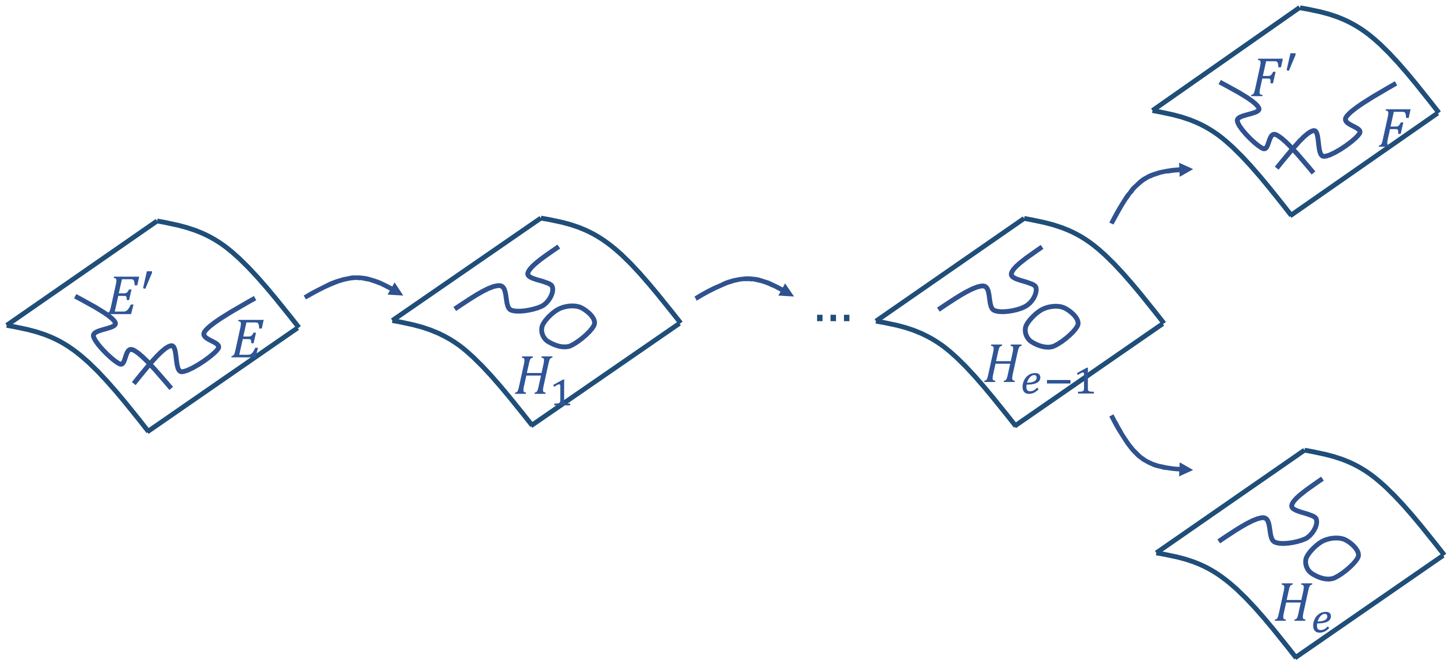
An efficient key recovery attack on SIKE

(and the future of isogeny-based cryptography)

j.w. Thomas Decru

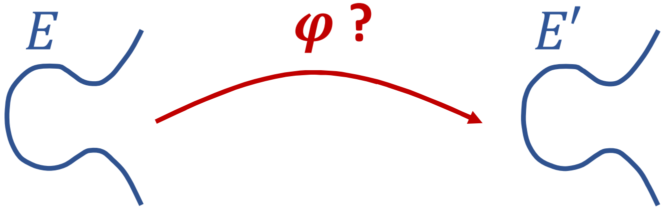


9th ETSI/IQC Quantum Safe Cryptography Event, 15 February 2023

1. Quick overview

SIKE: Supersingular Isogeny Key Encapsulation

- certain kind of map between elliptic curves



- in general: very hard to find such a map explicitly, even for quantum computers
- problem lies at the root of isogeny-based cryptography

1. Quick overview

1997—2006: prehistory of isogeny-based cryptography

main legacy: CRS key exchange (inefficient drop-in for Diffie-Hellman)

2009: Childs, Jao and Soukharev find sub-exponential time quantum attack on CRS

2011: Jao and De Feo respond with Supersingular Isogeny Diffie-Hellman (SIDH)

2016: SIKE (= concrete instance of SIDH) submitted to NIST PQ Crypto competition

✓

- best attacks (until 2022): exponential
- good efficiency
- very low bandwidth requirements
- diversification: does not rely on “noisy linear algebra”
- within expertise of existing ECC community

1. Quick overview

1997—2006: prehistory of isogeny-based cryptography

main legacy: CRS key exchange (inefficient drop-in for Diffie-Hellman)

2009: Childs, Jao and Soukharev find sub-exponential time quantum attack on CRS

2011: Jao and De Feo respond with Supersingular Isogeny Diffie-Hellman (SIDH)

2016: SIKE (= concrete instance of SIDH) submitted to NIST PQ Crypto competition

✘

- ➢ isogeny-based cryptography = exotic new field
- ➢ impure isogeny problem

1. Quick overview

1997—2006: prehistory of isogeny-based cryptography

main legacy: CRS key exchange (inefficient drop-in for Diffie-Hellman)

2009: Childs, Jao and Soukharev find sub-exponential time quantum attack on CRS

2011: Jao and De Feo respond with Supersingular Isogeny Diffie-Hellman (SIDH)

2016: SIKE (= concrete instance of SIDH) submitted to NIST PQ Crypto competition

2019: SIKE advances to round 2

2020: SIKE becomes 'alternate' finalist

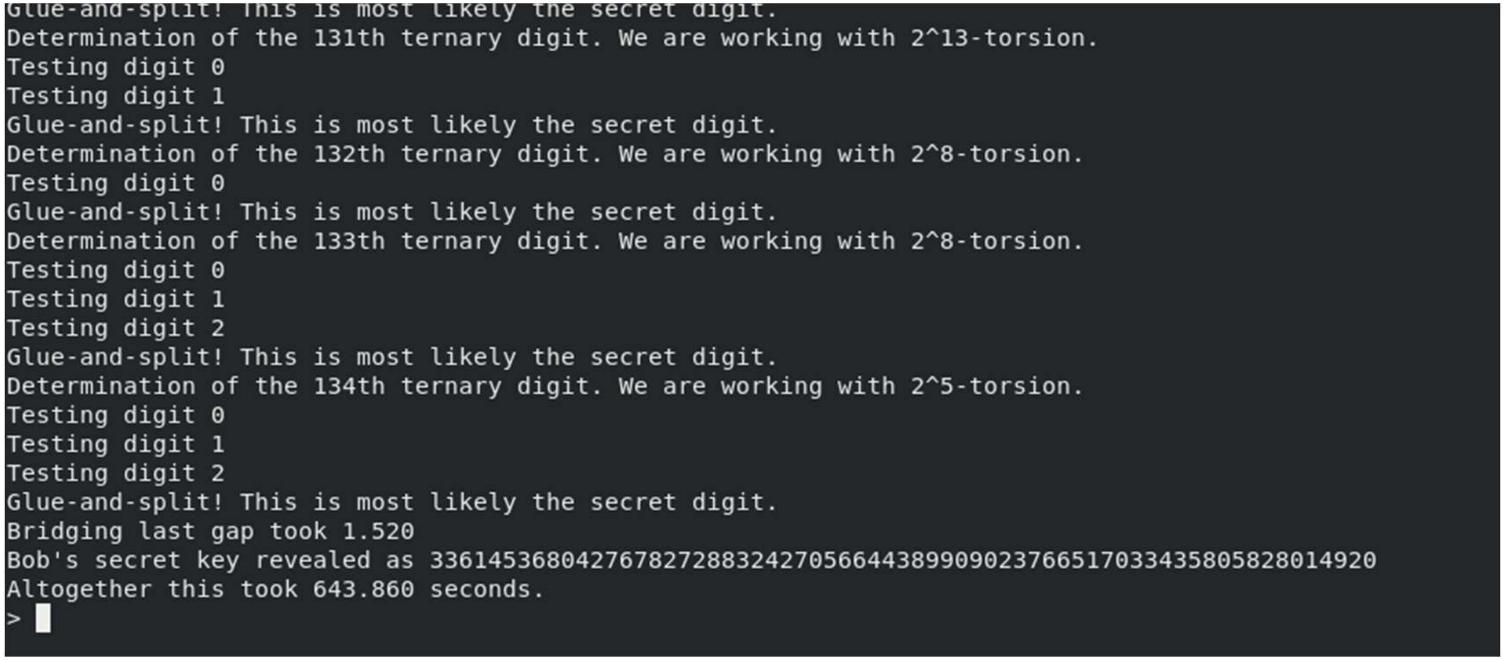
5 July 2022: SIKE advances to round 4

± two weeks later: we find an efficient break of SIKE

... quickly followed by Maino—Martindale, Wesolowski, Robert
who show that SIDH cannot be (easily) reanimated

1. Quick overview

Screenshot from run on **SIKEp434** targetting NIST level 1 security:



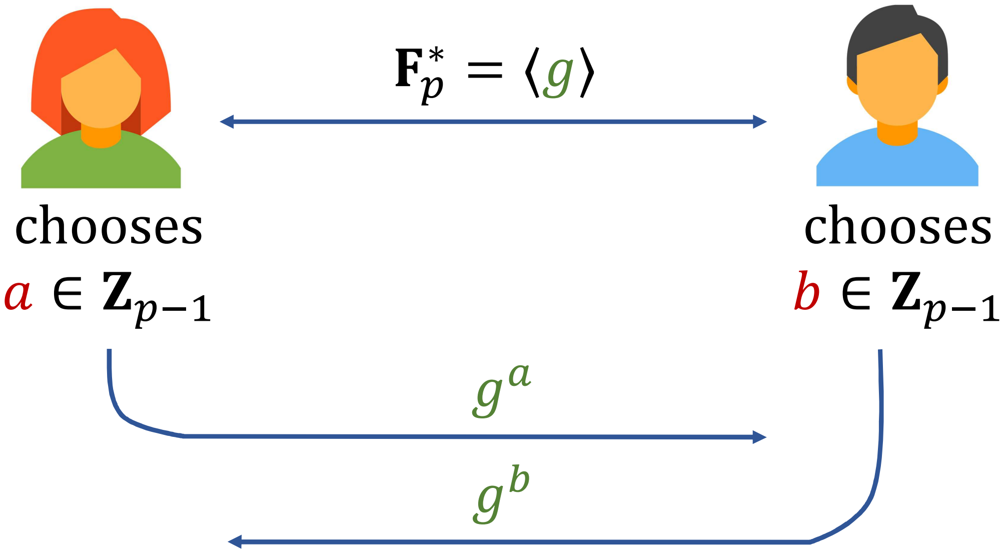
```
Glue-and-split! This is most likely the secret digit.
Determination of the 131th ternary digit. We are working with 2^13-torsion.
Testing digit 0
Testing digit 1
Glue-and-split! This is most likely the secret digit.
Determination of the 132th ternary digit. We are working with 2^8-torsion.
Testing digit 0
Glue-and-split! This is most likely the secret digit.
Determination of the 133th ternary digit. We are working with 2^8-torsion.
Testing digit 0
Testing digit 1
Testing digit 2
Glue-and-split! This is most likely the secret digit.
Determination of the 134th ternary digit. We are working with 2^5-torsion.
Testing digit 0
Testing digit 1
Testing digit 2
Glue-and-split! This is most likely the secret digit.
Bridging last gap took 1.520
Bob's secret key revealed as 33614536804276782728832427056644389909023766517033435805828014920
Altogether this took 643.860 seconds.
> █
```

Average timings on single core using 10-year old PC:

- **SIKEp434** (NIST level 1): ≈ 11 minutes

2. Supersingular Isogeny Diffie-Hellman (SIDH)

Classical Diffie-Hellman (1976):



$\mathbf{F}_p^* = \langle g \rangle$

chooses $a \in \mathbf{Z}_{p-1}$

chooses $b \in \mathbf{Z}_{p-1}$

g^a

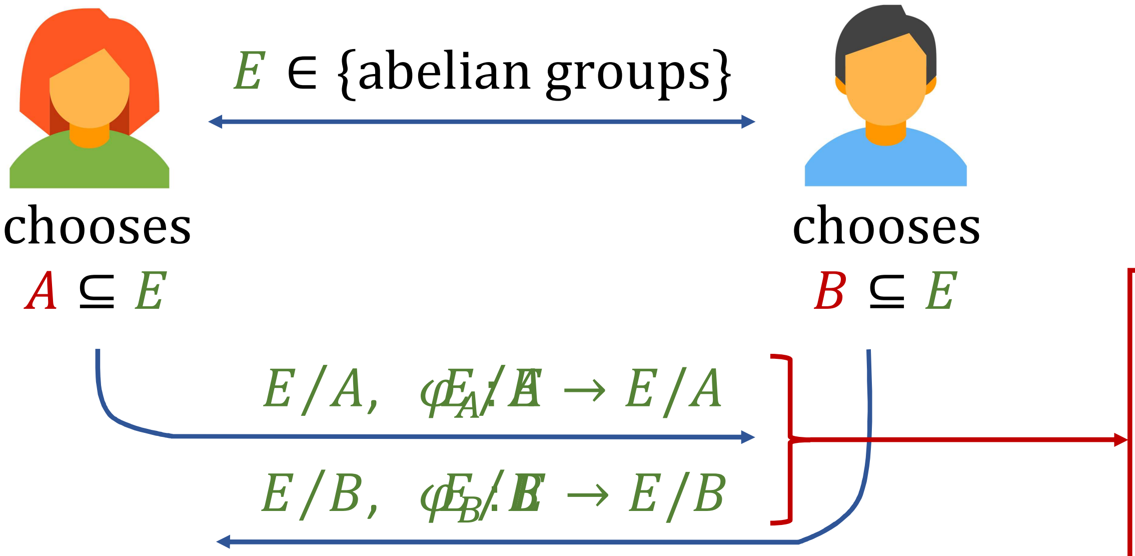
g^b

common secret:

$$\left(g^b\right)^a = g^{ab} = \left(g^a\right)^b$$

2. Supersingular Isogeny Diffie-Hellman (SIDH)

Jao, De Feo 2011: can we do Diffie-Hellman with subgroups and quotients?



$E \in \{\text{abelian groups}\}$

chooses $A \subseteq E$

chooses $B \subseteq E$

$E/A, \ \varphi_A: E \to E/A$

$E/B, \ \varphi_B: E \to E/B$

Problem! This reveals

$$A = \ker \varphi_A$$

$$B = \ker \varphi_B$$

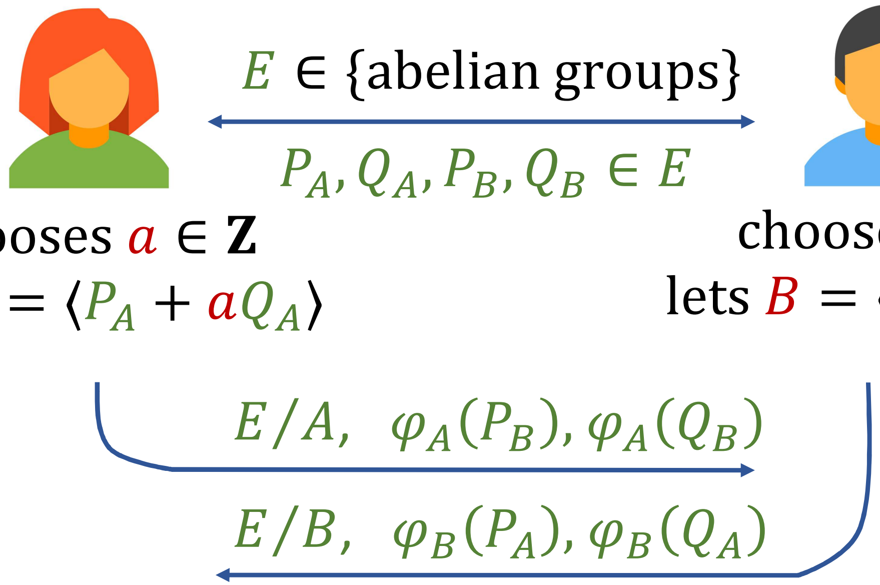
? **?**

common secret:

$$(E/B)/\varphi_B(A) \cong E/(A+B) \cong (E/A)/\varphi_A(B)$$

2. Supersingular Isogeny Diffie-Hellman (SIDH)

Jao, De Feo 2011: can get around this by using ‘auxiliary points’



$E \in$ {abelian groups}

$P_A, Q_A, P_B, Q_B \in E$

chooses $a \in \mathbf{Z}$
lets $A = \langle P_A + aQ_A \rangle$

chooses $b \in \mathbf{Z}$
lets $B = \langle P_B + bQ_B \rangle$

$E/A, \;\; \varphi_A(P_B), \varphi_A(Q_B)$

$E/B, \;\; \varphi_B(P_A), \varphi_B(Q_A)$

common secret:

$$(E/B)/\varphi_B(A) \quad \cong \quad E/(A+B) \quad \cong \quad (E/A)/\varphi_A(B)$$

Fact: Alice can compute

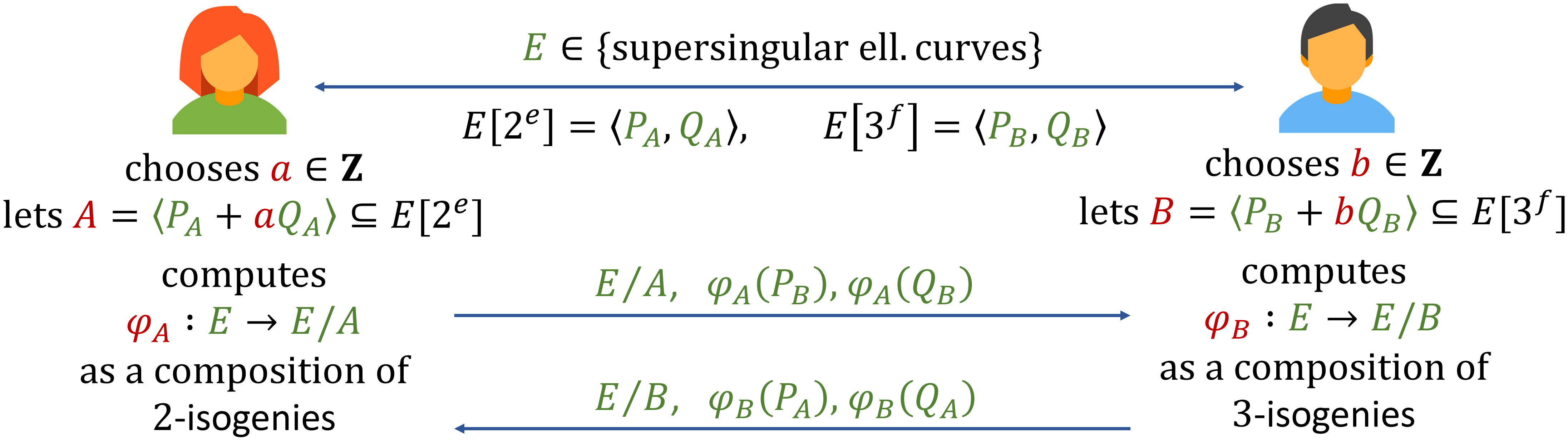
$$\varphi_B(A) = \varphi_B(\langle P_A + aQ_A \rangle)$$

as $\langle \varphi_B(P_A) + a\varphi_B(Q_A) \rangle$

(and likewise for Bob).

2. Supersingular Isogeny Diffie-Hellman (SIDH)

Jao, De Feo 2011: concrete proposal (high-level)



$E \in \{\text{supersingular ell. curves}\}$

$E[2^e] = \langle P_A, Q_A \rangle, \qquad E[3^f] = \langle P_B, Q_B \rangle$

chooses $a \in \mathbf{Z}$
lets $A = \langle P_A + aQ_A \rangle \subseteq E[2^e]$

computes
$\varphi_A : E \to E/A$
as a composition of
2-isogenies

chooses $b \in \mathbf{Z}$
lets $B = \langle P_B + bQ_B \rangle \subseteq E[3^f]$

computes
$\varphi_B : E \to E/B$
as a composition of
3-isogenies

$E/A, \ \ \varphi_A(P_B), \varphi_A(Q_B)$

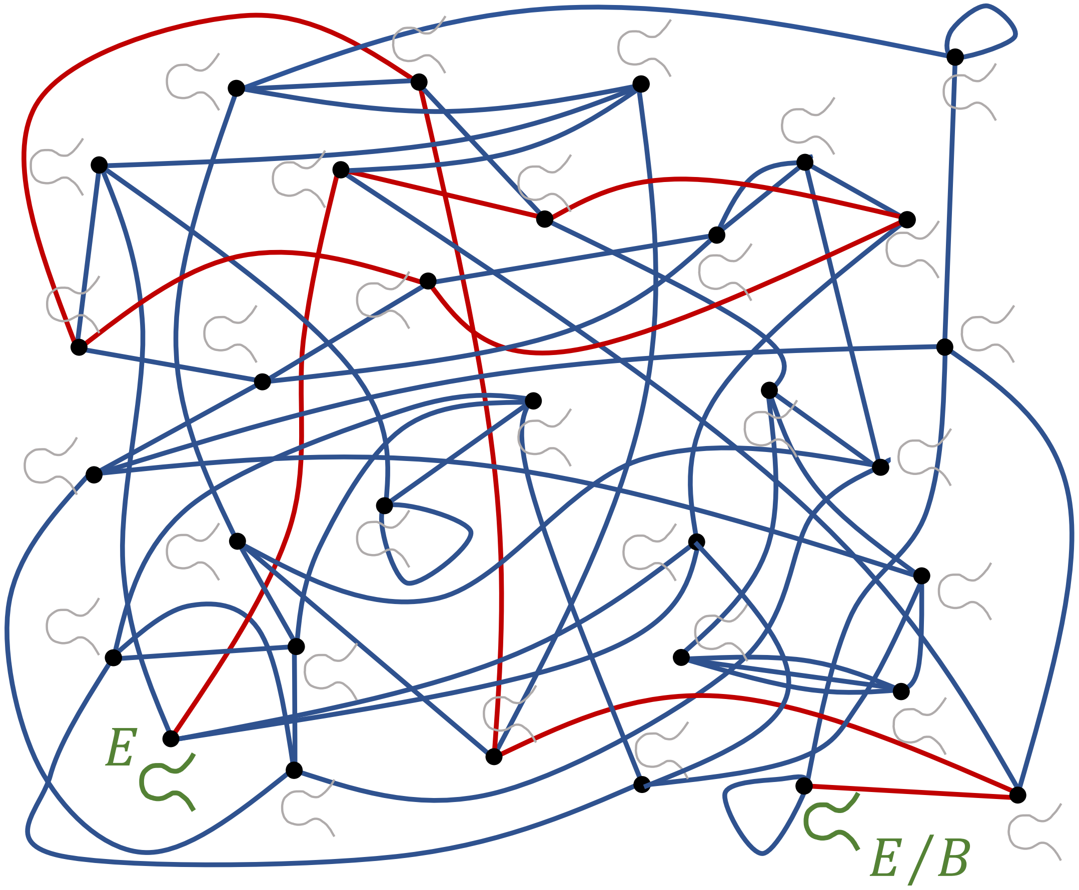
$E/B, \ \ \varphi_B(P_A), \varphi_B(Q_A)$

common secret: j-invariant of

$$(E/B)/\varphi_B(A) \quad \cong \quad E/(A+B) \quad \cong \quad (E/A)/\varphi_A(B)$$

3. Attack idea

We target Bob's secret isogeny $\varphi_B \colon E \to E/B$, which can be viewed as a secret walk in the 3-isogeny graph: can be shown to have rapid mixing



Main security reasoning: E/B is indistinguishable from a random curve, so finding isogeny is hard

However: key recovery amounts to finding φ_B (or equiv. B) when being given

$E,\ E/B,\ \varphi_B(P_A),\ \varphi_B(Q_A)$

auxiliary points make for an impure isogeny problem

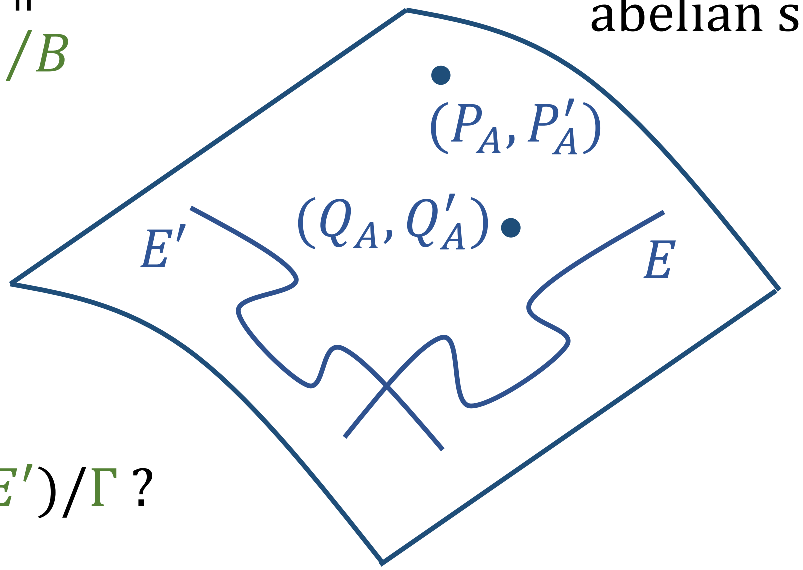
3. Attack idea

Main observation:

The auxiliary points $\varphi_B(P_A), \varphi_B(Q_A)$ allow to consider the subgroup

$$\Gamma = \langle (P_A, \underset{\overset{\shortparallel}{P_A{}'}}{\varphi_B(P_A)}), (Q_A, \underset{\overset{\shortparallel}{Q_A{}'}}{\varphi_B(Q_A)}) \rangle \subseteq E \times \overset{\overset{E'}{\shortparallel}}{E/B}$$

principally polarized abelian surface



The group Γ is isomorphic to $\frac{\mathbf{Z}}{2^e\mathbf{Z}} \times \frac{\mathbf{Z}}{2^e\mathbf{Z}}$.

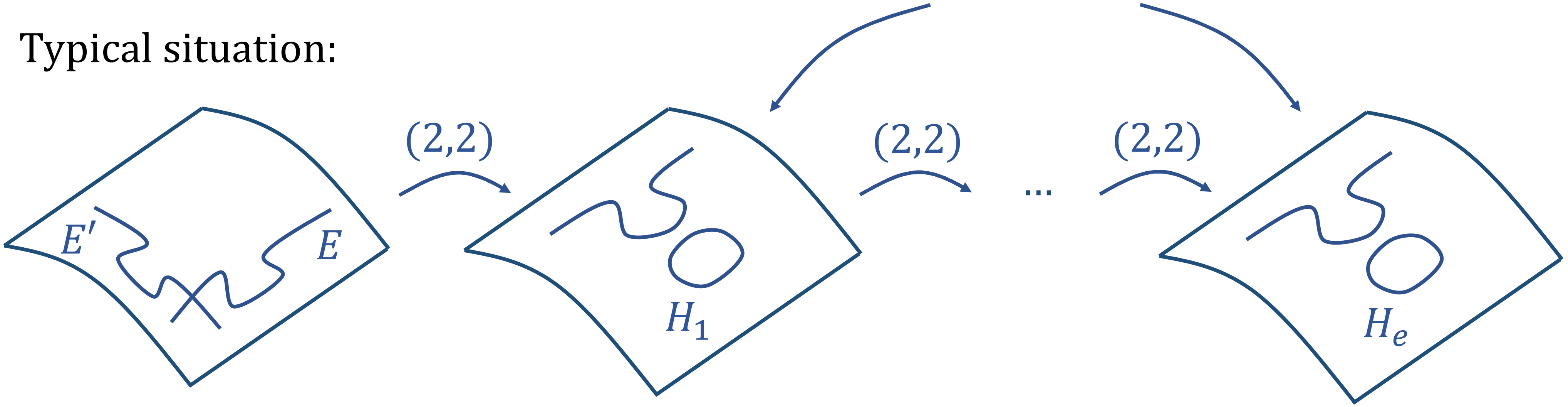
What happens if we take the quotient $(E \times E')/\Gamma$?

- composition of $(2,2)$-isogenies
- technicality swept under the rug: quotient does not always make sense

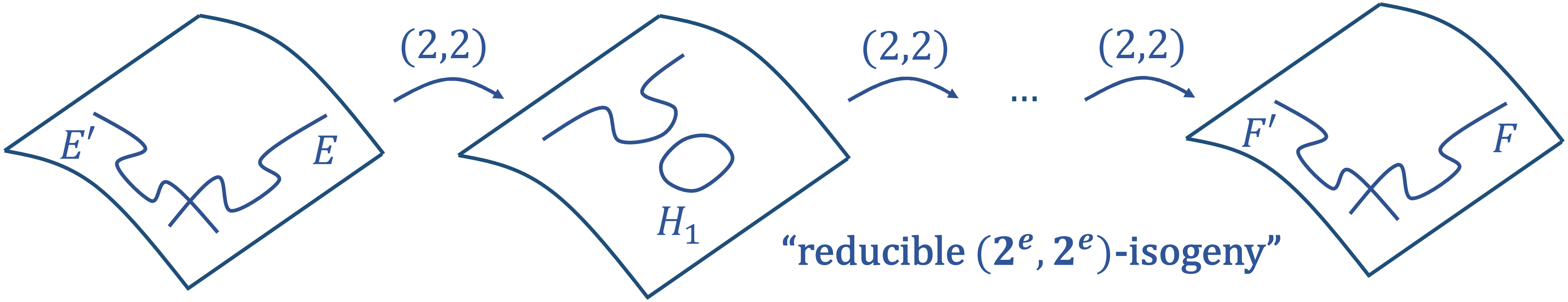
3. Attack idea

jacobians of genus-2 curves

Typical situation:



However, in very exceptional situations:



“reducible $(\mathbf{2}^e, \mathbf{2}^e)$-isogeny”

3. Attack idea

Kani's theorem from 1997 characterizes reducibility.

In our case it (roughly) says:

a $(2^e, 2^e)$-isogeny $E \times E' \to (E \times E')/G$ is reducible

$$\Updownarrow$$

$$G = \langle (P_A, \psi(P_A)), (Q_A, \psi(Q_A)) \rangle$$

with $\psi: E \to E'$ a degree $r(2^e - r)$-isogeny (for some r)

This resembles our situation: we have $\Gamma = \langle (P_A, \varphi_B(P_A)), (Q_A, \varphi_B(Q_A)) \rangle$

but $\deg \varphi_B = 3^f$ is not of the form $r(2^e - r)$...

3. Attack idea

Strategy: **force reducibility**

- Construct auxiliary isogeny γ of degree $c = 2^e - 3^f$ (assume positive)

$$\begin{tikzcd}
 & E \arrow[r, "\varphi_B"] \arrow[dl, bend right, "\gamma"'] & E' \\
C \arrow[urr, dashed, bend right] & &
\end{tikzcd}$$

P_A

Q_A

$P'_A = \varphi_B(P_A)$

$Q'_A = \varphi_B(Q_A)$

$P_C = \gamma(P_A)$

$\deg \varphi_B \circ \hat{\gamma} = 3^f\left(2^e - 3^f\right)$

$\downarrow$

$Q_C = \gamma(Q_A)$

- By Kani's theorem, the subgroup $\langle (P_C, P'_A), (Q_C, Q'_A) \rangle \subseteq C \times E'$ is reducible

  of the desired form!

- Key idea: if P'_A, Q'_A were **not** the images of P_A, Q_A under a degree-3^f isogeny, then with overwhelming probability this does **not** result in a reducible subgroup!

3. Attack idea

Leads to the following candidate-method for unveiling Bob's secret walk:

secret 3-isogenies composing to φ_B

$$\begin{tikzcd}
E \arrow[r, "\varphi_1"] \arrow[dr, dashed, "\varphi_1^?"] & E_1 \arrow[r, "\varphi_2"] & E_2 \arrow[r, "\varphi_3"] & E_3 \arrow[r, "\varphi_4"] & \cdots \arrow[r, "\varphi_{f-1}"] & E_{f-1} \arrow[r, "\varphi_f"] & E' \\
& E_1^? \arrow[urrrrr, dashed, bend right] \arrow[dl, bend left, "\text{isogeny } \gamma \text{ of degree } 2^e - 3^{f-1}"'] & & & & & \\
C & & & & & &
\end{tikzcd}$$

P_A

Q_A

$P_A' = \varphi_B(P_A)$

$Q_A' = \varphi_B(Q_A)$

$P_1^? = \varphi_1^?(P_A)$

$Q_1^? = \varphi_1^?(Q_A)$

$P_C = \gamma(P_1^?)$

$Q_C = \gamma(Q_1^?)$

if guess is correct, then:

- $E_1^?$ connected to E' via isogeny of degree 3^{f-1}
- this isogeny maps $P_1^? \mapsto P_A'$ and $Q_1^? \mapsto Q_A'$

so: **build auxiliary isogeny γ and check reducibility** of the subgroup $\langle (P_C, P_A'), (Q_C, Q_A') \rangle \subseteq C \times E'$.

3. Attack idea

Leads to the following candidate-method for unveiling Bob’s secret walk:

secret 3-isogenies composing to φ_B

$$\begin{tikzcd}
\begin{array}{c} E \\ P_A \\ Q_A \end{array} \arrow[r, "\varphi_1"] & E_1 \arrow[r, "\varphi_2"] \arrow[rd, dashed, "\varphi_2^?"] & E_2 \arrow[r, "\varphi_3"] & E_3 \arrow[r, "\varphi_4"] & {} & \cdots \arrow[r, "\varphi_{f-1}"] & E_{f-1} \arrow[r, "\varphi_f"] & \begin{array}{l} E' \\ P'_A = \varphi_B(P_A) \\ Q'_A = \varphi_B(Q_A) \end{array} \\
& & \begin{array}{l} E_2^? \\ P_2^? = \varphi_2^?(\varphi_1(P_A)) \\ Q_2^? = \varphi_2^?(\varphi_1(Q_A)) \end{array} \arrow[rrrrru, dashed, bend right] \arrow[ld, "\text{isogeny } \gamma \text{ of degree } 2^e - 3^{f-2}"'] & & & & & \\
& \begin{array}{l} C \\ P_C = \gamma(P_2^?) \\ Q_C = \gamma(Q_2^?) \end{array} & & & & & &
\end{tikzcd}$$

3. Attack idea

Leads to the following candidate-method for unveiling Bob’s secret walk:

secret 3-isogenies composing to φ_B

$$\begin{tikzcd}
\begin{array}{c}E\\P_A\\Q_A\end{array} \arrow[r, "\varphi_1"] & E_1 \arrow[r, "\varphi_2"] & E_2 \arrow[r, "\varphi_3"] \arrow[dr, dashed, "\varphi_3^?"] & E_3 \arrow[r, "\varphi_4"] & \cdots \arrow[r, "\varphi_{f-1}"] & E_{f-1} \arrow[r, "\varphi_f"] & \begin{array}{l}E'\\P_A' = \varphi_B(P_A)\\Q_A' = \varphi_B(Q_A)\end{array} \\
 & & & \begin{array}{l}E_2^?\\P_3^? = \varphi_3^?(\varphi_2(\varphi_1(P_A)))\\Q_3^? = \varphi_3^?(\varphi_2(\varphi_1(Q_A)))\end{array} \arrow[urrr, dashed, bend right] \arrow[dl, "\text{isogeny } \gamma \text{ of degree } 2^e - 3^{f-3}"'] & & & \\
 & & \begin{array}{l}C\\P_C = \gamma(P_3^?)\\Q_C = \gamma(Q_3^?)\end{array} & & & &
\end{tikzcd}$$

and so on…

4. What’s next for isogeny-based crypto?

Conclusions for isogenies:

- SIDH is dead, despite having withstood 11 years of cryptanalysis

are we rushing things?
(also Rainbow was broken early 2022)

plea for hybrid and
adaptable encryption

- no practical consequences (not in pipeline for deployment)
- finding isogenies remains a hard problem

way to rediversify post-quantum cryptography?

other schemes such as CSIDH, CSI-FiSh, SQISign, … are unaffected

next big thing in isogeny-based crypto
(most compact signatures)

Questions?

Thanks for listening!