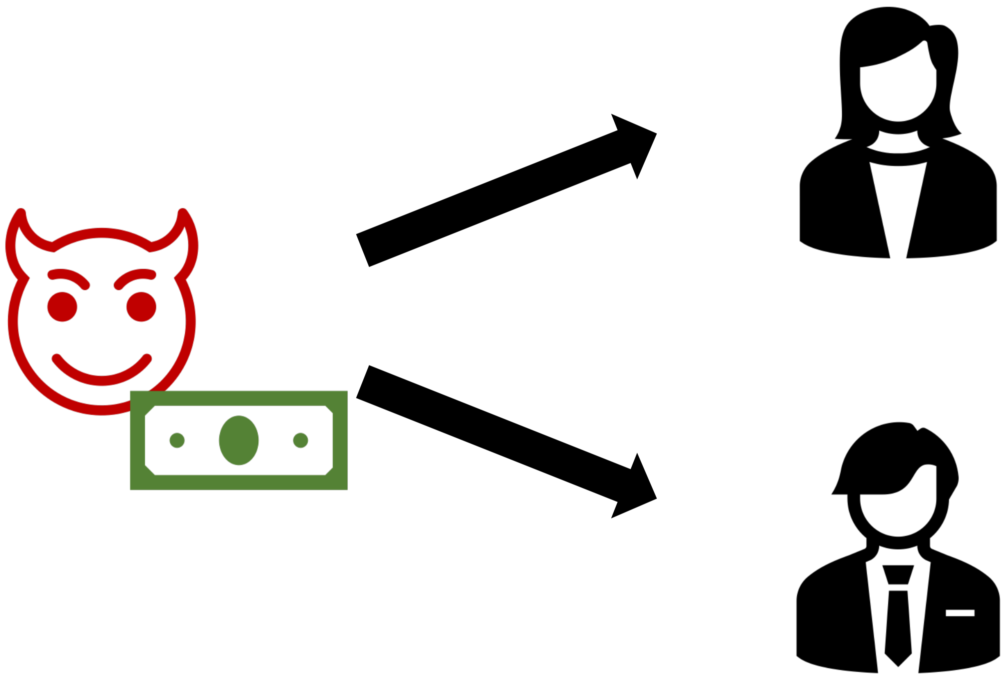
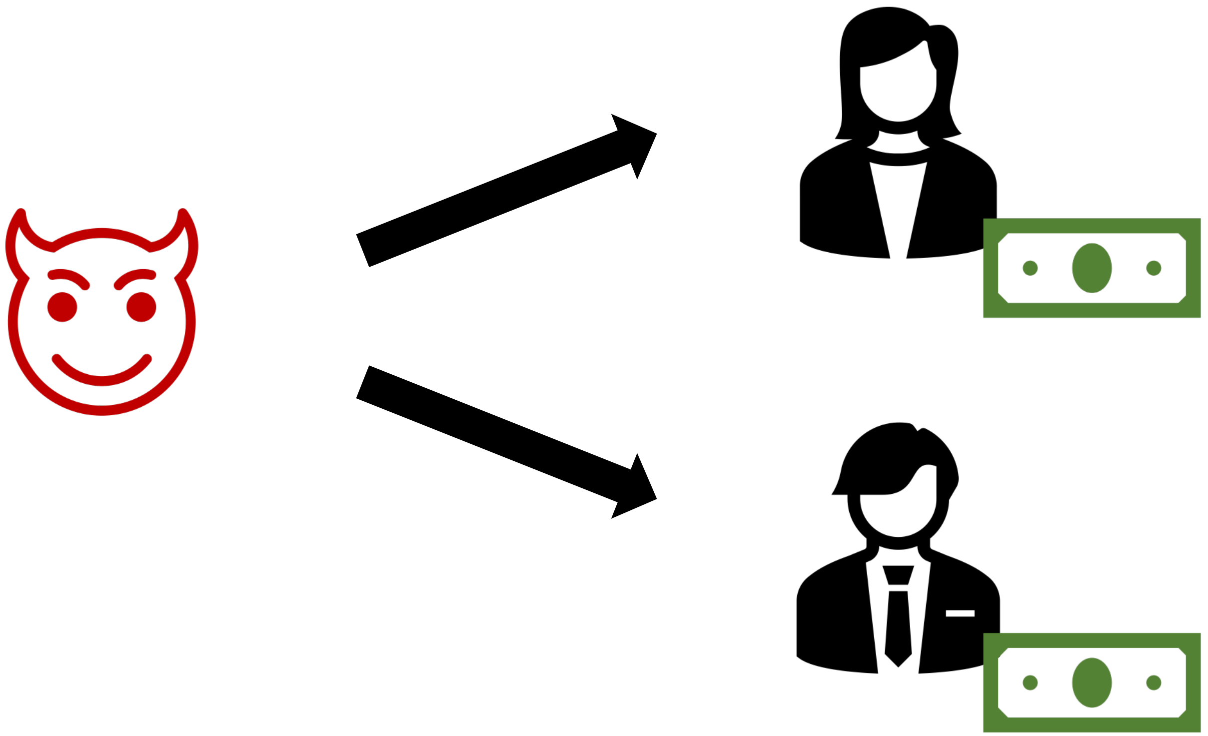
Quantum Money from Abelian Group Actions

Mark Zhandry
NTT Research

The Double Spend Problem

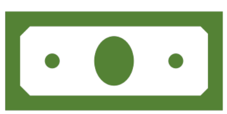
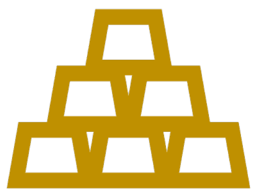


The Double Spend Problem



Classical Solutions

Physical currency

 = 

or at least too expensive
to convincingly copy

Digital currency

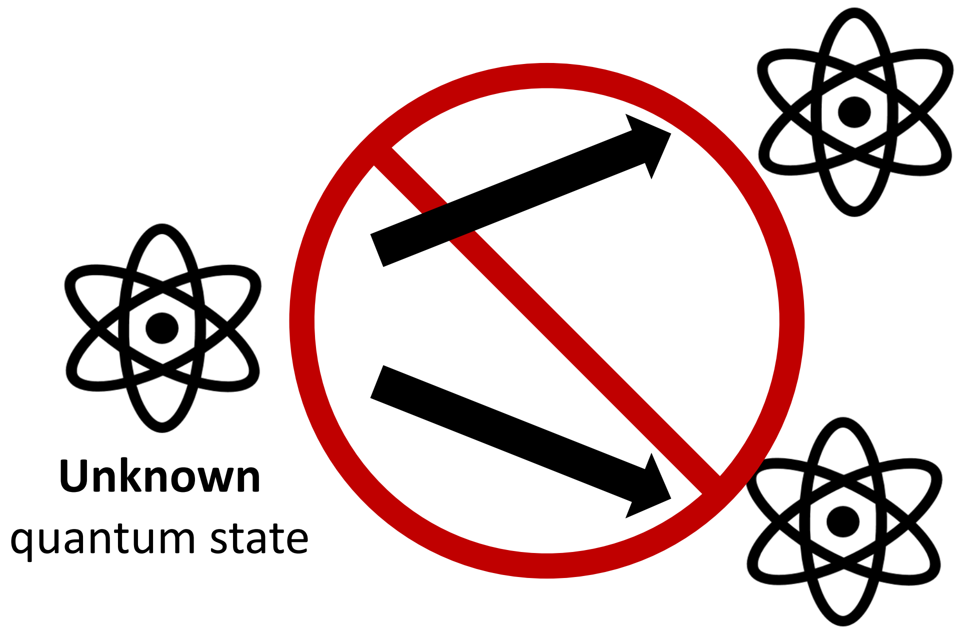
 

All need trusted third party to make
sure the money is yours to spend

Enter Quantum…

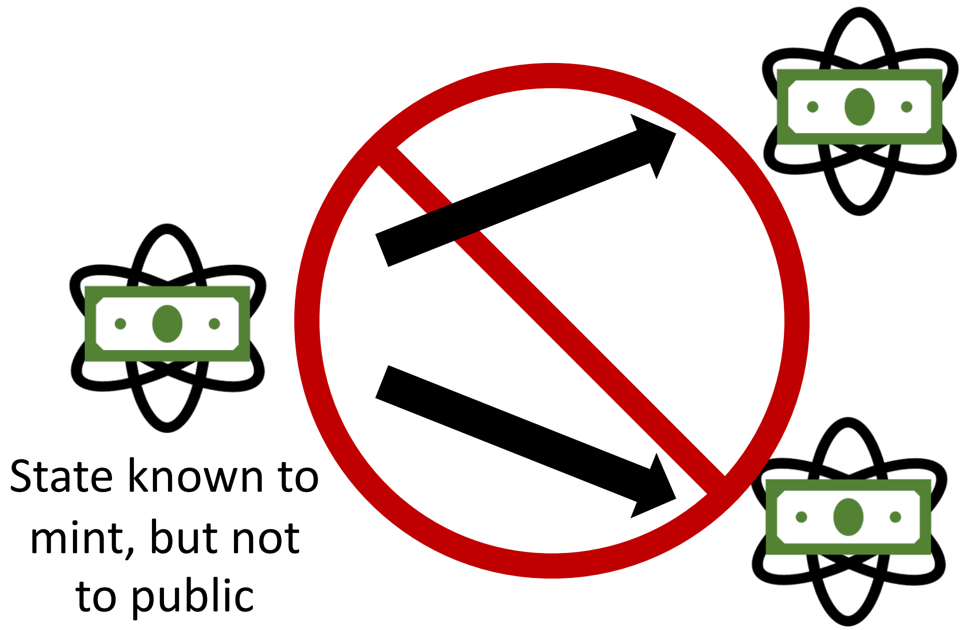
No-cloning Theorem

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



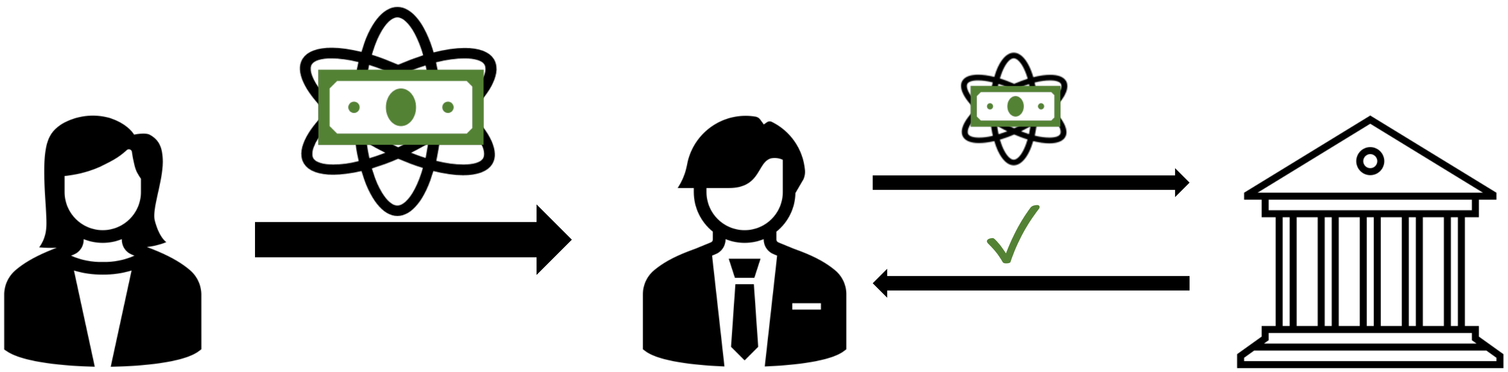
“Secret key” quantum money

[Wiesner’70]



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

Problem with SK quantum money



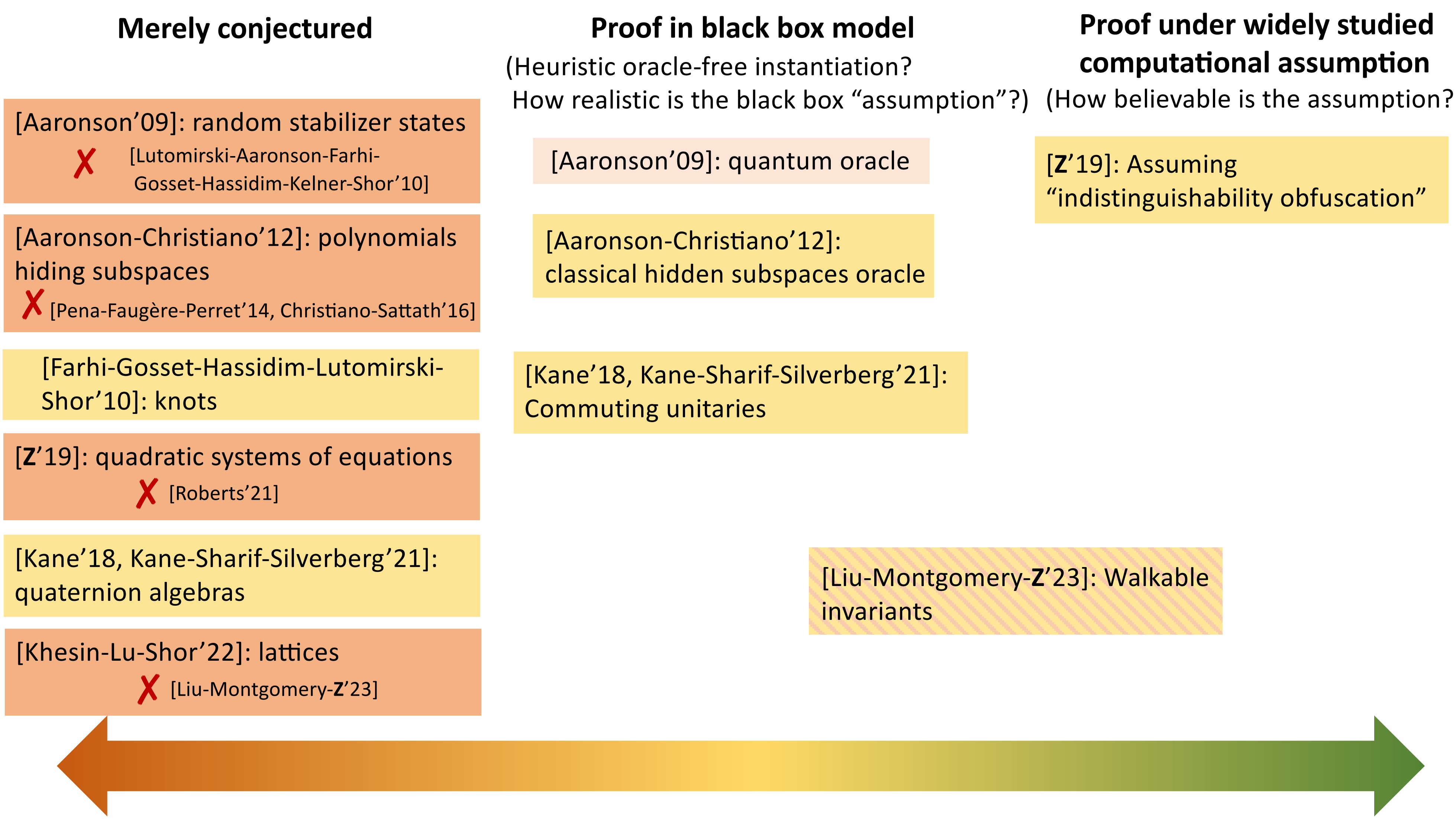
Because state is unknown to public, only mint can verify

"Public key" quantum money

[Aaronson'09]

Mint only involved in making new notes, not verification

Numerous other advantages, for free



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
[**Z**'19]: Assuming "indistinguishability obfuscation"
[Liu-Montgomery-**Z**'23]: Walkable invariants

New Result:

Quantum Money from Abelian Group Actions

(Abelian) Group Actions

abelian

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

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

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)

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

$$\Big\downarrow *$$

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

$$\Big\downarrow \text{QFT}$$

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

$$h = \text{Serial \#}$$

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

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

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

$$\Big\downarrow$$

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

$$\Big\downarrow *$$

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

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

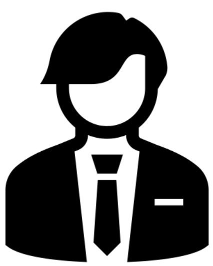
$$= \sum_{u,g} e^{i2\pi gh/N} |u\rangle |(u+g) * x\rangle$$

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

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

$$\Big\downarrow \text{QFT}$$

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



Intuition for Security

Suppose discrete logs were easy:

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

$$\swarrow$$

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

$$\downarrow$$

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

Security Justification

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

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

Analogous to Diffie-Hellman exponent assumptions in plain groups

(g, g^u, g^{u^2}) vs (g, g^u, g^r)

r chosen by adversary adaptively based on $x, u * x$ potentially in superposition

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 $(\mathbb{G}, \star, \mathcal{X}')$

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

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

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

$$y = u * x$$

from Assumption 1

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

*** Some technicalities here. 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:

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

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

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

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

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 bad set hidden using standard quantum query complexity techniques

Conclusion

This talk: Public key quantum money from abelian group actions, with plausible security justification

Also in paper:

- Extension to isogenies over elliptic curves (REGAs)
- Comparison of various idealized models for group actions
- Cryptanalysis of certain ``knowledge assumption” on group actions

  → similar to ”knowledge of path” assumption used in [Liu-Montgomery-**Z**’23]