Curves you can trust

Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo,
Tako Boris Fouotsa, Péter Kutas, Guido Maria Lido,
Simon-Philipp Merz, Travis Morrison, Lorenz Panny*,
Sikhar Patranabis, Benjamin Wesolowski, *et al.*

* Academia Sinica, Taipei, Taiwan

Crypto 2022 Rump Session, Santa Barbara, 16 August 2022

SECUERity

Common tool for attacking isogeny schemes:

KNOWN ENDOMORPHISMS

SECUERity

Common tool for attacking isogeny schemes:

KNOWN ENDOMORPHISMS

Obvious solution: **UNKNOWN ENDOMORPHISMS**.

SECUERity

Common tool for attacking isogeny schemes:

KNOWN ENDOMORPHISMS

Obvious solution: **UNKNOWN ENDOMORPHISMS**.

$\Longrightarrow$ *Supersingular Elliptic Curve of Unknown Endomorphism Ring*

SECUERity

Common tool for attacking isogeny schemes:

KNOWN ENDOMORPHISMS

Obvious solution: **UNKNOWN ENDOMORPHISMS**.

$\Longrightarrow$ *Supersingular Elliptic Curve of Unknown Endomorphism Ring*

For short: **SECUER**.

SECUERity

Common tool for attacking isogeny schemes:

KNOWN ENDOMORPHISMS

Obvious solution: **UNKNOWN ENDOMORPHISMS**.

$\Longrightarrow$ *Supersingular Elliptic Curve of Unknown Endomorphism Ring*

For short: **SECUER**.

British spelling: **SECURE**.

SECUERity

Common tool for attacking isogeny schemes:

KNOWN ENDOMORPHISMS

Obvious solution: **UNKNOWN ENDOMORPHISMS**.

$\Longrightarrow$ *Supersingular Elliptic Curve of Unknown Endomorphism Ring*

For short: **SECUER**.

British spelling: **SECURE**. [This joke stolen from Captain Luca De Feo.]

SECUERity

Common tool for attacking isogeny schemes:

KNOWN ENDOMORPHISMS

Obvious solution: **UNKNOWN ENDOMORPHISMS**.

$\Longrightarrow$ *Supersingular Elliptic Curve of Unknown Endomorphism Ring*

For short: **SECUER**.

British spelling: **SECURE**. [This joke stolen from Captain Luca De Feo.]

Tiny little problem: How to construct curves with **UNKNOWN ENDOMORPHISMS**?

Folklore solution

- Random curves have **UNKNOWN ENDOMORPHISMS**.

Folklore solution

- Random curves have **UNKNOWN ENDOMORPHISMS**.
- Only know how to sample randomly using random walks, which transport **KNOWN ENDOMORPHISMS**.

Folklore solution

- Random curves have **UNKNOWN ENDOMORPHISMS**.
- Only know how to sample randomly using random walks, which transport **KNOWN ENDOMORPHISMS**.

$\Longrightarrow$ Potential for **backdoors**; need ***trusted* setup**.

Folklore solution

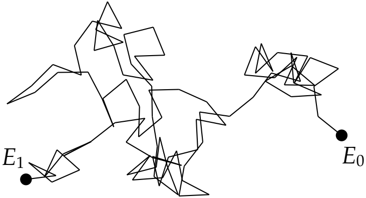
- Random curves have **UNKNOWN ENDOMORPHISMS**.
- Only know how to sample randomly using random walks, which transport **KNOWN ENDOMORPHISMS**.

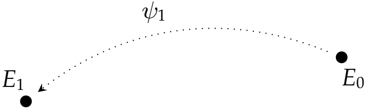
$\Longrightarrow$ Potential for **backdoors**; need ***trusted* setup**.

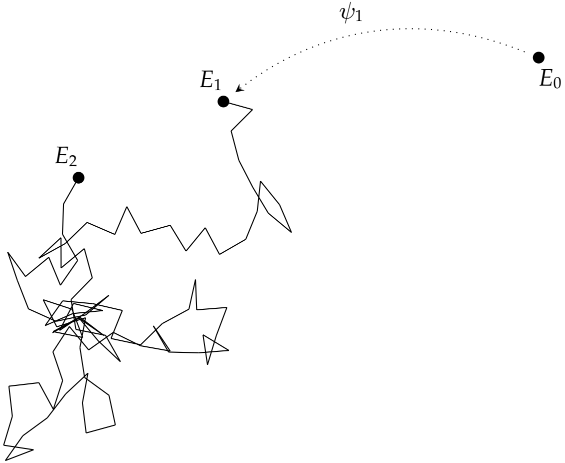
$\Longrightarrow$ **Distribute the trust:**

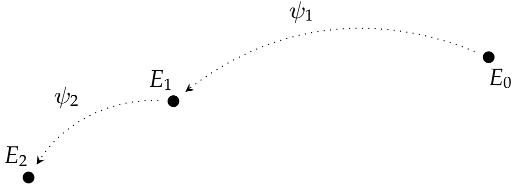
Chain secret random walks generated by different people.
Prevent cheating with a **Proof of Isogeny Knowledge**.

E_0


E_1
E_0


ψ_1
E_1
E_0


ψ_1
E_1
E_0
E_2


ψ_1
E_1
E_0
ψ_2
E_2

Our work

- PoIK for supersingular curves (any base field).

Our work

- PoIK for supersingular curves (any base field).
- Statistically zero-knowledge.

Our work

- PoIK for supersingular curves (any base field).
- Statistically zero-knowledge.
- Computationally sound (*pure* isogeny problem).

Our work

- PoIK for supersingular curves (any base field).
- Statistically zero-knowledge.
- Computationally sound (*pure* isogeny problem).
- Planning to run a ceremony in reality!

Application: Defending SIDH/SIKE in depth

Application: Defending SIDH/SIKE in depth

```
https://ia.cr/2022/975
https://ia.cr/2022/1026
https://ia.cr/2022/1038
```

SIDH squares are (still!) our best friend

$$\begin{tikzcd}
E_0 \arrow[r] \arrow[d] & E_A \arrow[d] \\
E_B \arrow[r] & E_{AB}
\end{tikzcd}$$

Formerly known as “SIDH square” ☠.

SIDH squares are (still!) our best friend

$$\begin{tikzcd}
& E_0 \arrow[dl] \arrow[dr] & \\
E_A \arrow[dr] & & E_B \arrow[dl] \\
& E_{AB} &
\end{tikzcd}$$

Formerly known as “SIDH square” ☠.

Diamonds are our best friend

Formerly known as "SIDH square" ☠. Now rebranded as

isogeny diamond.

Thanks!