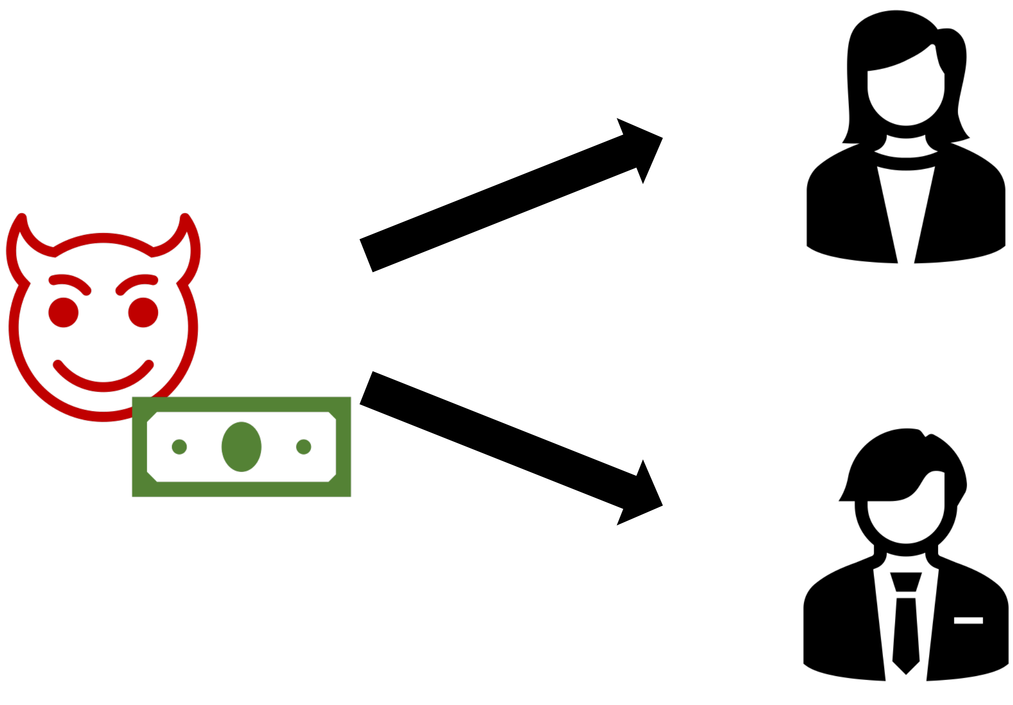
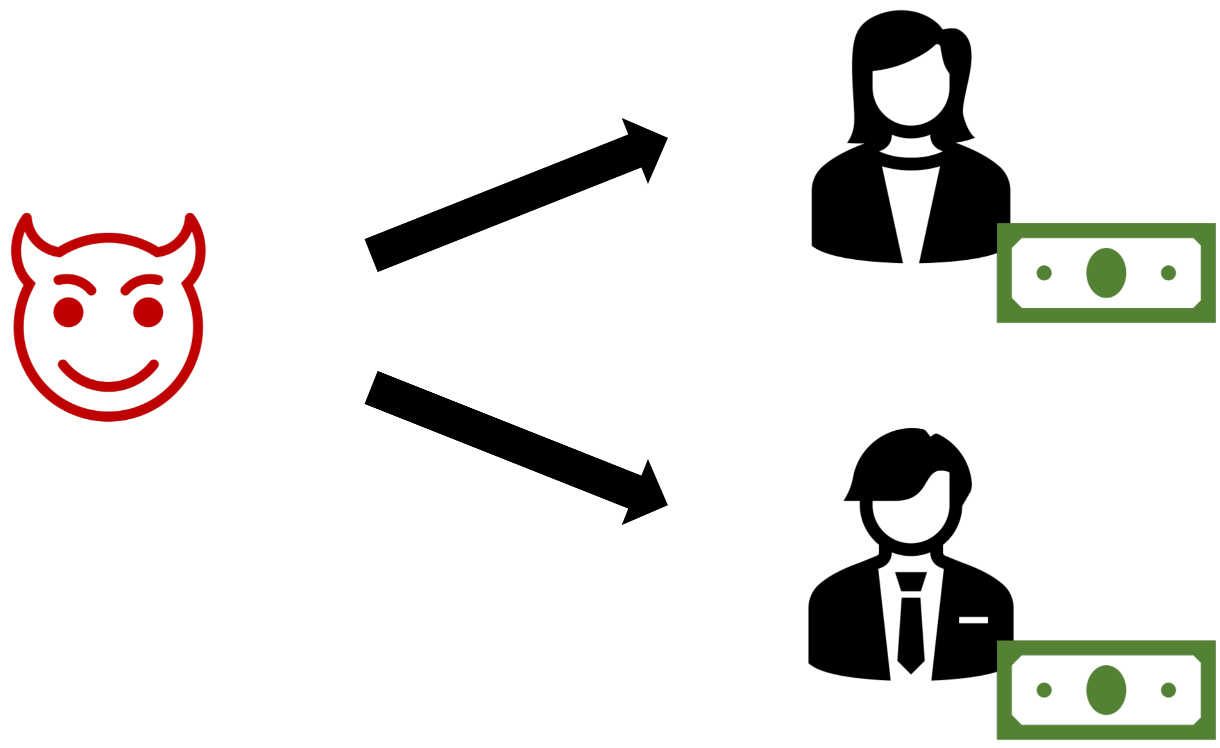
Recent Developments in Quantum Money

Mark Zhandry
NTT Research

The Double Spend Problem



The Double Spend Problem

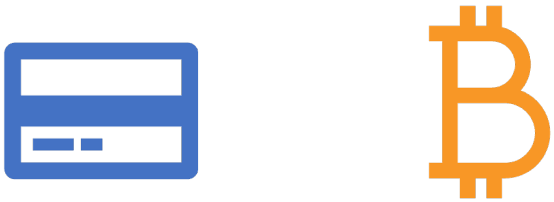


Classical Solutions

<u>Physical currency</u>

or at least too expensive
to convincingly copy

<u>Digital currency</u>

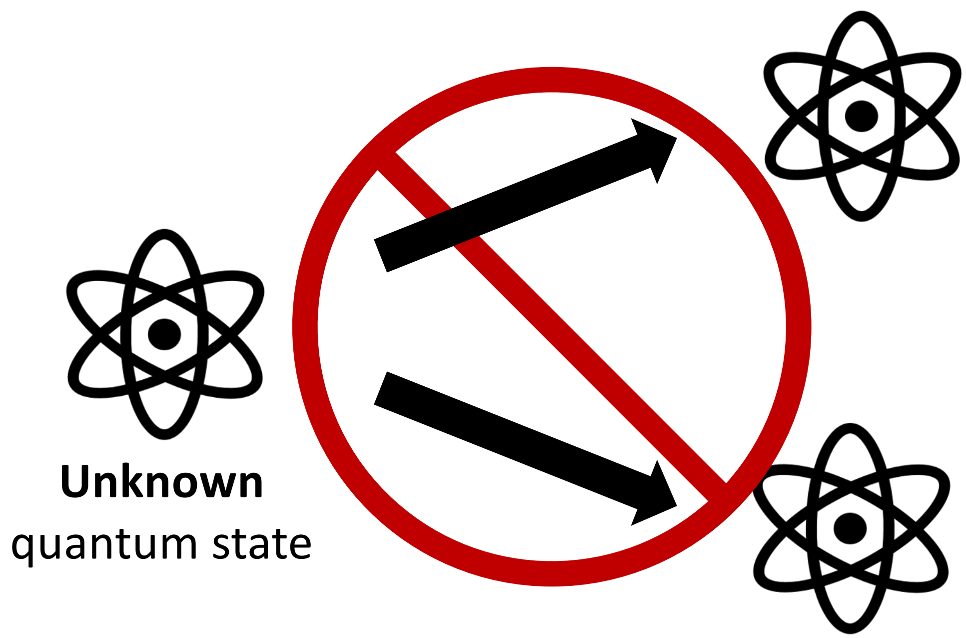


All need trusted third party to make
sure the money is yours to spend

Enter Quantum…

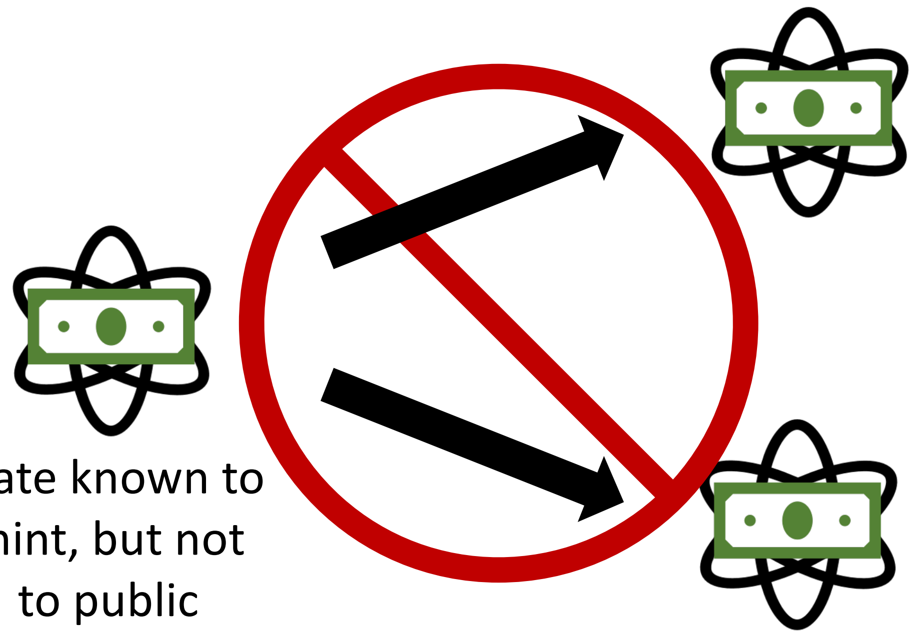
No-cloning Theorem

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



“Secret key” quantum money

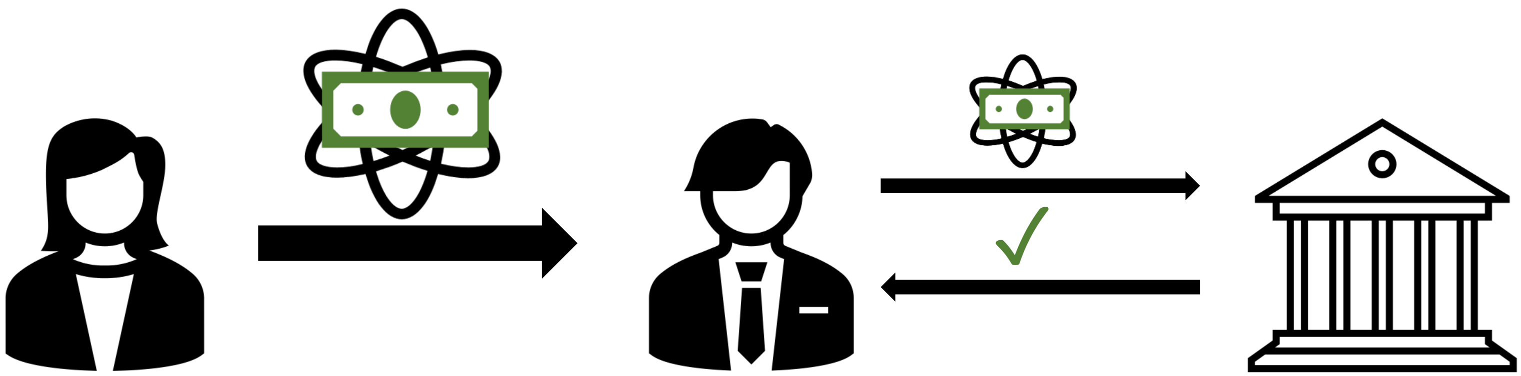
[Wiesner’70]



State known to mint, but not to public

$$\in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^n$$

Problem with SK quantum money



Because state is unknown to public, only mint can verify

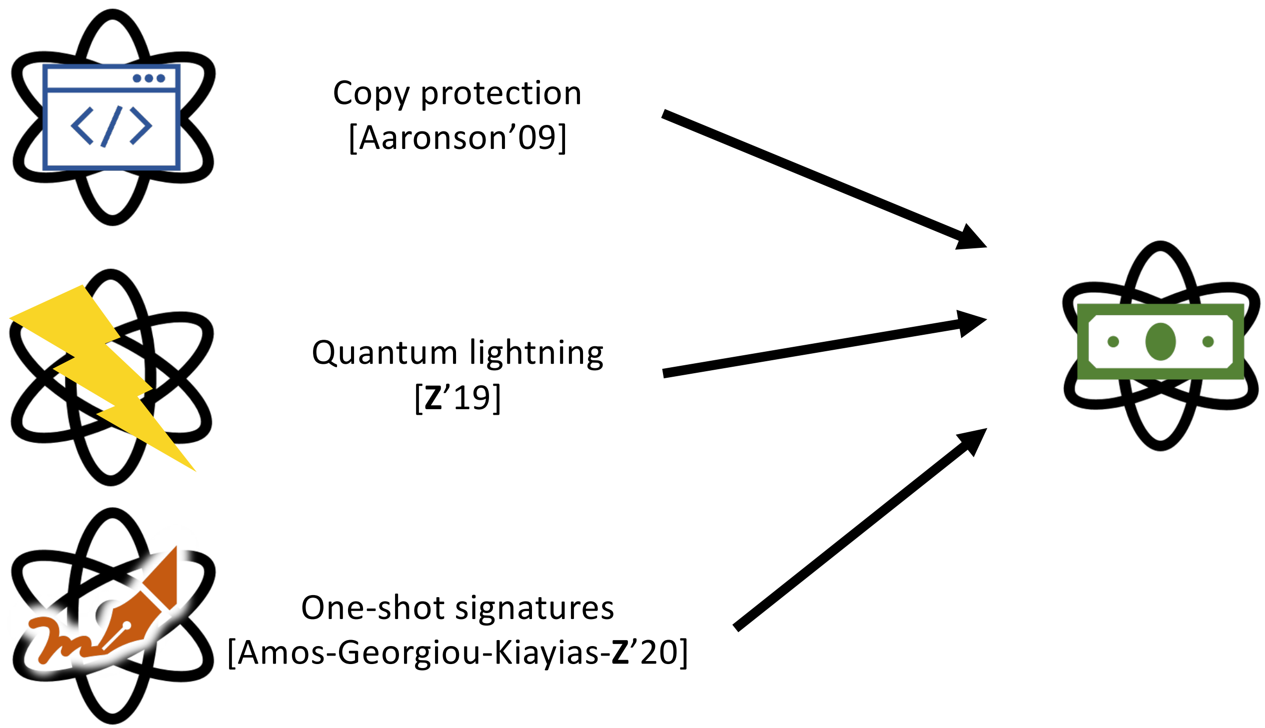
“Public key” quantum money

[Aaronson’09]

Mint only involved in making new notes, not verification

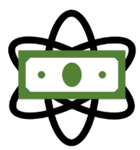
Numerous other advantages, for free

Beyond Quantum Money



Must construct PK quantum money on the way to realizing these objects

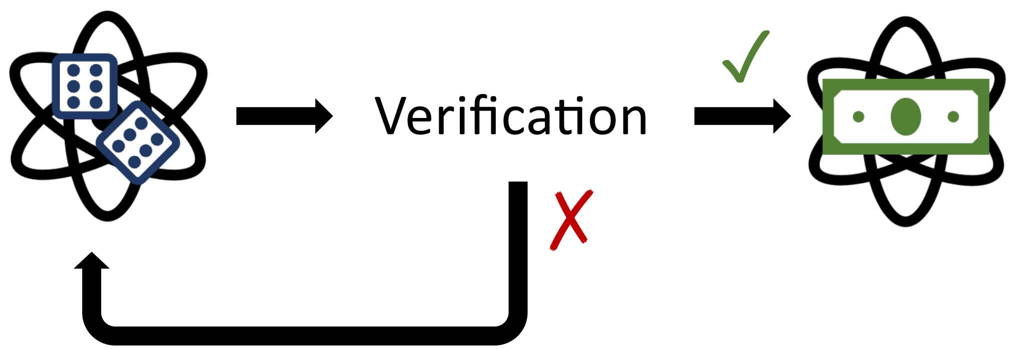
Beyond Quantum Money

Ideas (and failures) from 

- QKD [Bennet-Brassard’84]
- Certified deletion [Poremba’23, Bartusek-Garg-Goyal-Khurana-Malavolta-Raizes-Roberts’23, …]
- Post-quantum secure hash functions, signatures [Liu-**Z**’19, Liu-Montgomery-**Z**’23, **Z**’22]
- Verifiable quantum advantage, certified randomness [Yamakawa-**Z**’22]

Challenge with PK quantum money

Brute force attack:



Ability to verify → banknotes info.-theoretically determined

Cryptographic solution: computational security

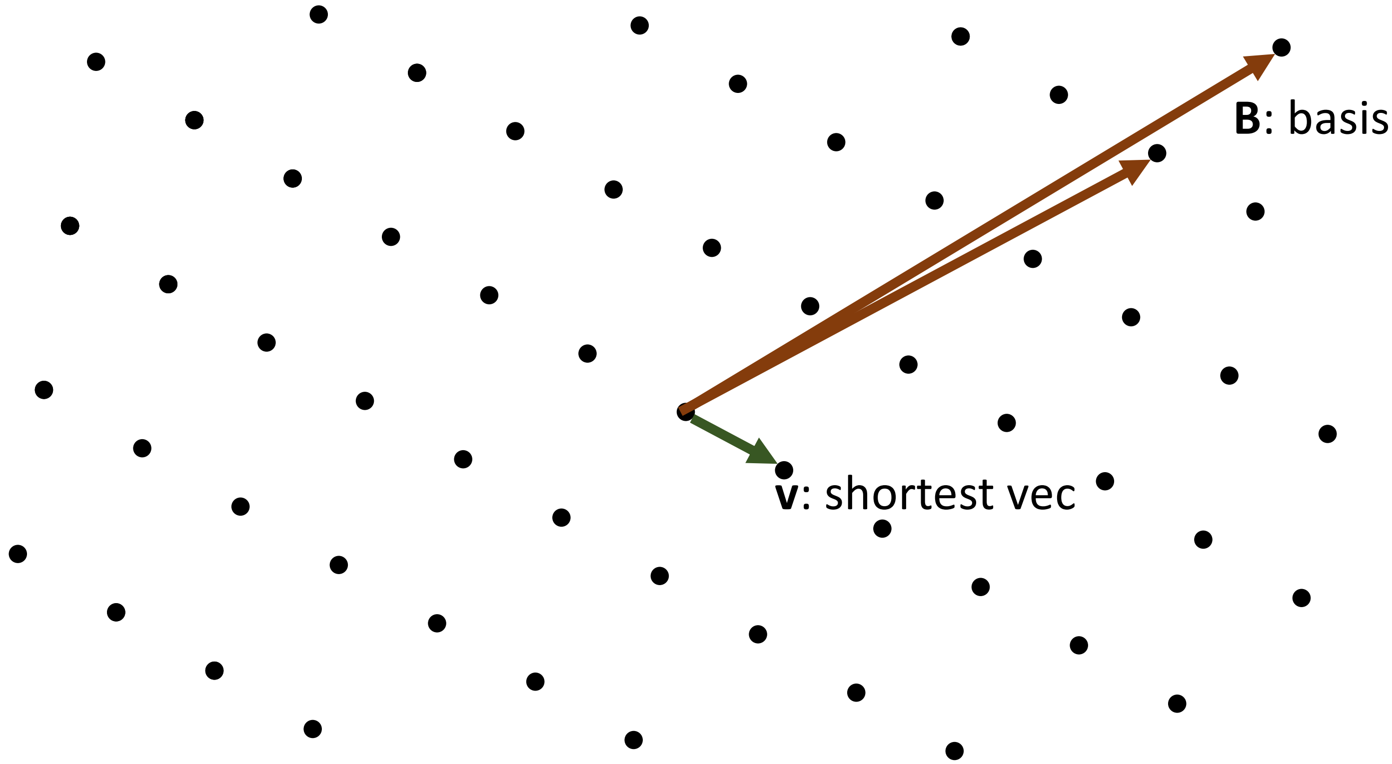
Time for brute-force attack = 2^#(qubits)   (aka HUGE)

→ only ask for security against time-bounded attacks

More efficient attacks? Can't rule out unconditionally without major breakthroughs in complexity theory (e.g. P vs NP)

Usual Solution: prove security under widely believed, well-studied, computational assumptions (e.g. assumed hardness of lattice problems)

Shortest vector problem (SVP)



SVP: Given **B**, find **v**

Still potential problems

No-cloning theorem no longer valid: states information-theoretically known

Typical crypto assumptions don't talk about cloning: problem statements purely classical

How to justify computational no-cloning? Cloning can't come from computational assumption or information-theory alone

Merely conjectured

[Aaronson’09]: random stabilizer states
✗ [Lutomirski-Aaronson-Farhi-Gosset-Hassidim-Kelner-Shor’10]

[Aaronson-Christiano’12]: polynomials hiding subspaces
✗ [Pena-Faugère-Perret’14, Christiano-Sattath’16]

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

[**Z**’19]: quadratic systems of equations
✗ [Roberts’21]

[Kane’18, Kane-Sharif-Silverberg’21]: quaternion algebras

[Khesin-Lu-Shor’22]: lattices
✗ [Liu-Montgomery-**Z**’23]

Merely conjectured

[Aaronson'09]: random stabilizer states
✗ [Lutomirski-Aaronson-Farhi-Gosset-Hassidim-Kelner-Shor'10]

[Aaronson-Christiano'12]: polynomials hiding subspaces
✗ [Pena-Faugère-Perret'14, Christiano-Sattath'16]

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

[**Z**'19]: quadratic systems of equations
✗ [Roberts'21]

[Kane'18, Kane-Sharif-Silverberg'21]: quaternion algebras

[Khesin-Lu-Shor'22]: lattices
✗ [Liu-Montgomery-**Z**'23]

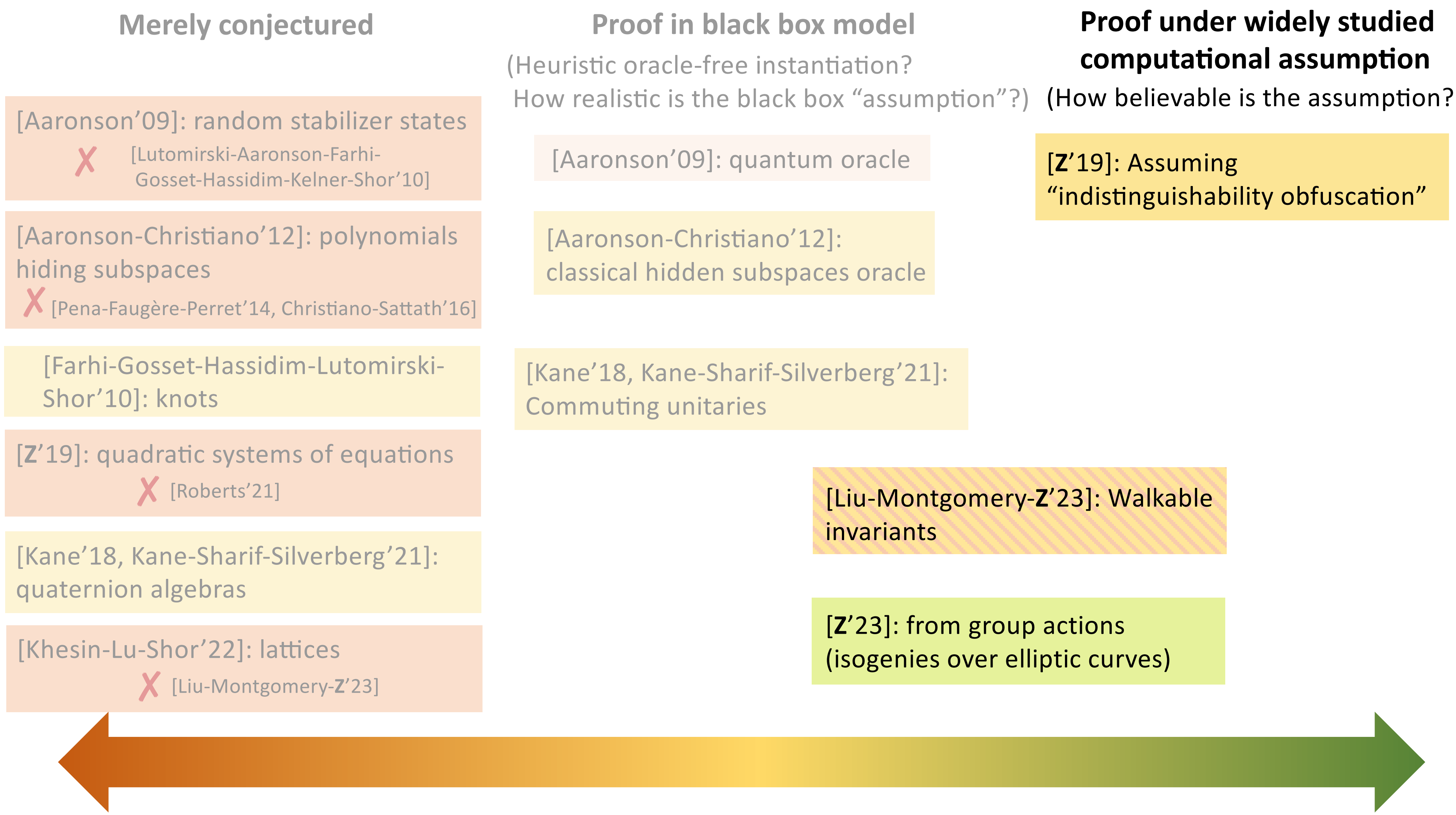
Proof in black box model

(Heuristic oracle-free instantiation?
How realistic is the black box "assumption"?)

[Aaronson'09]: quantum oracle

[Aaronson-Christiano'12]: classical hidden subspaces oracle

[Kane'18, Kane-Sharif-Silverberg'21]: Commuting unitaries

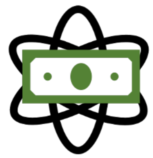

Merely conjectured
Proof in black box model
(Heuristic oracle-free instantiation?
How realistic is the black box "assumption"?)
Proof under widely studied computational assumption
(How believable is the assumption?)
[Aaronson'09]: random stabilizer states
✗ [Lutomirski-Aaronson-Farhi-Gosset-Hassidim-Kelner-Shor'10]
[Aaronson-Christiano'12]: polynomials hiding subspaces
✗ [Pena-Faugère-Perret'14, Christiano-Sattath'16]
[Farhi-Gosset-Hassidim-Lutomirski-Shor'10]: knots
[Z'19]: quadratic systems of equations
✗ [Roberts'21]
[Kane'18, Kane-Sharif-Silverberg'21]: quaternion algebras
[Khesin-Lu-Shor'22]: lattices
✗ [Liu-Montgomery-Z'23]
[Aaronson'09]: quantum oracle
[Aaronson-Christiano'12]: classical hidden subspaces oracle
[Kane'18, Kane-Sharif-Silverberg'21]: Commuting unitaries
[Liu-Montgomery-Z'23]: Walkable invariants
[Z'23]: from group actions (isogenies over elliptic curves)
[Z'19]: Assuming "indistinguishability obfuscation"

Example abstract approach:
Classical Test + Superposition Test

Simplifying assumption: mint only ever produces one banknote

Called "mini-scheme" by [Aaronson-Christiano'12]
Thm [AC'12]: Mini-scheme → full scheme

- Choose secret set $S \subseteq \{0,1\}^n$

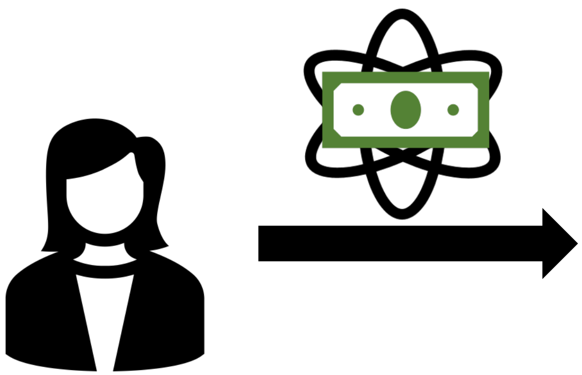
-  $= \sum_{x \in S} \alpha_x |x\rangle$

- Construct "membership checking" program

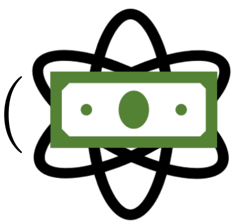
$$M_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise} \end{cases}$$

- Publish M_S to everyone

Classical Test



Accept if and only if

$M_S($  $) = 1$

Intuition: M_S should hide S while allowing to test for membership. Hiding comes from cryptography

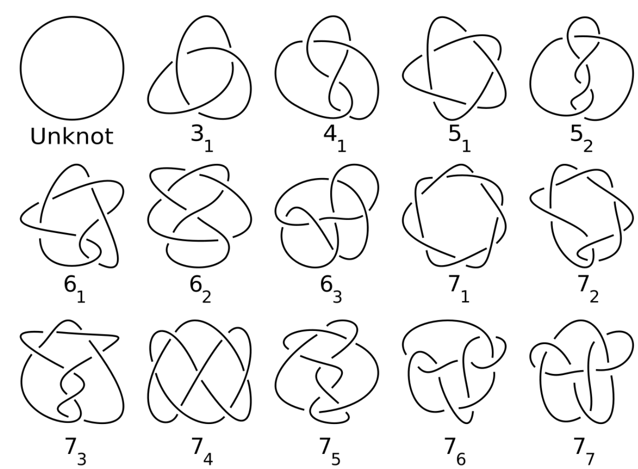
[Aaronson-Christiano'12]

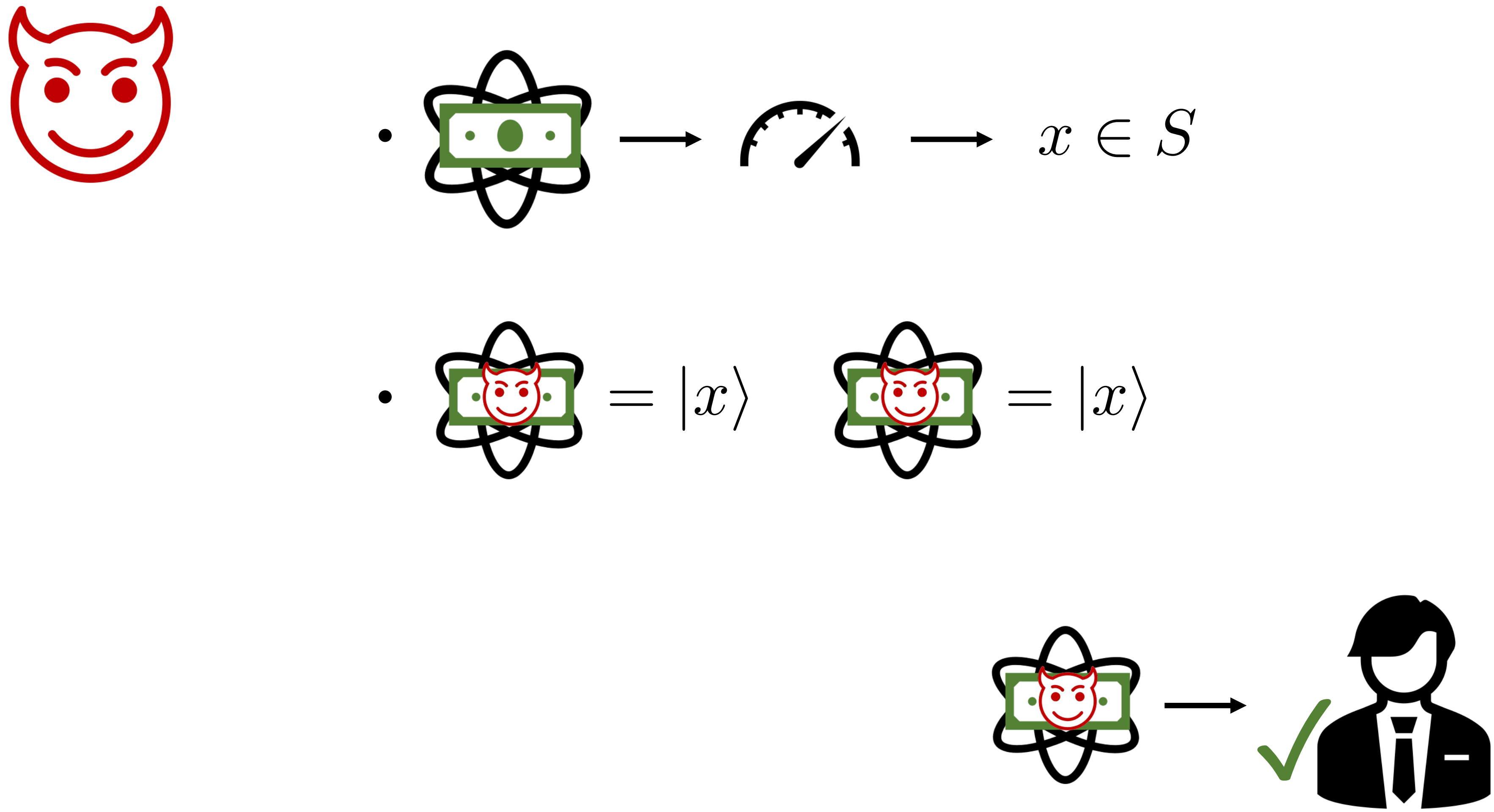
S = linear subspace of dimension $n/2$

[Farhi-Gosset-Hassidim-Lutomirski-Shor'10, Liu-Montgomery-**Z**'23]:

S = strings with same "invariant"

(e.g. Alexander polynomial,
points on elliptic curves)




$x \in S$
$= |x\rangle$
$= |x\rangle$

Problem: Not enough for honest banknotes to be hard to duplicate. Need hard to duplicate **any** notes accepted by verifier

Superposition Test

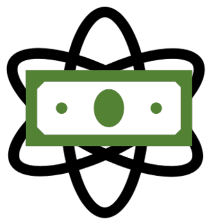
To prevent attack, need to have only honest banknotes accepted
Or at least, reject $|x\rangle$

[Aaronson-Christiano'12]

S = linear subspace of dimension $n/2$

Additionally give out $M_{S^\perp}$

Superposition test:

$$M_{S^\perp}(\text{QFT}($$  $$)) = 1$$

Thm [AC'12]: Secure if $M_S, M_{S^\perp}$ given as oracles

Thm [**Z**'19]: Secure if obfuscated with *indistinguishability obfuscation*

[Farhi-Gosset-Hassidim-Lutomirski-Shor'10, Liu-Montgomery-**Z**'23]:

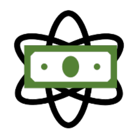
S = strings with same "invariant"

(e.g. Alexander polynomial, points on elliptic curves)

Superposition test:

Need permutations $\sigma_1, \cdots, \sigma_\ell$ which preserve invariant

(e.g. Reidemeister moves, isogenies)

Test that  preserved by $\sigma_1, \cdots, \sigma_\ell$

(variant of swap test)

New Result:

Quantum Money from Abelian Group Actions

(Abelian) Group Actions

abelian

$\mathbb{G}$ acts on $\mathcal{X}$ via $* : \mathbb{G} \times \mathcal{X} \to \mathcal{X}$

$$g * (h * x) = (g + h) * x$$

(Abelian) Group Actions

abelian

$\mathbb{G}$ acts on $\mathcal{X}$ via $* : \mathbb{G} \times \mathcal{X} \to \mathcal{X}$

$$g * (h * x) = (g + h) * x$$

Assume: $(g, x) \mapsto (g * x, x)$ a bijection,

$\mathcal{X}$ sparse, *recognizable*

Explicit known starting element $x \in \mathcal{X}$

(Abelian) Group Actions

abelian

$\mathbb{G}$ acts on $\mathcal{X}$ via $* : \mathbb{G} \times \mathcal{X} \to \mathcal{X}$

$$g * (h * x) = (g + h) * x$$

Assume: $(g, x) \mapsto (g * x, x)$ a bijection,

$\mathcal{X}$ sparse, recognizable

Explicit known starting element $x \in \mathcal{X}$

$(g * x, x) \mapsto (g, x)$ should be computationally infeasible

("Discrete log" problem)

$$\sum_{g \in \mathbb{G}} |g\rangle$$

$$\Big\downarrow *$$

$$\sum_{g \in \mathbb{G}} |g, g * x\rangle$$

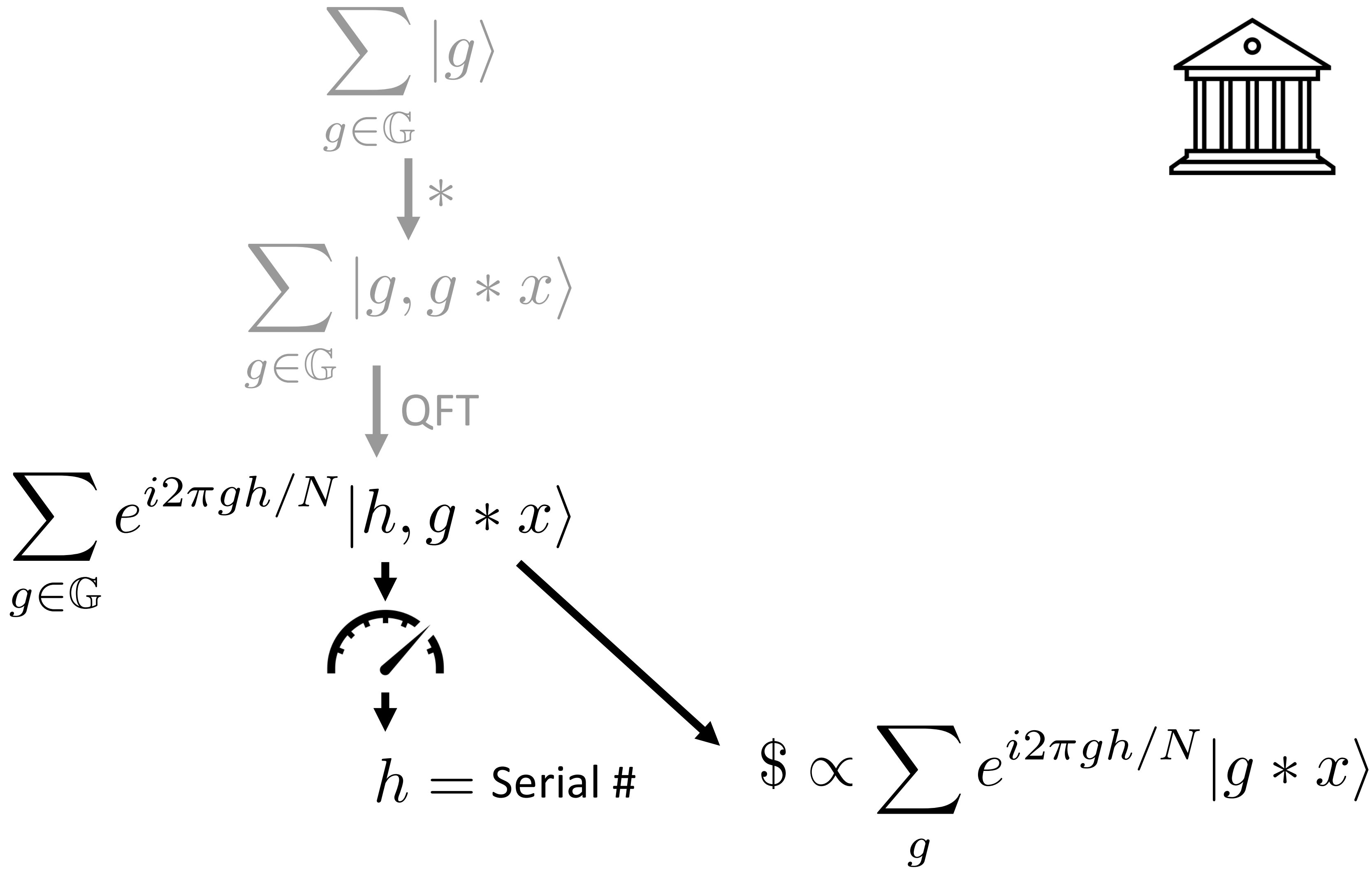
$$\sum_{g \in \mathbb{G}} |g\rangle$$

$\downarrow *$

$$\sum_{g \in \mathbb{G}} |g, g * x\rangle$$

$\downarrow$ QFT

$$\sum_{g \in \mathbb{G}} e^{i2\pi gh/N} |h, g * x\rangle$$



$\sum_{g\in\mathbb{G}} |g\rangle$
$*$
$\sum_{g\in\mathbb{G}} |g, g*x\rangle$
QFT
$\sum_{g\in\mathbb{G}} e^{i2\pi gh/N} |h, g*x\rangle$
$h =$ Serial #
$\$ \propto \sum_{g} e^{i2\pi gh/N} |g*x\rangle$

First check that support of $\$$ contained in $\mathcal{X}$

$$\$ \propto \sum_g e^{i2\pi gh/N} |g * x\rangle$$

$$\downarrow$$

$$\sum_u |u\rangle \otimes \sum_g e^{i2\pi gh/N} |g * x\rangle$$

$$\$ \propto \sum_g e^{i2\pi gh/N}|g * x\rangle$$

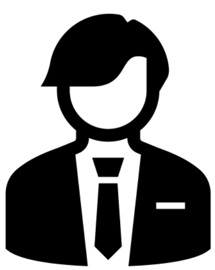
$$\downarrow$$

$$\sum_u |u\rangle \otimes \sum_g e^{i2\pi gh/N}|g * x\rangle$$

$$\downarrow *$$

$$\sum_u |u\rangle \sum_g e^{i2\pi gh/N}|u * (g * x)\rangle$$

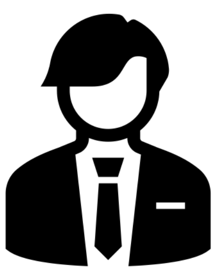
$$\sum_u |u\rangle \sum_g e^{i2\pi gh/N} |u * (g * x)\rangle$$
$$= \sum_{u,g} e^{i2\pi gh/N} |u\rangle |(u+g) * x\rangle$$



$$\sum_u |u\rangle \sum_g e^{i2\pi gh/N} |u * (g * x)\rangle$$

$$= \sum_{u,g} e^{i2\pi gh/N} |u\rangle |(u + g) * x\rangle$$

$$= \sum_{u,g'} e^{i2\pi (g' - u)h/N} |u\rangle |g' * x\rangle$$

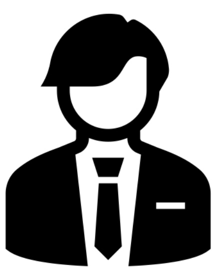


$$\sum_{u} |u\rangle \sum_{g} e^{i2\pi gh/N} |u * (g * x)\rangle$$

$$= \sum_{u,g} e^{i2\pi gh/N} |u\rangle |(u + g) * x\rangle$$

$$= \sum_{u,g'} e^{i2\pi (g' - u)h/N} |u\rangle |g' * x\rangle$$

$$= \sum_{u} e^{-i2\pi uh/N} |u\rangle \otimes \$$$



$$\sum_u |u\rangle \sum_g e^{i2\pi gh/N} |u * (g * x)\rangle$$

$$= \sum_{u,g} e^{i2\pi gh/N} |u\rangle |(u+g) * x\rangle$$

$$= \sum_{u,g'} e^{i2\pi (g'-u)h/N} |u\rangle |g' * x\rangle$$

$$= \sum_u e^{-i2\pi uh/N} |u\rangle \otimes \$$$

QFT

$$|h\rangle \otimes \$$$

Intuition for Security

Suppose discrete logs were easy:

$$\sum_{g\in\mathbb{G}} |g\rangle \longrightarrow \sum_{g\in\mathbb{G}} |g, g*x\rangle$$

Intuition for Security

Suppose discrete logs were easy:

$$\sum_{g\in\mathbb{G}} |g\rangle \longrightarrow \sum_{g\in\mathbb{G}} |g, g * x\rangle$$

$$\sum_{g} e^{i2\pi gh/N} |g, g * x\rangle$$

Intuition for Security

Suppose discrete logs were easy:

$$\sum_{g \in \mathbb{G}} |g\rangle \longrightarrow \sum_{g \in \mathbb{G}} |g, g * x\rangle$$

$$\sum_{g} e^{i2\pi gh/N} |g, g * x\rangle$$

$$\sum_{g} e^{i2\pi gh/N} |g * x\rangle = \$$$

Security Justification

Thm: Assumption 1 → protocol is secure for *black box* group actions

Assumption 1 ≈ Hard to distinguish $(x, u * x, (2u) * r)$ from $(x, u * x, v * r)$

r chosen by adversary

Notes:

- No mention of cloning in Assumption 1!
- First (post-)quantum security proof using black box group actions

Remark: DLog query complexity is polynomial [Ettinger-Høyer'00] → unconditional black box lower-bounds impossible for generic group actions

Typical proofs in crypto:

"standard model" → proof via reduction to underlying assumption

"black box model" → direct proof via query complexity

Any quantum proof using black box group actions must use *both*

Proof idea:

Suppose Assumption 1 is true for some group action $(\mathbb{G}, *, \mathcal{X})$

Construct new group action $(\mathbb{G}, \star, \mathcal{X}')$

$$\mathcal{X}' = \{(g * x, g * y)\}$$

$$y = u * x$$

from Assumption 1

$$g \star (z_1, z_2) = (g * z_1, g * z_2)$$

Starting element $x' = (x, y)$

Any black box adversary should also work for $(\mathbb{G}, \star, \mathcal{X}')$

False! But we will revisit later

Proof idea:

Suppose (toward contradiction) black box adversary produces two banknotes with same serial #

$$\$_1 \propto \sum_g e^{i2\pi gh/N} |g * x, g * y\rangle \qquad \$_2 \propto \sum_g e^{i2\pi gh/N} |g * x, g * y\rangle$$

1) Set $r = g * x$. Assumption maps to $v * r = (v + g) * x$ where $v = 2u$ or $v \neq 2u$

2) Swap $(v + g) * x$ and $g * y$

Proof idea:

$$\$_1 \mapsto \sum_g e^{i2\pi gh/N} |g * y, (v+g) * x\rangle$$

$$= \sum_g e^{i2\pi gh/N} |(g+u) * x, (v+g) * x\rangle$$

Proof idea:

$$\$_1 \mapsto \sum_g e^{i2\pi gh/N} |g * y, (v+g) * x\rangle$$

$$= \sum_g e^{i2\pi gh/N} |(g+u) * x, (v+g) * x\rangle$$

$$= e^{-i2\pi uh/N} \sum_{g'} e^{i2\pi g'h/N} |g' * x, (g'+v-u) * x\rangle$$

Proof idea:

$$\$_1 \mapsto \sum_g e^{i2\pi gh/N} |g * y, (v+g) * x\rangle$$

$$= \sum_g e^{i2\pi gh/N} |(g+u) * x, (v+g) * x\rangle$$

$$= e^{-i2\pi uh/N} \sum_{g'} e^{i2\pi g'h/N} |g' * x, (g'+v-u) * x\rangle$$

$$= e^{-i2\pi uh/N} \sum_{g'} e^{i2\pi g'h/N} |g' * x, (g'+v-2u) * y\rangle$$

Proof idea:

$$\$_1 \mapsto \$_1' := e^{-i2\pi uh/N} \sum_g e^{i2\pi gh/N} |g * x, (g + v - 2u) * y\rangle$$

$v = 2u$: $\$_1' = \$_1$ up to phase

$v \neq 2u$: $\$_1' \perp \$_1$

Distinguish using swap test with $\$_2$

→ Break Assumption 1, a contradiction

Proof idea:

Lingering issue: can't recognize $\mathcal{X}' = \{(g * x, g * y)\} \subseteq \mathcal{X}^2$

$\mathcal{X}'$ does not fit our criteria for group action

Solution: $\mathcal{X}' = \{\Pi(g * x, g * y)\}$ for random injection Π

"Bad" strings $\Pi(g * x, g' * y), g \neq g'$ are sparse

Can show hidden using standard quantum query complexity techniques

?