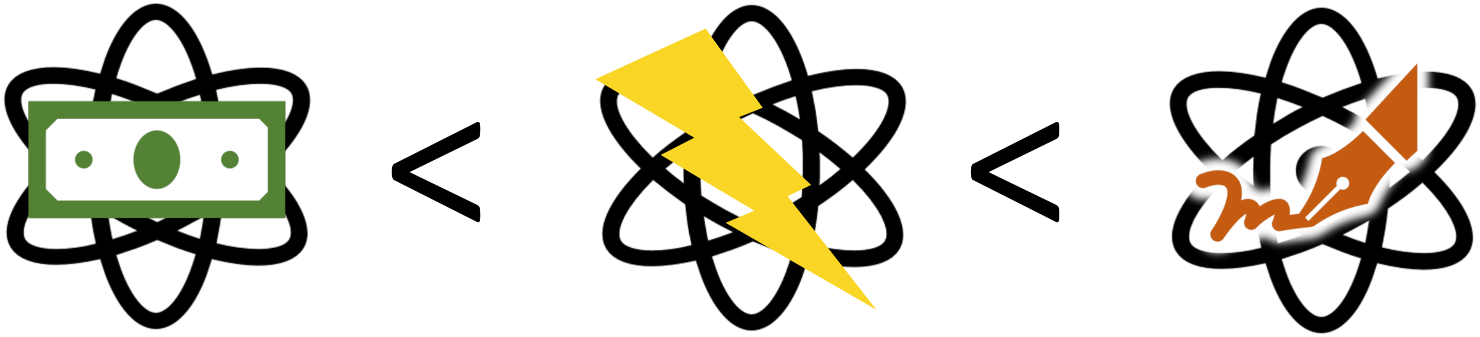
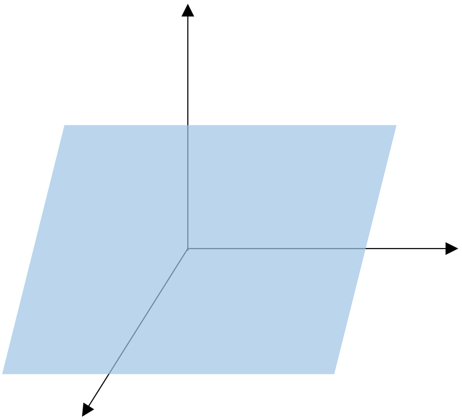
The Status of Quantum Money and Variants

Mark Zhandry
NTT Research



Hidden Subspaces [Aaronson-Christiano'12]



Provably secure from iO [Z'19] ✓

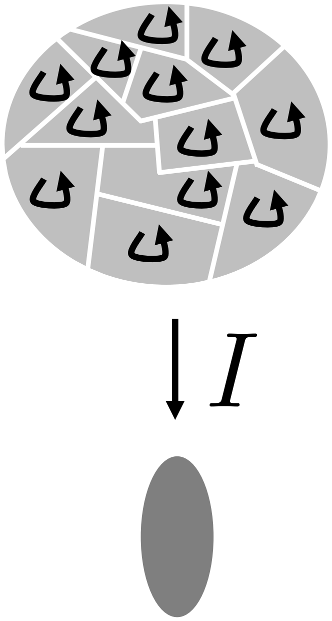
iO impractical, no other known instantiations ✗

Does not seem amenable to quantum lightning ✗

- Need to know subspace to mint, knowledge of subspace allows for minting many copies

Major open question: (non-evasive) obfuscation of subspaces without iO

Walkable Invariants [Farhi-Gosset-Hassidim-Lutomirski-Shor’10, Liu-Montgomery-**Z**’23]



Can prove under knowledge assumption + statistical assumption [Liu-Montgomery-**Z**’23] ?

- Knowledge assumption questionable [**Z**’24]
- Seems hard to analyze under “nice” assumptions

Practicality unclear ?

- Knots: what’s the security parameter?
- Isogenies: currently incomplete protocol

Readily gives quantum lightning ✓

Does not seem amenable to OSS ✗

- Inherently not collision-resistant

Commuting Unitaries [Kane-Sharif-Silverberg'21]

$$U_0 U_1 = U_1 U_0$$

Only known instantiation (quaternion algebras) needs more study ?

- Efficiency? Security?

Does not seem amenable to OSS ✗

- Basically no classical structure

Open question: Find other instantiations

Abelian Group Actions [Z'24]

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

Provably secure under "reasonable" assumptions + black box model for isogenies ✓

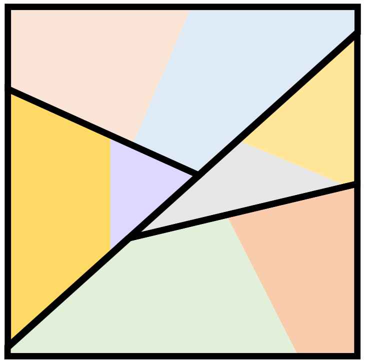
Should be practical with fault-tolerant QC ✓

Isogenies only known instantiation ✗

Does not seem amenable to OSS ✗

- Inherently not collision-resistant

“Fractured Subspaces” [Amos-Georgiou-Kiayias-**Z**’20]



Poor understanding of candidate security ✗

Uses impractical obfuscation ✗

Assuming collision resistance, gives OSS ✓

Open question: Security justification in black-box model

Speculative: Quantum Obfuscation

[Unruh'16] gives quantum oracle relative to which OSS exist

Can we obfuscate this oracle?

Note: existing quantum obfuscation schemes only for classical input/output
[Bartusek-Malavolta'20, Bartusek-Kitagawa-Nishimaki-Yamakawa'23, Bartusek-Brakerski-Vaikuntanathan'14]