

# Another Round of Breaking and Making Quantum Money: How Not to Do It, and More

*Authors:*

**Jiahui Liu**

University of Texas, Austin

**Hart Montgomery**

Linux Foundation

(Formerly Fujitsu)

**Mark Zhandry**

NTT Research

(Formerly Princeton)

*Presented by:*

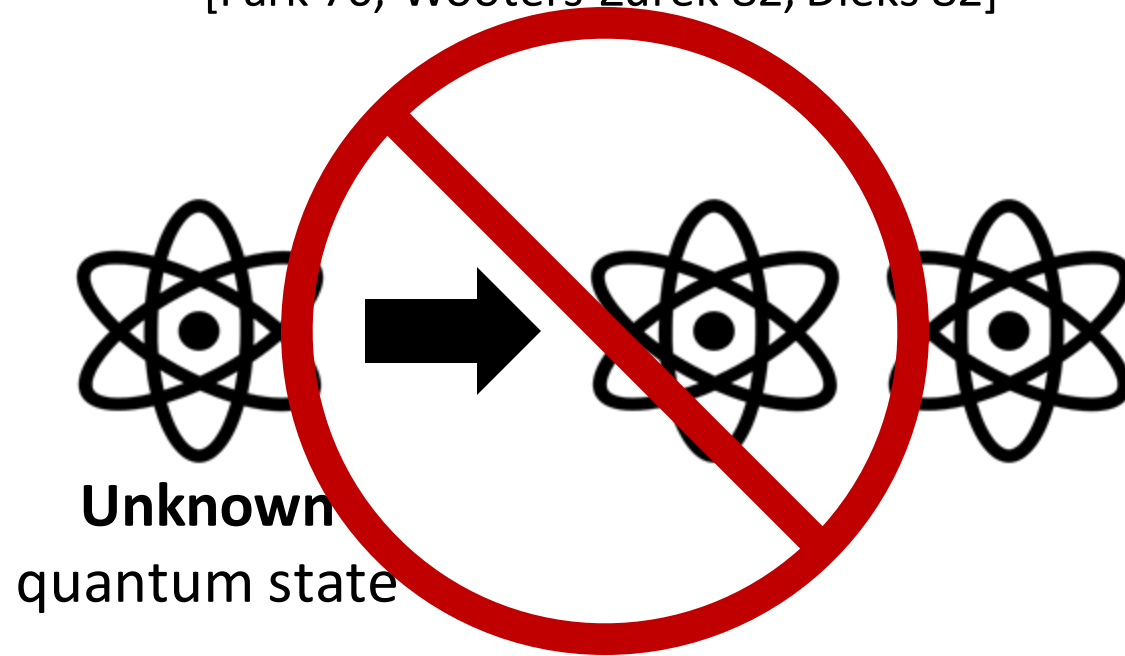
**Barak Nehoran**

Princeton University

Background

# No-cloning Theorem

[Park'70, Wootters-Zurek'82, Dieks'82]



# Secret key quantum money

[Wiesner'70]

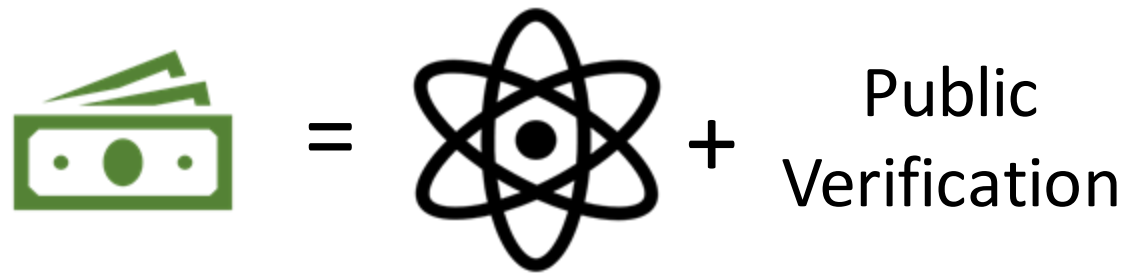


No-cloning → banknotes unforgeable

**Problem:** only mint can verify

# Public key quantum money

[Aaronson'09]



**Challenge:** state information-theoretically “known”

→ information-theoretically clonable

→ need **crypto** + quantum info to get no-cloning

# (Public Key) Quantum Money is Hard!

[Aaronson'09]: random stabilizer states

X

[Lutomirski-Aaronson-Farhi-Gosset-Hassidim-Kelner-Shor'10]

[Farhi-Gosset-Hassidim-Lutomirski-Shor'10]: knots

?

little published cryptanalysis effort

[Aaronson-Christiano'12]: polynomials hiding subspaces

X

[Pena-Faugère-Perret'14, Christiano-Sattath'16]

[Kane'18]: Modular forms

?

[Bilyk-Doliskani-Gong'22] some analysis

[Zhandry'19]: quadratic systems of equations

X

[Roberts'21]

[Zhandry'19]: post-quantum iO

?

Post-quantum iO not well understood

[Kane-Sharif-Silverberg'21]: Quaternion Algebras

?

No published cryptanalysis effort

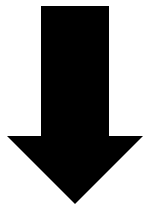
[Khesin-Lu-Shor'22]: lattices

?

No (prior) cryptanalysis effort

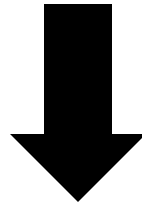
# This Work: Breaking and making quantum money

Attack on general class  
of lattice-based schemes



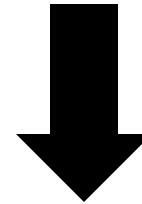
[Khesin-Lu-Shor'22]  
is insecure

“Walkable Invariant”  
framework + analysis



Identify sufficient  
conditions for  
[FGHLS'12] to be secure  
  
(unclear if conditions met)

New candidate walkable  
invariants



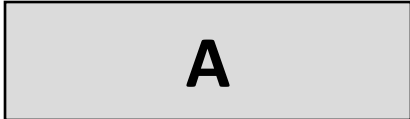

Approach to building  
quantum money from  
isogenies  
  
(one crucial missing piece)

# How *Not* To Build Quantum Money



# A lattice-based proposal

(folklore)

Verification key  
(aka serial number) =  , 

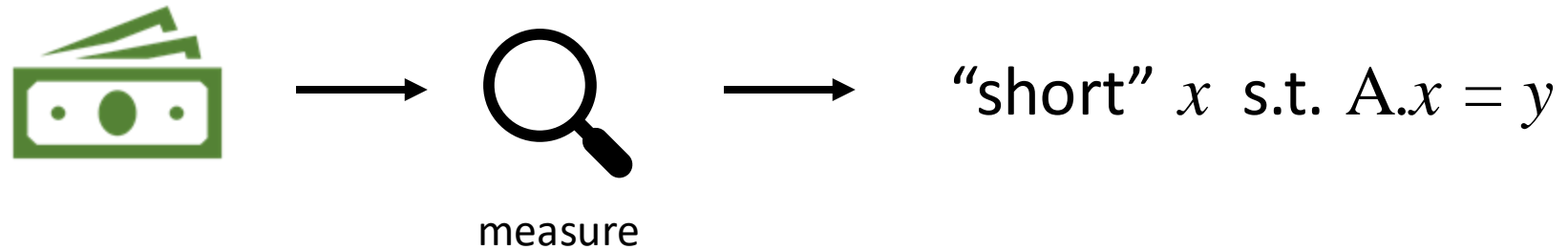


$$\propto \sum |x\rangle$$

“short”  $x$  s.t.  
 $A \cdot x \bmod q = y$

# Attack

( consequence of [Liu-Zhandry'19] )

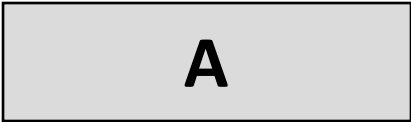



$$\text{money}_1 = |x\rangle \quad \text{money}_2 = |x\rangle$$

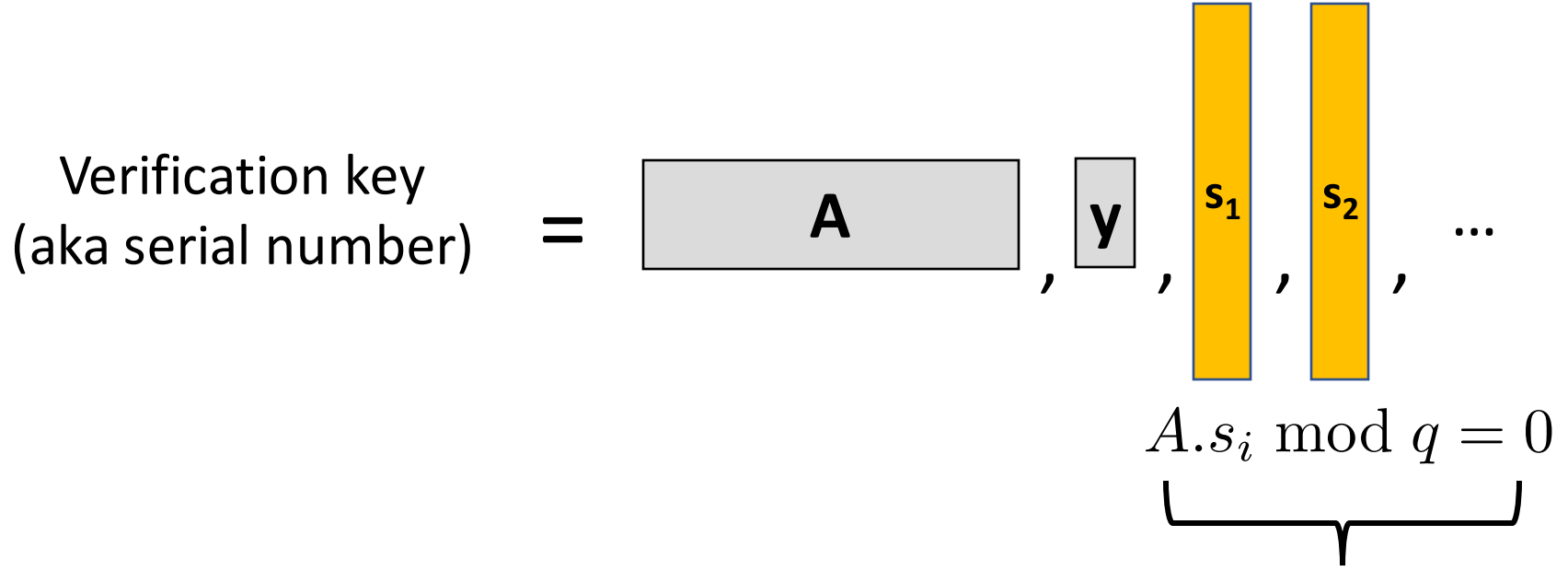
**Thm** [Liu-Zhandry'19]:  $\text{LWE} + \text{super-poly } q \rightarrow \text{SIS hash function is } \textit{collapsing}$

**Cor:** Attack fools *any* efficient verification procedure

# A more general proposal

Verification key  
(aka serial number) =  , 

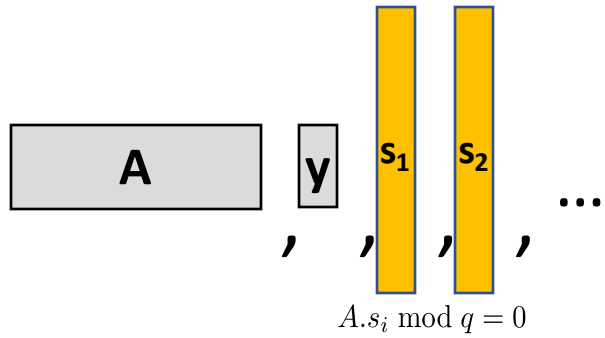
# A more general proposal



Trapdoors for A,  
help with verification

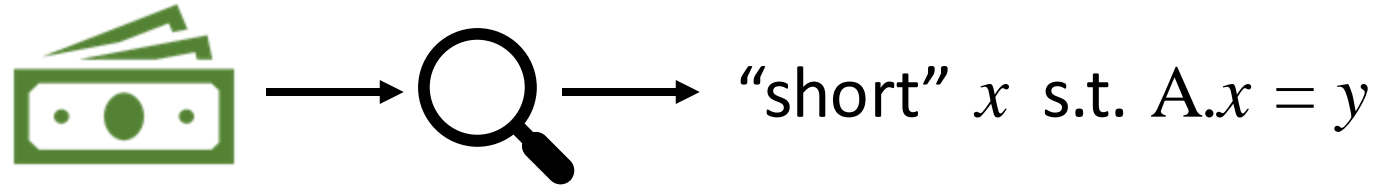
Example: can re-interpret  
[Khesin-Lu-Shor'22] in this form

= "short"



Attack  
(this work)

$$\propto \sum_{\text{"short"} x \text{ s.t. } A \cdot x \bmod q = y} |x\rangle$$



$$1, 2 = \sum_{u_1, u_2, \dots \text{ s.t. } z \text{ is "short"}} |z = x + u_1 s_1 + u_2 s_2 + \dots\rangle$$

**Thm** (this work):

1. LWE + **any**  $q \rightarrow$  fools any efficient verification
2. Efficiently construct fake money state from  $x$  in many natural settings

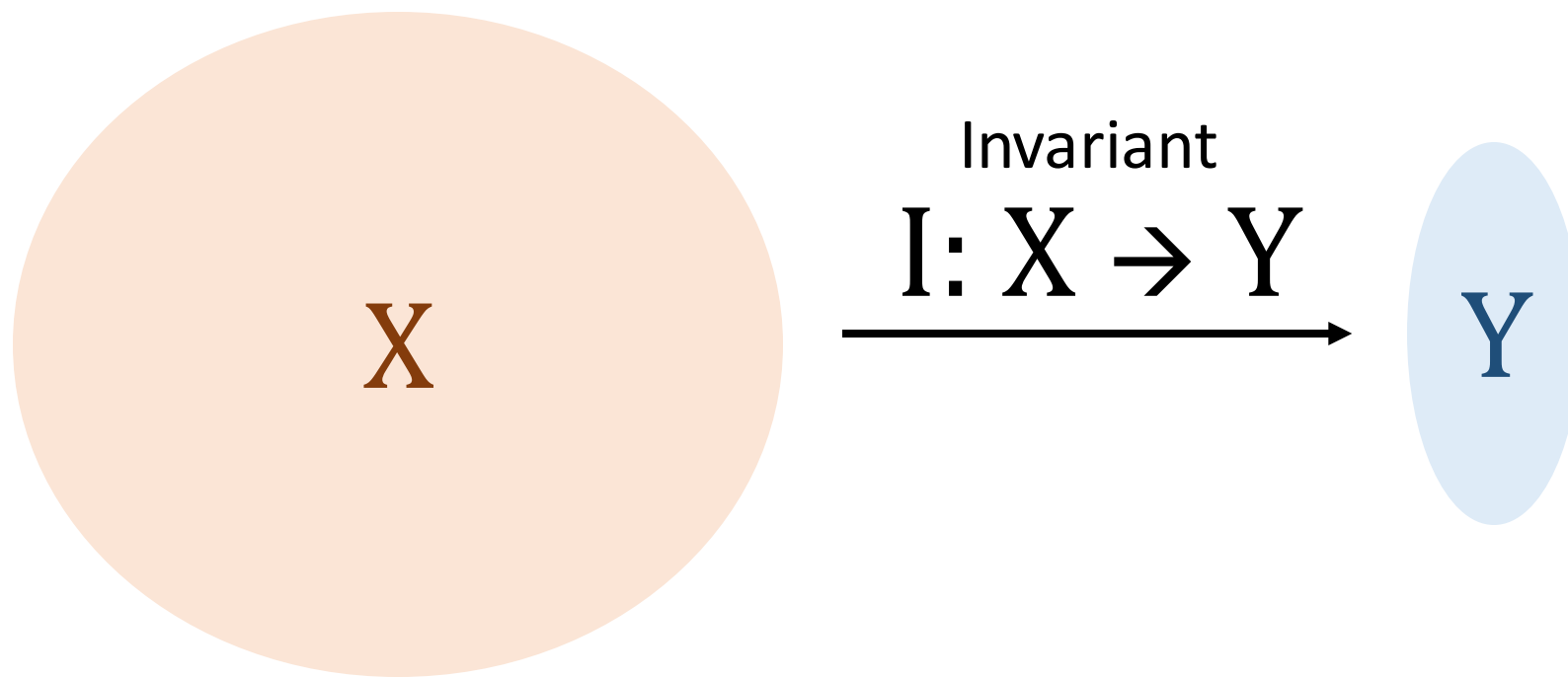
**Cor:** Scheme from [Khesin-Lu-Shor'22] is insecure

Along the way, improve known results about k-LWE problem

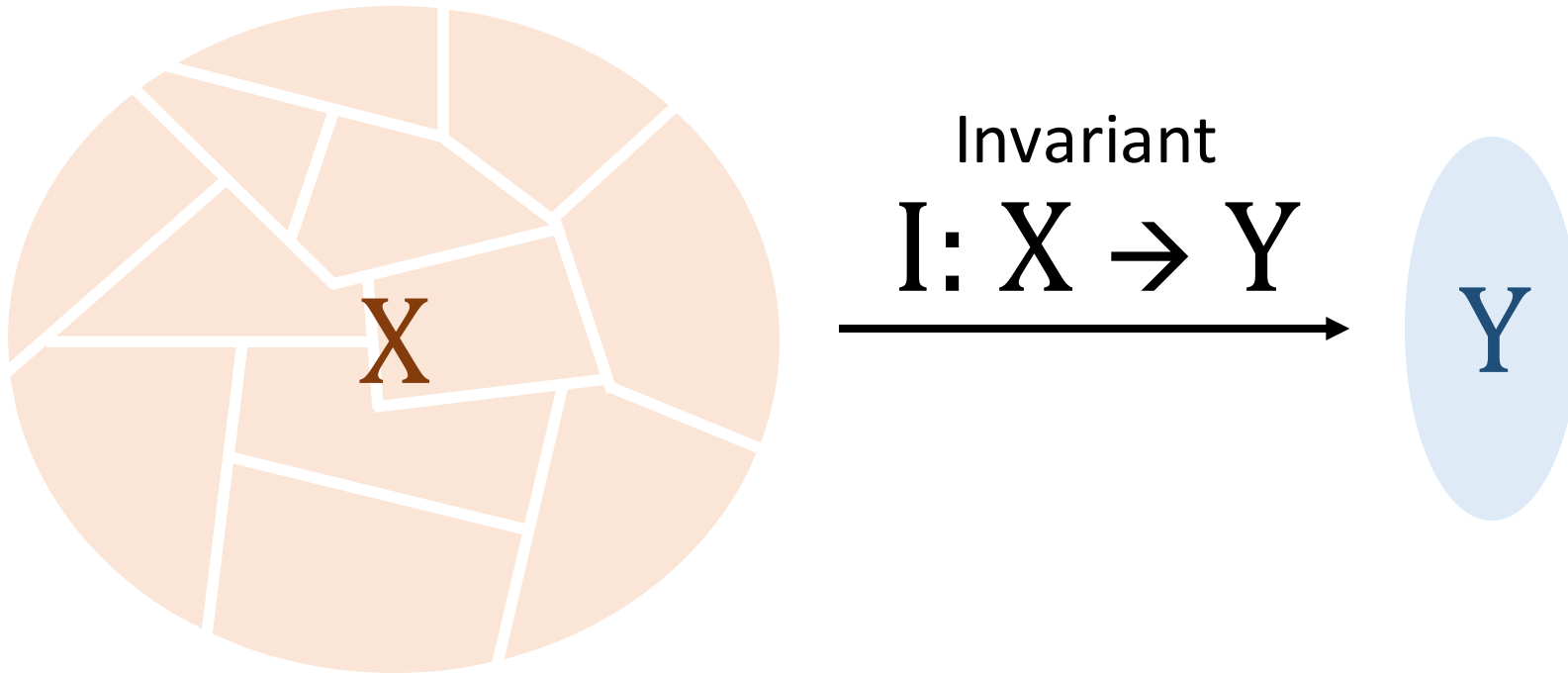
# Walkable Invariant Framework

(abstraction of [FGHLS'12])

# The Walkable Invariant Framework



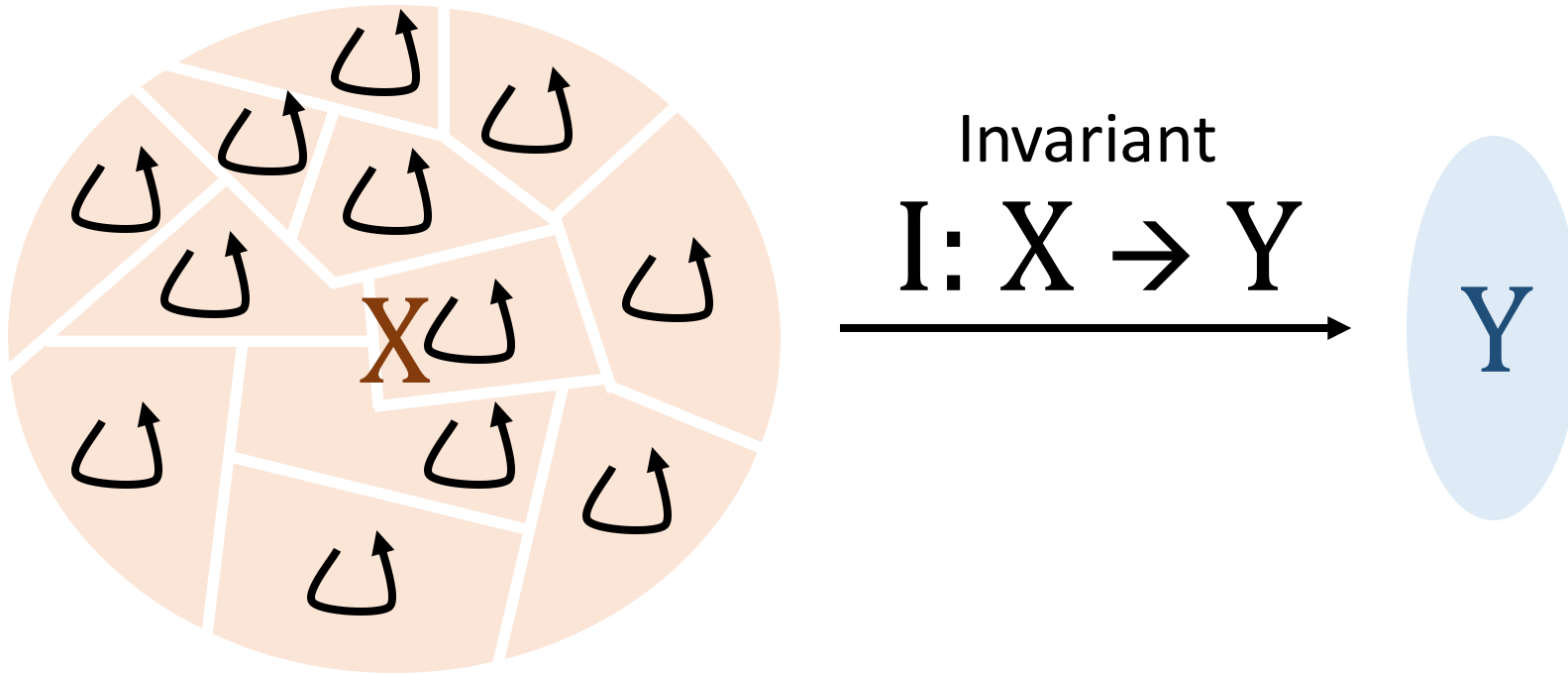
# The Walkable Invariant Framework



Permutations  $\sigma_i : X \rightarrow X$



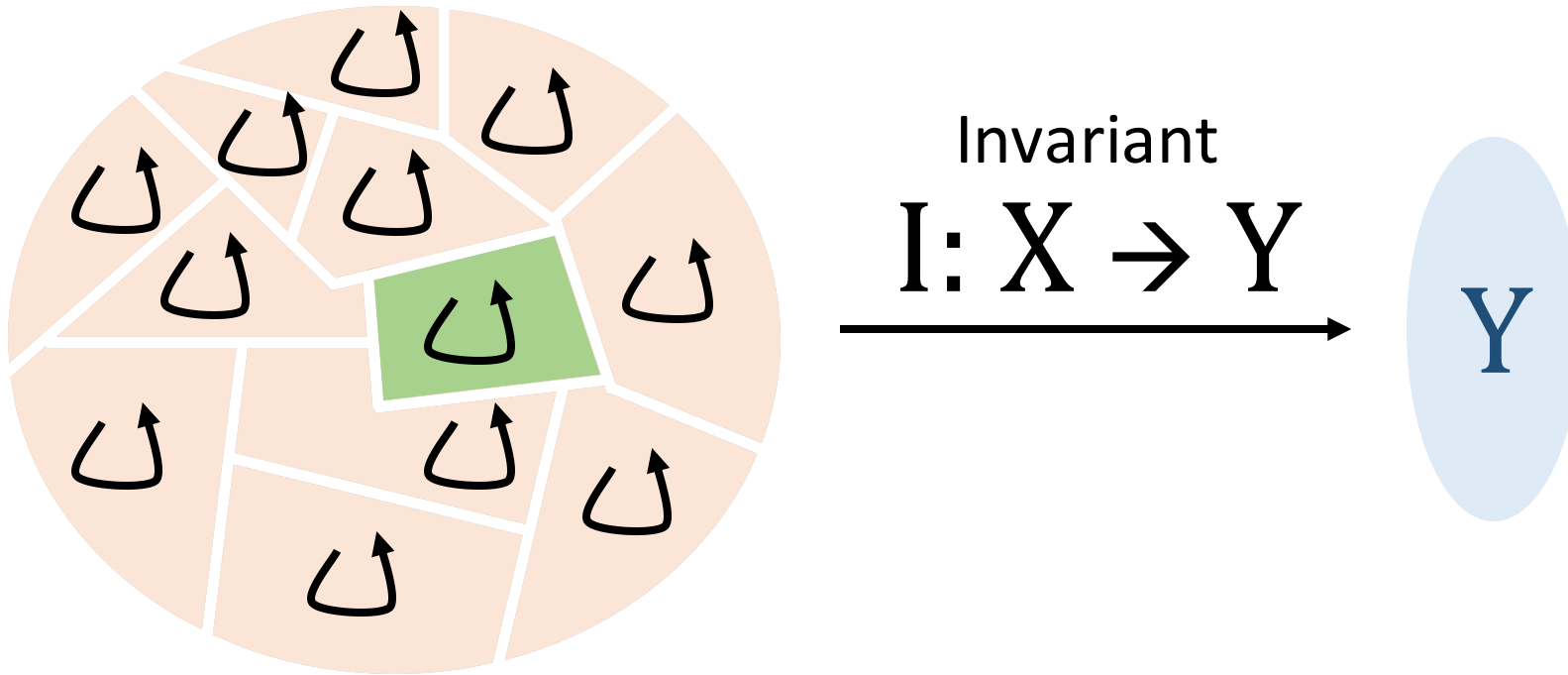
# The Walkable Invariant Framework



Permutations  $\sigma_i : X \rightarrow X$

$$I(\sigma_i(x)) = I(x)$$

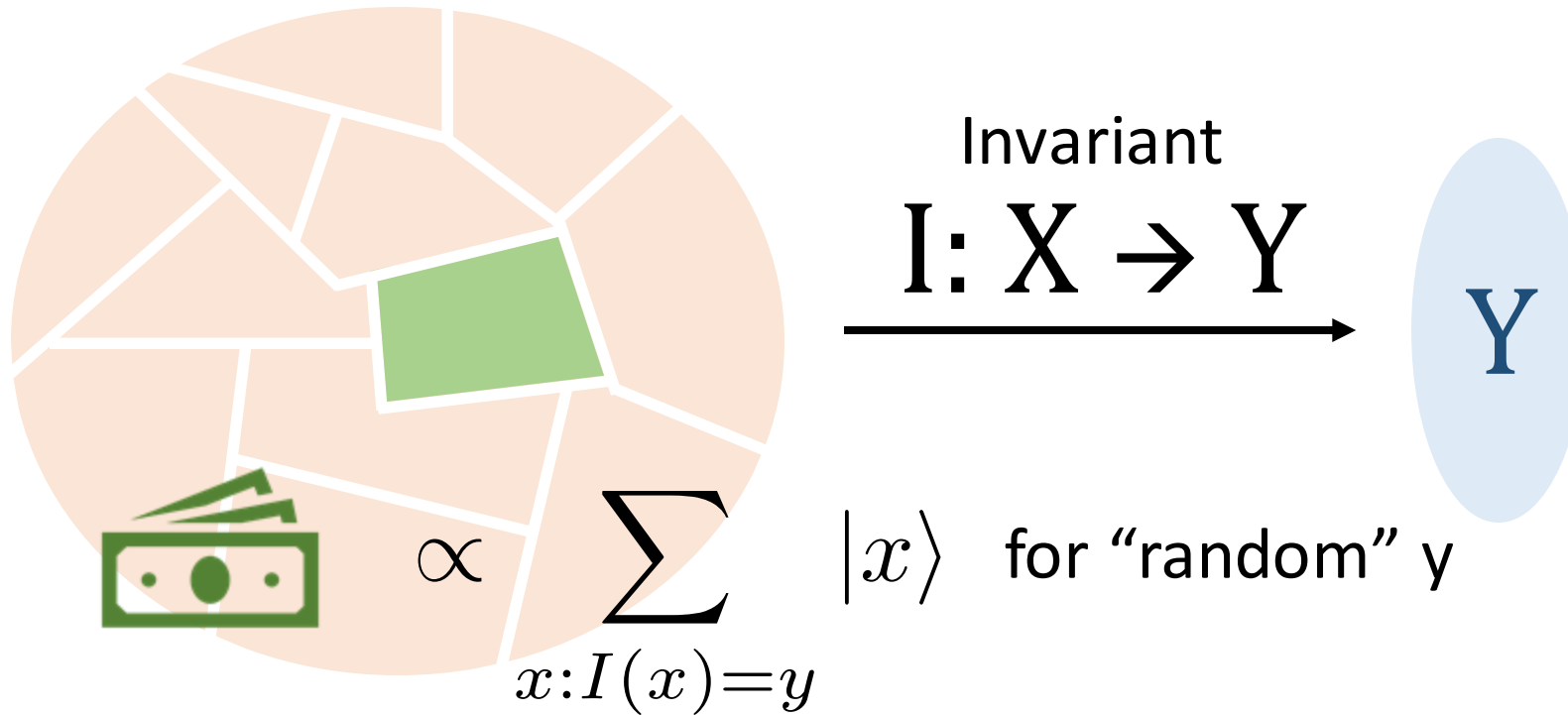
# The Walkable Invariant Framework



Permutations  $\sigma_i : X \rightarrow X$

$$I(\sigma_i(x)) = I(x)$$

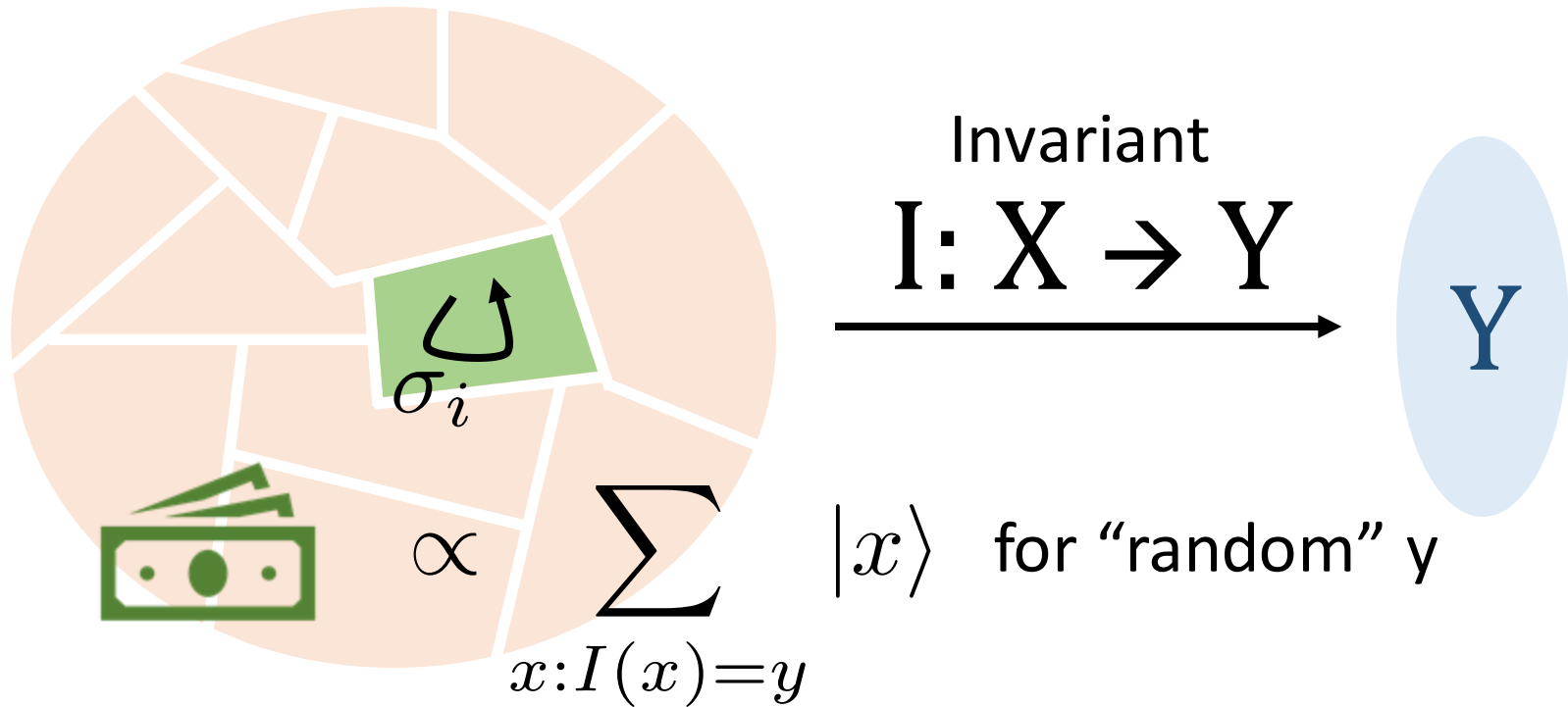
# The Walkable Invariant Framework



Mint

- 1. Creates uniform superposition over  $X$
- 2. Measure  $I(x)$

# The Walkable Invariant Framework

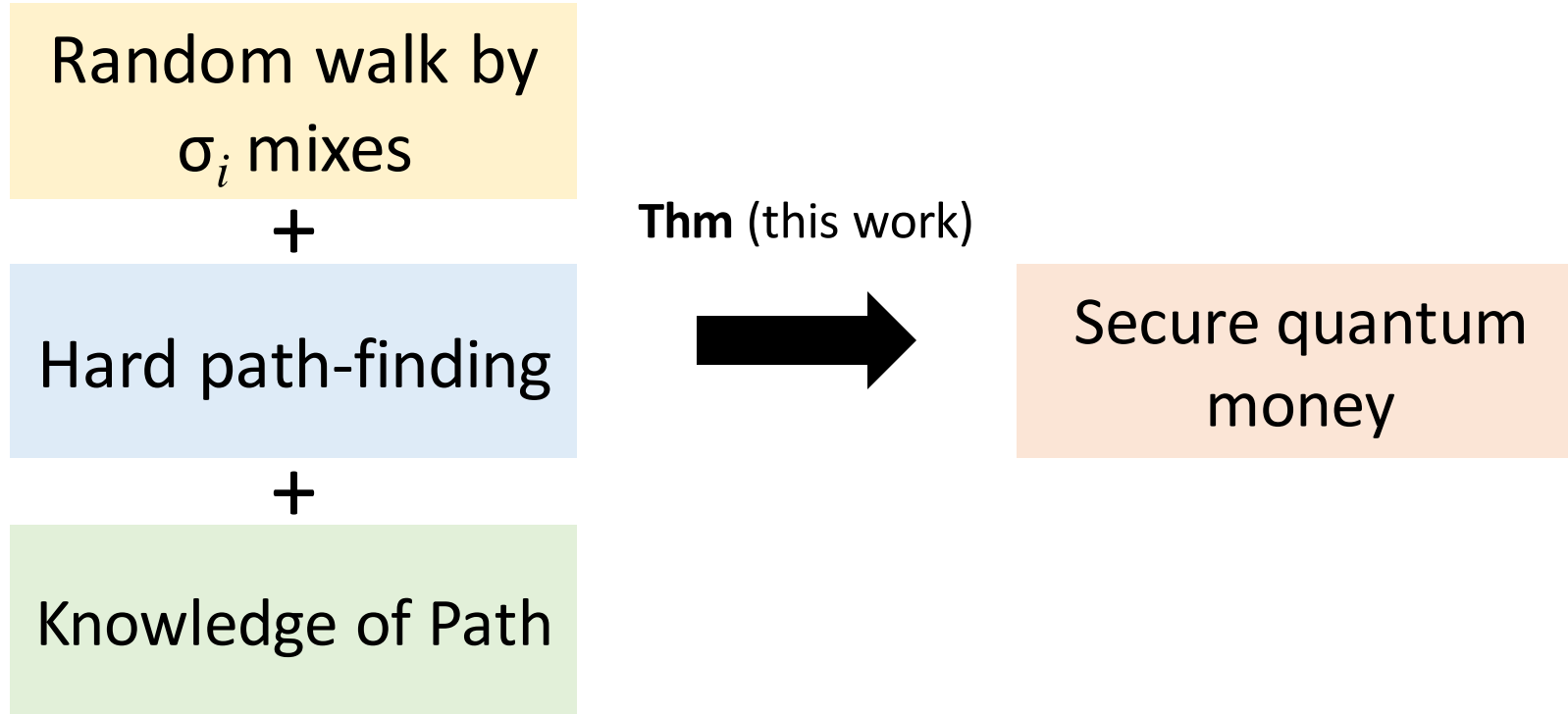


Public Verification

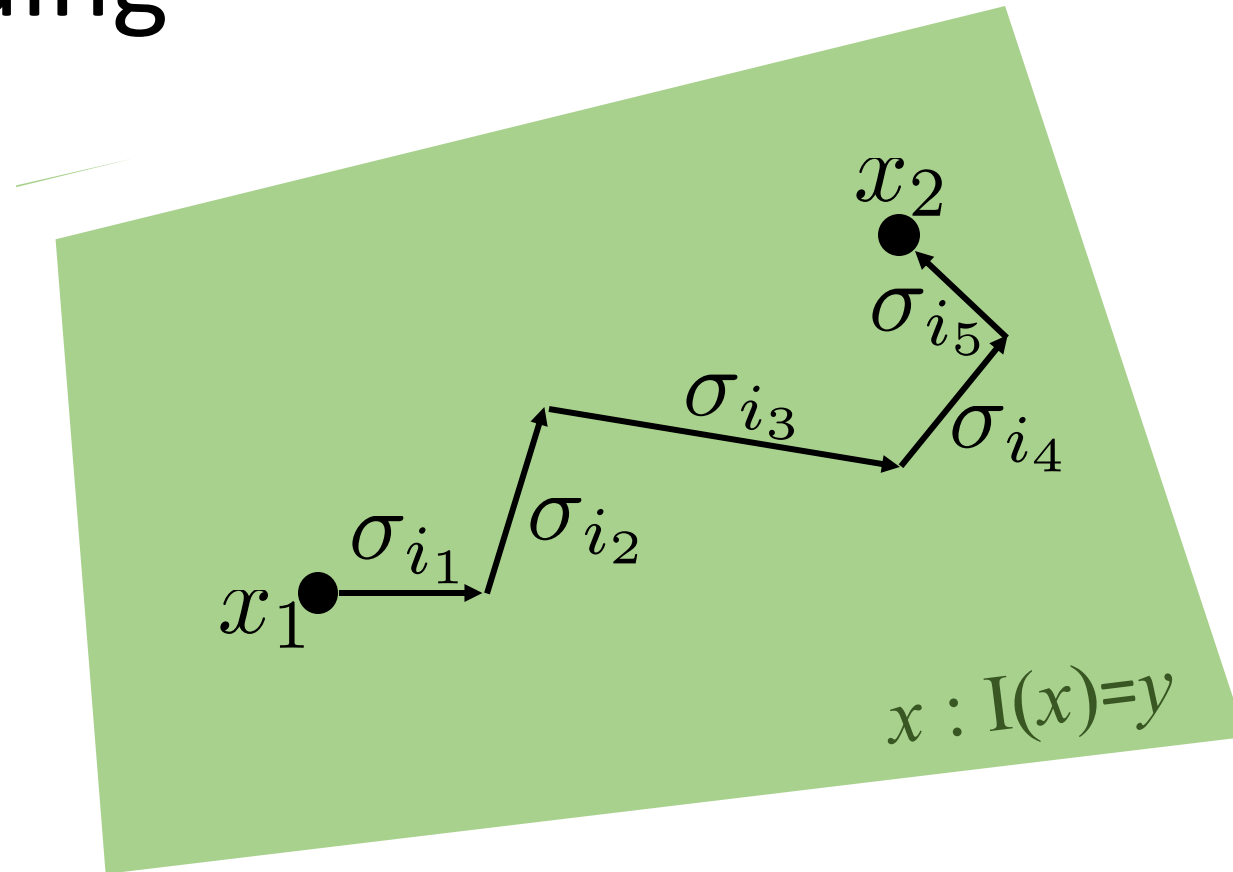
1. Test that support is on  $x$  s.t.  $I(x)=y$
2. Test that state is unchanged under action by  $\sigma_i$

Use a version of the swap test

# Recipe for Quantum Money from Invariants

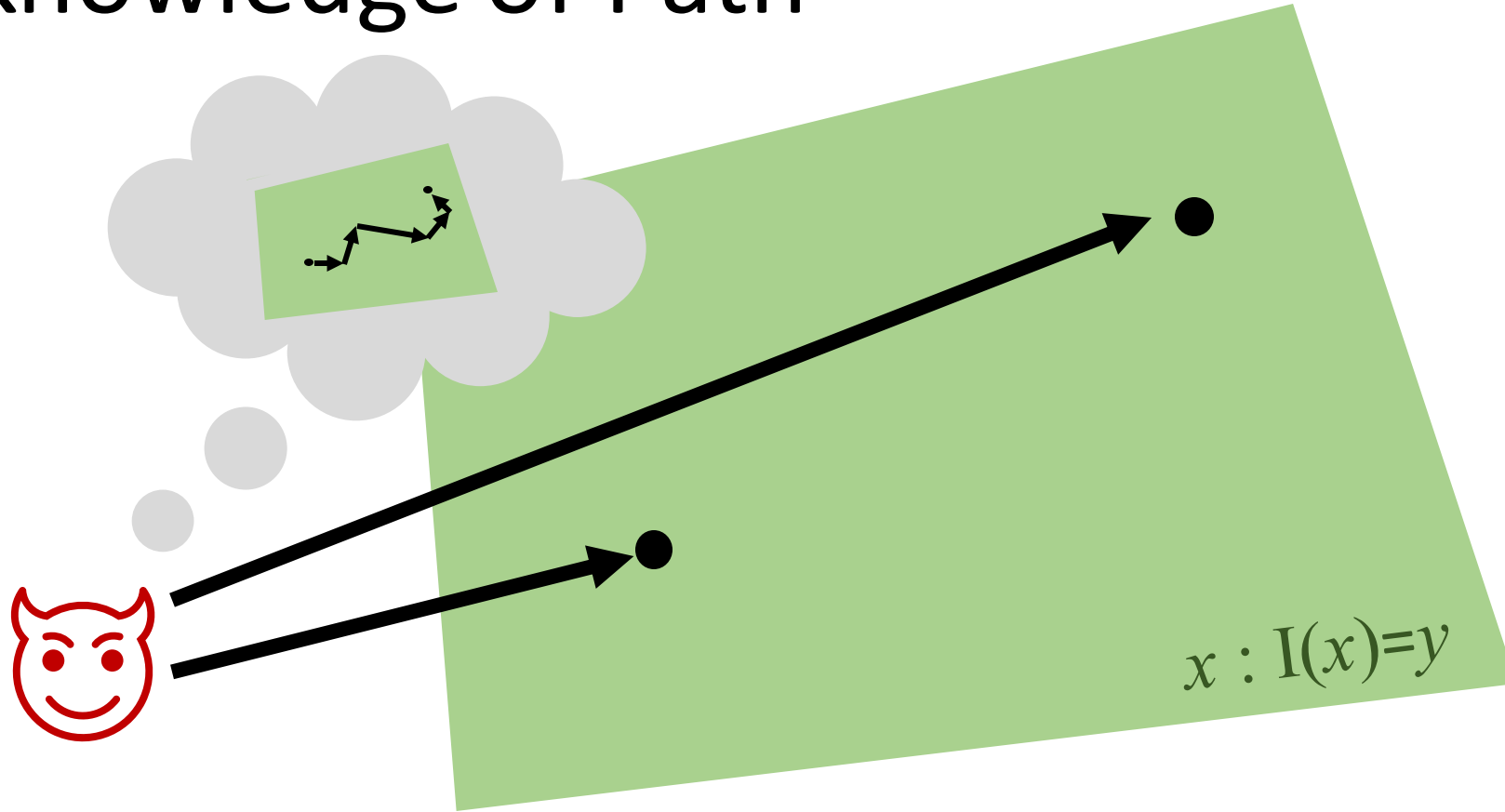


# Hardness of Path-finding



Given random  $x_1, x_2$  with same invariant, hard to compute a “path” =  $i_1, i_2, \dots$

# Knowledge of Path



Impossible to generate  $x_1, x_2$  with same invariant without knowing path

# Applying to Quantum Money from Knots [FGHLS'12]

Previously: security merely conjectured, with minimal analysis.  
 This framework allows justifying security.

$X$  = knot diagrams

$\sigma_i$  = Reidemeister moves

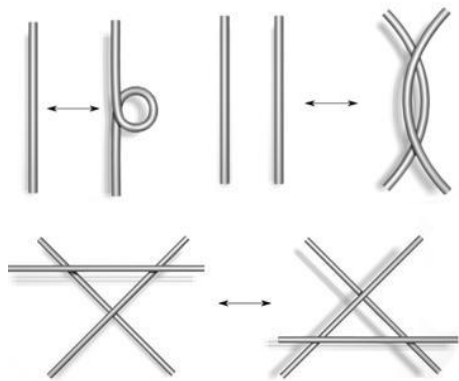


Image credit: Wikimedia

$I(x)$  = Alexander polynomial

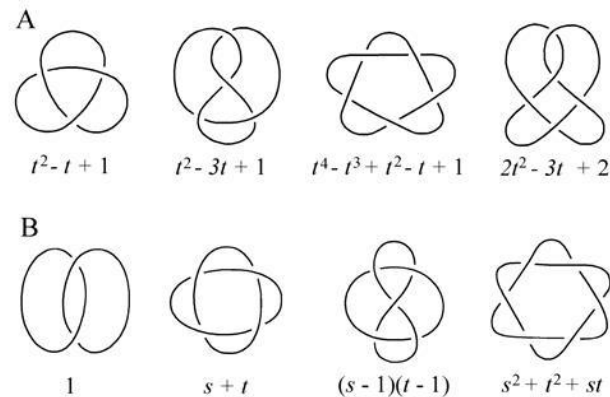


Image credit: [Vologodskii'06]

Hard path-finding

Knowledge of Path

Random walk by  $\sigma_i$  mixes

appear plausible

unclear



**New Instantiations**

# Isogenies over (supersingular) elliptic curves

Path finding = computing isogenies, widely believe to be hard

Knowledge of Path = analog of knowledge of exponent from groups

Seems quite plausible, but need more cryptanalysis effort

**Problem:** unknown how to create  
uniform superposition over  $X$  for minting

Closely related to major open question of  
obliviously sampling super-singular elliptic curves

# Other instantiations



Re-randomizeable Functional Encryption



Group actions + classical oracle

Thanks!