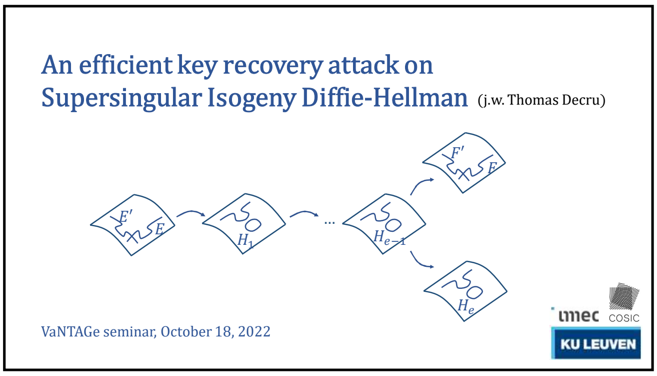


An efficient key recovery attack on Supersingular Isogeny Diffie-Hellman

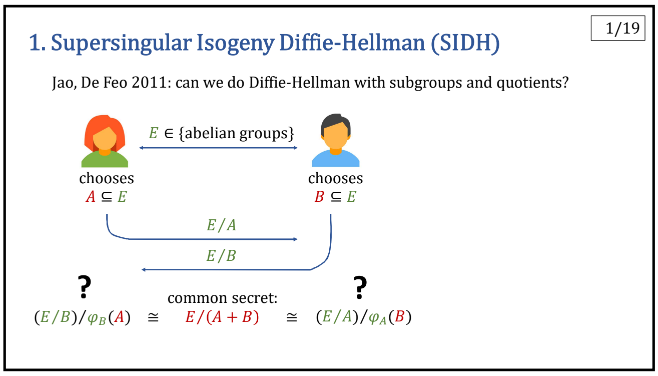
(j.w. Thomas Decru)

VaNTAGe seminar, October 18, 2022

imec COSIC

KU LEUVEN

1



1. Supersingular Isogeny Diffie-Hellman (SIDH)

1/19

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

$E \in$ {abelian groups}

chooses $A \subseteq E$

chooses $B \subseteq E$

E/A

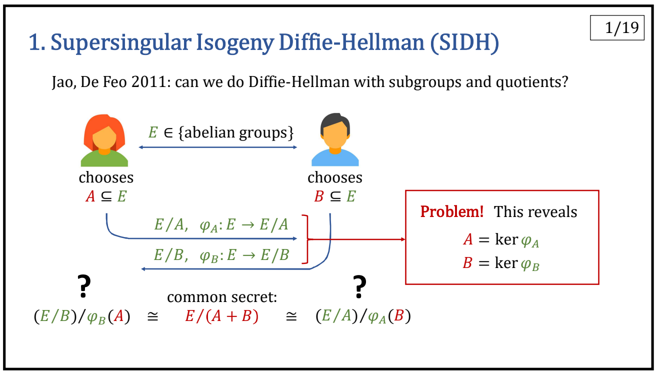
E/B

? **?**

common secret:

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

2



1. Supersingular Isogeny Diffie-Hellman (SIDH)

1/19

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

$E \in$ {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

$A = \ker \varphi_A$

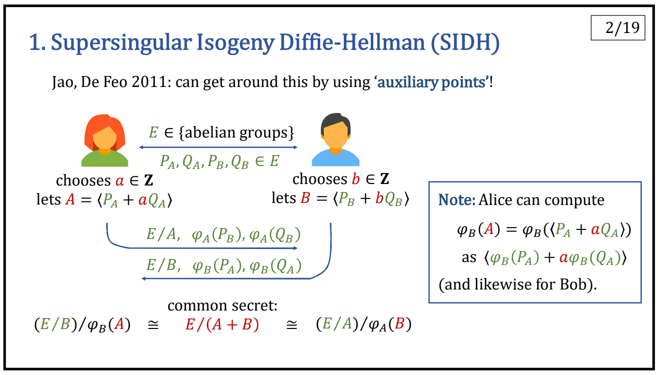
$B = \ker \varphi_B$

? **?**

common secret:

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

3



1. Supersingular Isogeny Diffie-Hellman (SIDH)

2/19

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 $B = \langle P_B + bQ_B \rangle$

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

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

Note: Alice can compute

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

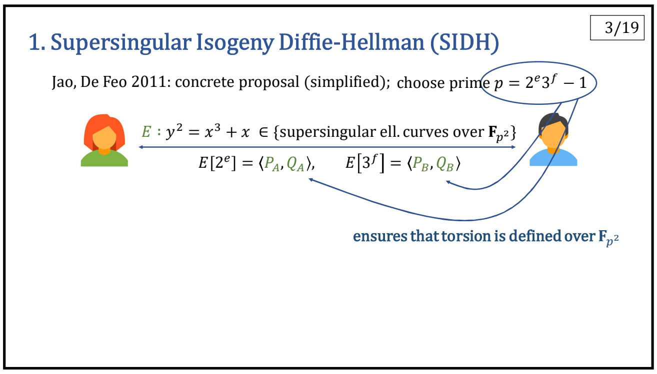
as $\langle \varphi_B(P_A) + a\varphi_B(Q_A) \rangle$

(and likewise for Bob).

common secret:

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

4



1. Supersingular Isogeny Diffie-Hellman (SIDH)

3/19

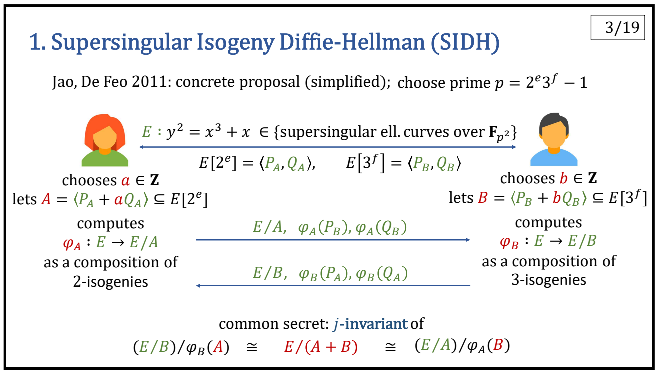
Jao, De Feo 2011: concrete proposal (simplified); choose prime $p = 2^e 3^f - 1$

$E : y^2 = x^3 + x \ \in$ {supersingular ell. curves over $\mathbf{F}_{p^2}$}

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

ensures that torsion is defined over $\mathbf{F}_{p^2}$

5



1. Supersingular Isogeny Diffie-Hellman (SIDH)

3/19

Jao, De Feo 2011: concrete proposal (simplified); choose prime $p = 2^e 3^f - 1$

$E : y^2 = x^3 + x \ \in$ {supersingular ell. curves over $\mathbf{F}_{p^2}$}

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

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

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

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

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

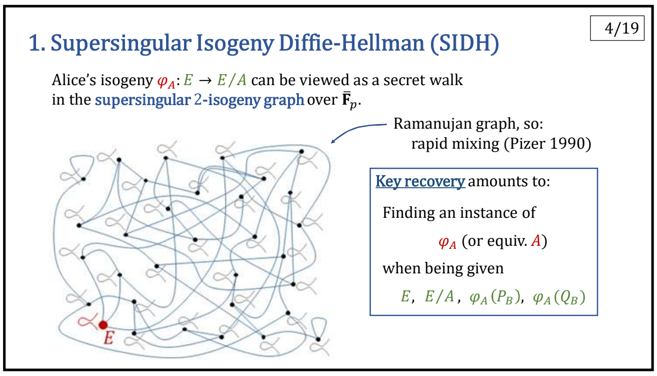
$E/B, \ \ \varphi_B(P_A), \varphi_B(Q_A)$

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

common secret: **j-invariant** of

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

6



1. Supersingular Isogeny Diffie-Hellman (SIDH)

Alice's isogeny $\varphi_A : E \to E/A$ can be viewed as a secret walk in the **supersingular 2-isogeny graph** over $\bar{\mathbf{F}}_p$.

Ramanujan graph, so:
rapid mixing (Pizer 1990)

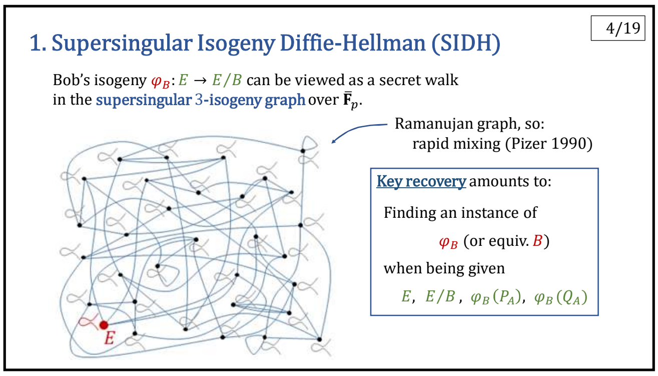
Key recovery amounts to:

Finding an instance of

φ_A (or equiv. A)

when being given

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



1. Supersingular Isogeny Diffie-Hellman (SIDH)

Bob's isogeny $\varphi_B : E \to E/B$ can be viewed as a secret walk in the **supersingular 3-isogeny graph** over $\bar{\mathbf{F}}_p$.

Ramanujan graph, so:
rapid mixing (Pizer 1990)

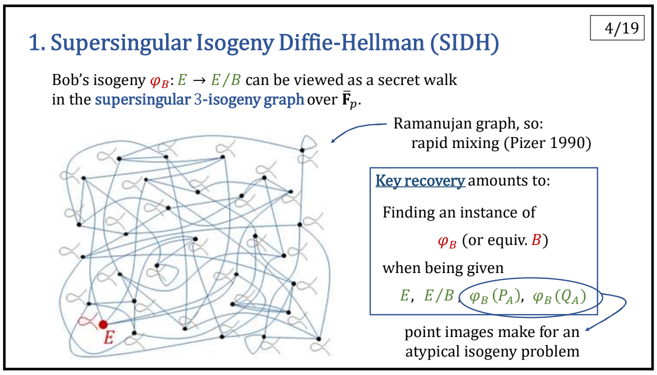
Key recovery amounts to:

Finding an instance of

φ_B (or equiv. B)

when being given

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



1. Supersingular Isogeny Diffie-Hellman (SIDH)

Bob's isogeny $\varphi_B : E \to E/B$ can be viewed as a secret walk in the **supersingular 3-isogeny graph** over $\bar{\mathbf{F}}_p$.

Ramanujan graph, so:
rapid mixing (Pizer 1990)

Key recovery amounts to:

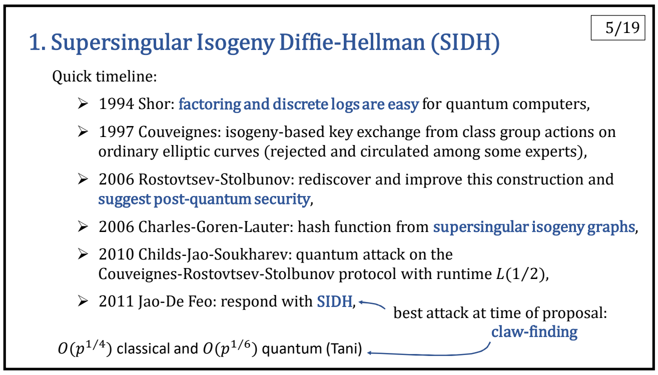
Finding an instance of

φ_B (or equiv. B)

when being given

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

point images make for an
atypical isogeny problem



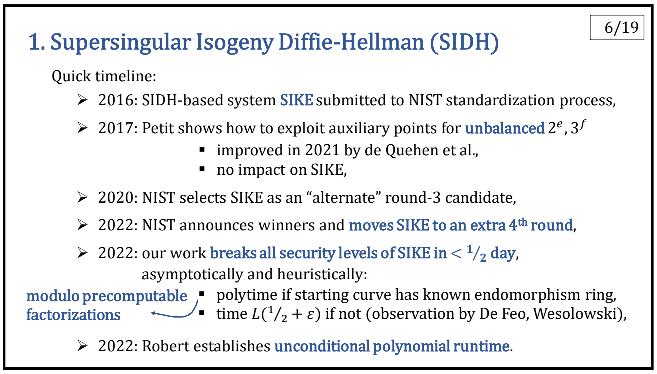
1. Supersingular Isogeny Diffie-Hellman (SIDH)

Quick timeline:

- 1994 Shor: **factoring and discrete logs are easy** for quantum computers,
- 1997 Couveignes: isogeny-based key exchange from class group actions on ordinary elliptic curves (rejected and circulated among some experts),
- 2006 Rostovtsev-Stolbunov: rediscover and improve this construction and **suggest post-quantum security**,
- 2006 Charles-Goren-Lauter: hash function from **supersingular isogeny graphs**,
- 2010 Childs-Jao-Soukharev: quantum attack on the Couveignes-Rostovtsev-Stolbunov protocol with runtime $L(1/2)$,
- 2011 Jao-De Feo: respond with **SIDH**,

best attack at time of proposal:
claw-finding

$O(p^{1/4})$ classical and $O(p^{1/6})$ quantum (Tani)

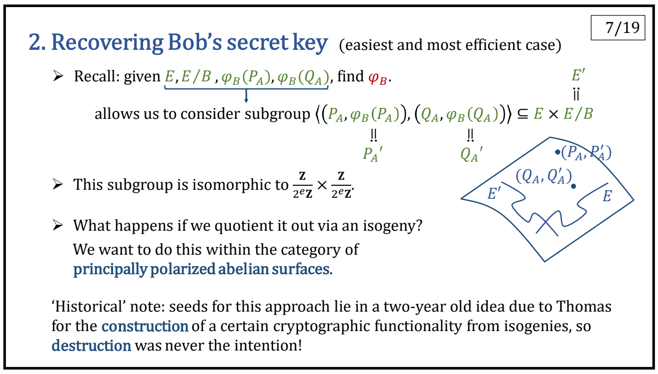


1. Supersingular Isogeny Diffie-Hellman (SIDH)

Quick timeline:

- 2016: SIDH-based system **SIKE** submitted to NIST standardization process,
- 2017: Petit shows how to exploit auxiliary points for **unbalanced** $2^e, 3^f$
  - improved in 2021 by de Quehen et al.,
  - no impact on SIKE,
- 2020: NIST selects SIKE as an "alternate" round-3 candidate,
- 2022: NIST announces winners and **moves SIKE to an extra 4th round**,
- 2022: our work **breaks all security levels of SIKE in $< {}^1/_2$ day**, asymptotically and heuristically:
  - polytime if starting curve has known endomorphism ring,
  - time $L({}^1/_2 + \varepsilon)$ if not (observation by De Feo, Wesolowski),
- 2022: Robert establishes **unconditional polynomial runtime**.

modulo precomputable factorizations



2. Recovering Bob's secret key (easiest and most efficient case)

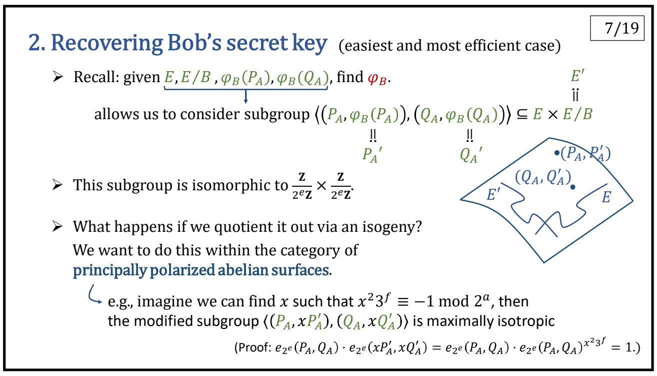
- Recall: given $\underbrace{E, E/B, \varphi_B(P_A), \varphi_B(Q_A)}$, find φ_B.

  allows us to consider subgroup $\langle (P_A, \underset{P_A'}{\underset{\shortparallel}{\varphi_B(P_A)}}), (Q_A, \underset{Q_A'}{\underset{\shortparallel}{\varphi_B(Q_A)}}) \rangle \subseteq E \times \overset{E'}{\overset{\shortparallel}{E/B}}$

- This subgroup is isomorphic to $\frac{\mathbf{Z}}{2^e\mathbf{Z}} \times \frac{\mathbf{Z}}{2^e\mathbf{Z}}$.
- What happens if we quotient it out via an isogeny?

  We want to do this within the category of **principally polarized abelian surfaces**.

'Historical' note: seeds for this approach lie in a two-year old idea due to Thomas for the **construction** of a certain cryptographic functionality from isogenies, so **destruction** was never the intention!



2. Recovering Bob's secret key (easiest and most efficient case)

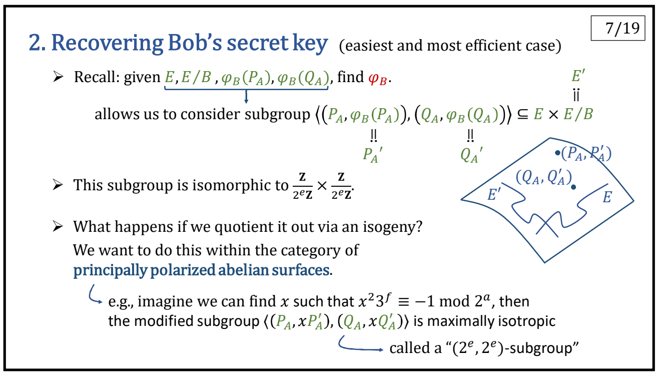
- Recall: given $\underbrace{E, E/B, \varphi_B(P_A), \varphi_B(Q_A)}$, find φ_B.

  allows us to consider subgroup $\langle (P_A, \varphi_B(P_A)), (Q_A, \varphi_B(Q_A)) \rangle \subseteq E \times E/B$

  $\varphi_B(P_A) = {P_A}'$, $\varphi_B(Q_A) = {Q_A}'$, $E/B = E'$

- This subgroup is isomorphic to $\frac{\mathbf{Z}}{2^e\mathbf{Z}} \times \frac{\mathbf{Z}}{2^e\mathbf{Z}}$.
- What happens if we quotient it out via an isogeny?
  We want to do this within the category of **principally polarized abelian surfaces**.
  - e.g., imagine we can find x such that $x^2 3^f \equiv -1 \bmod 2^a$, then the modified subgroup $\langle (P_A, xP'_A), (Q_A, xQ'_A) \rangle$ is maximally isotropic

(Proof: $e_{2^e}(P_A, Q_A) \cdot e_{2^e}(xP'_A, xQ'_A) = e_{2^e}(P_A, Q_A) \cdot e_{2^e}(P_A, Q_A)^{x^2 3^f} = 1$.)



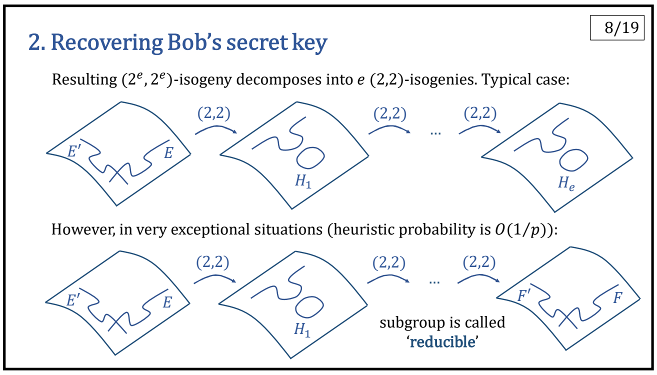
2. Recovering Bob's secret key (easiest and most efficient case)

- Recall: given $\underbrace{E, E/B, \varphi_B(P_A), \varphi_B(Q_A)}$, find φ_B.

  allows us to consider subgroup $\langle (P_A, \varphi_B(P_A)), (Q_A, \varphi_B(Q_A)) \rangle \subseteq E \times E/B$

  $\varphi_B(P_A) = {P_A}'$, $\varphi_B(Q_A) = {Q_A}'$, $E/B = E'$

- This subgroup is isomorphic to $\frac{\mathbf{Z}}{2^e\mathbf{Z}} \times \frac{\mathbf{Z}}{2^e\mathbf{Z}}$.
- What happens if we quotient it out via an isogeny?
  We want to do this within the category of **principally polarized abelian surfaces**.
  - e.g., imagine we can find x such that $x^2 3^f \equiv -1 \bmod 2^a$, then the modified subgroup $\langle (P_A, xP'_A), (Q_A, xQ'_A) \rangle$ is maximally isotropic
    - called a "$(2^e, 2^e)$-subgroup"

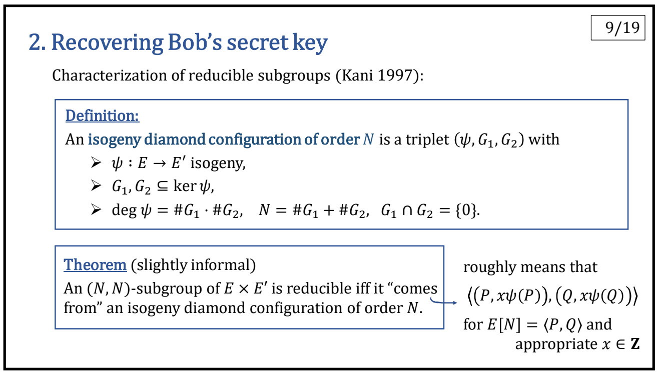


2. Recovering Bob's secret key

Resulting $(2^e, 2^e)$-isogeny decomposes into e (2,2)-isogenies. Typical case:

However, in very exceptional situations (heuristic probability is $O(1/p)$):

subgroup is called **'reducible'**



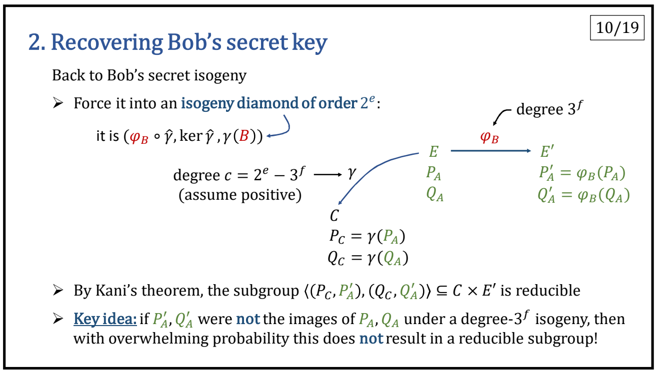
2. Recovering Bob's secret key

Characterization of reducible subgroups (Kani 1997):

Definition:
An **isogeny diamond configuration of order N** is a triplet (ψ, G_1, G_2) with
- $\psi : E \to E'$ isogeny,
- $G_1, G_2 \subseteq \ker \psi$,
- $\deg \psi = \#G_1 \cdot \#G_2$, $N = \#G_1 + \#G_2$, $G_1 \cap G_2 = \{0\}$.

Theorem (slightly informal)
An (N, N)-subgroup of $E \times E'$ is reducible iff it "comes from" an isogeny diamond configuration of order N.

roughly means that $\langle (P, x\psi(P)), (Q, x\psi(Q)) \rangle$ for $E[N] = \langle P, Q \rangle$ and appropriate $x \in \mathbf{Z}$



2. Recovering Bob's secret key

Back to Bob's secret isogeny

- Force it into an **isogeny diamond of order 2^e**:

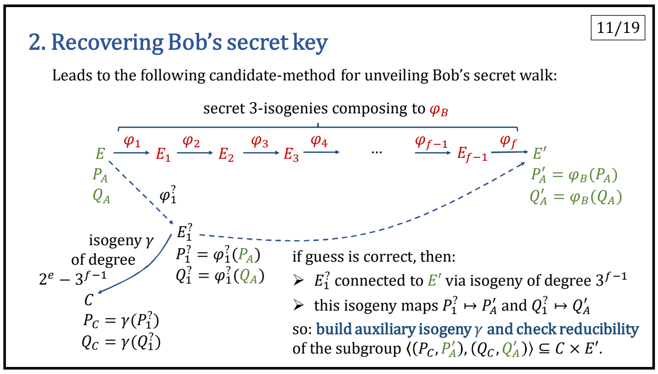
  it is $(\varphi_B \circ \hat{\gamma}, \ker \hat{\gamma}, \gamma(B))$

$$\begin{tikzcd} & E, P_A, Q_A \arrow[r, "\varphi_B"] \arrow[dl, bend right, "\gamma"'] & E', P'_A = \varphi_B(P_A), Q'_A = \varphi_B(Q_A) \\ C, P_C = \gamma(P_A), Q_C = \gamma(Q_A) & & \end{tikzcd}$$

degree 3^f

degree $c = 2^e - 3^f \longrightarrow \gamma$
(assume positive)

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



2. Recovering Bob's secret key

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

secret 3-isogenies composing to φ_B

$$\begin{tikzcd} E, P_A, Q_A \arrow[r, "\varphi_1"] \arrow[d, dashed, "\varphi_1^?"] & E_1 \arrow[r, "\varphi_2"] & E_2 \arrow[r, "\varphi_3"] & E_3 \arrow[r, "\varphi_4"] & \cdots \arrow[r, "\varphi_{f-1}"] & E_{f-1} \arrow[r, "\varphi_f"] & E', P'_A = \varphi_B(P_A), Q'_A = \varphi_B(Q_A) \\ E_1^?, P_1^? = \varphi_1^?(P_A), Q_1^? = \varphi_1^?(Q_A) \arrow[rrrrrru, dashed, bend right] \arrow[d, "\gamma"'] & & & & & & \\ C, P_C = \gamma(P_1^?), Q_C = \gamma(Q_1^?) & & & & & & \end{tikzcd}$$

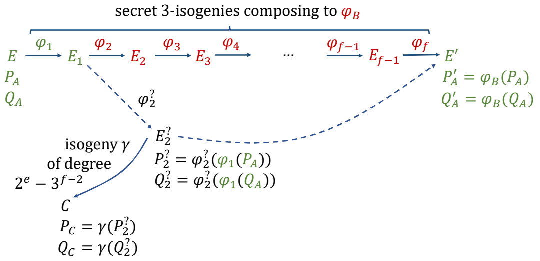
isogeny γ of degree $2^e - 3^{f-1}$

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 $\langle (P_C, P'_A), (Q_C, Q'_A) \rangle \subseteq C \times E'$.

2. Recovering Bob’s secret key

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



secret 3-isogenies composing to φ_B

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

P_A
Q_A

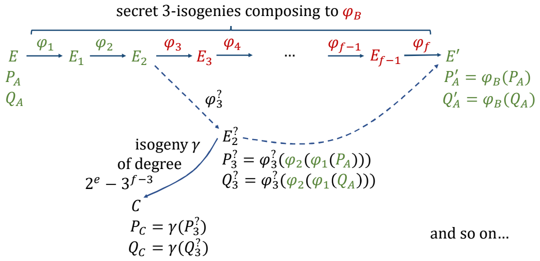
$P'_A = \varphi_B(P_A)$
$Q'_A = \varphi_B(Q_A)$

$P_2^? = \varphi_2^?(\varphi_1(P_A))$
$Q_2^? = \varphi_2^?(\varphi_1(Q_A))$

$P_C = \gamma(P_2^?)$
$Q_C = \gamma(Q_2^?)$

2. Recovering Bob’s secret key

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



secret 3-isogenies composing to φ_B

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

P_A
Q_A

$P'_A = \varphi_B(P_A)$
$Q'_A = \varphi_B(Q_A)$

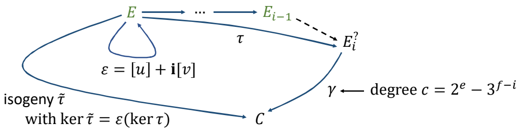
$P_3^? = \varphi_3^?(\varphi_2(\varphi_1(P_A)))$
$Q_3^? = \varphi_3^?(\varphi_2(\varphi_1(Q_A)))$

$P_C = \gamma(P_3^?)$
$Q_C = \gamma(Q_3^?)$

and so on…

3. Constructing the auxiliary isogeny γ

At iteration i: want to construct an isogeny



$$\begin{tikzcd}
E \arrow[r] \arrow[loop below, "\varepsilon = {[u]} + \mathbf{i}{[v]}"] \arrow[rrr, bend right, "\tau"] \arrow[dr, bend right, "\text{isogeny } \tilde{\tau} \text{ with } \ker\tilde{\tau} = \varepsilon(\ker\tau)"'] & \cdots \arrow[r] & E_{i-1} \arrow[r, dashed] & E_i^? \arrow[dll, "\gamma"] \\
& C & &
\end{tikzcd}$$

$\gamma \longleftarrow$ degree $c = 2^e - 3^{f-i}$

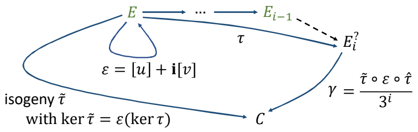
We know:

- a path $\tau : E \to E_i^?$.
- that $E : y^2 = x^3 + x$ comes equipped with $\mathbf{i} : E \to E : (x, y) \mapsto (-x, \mathbf{i}y)$

Hope: $c = 2^e - 3^{f-i} = u^2 + v^2 = (u + \mathbf{i}v)(u - \mathbf{i}v)$ for certain integers u, v.

3. Constructing the auxiliary isogeny γ

At iteration i: want to construct an isogeny



$$\begin{tikzcd}
E \arrow[r] \arrow[loop below, "\varepsilon = {[u]} + \mathbf{i}{[v]}"] \arrow[rrr, bend right, "\tau"] \arrow[dr, bend right, "\text{isogeny } \tilde{\tau} \text{ with } \ker\tilde{\tau} = \varepsilon(\ker\tau)"'] & \cdots \arrow[r] & E_{i-1} \arrow[r, dashed] & E_i^? \arrow[dll, "\gamma = \frac{\tilde{\tau} \circ \varepsilon \circ \hat{\tau}}{3^i}"] \\
& C & &
\end{tikzcd}$$

We know:

- a path $\tau : E \to E_i^?$.
- that $E : y^2 = x^3 + x$ comes equipped with $\mathbf{i} : E \to E : (x, y) \mapsto (-x, \mathbf{i}y)$

Hope: $c = 2^e - 3^{f-i} = u^2 + v^2 = (u + \mathbf{i}v)(u - \mathbf{i}v)$ for certain integers u, v.

3. Constructing the auxiliary isogeny γ

Hope: $c = 2^e - 3^{f-i} = u^2 + v^2 = (u + \mathbf{i}v)(u - \mathbf{i}v)$ for certain integers u, v.

- Cost of deciding existence of u, v and finding them:
  - **factoring** c,
  - Euclid’s algorithm over $\mathbf{Z}[\mathbf{i}]$ (special case of Cornacchia)
- Note: **only depends on system parameters**, not on concrete SIDH instance.
- If c does not admit decomposition: **create more leeway** by
  - reducing e (2^e-torsion info implies 2^{e-j}-torsion info),
  - increasing $f - i$ (extend Bob’s secret walk if useful).
- In practice:
  - need to guess first degree-3^i component so that $2^e > 3^{f-i}$,
  - from that point onwards: can guess one degree-3 component at a time.
- Altogether, attack runs heuristically in time $L(1/4)$, modulo precomputation.

3. Constructing the auxiliary isogeny γ

What about other starting curves than $E : y^2 = x^3 + x$?

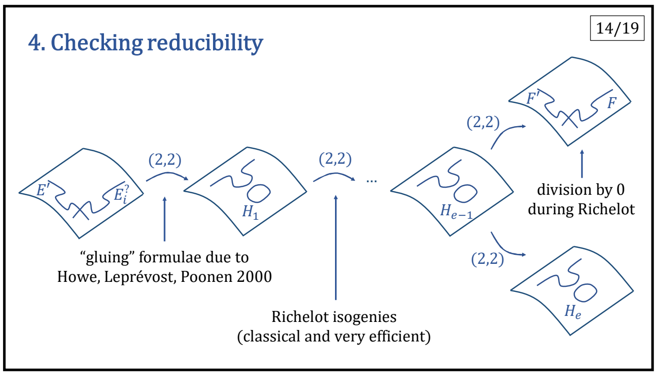
Known endomorphism ring:

- SIKE uses $E : y^2 = x^3 + 6x^2 + x$ which carries endomorphism $2\mathbf{i}$: same works
- more general: approach works if $\mathrm{End}(E)$ contains small-norm endomorphism
- totally general: walk to appropriate curve with small-norm endomorphism
  - ↪ selecting best curve leads to heuristic polynomial time (mod factoring)

Unknown endomorphism ring:

- auxiliary isogeny can always be constructed if $c = 2^e - 3^{f-i}$ is smooth
- create more leeway by considering $c = d2^{e-j} - d'3^{f-i}$

guess action on d-torsion ←
rely on smaller torsion info ←
→ extend Bob’s walk

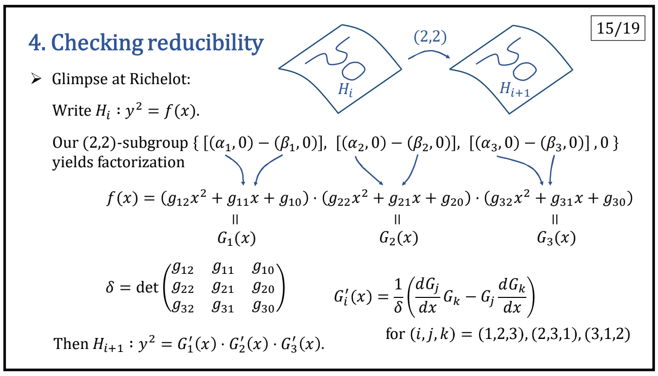


4. Checking reducibility

division by 0
during Richelot

“gluing” formulae due to
Howe, Leprévost, Poonen 2000

Richelot isogenies
(classical and very efficient)



4. Checking reducibility

- Glimpse at Richelot:

Write $H_i : y^2 = f(x)$.

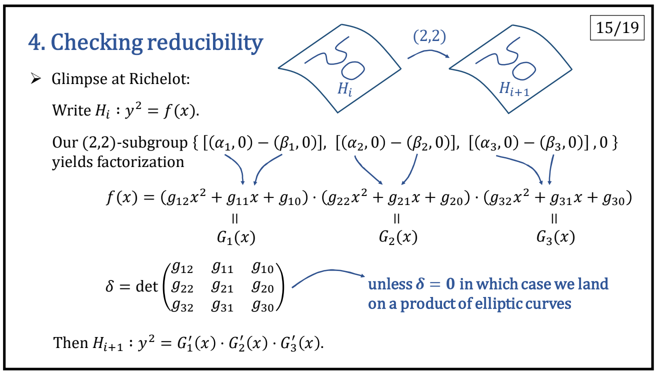
Our (2,2)-subgroup $\{\, [(\alpha_1,0)-(\beta_1,0)],\ [(\alpha_2,0)-(\beta_2,0)],\ [(\alpha_3,0)-(\beta_3,0)]\,,0\,\}$ yields factorization

$$f(x) = \underset{\substack{\| \\ G_1(x)}}{(g_{12}x^2+g_{11}x+g_{10})} \cdot \underset{\substack{\| \\ G_2(x)}}{(g_{22}x^2+g_{21}x+g_{20})} \cdot \underset{\substack{\| \\ G_3(x)}}{(g_{32}x^2+g_{31}x+g_{30})}$$

$$\delta = \det\begin{pmatrix} g_{12} & g_{11} & g_{10} \\ g_{22} & g_{21} & g_{20} \\ g_{32} & g_{31} & g_{30} \end{pmatrix} \qquad G_i'(x) = \frac{1}{\delta}\left(\frac{dG_j}{dx}G_k - G_j\frac{dG_k}{dx}\right)$$

for $(i,j,k) = (1,2,3),(2,3,1),(3,1,2)$

Then $H_{i+1} : y^2 = G_1'(x)\cdot G_2'(x)\cdot G_3'(x)$.



4. Checking reducibility

- Glimpse at Richelot:

Write $H_i : y^2 = f(x)$.

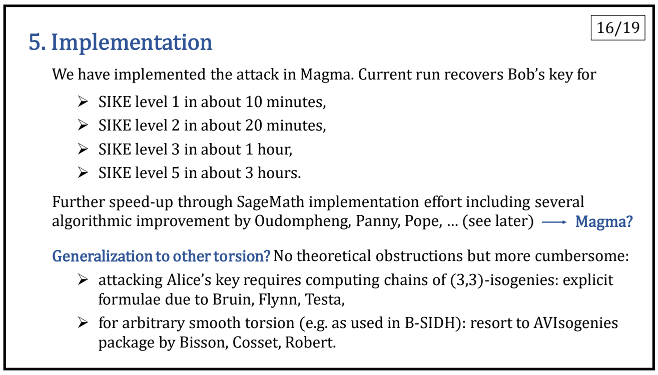
Our (2,2)-subgroup $\{\, [(\alpha_1,0)-(\beta_1,0)],\ [(\alpha_2,0)-(\beta_2,0)],\ [(\alpha_3,0)-(\beta_3,0)]\,,0\,\}$ yields factorization

$$f(x) = \underset{\substack{\| \\ G_1(x)}}{(g_{12}x^2+g_{11}x+g_{10})} \cdot \underset{\substack{\| \\ G_2(x)}}{(g_{22}x^2+g_{21}x+g_{20})} \cdot \underset{\substack{\| \\ G_3(x)}}{(g_{32}x^2+g_{31}x+g_{30})}$$

$$\delta = \det\begin{pmatrix} g_{12} & g_{11} & g_{10} \\ g_{22} & g_{21} & g_{20} \\ g_{32} & g_{31} & g_{30} \end{pmatrix}$$

unless $\delta = 0$ in which case we land on a product of elliptic curves

Then $H_{i+1} : y^2 = G_1'(x)\cdot G_2'(x)\cdot G_3'(x)$.



5. Implementation

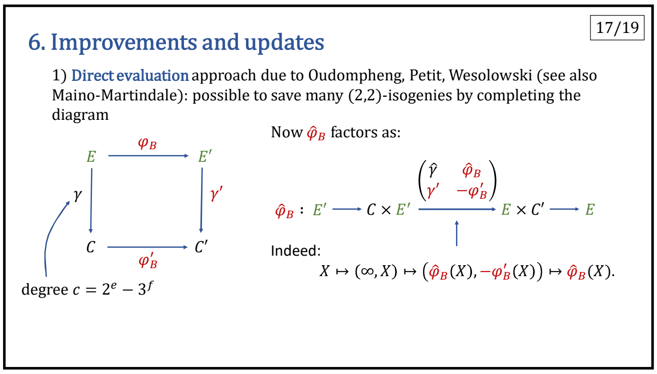
We have implemented the attack in Magma. Current run recovers Bob’s key for

- SIKE level 1 in about 10 minutes,
- SIKE level 2 in about 20 minutes,
- SIKE level 3 in about 1 hour,
- SIKE level 5 in about 3 hours.

Further speed-up through SageMath implementation effort including several algorithmic improvement by Oudompheng, Panny, Pope, … (see later) ⟶ **Magma?**

Generalization to other torsion? No theoretical obstructions but more cumbersome:

- attacking Alice’s key requires computing chains of (3,3)-isogenies: explicit formulae due to Bruin, Flynn, Testa,
- for arbitrary smooth torsion (e.g. as used in B-SIDH): resort to AVIsogenies package by Bisson, Cosset, Robert.



6. Improvements and updates

1) **Direct evaluation** approach due to Oudompheng, Petit, Wesolowski (see also Maino-Martindale): possible to save many (2,2)-isogenies by completing the diagram

$$\begin{tikzcd} E \arrow[r, "\varphi_B"] \arrow[d, "\gamma"'] & E' \arrow[d, "\gamma'"] \\ C \arrow[r, "\varphi'_B"'] & C' \end{tikzcd}$$

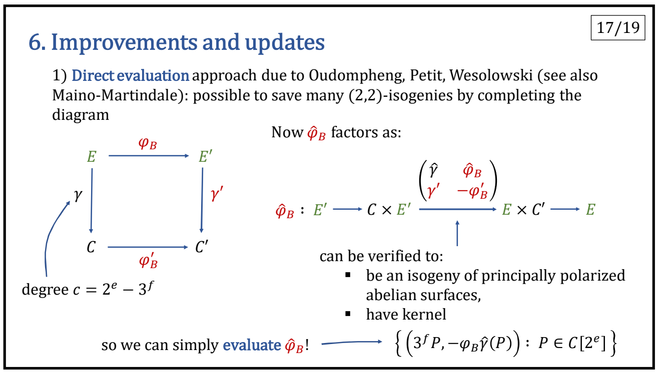
degree $c = 2^e - 3^f$

Now $\hat\varphi_B$ factors as:

$$\hat\varphi_B :\ E' \longrightarrow C \times E' \xrightarrow{\begin{pmatrix} \hat\gamma & \hat\varphi_B \\ \gamma' & -\varphi'_B \end{pmatrix}} E \times C' \longrightarrow E$$

Indeed:

$$X \mapsto (\infty, X) \mapsto \big(\hat\varphi_B(X), -\varphi'_B(X)\big) \mapsto \hat\varphi_B(X).$$



6. Improvements and updates

1) **Direct evaluation** approach due to Oudompheng, Petit, Wesolowski (see also Maino-Martindale): possible to save many (2,2)-isogenies by completing the diagram

$$\begin{tikzcd} E \arrow[r, "\varphi_B"] \arrow[d, "\gamma"'] & E' \arrow[d, "\gamma'"] \\ C \arrow[r, "\varphi'_B"'] & C' \end{tikzcd}$$

degree $c = 2^e - 3^f$

Now $\hat\varphi_B$ factors as:

$$\hat\varphi_B :\ E' \longrightarrow C \times E' \xrightarrow{\begin{pmatrix} \hat\gamma & \hat\varphi_B \\ \gamma' & -\varphi'_B \end{pmatrix}} E \times C' \longrightarrow E$$

can be verified to:

- be an isogeny of principally polarized abelian surfaces,
- have kernel

so we can simply **evaluate $\hat\varphi_B$**! ⟶ $\left\{ \left(3^f P, -\varphi_B\hat\gamma(P)\right) :\ P \in C[2^e] \right\}$

6. Improvements and updates

1) **Direct evaluation** approach due to Oudompheng, Petit, Wesolowski (see also Maino-Martindale): possible to save many (2,2)-isogenies by completing the diagram

$$\begin{tikzcd} E \arrow[r, "\varphi_B"] \arrow[d, "\gamma"'] & E' \arrow[d, "\gamma'"] \\ C \arrow[r, "\varphi'_B"'] & C' \end{tikzcd}$$

degree $c = 2^e - 3^f$

Now:

- evaluate $\hat{\varphi}_B$ on basis $\{ X, Y \}$ of $E'[3^f]$,
- determine $\ker \hat{\varphi}_B$ by solving
  $\hat{\varphi}_B(xX + yY) = x\hat{\varphi}_B(X) + y\hat{\varphi}_B(Y) = \infty$,
- recover $B = \hat{\varphi}_B(\ker \hat{\varphi}_B)$

6. Improvements and updates

2) Using this and various other speed-ups: SageMath implementation by Pope et al. has **dramatically reduced the attack runtimes**. E.g., SIKE level 1 now falls in 22 seconds.

3) Wesolowski described a direct way of constructing a degree-c isogeny using knowledge of the endomorphism ring, **without assuming special form of c** and **without the need for factorization**; leads to polynomial time only assuming GRH.

4) Re: **smoothness:** using standard heuristics it is easy to obtain $L(^1/_2)$-smooth

$$c = d2^{e-j} - d'3^{f-i}$$

with $c, d' \in L(^1/_2)$. So the algorithm (as does Maino-Martindale's) breaks SIDH with unknown endomorphism ring in $L(^1/_2 + \varepsilon)$. Pointed out by De Feo and Wesolowski.

6. Improvements and updates

5) Beautiful trick by Robert reduces this further to **unconditional polynomial runtime**.

Idea: write $c = a_1^2 + a_2^2 + a_3^2 + a_4^2 \longleftarrow$ Lagrange's four-square theorem

Explicit check:

$$M = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & -a_4 & a_3 \\ a_3 & a_4 & a_1 & -a_2 \\ a_4 & -a_3 & a_2 & a_1 \end{pmatrix} \quad \text{satisfies} \quad M^t \cdot M = M \cdot M^t = cI.$$

Now

$$F = \begin{pmatrix} M & \hat{\varphi}_B \\ -\varphi_B & M^t \end{pmatrix} \in \mathrm{End}(E^4 \times E'^4) \quad \text{with dual} \quad \hat{F} = \begin{pmatrix} M^t & -\hat{\varphi}_B \\ \varphi_B & M \end{pmatrix}$$

satisfies $\hat{F}F = F\hat{F} = (c + 3^f)I = 2^e I$, so $\ker F \subseteq (E^4 \times E'^4)[2^e]$ can be computed from torsion-point info. So we can directly evaluate φ_B as before.

6. Improvements and updates

5) Beautiful trick by Robert reduces this further to **unconditional polynomial runtime**.

Idea: write $c = a_1^2 + a_2^2 + a_3^2 + a_4^2 \longleftarrow$ Lagrange's four-square theorem

Explicit check:

$$M = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & -a_4 & a_3 \\ a_3 & a_4 & a_1 & -a_2 \\ a_4 & -a_3 & a_2 & a_1 \end{pmatrix} \quad \text{satisfies} \quad M^t \cdot M = M \cdot M^t = cI.$$

Now

$$F = \begin{pmatrix} M & \hat{\varphi}_B \\ -\varphi_B & M^t \end{pmatrix} \in \mathrm{End}(E^4 \times E'^4) \quad \text{with dual} \quad \hat{F} = \begin{pmatrix} M^t & -\hat{\varphi}_B \\ \varphi_B & M \end{pmatrix}$$

component-wise evaluation

satisfies $\hat{F}F = F\hat{F} = (c + 3^f)I = 2^e I$, so $\ker F \subseteq (E^4 \times E'^4)[2^e]$ can be computed from torsion-point info. So we can directly evaluate φ_B as before.

Questions?

Thanks for listening!