SIDH Proof of Knowledge

Luca De Feo[1], Samuel Dobson[2], Steven D. Galbraith[2], Lukas Zobernig[2]

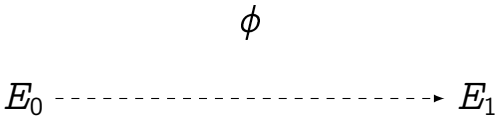
[1] IBM Research Europe, Switzerland
[2] Mathematics Department, University of Auckland, New Zealand

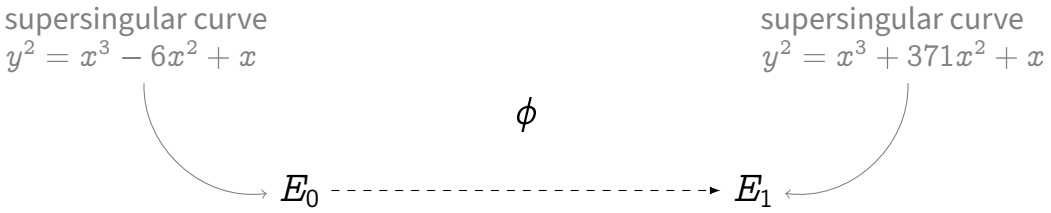
December 6, 2022, Asiacrypt, Taipei

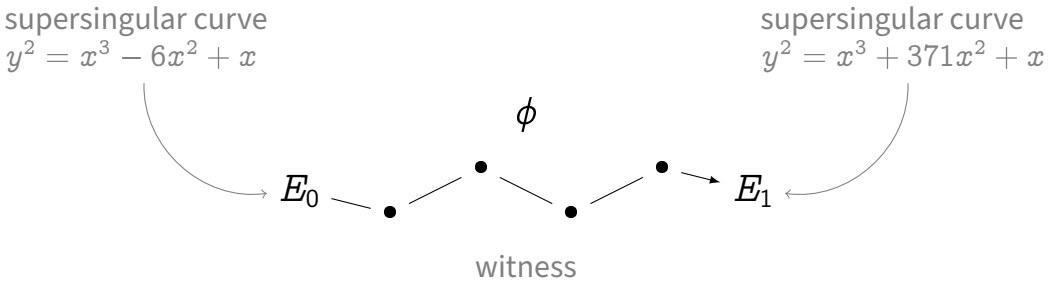
Proofs of Isogeny Knowledge…Why?

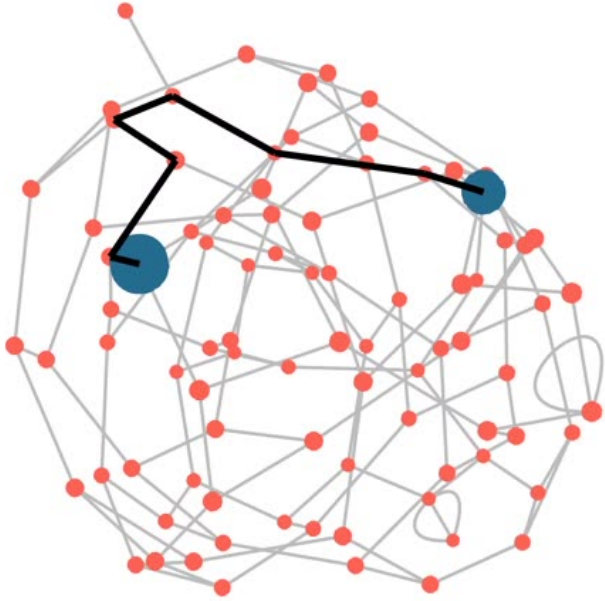
$$\phi : E_0 \longrightarrow E_1$$

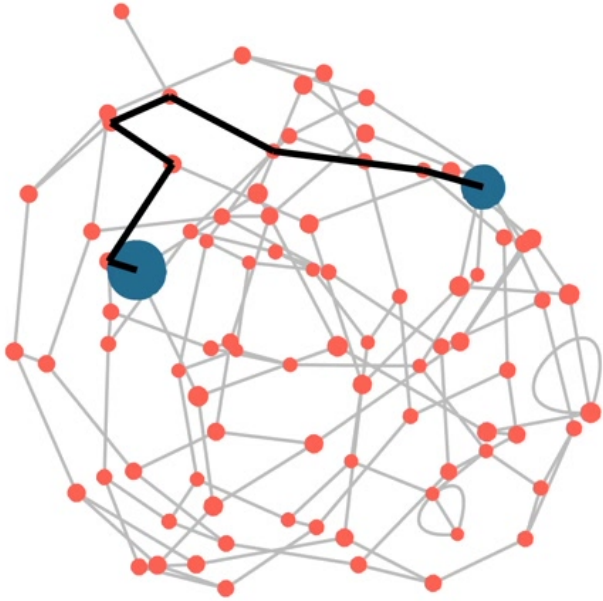
- Signatures,
- Verifiable *<insert your favorite primitive>*,
- Non-interactive SIDH (†) key exchange,
- …Why not?

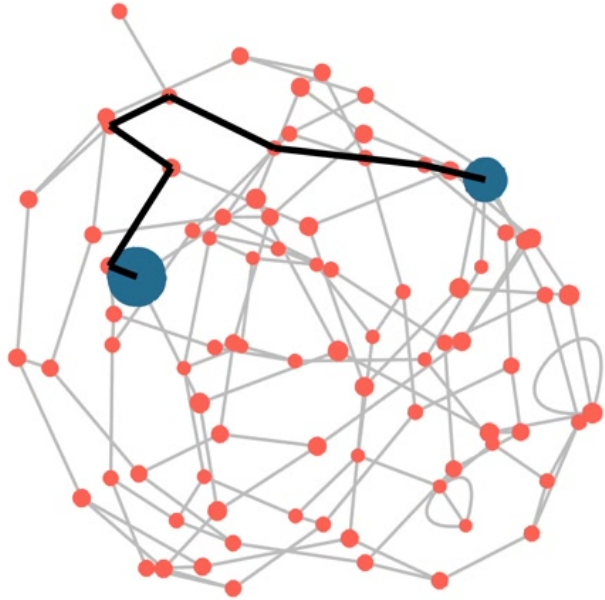

ϕ
E_0
E_1

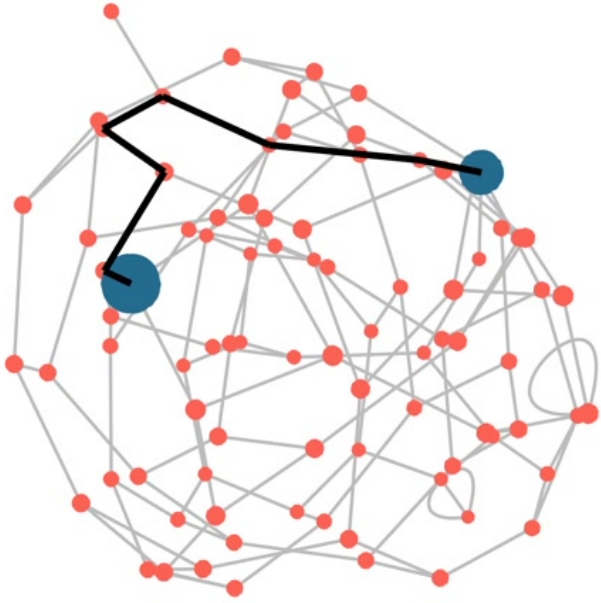

supersingular curve
$y^2 = x^3 - 6x^2 + x$
supersingular curve
$y^2 = x^3 + 371x^2 + x$
ϕ
E_0
E_1

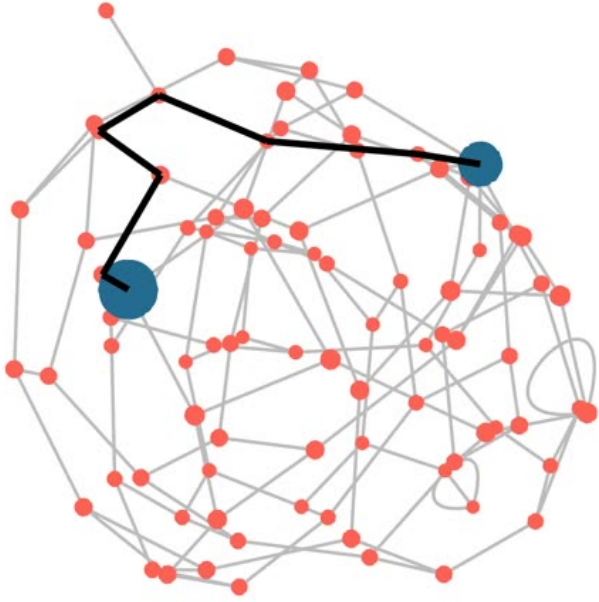

supersingular curve
$y^2 = x^3 - 6x^2 + x$
supersingular curve
$y^2 = x^3 + 371x^2 + x$
ϕ
E_0
E_1
witness

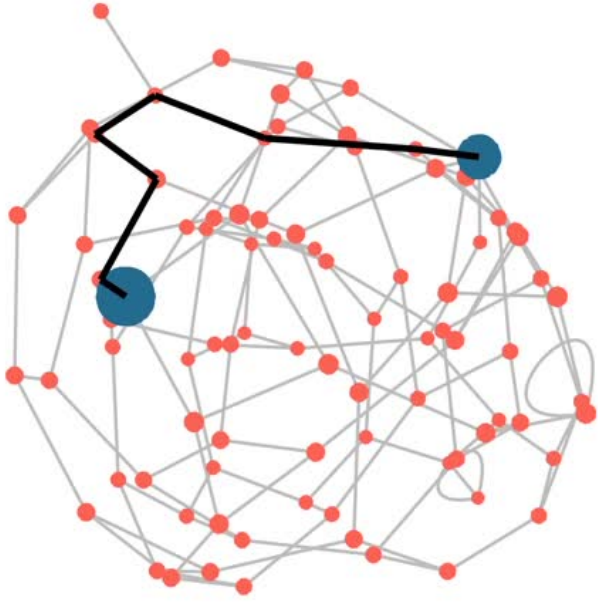


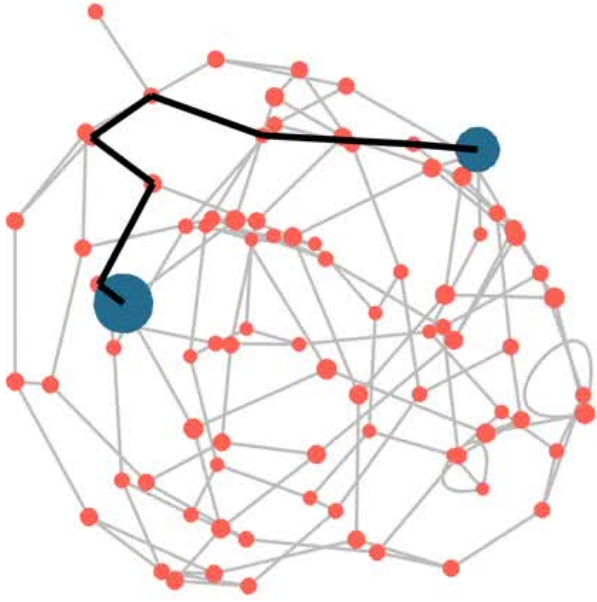


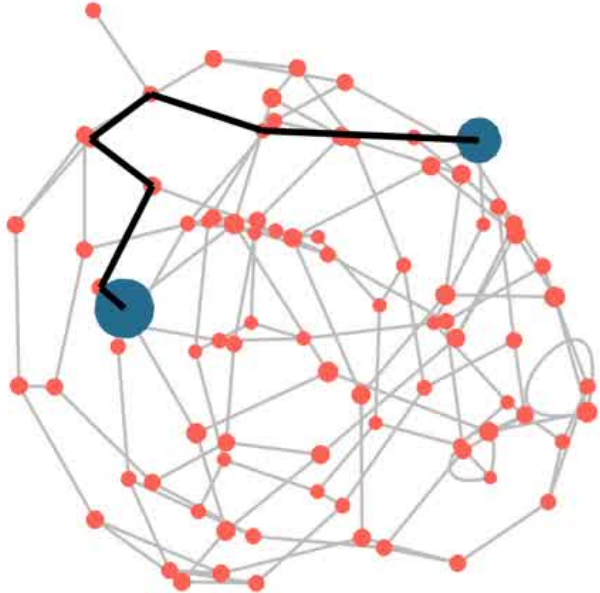


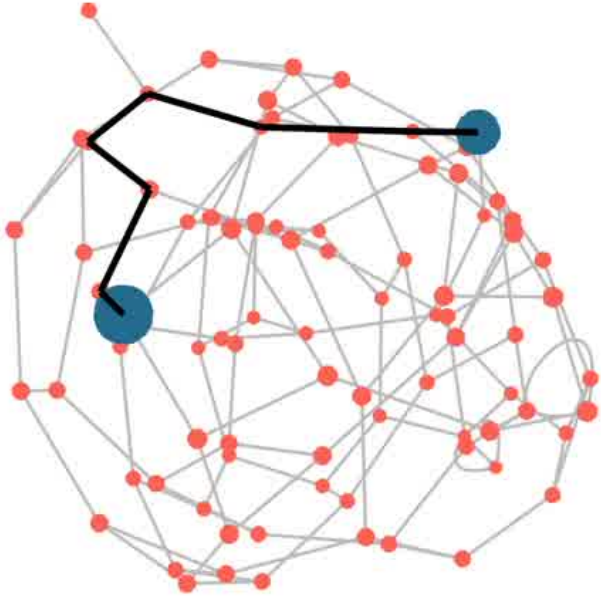


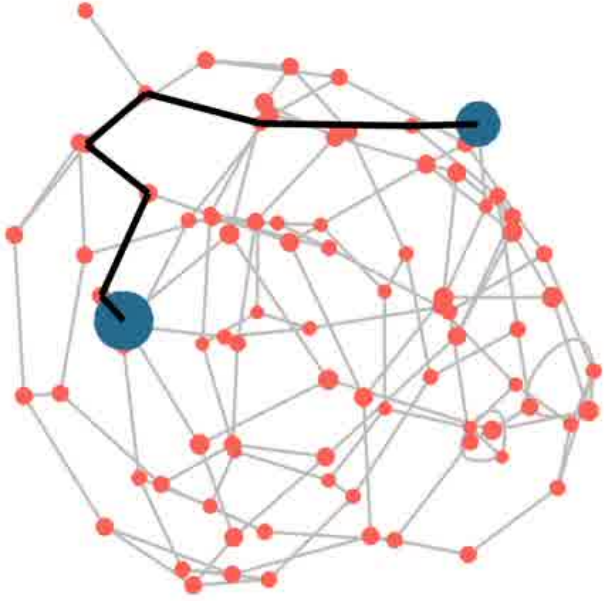




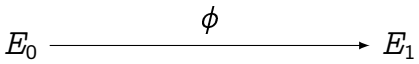






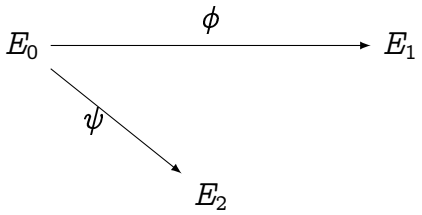


Something that doesn't work



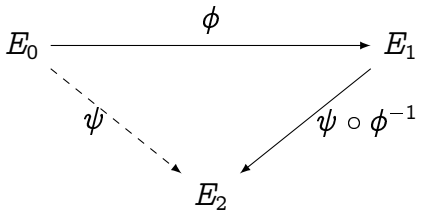
- Ok for CSIDH / ordinary curves / group actions (see SeaSign, CSI-FiSh).
- Galbraith-Petit-Silva: ok if E_0 is supersingular and has known endomorphism ring.
- Not known how to make ZK for general supersingular curves.

Something that doesn't work



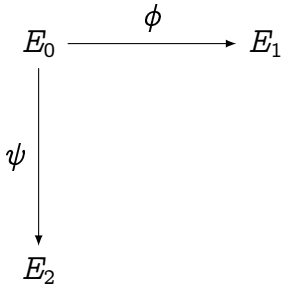
- Ok for CSIDH / ordinary curves / group actions (see SeaSign, CSI-FiSh).
- Galbraith-Petit-Silva: ok if E_0 is supersingular and has known endomorphism ring.
- Not known how to make ZK for general supersingular curves.

Something that doesn't work

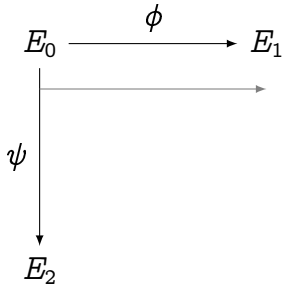


- Ok for CSIDH / ordinary curves / group actions (see SeaSign, CSI-FiSh).
- Galbraith-Petit-Silva: ok if E_0 is supersingular and has known endomorphism ring.
- Not known how to make ZK for general supersingular curves.

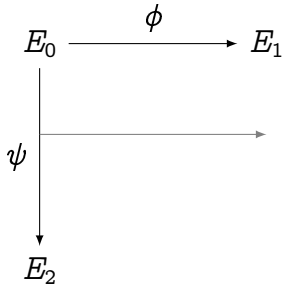
SIDH squares (pushouts)



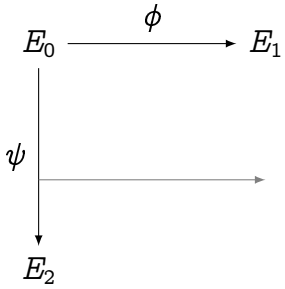
SIDH squares (pushouts)



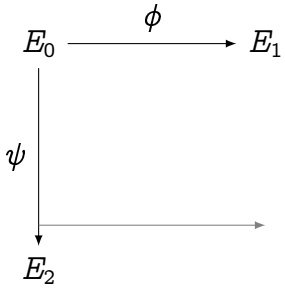
SIDH squares (pushouts)



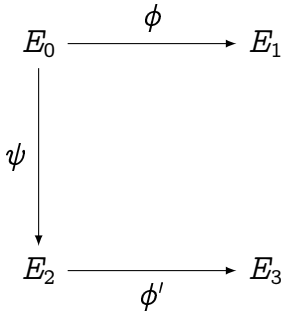
SIDH squares (pushouts)



SIDH squares (pushouts)

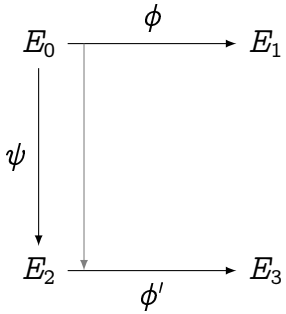


SIDH squares (pushouts)



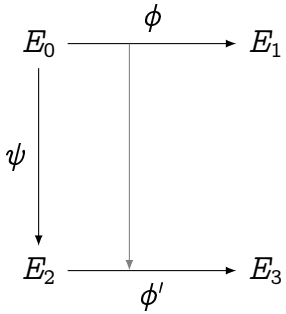
- $\ker \phi' = \psi(\ker \phi)$,

SIDH squares (pushouts)



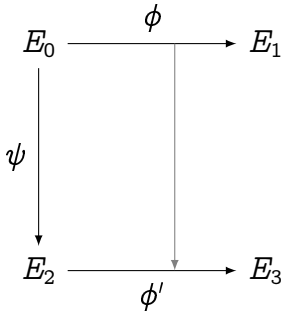
- $\ker \phi' = \psi(\ker \phi)$,

SIDH squares (pushouts)



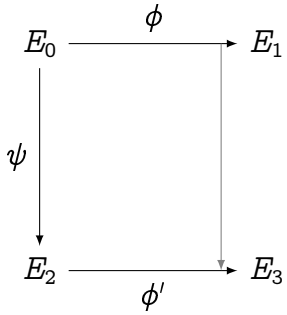
- $\ker \phi' = \psi(\ker \phi)$,

SIDH squares (pushouts)



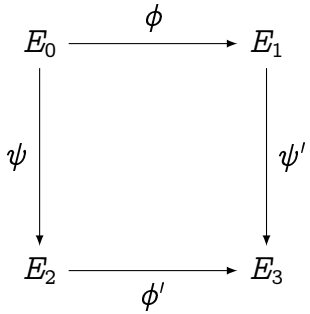
- $\ker \phi' = \psi(\ker \phi)$,

SIDH squares (pushouts)



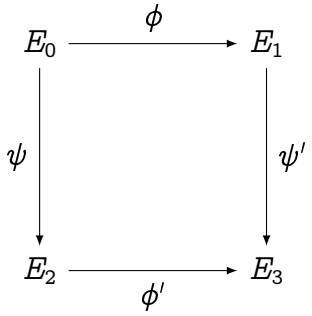
- $\ker \phi' = \psi(\ker \phi)$,

SIDH squares (pushouts)



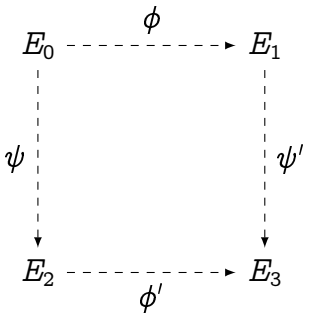
- $\ker \phi' = \psi(\ker \phi)$,
- $\ker \psi' = \phi(\ker \psi)$,

SIDH squares (pushouts)

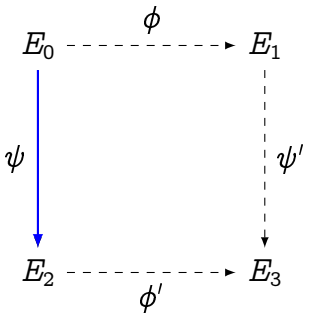


- $\ker \phi' = \psi(\ker \phi)$,
- $\ker \psi' = \phi(\ker \psi)$,
- $\deg \phi = \deg \phi' = A = 2^n$,
- $\deg \psi = \deg \psi' = B = 3^n$,
- $\gcd(A, B) = 1$,

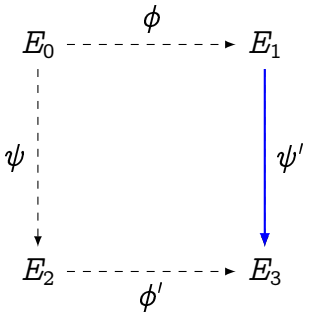
Something that should work: De Feo–Jao–Plût, 2012 (roughly)



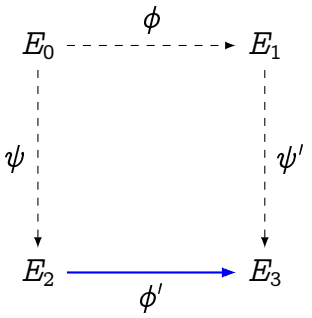
Something that should work: De Feo–Jao–Plût, 2012 (roughly)



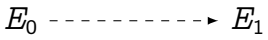
Something that should work: De Feo–Jao–Plût, 2012 (roughly)



Something that should work: De Feo–Jao–Plût, 2012 (roughly)

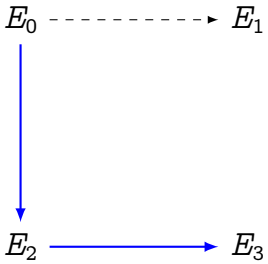


Special soundness (as claimed in DFJP11)

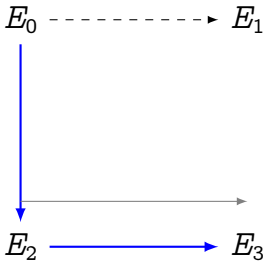


E_2 E_3

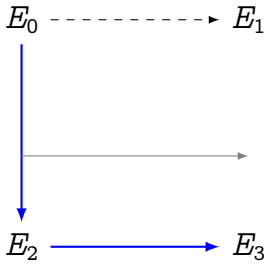
Special soundness (as claimed in DFJP11)



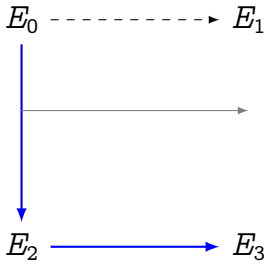
Special soundness (as claimed in DFJP11)



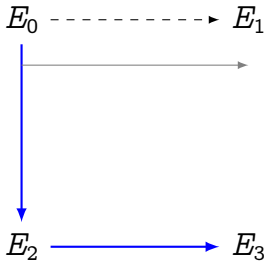
Special soundness (as claimed in DFJP11)



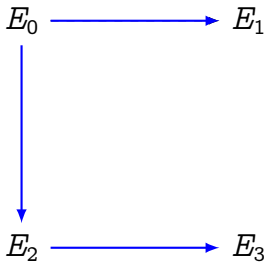
Special soundness (as claimed in DFJP11)



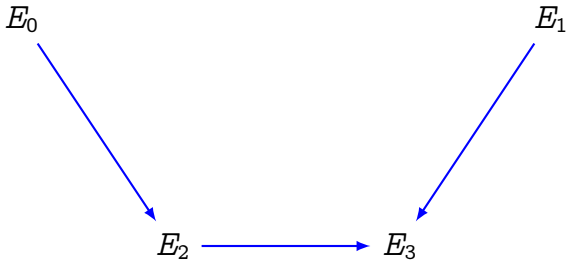
Special soundness (as claimed in DFJP11)



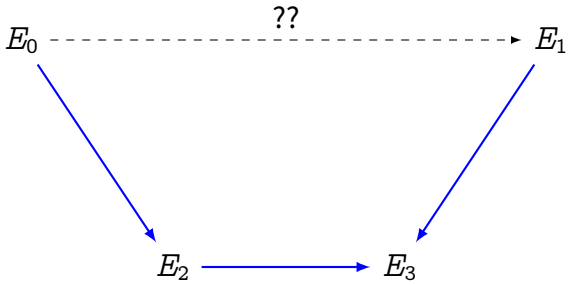
Special soundness (as claimed in DFJP11)



Epic fail!



Epic fail!



Our (not) elegant fix!

E_0 E_1

$E_2[B] = \langle P_2, Q_2 \rangle$ $E_3[B] = \langle P_3, Q_3 \rangle$

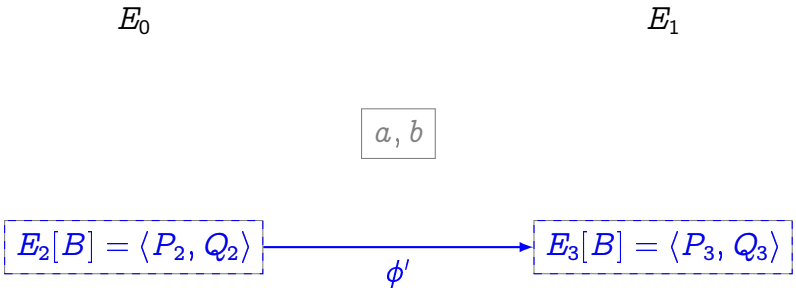
Our (not) elegant fix!

E_0 E_1

a, b

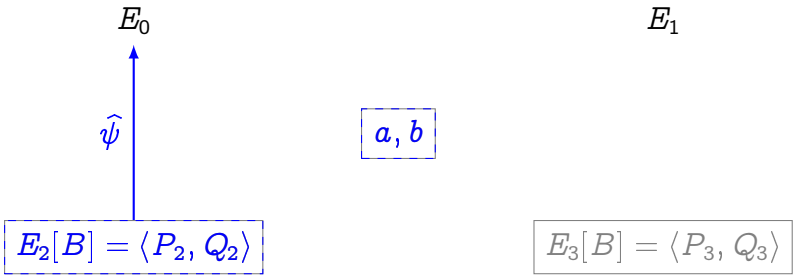
$E_2[B] = \langle P_2, Q_2 \rangle$ $E_3[B] = \langle P_3, Q_3 \rangle$

Our (not) elegant fix!



$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$

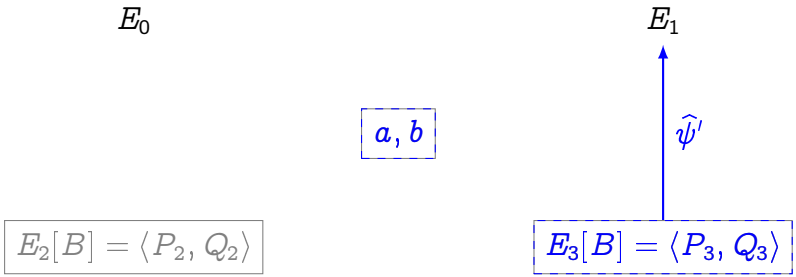
Our (not) elegant fix!



$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$

$$\ker \widehat{\psi} = aP_2 + bQ_2$$

Our (not) elegant fix!

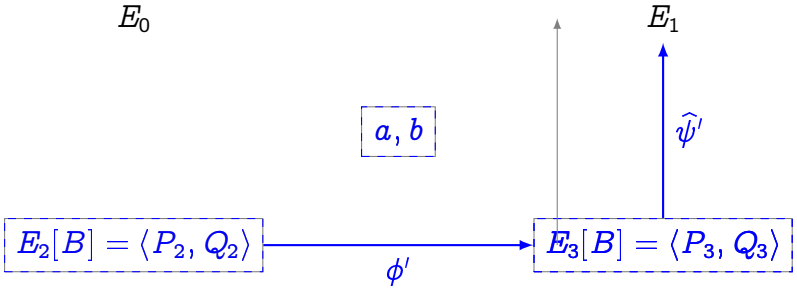


$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$

$$\ker \widehat{\psi} = aP_2 + bQ_2$$

$$\ker \widehat{\psi}' = aP_3 + bQ_3$$

Our (not) elegant fix!

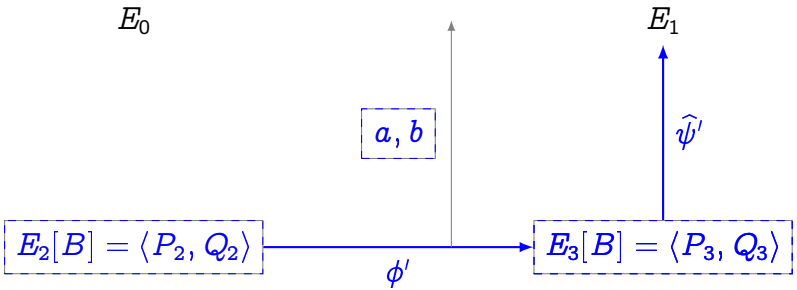


$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$

$$\ker \widehat{\psi} = aP_2 + bQ_2$$

$$\ker \widehat{\psi}' = aP_3 + bQ_3$$

Our (not) elegant fix!

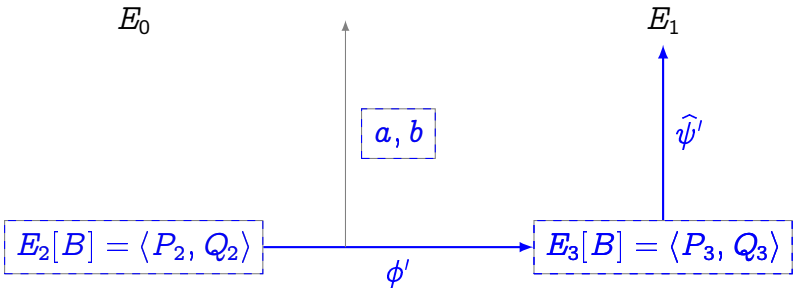


$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$

$$\ker \widehat{\psi} = aP_2 + bQ_2$$

$$\ker \widehat{\psi}' = aP_3 + bQ_3$$

Our (not) elegant fix!

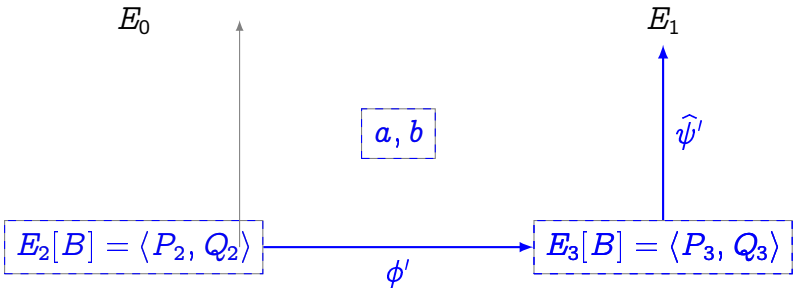


$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$

$$\ker \widehat{\psi} = aP_2 + bQ_2$$

$$\ker \widehat{\psi}' = aP_3 + bQ_3$$

Our (not) elegant fix!

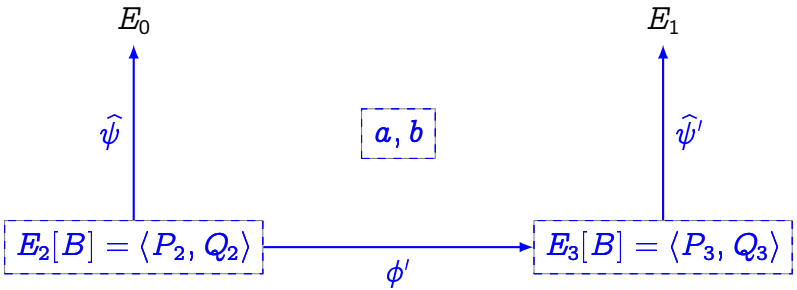


$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$

$$\ker \widehat{\psi} = aP_2 + bQ_2$$

$$\ker \widehat{\psi}' = aP_3 + bQ_3$$

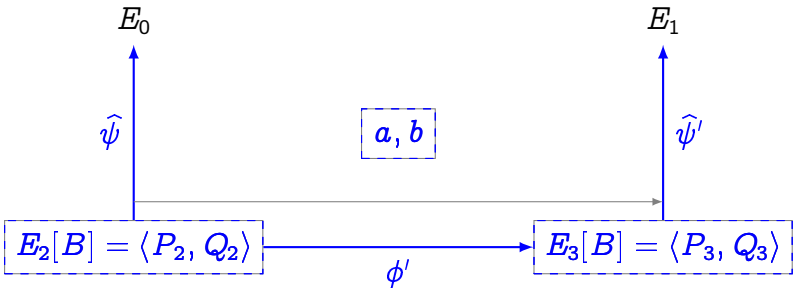
Our (not) elegant fix!



$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$
$$\ker \widehat{\psi} = aP_2 + bQ_2$$
$$\ker \widehat{\psi}' = aP_3 + bQ_3$$

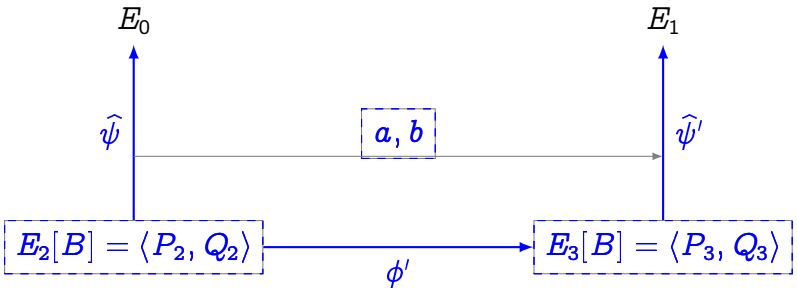
$$\Rightarrow \quad \ker \widehat{\psi}' = \phi'(\ker \widehat{\psi})$$

Our (not) elegant fix!



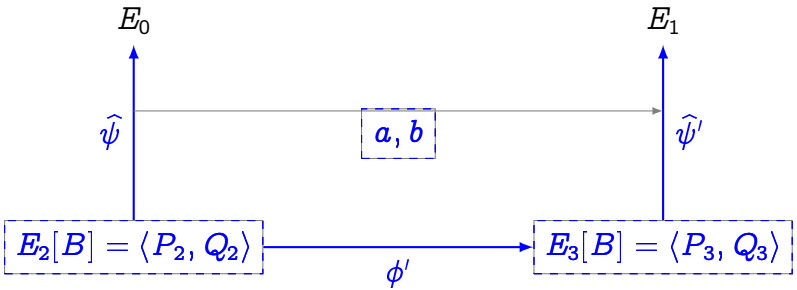
$$\left.\begin{aligned} P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2) \\ \ker \widehat{\psi} = aP_2 + bQ_2 \\ \ker \widehat{\psi}' = aP_3 + bQ_3 \end{aligned}\right\} \Rightarrow \quad \ker \widehat{\psi}' = \phi'(\ker \widehat{\psi})$$

Our (not) elegant fix!



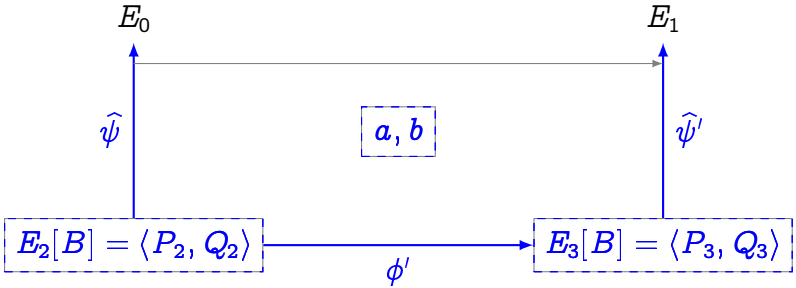
$$\left.\begin{aligned} P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2) \\ \ker \widehat{\psi} = aP_2 + bQ_2 \\ \ker \widehat{\psi}' = aP_3 + bQ_3 \end{aligned}\right\} \Rightarrow \quad \ker \widehat{\psi}' = \phi'(\ker \widehat{\psi})$$

Our (not) elegant fix!



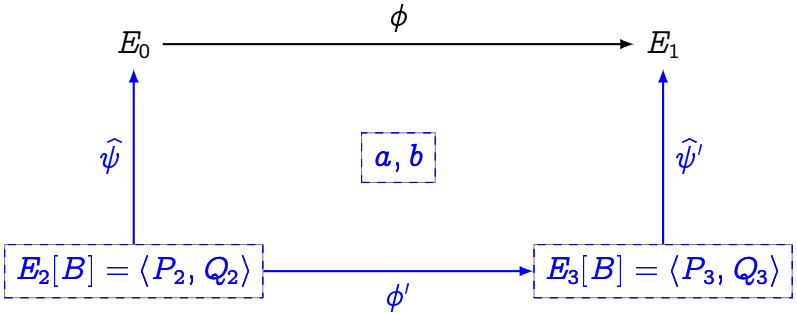
$$\left.\begin{aligned} P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2) \\ \ker \widehat{\psi} = aP_2 + bQ_2 \\ \ker \widehat{\psi}' = aP_3 + bQ_3 \end{aligned}\right\} \Rightarrow \quad \ker \widehat{\psi}' = \phi'(\ker \widehat{\psi})$$

Our (not) elegant fix!



$$\left.\begin{aligned} P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2) \\ \ker \widehat{\psi} = aP_2 + bQ_2 \\ \ker \widehat{\psi}' = aP_3 + bQ_3 \end{aligned}\right\} \Rightarrow \quad \ker \widehat{\psi}' = \phi'(\ker \widehat{\psi})$$

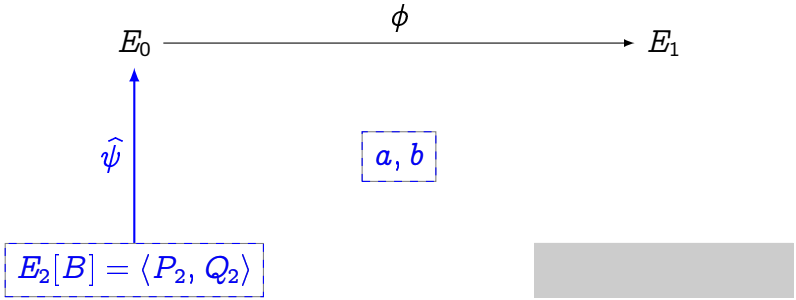
Our (not) elegant fix!



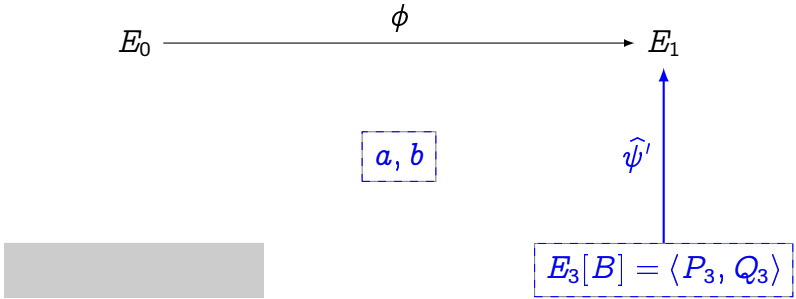
$$P_3 = \phi'(P_2), \qquad Q_3 = \phi'(Q_2)$$
$$\ker \widehat{\psi} = aP_2 + bQ_2$$
$$\ker \widehat{\psi}' = aP_3 + bQ_3$$

$$\Rightarrow \quad \ker \widehat{\psi}' = \phi'(\ker \widehat{\psi})$$
$$\ker \phi = \widehat{\psi}(\ker \phi')$$

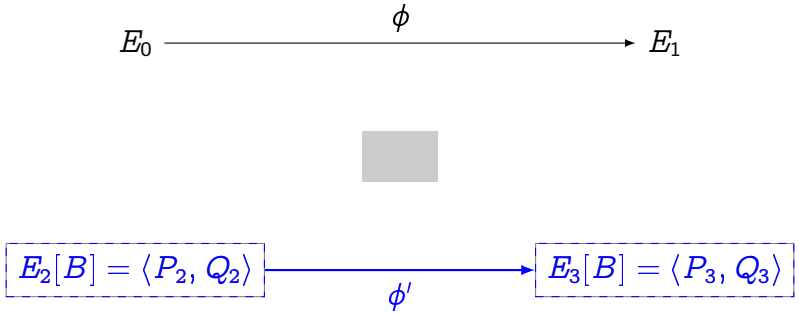
Zero-knowledge



Zero-knowledge

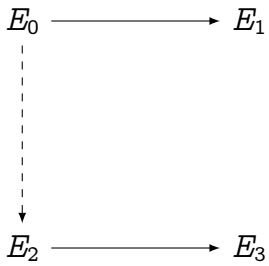


Zero-knowledge

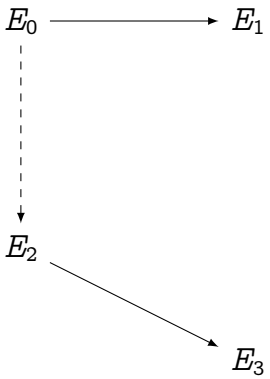


Assumption: Decisional Supersingular Product (DSSP)

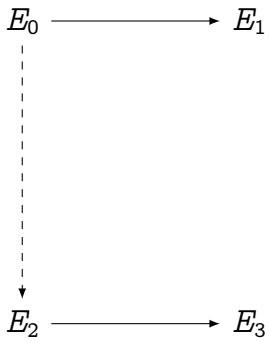
Statistical ZK (BCCDFLMPPW ’22)



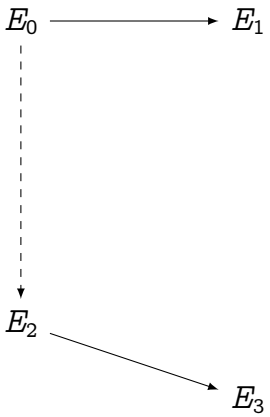
??



Statistical ZK (BCCDFLMPPW ’22)



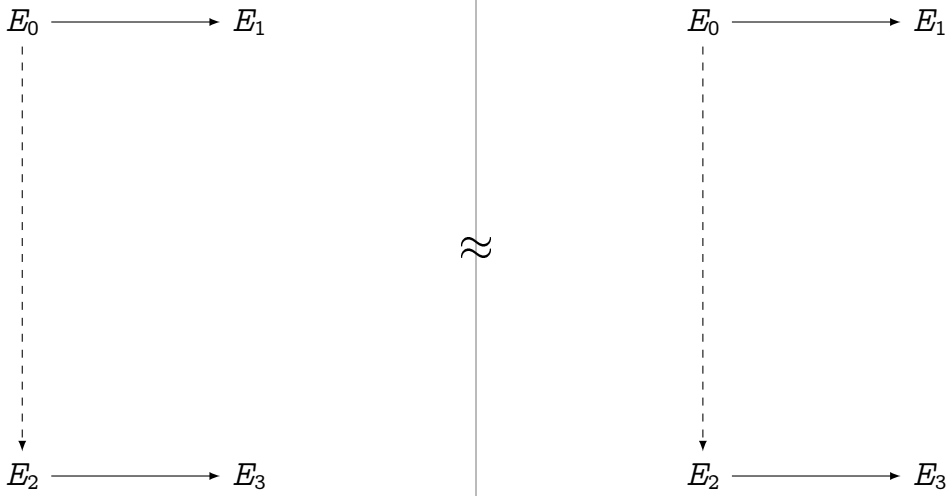
??



Statistical ZK (BCCDFLMPPW ’22)

??

Statistical ZK (BCCDFLMPPW '22)



Summary

This work:

- A knowledge sound, computational ZK protocol to prove knowledge of an isogeny of fixed degree… Finally!
- A variant to prove knowledge of an SIDH key… Because, why not?

Recent development:

- A statistically ZK protocol for the same… but knowledge soundness not as good.

Open problems:

- Statistical ZK + strong Knowledge soundness.
- Efficiency.
- An even remotely efficient protocol for the CSIDH setting:
  (SeaSign sucks and CSI-FiSh doesn't scale).