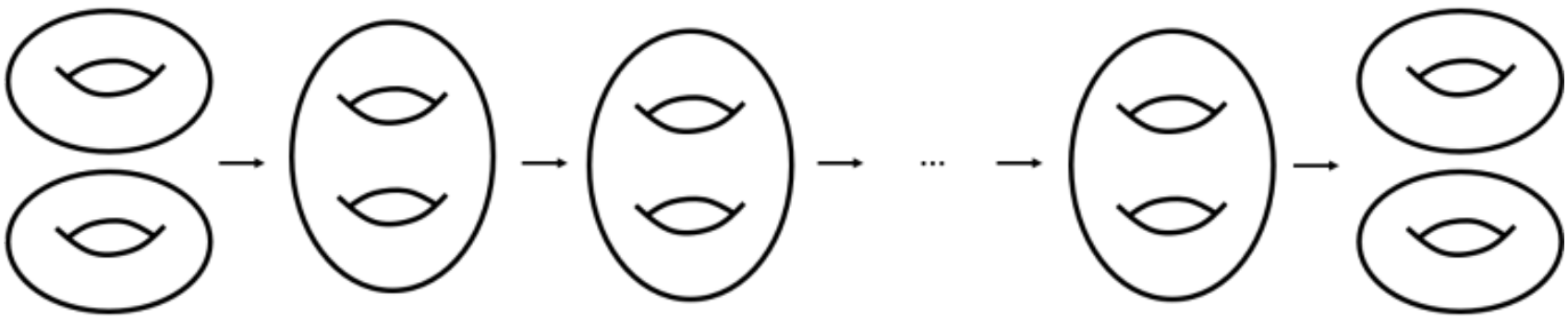
$\Longrightarrow$ Generic isogenies from $E \times E'$ will almost never lead to another product $E'' \times E'''$. But they can!

Splitting abelian surfaces

Fact:

Almost all abelian surfaces are *not products*.

$\Longrightarrow$ Generic isogenies from $E \times E'$ will almost never lead to another product $E'' \times E'''$. But they can!



Picture: Castryck–Decru

Kani's theorem

Let $\varphi : E_0 \to E$ (as in SIDH) and $\gamma : E_0 \to C$.

Kani's theorem

Let $\varphi : E_0 \to E$ (as in SIDH) and $\gamma : E_0 \to C$.

Kani [my academic granduncle!]

Kani's theorem

Let $\varphi\colon E_0 \to E$ (as in SIDH) and $\gamma\colon E_0 \to C$.

Kani [my academic granduncle!] showed **in 1997**:

Kani's theorem

Let $\varphi\colon E_0 \to E$ (as in SIDH) and $\gamma\colon E_0 \to C$.

Kani [my academic granduncle!] showed **in 1997**: (paraphrased)

Suppose $\gcd(\deg\varphi, \deg\gamma) = 1$ and write $N = \deg\varphi + \deg\gamma$.
The subgroup

$$H := \left\{ \big(\varphi(T), \gamma(T)\big) \;\middle|\; T \in E_0[N] \right\}$$

is the kernel of an (N, N)-isogeny

$$\rho\colon E \times C \longrightarrow E_0 \times C'.$$

Kani's theorem

Let $\varphi\colon E_0 \to E$ (as in SIDH) and $\gamma\colon E_0 \to C$.

Kani [my academic granduncle!] showed **in 1997**: (paraphrased)

Suppose $\gcd(\deg\varphi, \deg\gamma) = 1$ and write $N = \deg\varphi + \deg\gamma$.
The subgroup

$$H := \left\{ \left(\varphi(T), \gamma(T)\right) \;\middle|\; T \in E_0[N] \right\}$$

is the kernel of an (N, N)-isogeny

$$\rho\colon E \times C \longrightarrow E_0 \times C'.$$

Notice that we may choose γ freely.

Kani's theorem

Let $\varphi\colon E_0 \to E$ (as in SIDH) and $\gamma\colon E_0 \to C$.

Kani [my academic granduncle!] showed **in 1997**: (paraphrased)

Suppose $\gcd(\deg\varphi, \deg\gamma) = 1$ and write $N = \deg\varphi + \deg\gamma$. The subgroup

$$H := \left\{ \left(\varphi(T), \gamma(T)\right) \;\middle|\; T \in E_0[N] \right\}$$

is the kernel of an (N, N)-isogeny

$$\rho\colon E \times C \longrightarrow E_0 \times C'.$$

Notice that we may choose γ freely.

Crucial observation: If $N \mid 2^a$, we can compute H from $\varphi|_{E_0[2^a]}$!

Complications...

"Tiny" problem: Ideally we'd want $N = 2^a$, so $\deg \gamma = 2^a - 3^b$.

Complications...

"Tiny" problem: Ideally we'd want $N = 2^a$, so $\deg \gamma = 2^a - 3^b$.

But computing isogenies of large prime degree is expensive, and there is no reason for $2^a - 3^b$ to be smooth.

Complications...

"Tiny" problem: Ideally we'd want $N = 2^a$, so $\deg \gamma = 2^a - 3^b$.

But computing isogenies of large prime degree is expensive, and there is no reason for $2^a - 3^b$ to be smooth.

- Castryck–Decru: Choose an endomorphism of E_0 for γ.
  Efficient, but only works for "special" E_0 (which includes SIKE's choice).

Complications...

"Tiny" problem: Ideally we'd want $N = 2^a$, so $\deg \gamma = 2^a - 3^b$.

But computing isogenies of large prime degree is expensive, and there is no reason for $2^a - 3^b$ to be smooth.

- Castryck–Decru: Choose an endomorphism of E_0 for γ.
  Efficient, but only works for "special" E_0 (which includes SIKE's choice).
- Maino–Martindale: Pay with brute force for some more flexibility in the choice of $\deg \gamma$. Then hope for the best.
  "The best" is not great: Subexponential complexity, very painful in practice.

Complications...

"Tiny" problem: Ideally we'd want $N = 2^a$, so $\deg \gamma = 2^a - 3^b$.

But computing isogenies of large prime degree is expensive, and there is no reason for $2^a - 3^b$ to be smooth.

- Castryck–Decru: Choose an endomorphism of E_0 for γ.
  Efficient, but only works for "special" E_0 (which includes SIKE's choice).
- Maino–Martindale: Pay with brute force for some more flexibility in the choice of $\deg \gamma$. Then hope for the best.
  "The best" is not great: Subexponential complexity, very painful in practice.

(Actually, the CD attack also involves a tiny bit of brute force for reasons I'll sweep under the rug. One consequence is that in the actual attack we'll have $\deg \gamma = 2^a - 3^{b-\beta}$ for a small β, but I'm pretending $\beta = 0$ for simplicity.)

The “shortcut” attack

The original CD attack uses Kani’s theorem as a decision oracle: Guessing part of $\varphi|_{E_0[3^b]}$ wrong causes the splitting to fail.

The "shortcut" attack

The original CD attack uses Kani's theorem as a decision oracle: Guessing part of $\varphi|_{E_0[3^b]}$ wrong causes the splitting to fail.

Better: The ρ from Kani has the very explicit description

$$\rho\colon E \times C \longrightarrow E_0 \times C'$$
$$\rho(X, Y) = \big(\widehat{\varphi}(X) + \widehat{\gamma}(Y), \gamma'(X) - \varphi'(Y)\big)$$

where φ', γ' fit into the diagram:

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi} & E \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\gamma'} \\ C & \xrightarrow[\varphi']{} & C' \end{array}$$

The "shortcut" attack

The original CD attack uses Kani's theorem as a decision oracle:
Guessing part of $\varphi|_{E_0[3^b]}$ wrong causes the splitting to fail.

Better: The ρ from Kani has the very explicit description

$$\rho\colon E \times C \longrightarrow E_0 \times C'$$
$$\rho(X, Y) = \big(\widehat{\varphi}(X) + \widehat{\gamma}(Y), \gamma'(X) - \varphi'(Y)\big)$$

where φ', γ' fit into the diagram:

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi} & E \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\gamma'} \\ C & \xrightarrow[\varphi']{} & C' \end{array}$$

$\Longrightarrow$ We can simply evaluate $\widehat{\varphi}$ by computing $\rho(X, 0)$!

$\Longrightarrow$ As before: Evaluate on basis of $E[2^a]$ to find $\ker \varphi$.

Robert's generalization

Soon after: Unconditional polynomial-time attack [ePrint 2022/1038]

Robert's generalization

Soon after: Unconditional polynomial-time attack [ePrint 2022/1038]

- Based on gluing *even more* copies of E_0 and E!

Robert's generalization

Soon after: Unconditional polynomial-time attack [ePrint 2022/1038]

- Based on gluing *even more* copies of E_0 and E!
- Going to **dimension 8** adjoins enough freedom.
  - Example: *Every* $E \times E \times E \times E$ has an endomorphism of *any* degree.
    (Uses sum-of-four-squares theorem and quaternions! So cool!)

Robert's generalization

Soon after: Unconditional polynomial-time attack [ePrint 2022/1038]

- Based on gluing *even more* copies of E_0 and E!
- Going to **dimension 8** adjoins enough freedom.
  - Example: *Every* $E \times E \times E \times E$ has an endomorphism of *any* degree.
    (Uses sum-of-four-squares theorem and quaternions! So cool!)

The endomorphism of $E_0^4 \times E^4$:

$$\begin{pmatrix}
t & u & v & w & \varphi & 0 & 0 & 0 \\
-u & t & -w & v & 0 & \varphi & 0 & 0 \\
-v & w & t & -u & 0 & 0 & \varphi & 0 \\
-w & -v & u & t & 0 & 0 & 0 & \varphi \\
-\widehat{\varphi} & 0 & 0 & 0 & t & -u & -v & -w \\
0 & -\widehat{\varphi} & 0 & 0 & u & t & w & -v \\
0 & 0 & -\widehat{\varphi} & 0 & v & -w & t & u \\
0 & 0 & 0 & -\widehat{\varphi} & w & v & -u & t
\end{pmatrix}$$

Robert's generalization

Soon after: Unconditional polynomial-time attack [ePrint 2022/1038]

- Based on gluing *even more* copies of E_0 and E!
- Going to **dimension 8** adjoins enough freedom.
  - Example: *Every* $E \times E \times E \times E$ has an endomorphism of *any* degree.
    (Uses sum-of-four-squares theorem and quaternions! So cool!)

The endomorphism of $E_0^4 \times E^4$:

$$\begin{pmatrix}
t & u & v & w & \varphi & 0 & 0 & 0 \\
-u & t & -w & v & 0 & \varphi & 0 & 0 \\
-v & w & t & -u & 0 & 0 & \varphi & 0 \\
-w & -v & u & t & 0 & 0 & 0 & \varphi \\
-\widehat{\varphi} & 0 & 0 & 0 & t & -u & -v & -w \\
0 & -\widehat{\varphi} & 0 & 0 & u & t & w & -v \\
0 & 0 & -\widehat{\varphi} & 0 & v & -w & t & u \\
0 & 0 & 0 & -\widehat{\varphi} & w & v & -u & t
\end{pmatrix}$$

- Core trick: *Embedding lemma*.
  This also has cool constructive applications! [ePrints 2022/1068 and 2022/1704]

Robert's generalization

Soon after: Unconditional polynomial-time attack [ePrint 2022/1038]

- Based on gluing *even more* copies of E_0 and E!
- Going to **dimension 8** adjoins enough freedom.
  - Example: *Every* $E \times E \times E \times E$ has an endomorphism of *any* degree.
    (Uses sum-of-four-squares theorem and quaternions! So cool!)

The endomorphism of $E_0^4 \times E^4$:

$$\begin{pmatrix}
t & u & v & w & \varphi & 0 & 0 & 0 \\
-u & t & -w & v & 0 & \varphi & 0 & 0 \\
-v & w & t & -u & 0 & 0 & \varphi & 0 \\
-w & -v & u & t & 0 & 0 & 0 & \varphi \\
-\widehat{\varphi} & 0 & 0 & 0 & t & -u & -v & -w \\
0 & -\widehat{\varphi} & 0 & 0 & u & t & w & -v \\
0 & 0 & -\widehat{\varphi} & 0 & v & -w & t & u \\
0 & 0 & 0 & -\widehat{\varphi} & w & v & -u & t
\end{pmatrix}$$

- Core trick: *Embedding lemma*.
  This also has cool constructive applications! [ePrints 2022/1068 and 2022/1704]

!! These are theoretical results. Currently totally impractical.

Closing remark

Closing remark

What if (say) ECDLP is equally broken and noone has noticed??

Closing remark

What if (say) ECDLP is equally broken and noone has noticed??

Thank you!