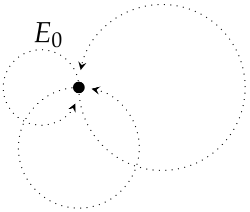
Supersingular Curves You Can Trust

Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo,
Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny,
Sikhar Patranabis, Benjamin Wesolowski

Lyon, 26 April 2023

Plenty of reasons to distrust a supersingular elliptic curve

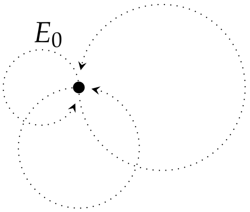
- Elliptic curves have a lot of structure, among which the endomorphism ring.



Plenty of reasons to distrust a supersingular elliptic curve

- Elliptic curves have a lot of structure, among which the endomorphism ring.

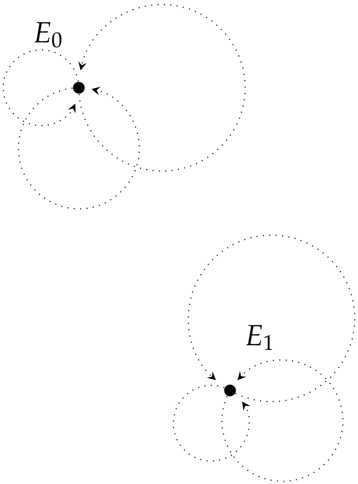
- Several hard problems become easy when you know $\mathrm{End}(E)$. Including the isogeny problem!



Plenty of reasons to distrust a supersingular elliptic curve

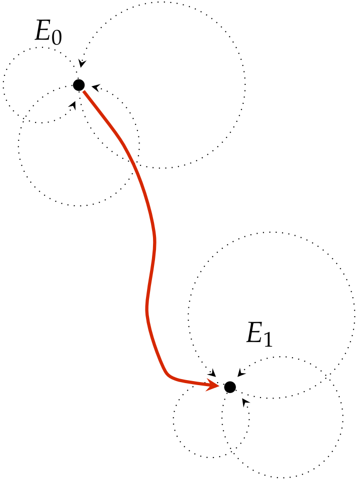
- Elliptic curves have a lot of structure, among which the endomorphism ring.

- Several hard problems become easy when you know $\mathrm{End}(E)$. Including the isogeny problem!



Plenty of reasons to distrust a supersingular elliptic curve

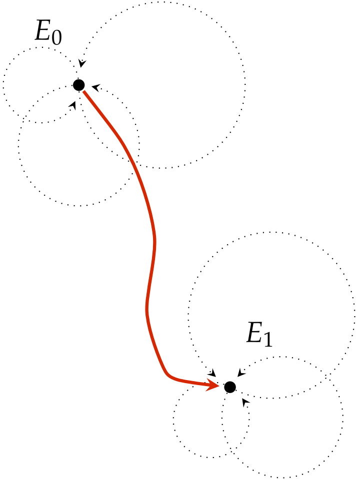
- Elliptic curves have a lot of structure, among which the endomorphism ring.
- Several hard problems become easy when you know $\mathrm{End}(E)$. Including the isogeny problem!



Plenty of reasons to distrust a supersingular elliptic curve

- Elliptic curves have a lot of structure, among which the endomorphism ring.
- Several hard problems become easy when you know End(E). Including the isogeny problem!

$\Longrightarrow$ End(E) can be used to backdoor several isogeny-based protocols.



A big open problem

Solution: **Supersingular Elliptic Curves with Unknown Endomorphism Ring**.

"SECUER"

A big open problem

Solution: **<u>S</u>upersingular <u>E</u>lliptic <u>C</u>urves with <u>U</u>nknown <u>E</u>ndomorphism <u>R</u>ing**.

"SECUER"

Concretely, a supersingular elliptic curve
for which there are good reasons to believe
that no one knows the endomorphism ring.

A big open problem

Solution: **<u>S</u>upersingular <u>E</u>lliptic <u>C</u>urves with <u>U</u>nknown <u>E</u>ndomorphism <u>R</u>ing**.

"SECUER"

Concretely, a supersingular elliptic curve
for which there are good reasons to believe
that no one knows the endomorphism ring.

<u>Utopia:</u> efficient algorithm [*random seed* $\longmapsto E$]
such that $\nexists$ efficient algorithm [*random seed* $\longmapsto \mathrm{End}(E)$].

A big open problem

Solution: **Supersingular Elliptic Curves with Unknown Endomorphism Ring**.

“SECUER”

Concretely, a supersingular elliptic curve
for which there are good reasons to believe
that no one knows the endomorphism ring.

Utopia: efficient algorithm $[\textit{random seed} \longmapsto E]$
such that $\nexists$ efficient algorithm $[\textit{random seed} \longmapsto \mathrm{End}(E)]$.

Reality: Less great; next slide.

Constructing supersingular curves

- Bröker's algorithm: Reduce a CM curve from characteristic zero to $\mathbb{F}_p$.

Constructing supersingular curves

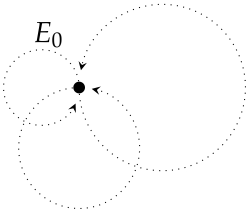
- Bröker's algorithm: Reduce a CM curve from characteristic zero to $\mathbb{F}_p$.
  Only efficient for small CM discriminants $\implies$ known endomorphism ring.

Constructing supersingular curves

- Bröker's algorithm: Reduce a CM curve from characteristic zero to $\mathbb{F}_p$.
  Only efficient for small CM discriminants $\implies$ known endomorphism ring.
- Random isogeny walking from such a curve.

Constructing supersingular curves

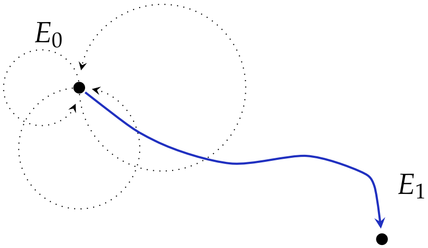
- Bröker's algorithm: Reduce a CM curve from characteristic zero to $\mathbb{F}_p$.
  Only efficient for small CM discriminants $\Longrightarrow$ known endomorphism ring.
- Random isogeny walking from such a curve.



Constructing supersingular curves

- Bröker's algorithm: Reduce a CM curve from characteristic zero to $\mathbb{F}_p$.
  Only efficient for small CM discriminants $\implies$ known endomorphism ring.

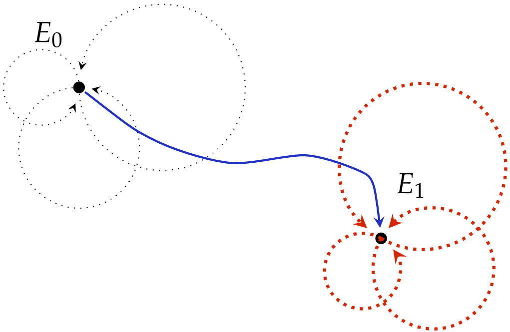
- Random isogeny walking from such a curve.



Constructing supersingular curves

- Bröker's algorithm: Reduce a CM curve from characteristic zero to $\mathbb{F}_p$.
  Only efficient for small CM discriminants $\Longrightarrow$ known endomorphism ring.

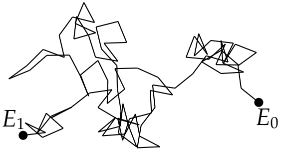
- Random isogeny walking from such a curve.



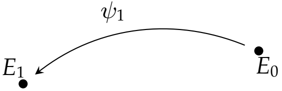
The connecting isogeny is a backdoor to the endomorphism ring.

Folklore workaround: Distributed trusted setup

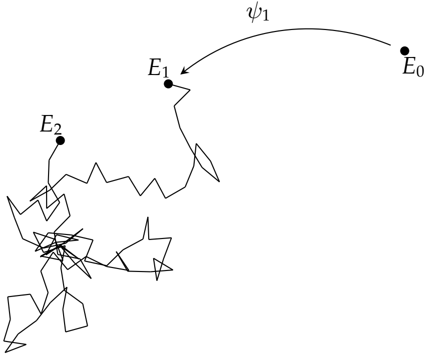
Folklore workaround: Distributed trusted setup



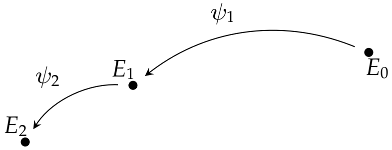
Folklore workaround: Distributed trusted setup



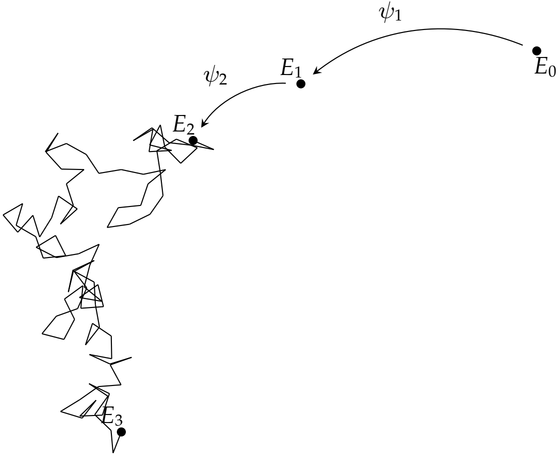
Folklore workaround: Distributed trusted setup



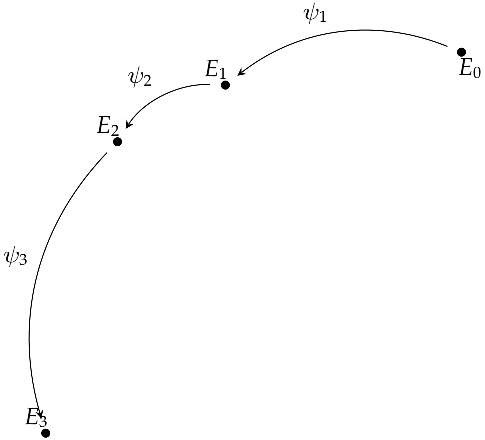
Folklore workaround: Distributed trusted setup



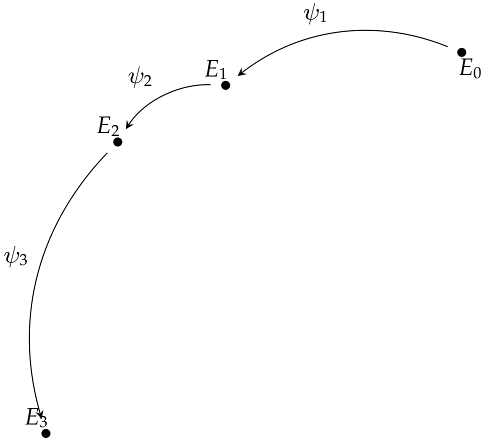
Folklore workaround: Distributed trusted setup



Folklore workaround: Distributed trusted setup

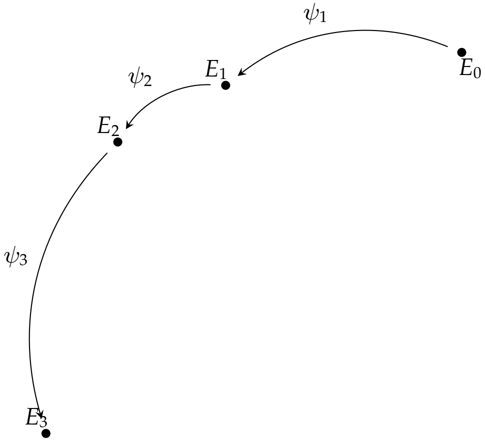


Folklore workaround: Distributed trusted setup



This is clearly secure as long as at least one participant is trustworthy.

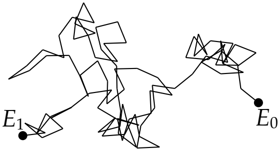
Folklore workaround: Distributed trusted setup



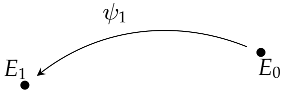
This is clearly secure as long as at least one participant is trustworthy — **or is it?**

Dumb attack: Simply restart from E_0

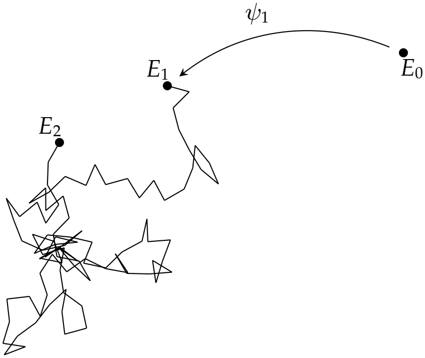
Dumb attack: Simply restart from E_0



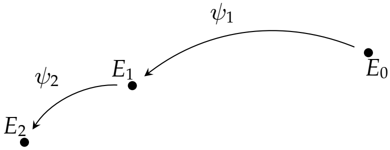
Dumb attack: Simply restart from E_0



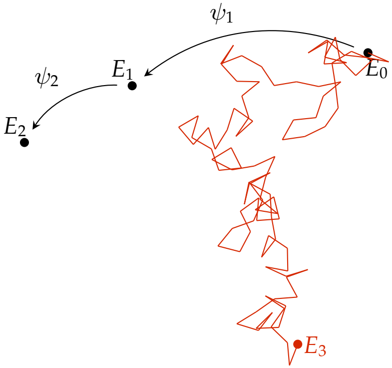
Dumb attack: Simply restart from E_0



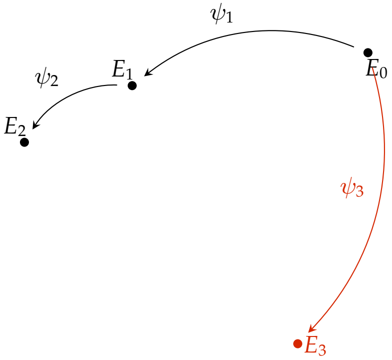
Dumb attack: Simply restart from E_0



Dumb attack: Simply restart from E_0



Dumb attack: Simply restart from E_0

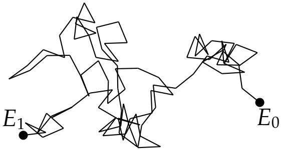


The solution: Proof of Isogeny Knowledge

Solution: **a zero-knowledge proof for each isogeny** $\psi_i \colon E_{i-1} \to E_i$.

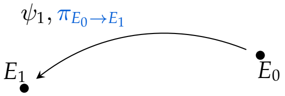
The solution: Proof of Isogeny Knowledge

Solution: **a zero-knowledge proof for each isogeny** $\psi_i \colon E_{i-1} \to E_i$.



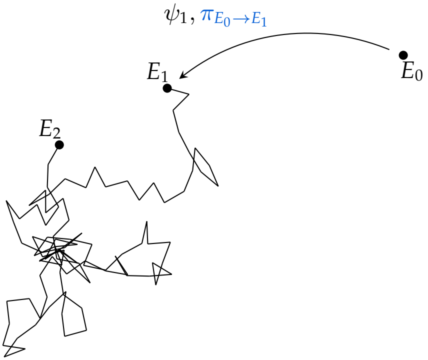
The solution: Proof of Isogeny Knowledge

Solution: **a zero-knowledge proof for each isogeny** $\psi_i : E_{i-1} \to E_i$.



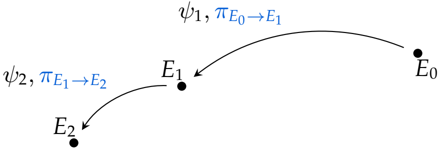
The solution: Proof of Isogeny Knowledge

Solution: **a zero-knowledge proof for each isogeny** $\psi_i \colon E_{i-1} \to E_i$.



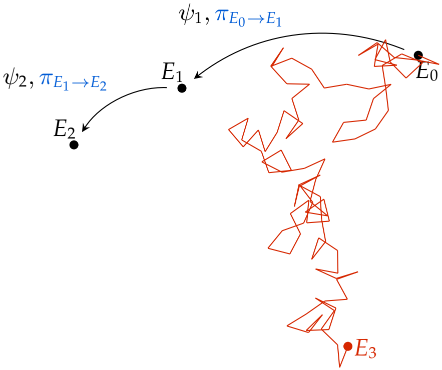
The solution: Proof of Isogeny Knowledge

Solution: **a zero-knowledge proof for each isogeny** $\psi_i \colon E_{i-1} \to E_i$.



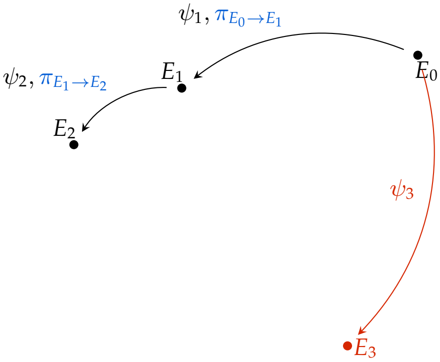
The solution: Proof of Isogeny Knowledge

Solution: **a zero-knowledge proof for each isogeny** $\psi_i \colon E_{i-1} \to E_i$.



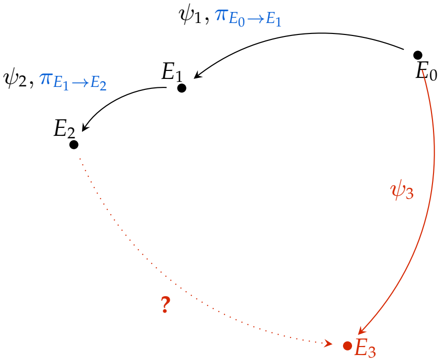
The solution: Proof of Isogeny Knowledge

Solution: **a zero-knowledge proof for each isogeny** $\psi_i \colon E_{i-1} \to E_i$.



The solution: Proof of Isogeny Knowledge

Solution: **a zero-knowledge proof for each isogeny** $\psi_i \colon E_{i-1} \to E_i$.



Main result

Assuming $\text{End}(E)$ is hard to compute, the trusted-setup protocol is provably secure in the simplified UC model if the proof of knowledge π is

- Correct for the relation

  $\varphi\colon E_0 \to E_1$ is a cyclic d-isogeny.

- Special-sound for the relation

  $\varphi\colon E_0 \to E_1$ is a cyclic isogeny (not necessarily of degree d).

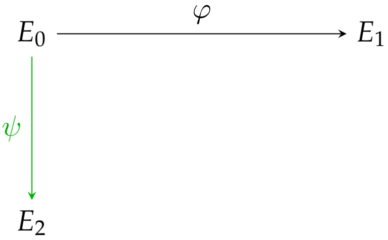
- Statistically **zero-knowledge**.

  $\Longrightarrow$ Trusted setup is resistant against future cryptanalysis.

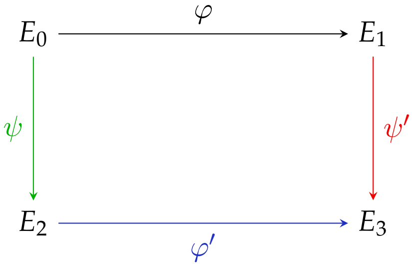
Starting point: proof of isogeny knowledge

$$E_0 \xrightarrow{\varphi} E_1$$

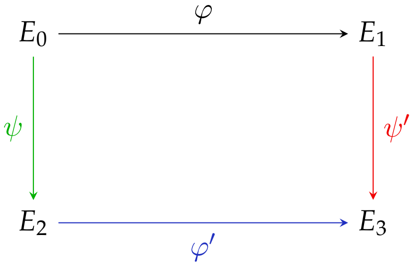
Starting point: proof of isogeny knowledge



Starting point: proof of isogeny knowledge



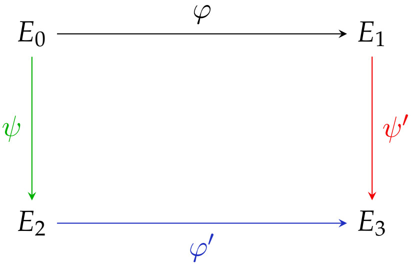
Starting point: proof of isogeny knowledge



Good things:

- No auxiliary points
- No SIDH attacks!!

Starting point: proof of isogeny knowledge



Good things:

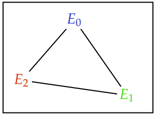
- No auxiliary points
- No SIDH attacks!!

Bad things:

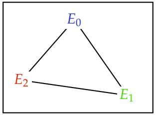
- Isogenies are rational $\Longrightarrow$ short
- Only computational ZK

Achieving statistical zero-knowledge (in theory)

- The supersingular isogeny graph is Ramanujan.
  $\implies$ Random walks quickly converge to $\approx$uniform.



Achieving statistical zero-knowledge (in theory)

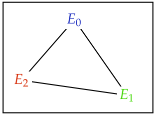


- The supersingular isogeny graph is Ramanujan.
  $\implies$ Random walks quickly converge to $\approx$uniform.

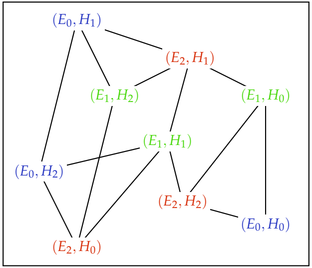
- ZK depends on uniformity of curve *with a subgroup*.
  $\implies$ Need supersingular graph *with level structure*.

Achieving statistical zero-knowledge (in theory)

- The supersingular isogeny graph is Ramanujan.
  $\implies$ Random walks quickly converge to ≈uniform.

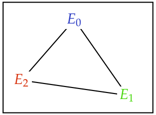


- ZK depends on uniformity of curve *with a subgroup*.
  $\implies$ Need supersingular graph *with level structure*.

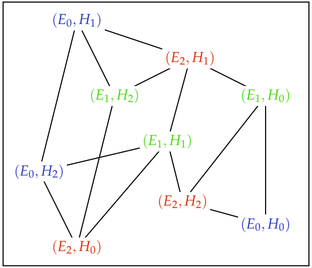


Achieving statistical zero-knowledge (in theory)

- The supersingular isogeny graph is Ramanujan.
  $\implies$ Random walks quickly converge to $\approx$uniform.



- ZK depends on uniformity of curve *with a subgroup*.
  $\implies$ Need supersingular graph *with level structure*.
- The graph with level structure is also Ramanujan!
  $\implies$ More information revealed, hence longer walks.



Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

$\Longrightarrow$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".

Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

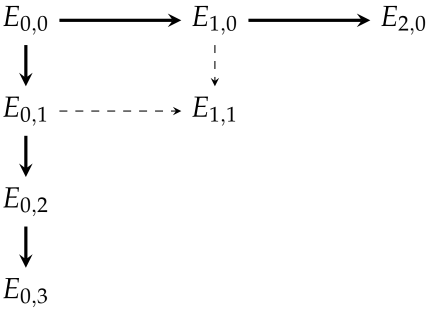
$\implies$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".

$$
\begin{array}{ccccc}
E_{0,0} & \longrightarrow & E_{1,0} & \longrightarrow & E_{2,0} \\
\downarrow & & & & \\
E_{0,1} & & & & \\
\downarrow & & & & \\
E_{0,2} & & & & \\
\downarrow & & & & \\
E_{0,3} & & & &
\end{array}
$$

Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

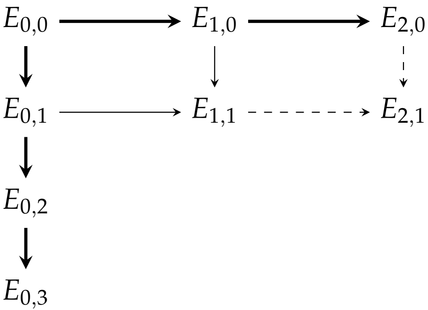
$\implies$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".



Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

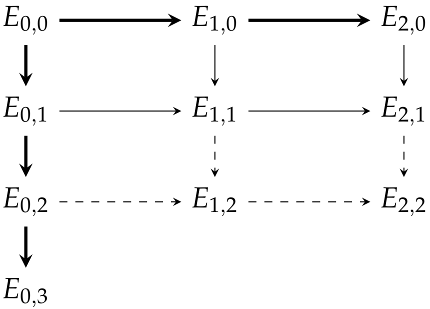
$\Longrightarrow$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".



Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

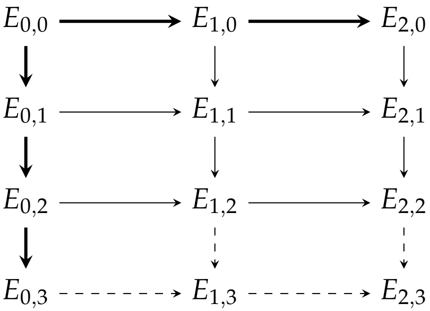
$\Longrightarrow$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".



Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

$\Longrightarrow$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".



Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

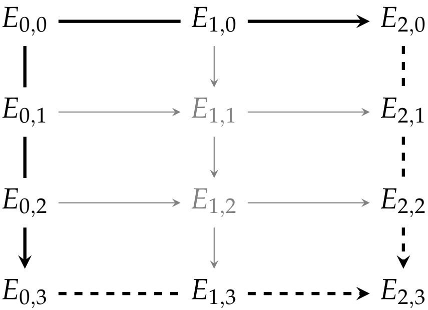
$\implies$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".

$$\begin{array}{ccccc}
E_{0,0} & \longrightarrow & E_{1,0} & \longrightarrow & E_{2,0} \\
\downarrow & & \downarrow & & \downarrow \\
E_{0,1} & \longrightarrow & E_{1,1} & \longrightarrow & E_{2,1} \\
\downarrow & & \downarrow & & \downarrow \\
E_{0,2} & \longrightarrow & E_{1,2} & \longrightarrow & E_{2,2} \\
\downarrow & & \downarrow & & \downarrow \\
E_{0,3} & \longrightarrow & E_{1,3} & \longrightarrow & E_{2,3}
\end{array}$$

Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

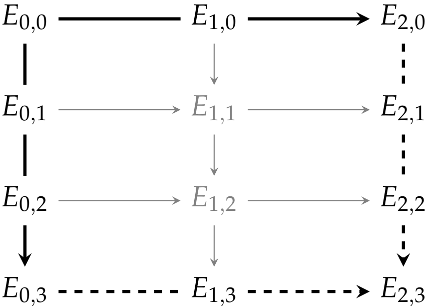
$\implies$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".



Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

$\Longrightarrow$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".

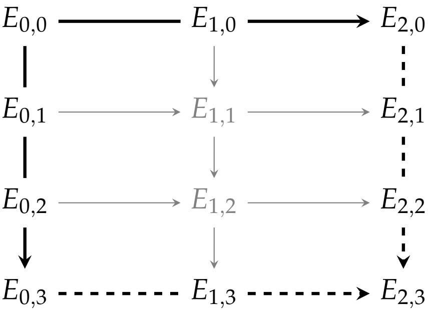


- Gluing $n \times m$ squares with degrees $2^a \times 3^b$: Complexity $nm \cdot \widetilde{O}(a+b)$.

Achieving statistical zero-knowledge (in reality)

- We need to construct SIDH squares with degrees much larger than p.
  Kernel points are irrational, which makes things tricky computationally.

$\Longrightarrow$ Solution: Glue together multiple SIDH squares. "**SIDH ladder**".



- Gluing $n \times m$ squares with degrees $2^a \times 3^b$: Complexity $nm \cdot \widetilde{O}(a+b)$.
- Any base field: Choose $a = b = 1$, potentially going to a degree-$O(1)$ extension.

Performance: Not great, not terrible

	Isogeny Lengths		Proof Size	Running Time	
$\log(p)$	$\rightarrow$	$\downarrow$	(kB)	Prove (s)	Verify (s)
434	705	890	191.19	2.96	0.32
503	774	977	215.75	4.17	0.44
610	1010	1275	404.32	12.12	1.24
751	1280	1616	662.63	26.07	2.89

Performance: Not great, not terrible

$\log(p)$	Isogeny Lengths $\rightarrow$	$\downarrow$	Proof Size (kB)	Running Time Prove (s)	Verify (s)
434	705	890	191.19	2.96	0.32
503	774	977	215.75	4.17	0.44
610	1010	1275	404.32	12.12	1.24
751	1280	1616	662.63	26.07	2.89

- Practical enough for trusted-setup protocols.
- We plan to run a trusted setup ceremony in the real world.

$\Longrightarrow$ Result: the world's first and only **SECUER**s!