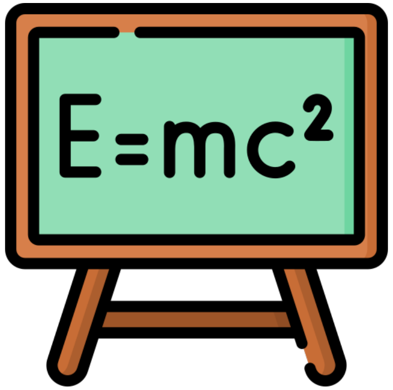
Quantum Cryptography
from Post-Quantum Security to Quantum Money

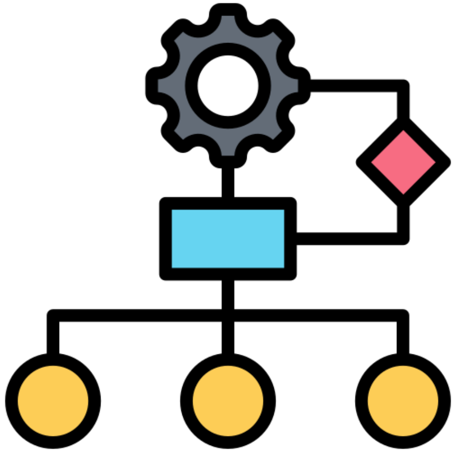
Qipeng Liu
UC San Diego

Backgrounds

- quantum computers
  - Google Sycamore, …, IBM Osprey



understanding physics/chemistry



faster algorithms

cryptography

threats

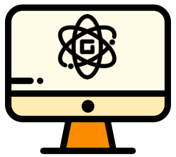
new functions

Examples

challenges:

Shor's algorithm

factoring in polynomial time

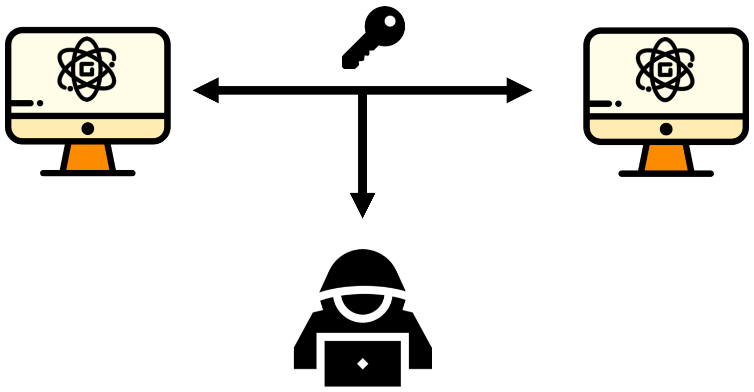
$N = pq \longrightarrow$  $\longrightarrow p, q$

encryption:

- RSA **broken**
- ElGamal **broken**
- …

opportunities:

quantum key distribution



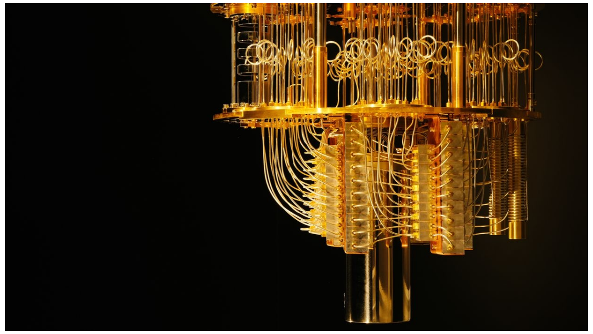
classically impossible!

Quantum Cryptography: A Landscape

post-quantum → NISQ → full-scale quantum

Noisy **I**ntermediate-**S**cale **Q**uantum

- 50 to few hundreds of qubits
- no error correction



Post-Quantum

post-quantum

Shor's algorithm → break many crypto in polynomial time

- faster factoring
- post-quantum candidate: lattice, code-based, isogeny

Grover's algorithm → quadratically speed up attacks

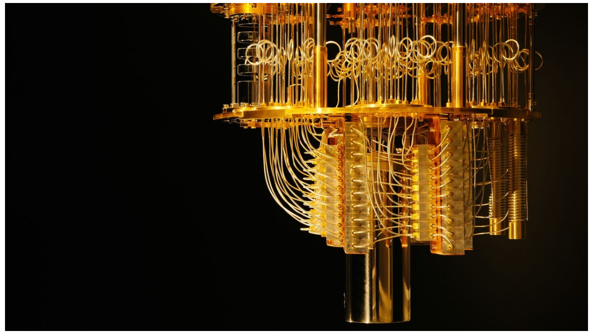
- 2^{64} v.s. 2^{32}

Goal: understand **post-quantum** security and countermeasures

NISQ

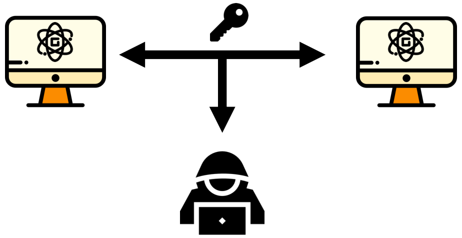
NISQ

not capable of running Shor/Grover



NISQ quantum attacks

- unstable memory, shallow depth



utilizing quantum information

- quantum key distribution

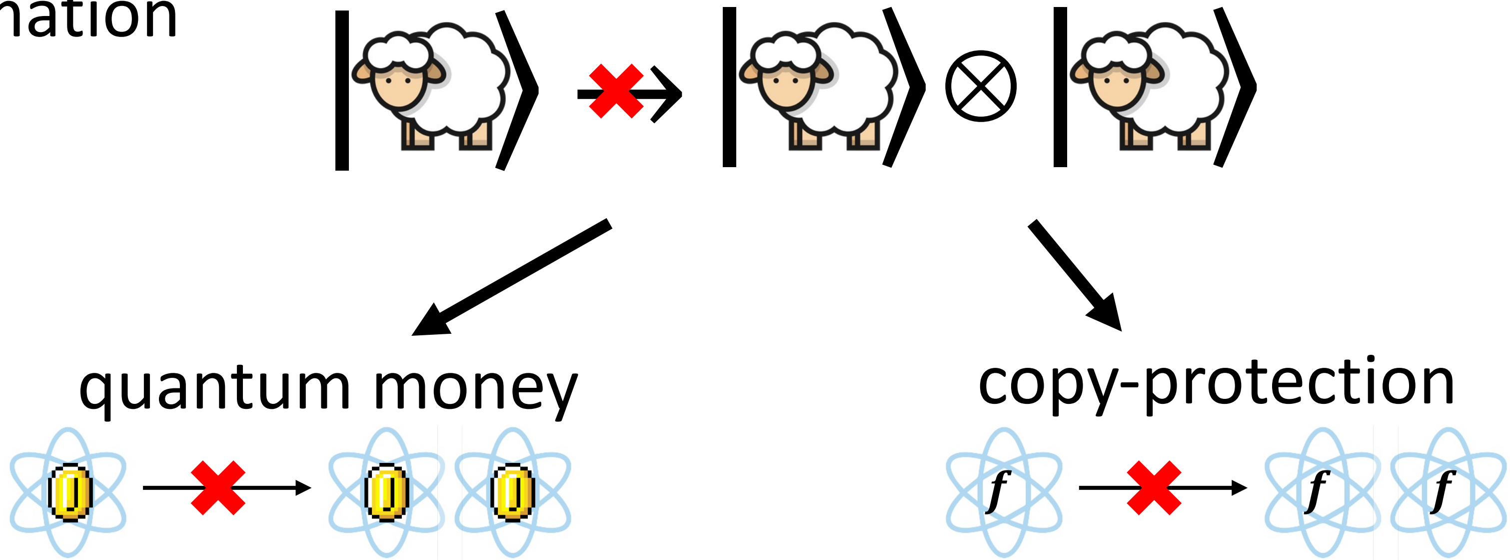
Goal: interesting applications even with **NISQ** devices

Full-Scale Quantum

beyond encryption and key distribution

utilizing quantum information

- no-cloning theorem



Goal: **classically-impossible** applications

Quantum Cryptography: A Landscape

post-quantum

understand post-quantum security and countermeasures

app

eve

m

sible

This Talk:

1. quantum properties, and **challenges** to post-quantum crypto

2. **opportunities** on new applications

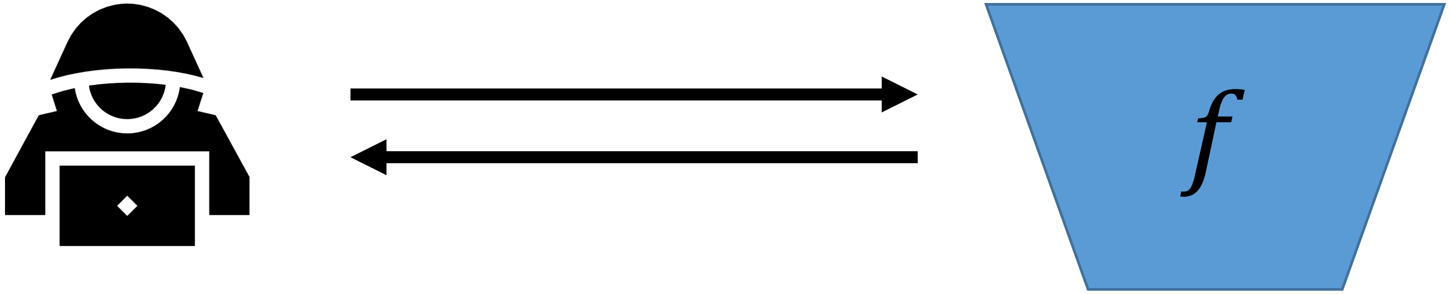
2. future

This Talk:

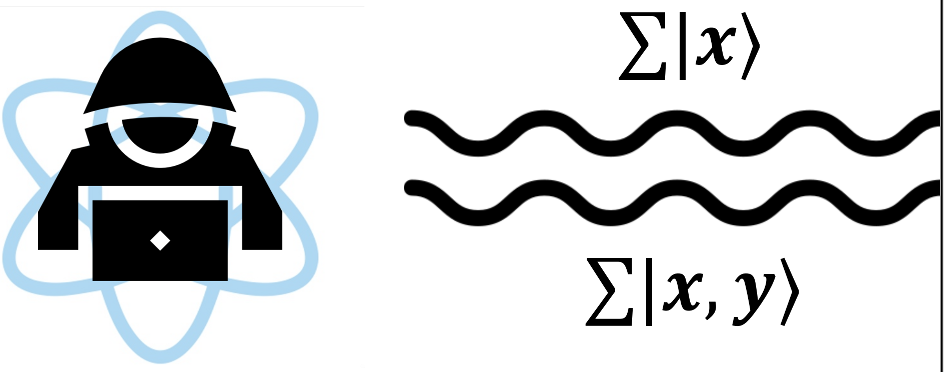
1. **quantum properties, and challenges to post-quantum crypto**
2. **opportunities** on new applications
3. future

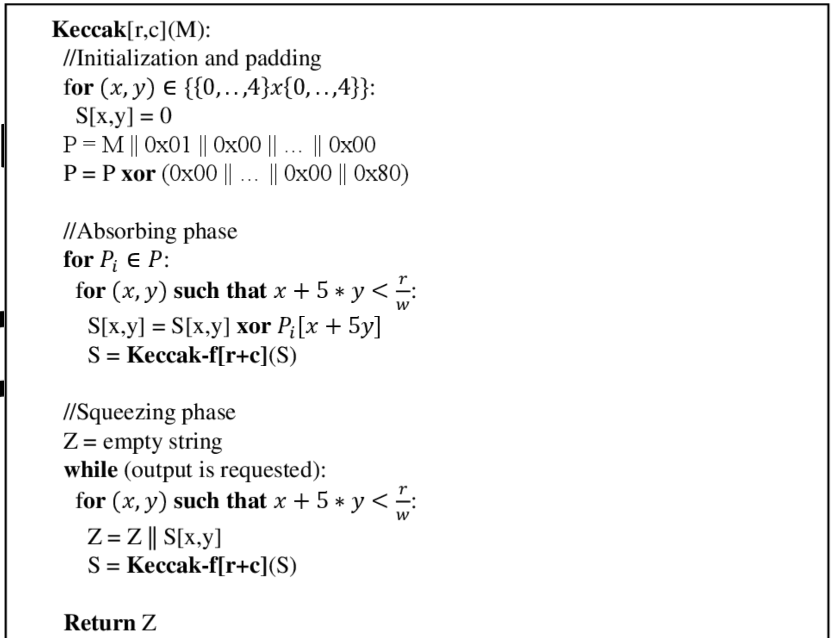
1. Superposition Access

- **classical**



- **quantum: superposition access**
  - Examples: Shor's algorithm and Grover's al





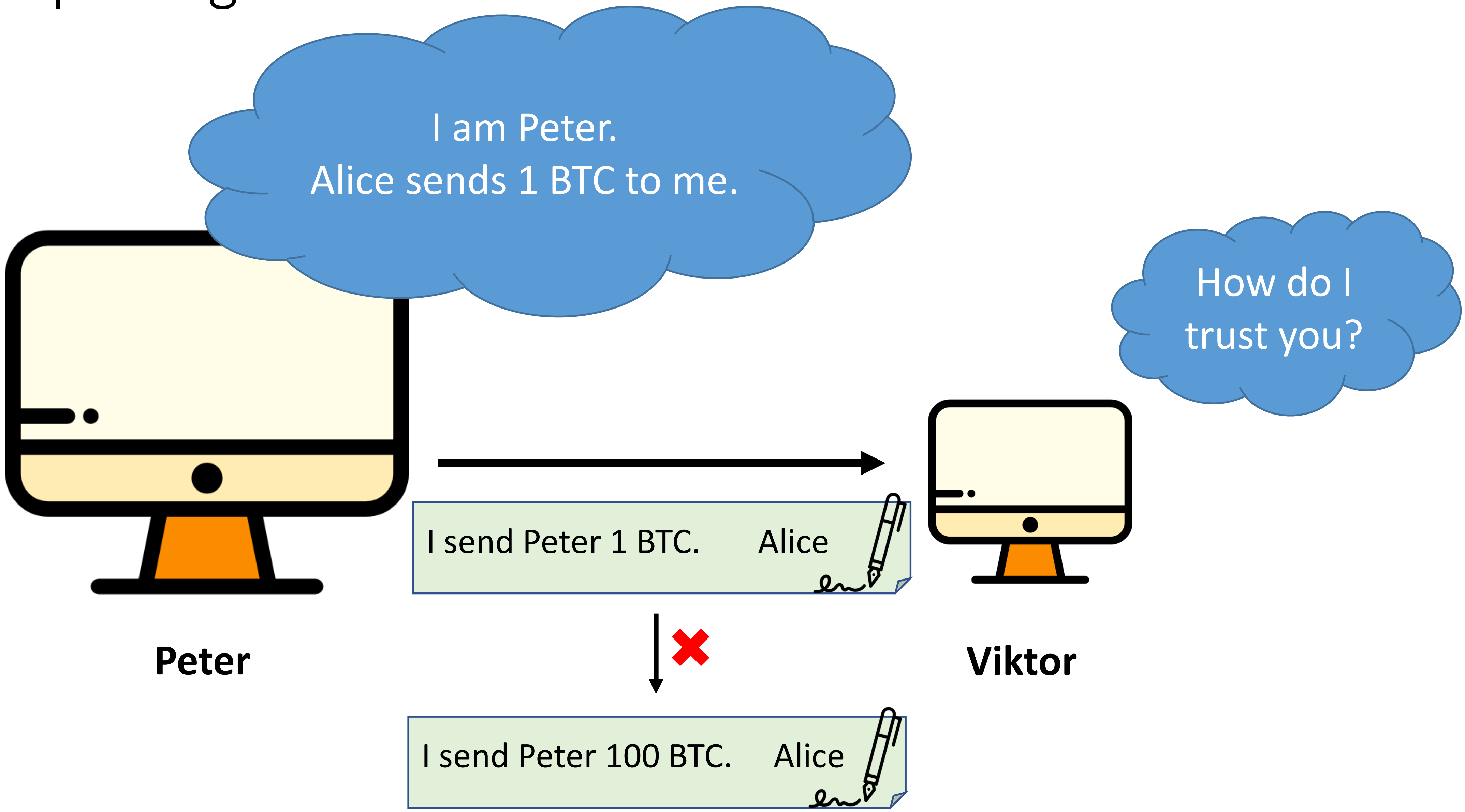
```
Keccak[r,c](M):
  //Initialization and padding
  for (x, y) ∈ {{0,..,4}x{0,..,4}}:
    S[x,y] = 0
  P = M || 0x01 || 0x00 || … || 0x00
  P = P xor (0x00 || … || 0x00 || 0x80)

  //Absorbing phase
  for P_i ∈ P:
    for (x, y) such that x + 5 * y < r/w:
      S[x,y] = S[x,y] xor P_i[x + 5y]
      S = Keccak-f[r+c](S)

  //Squeezing phase
  Z = empty string
  while (output is requested):
    for (x, y) such that x + 5 * y < r/w:
      Z = Z || S[x,y]
      S = Keccak-f[r+c](S)

  Return Z
```

Example: Signatures

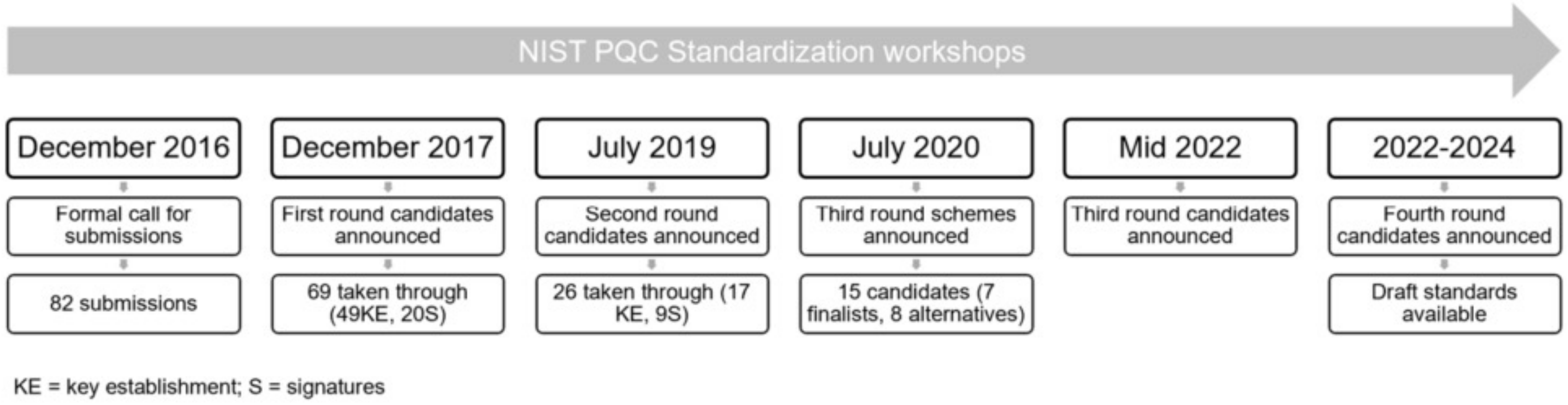


Quantum-safe Signatures

Issues with quantum:

1. Existing Signatures are based on factoring, e.g., that used in BTC
2. Even replaced with assumptions based on lattices, security was little known
   (especially those based on hash, e.g. **Fiat-Shamir**)

superposition access



Examples

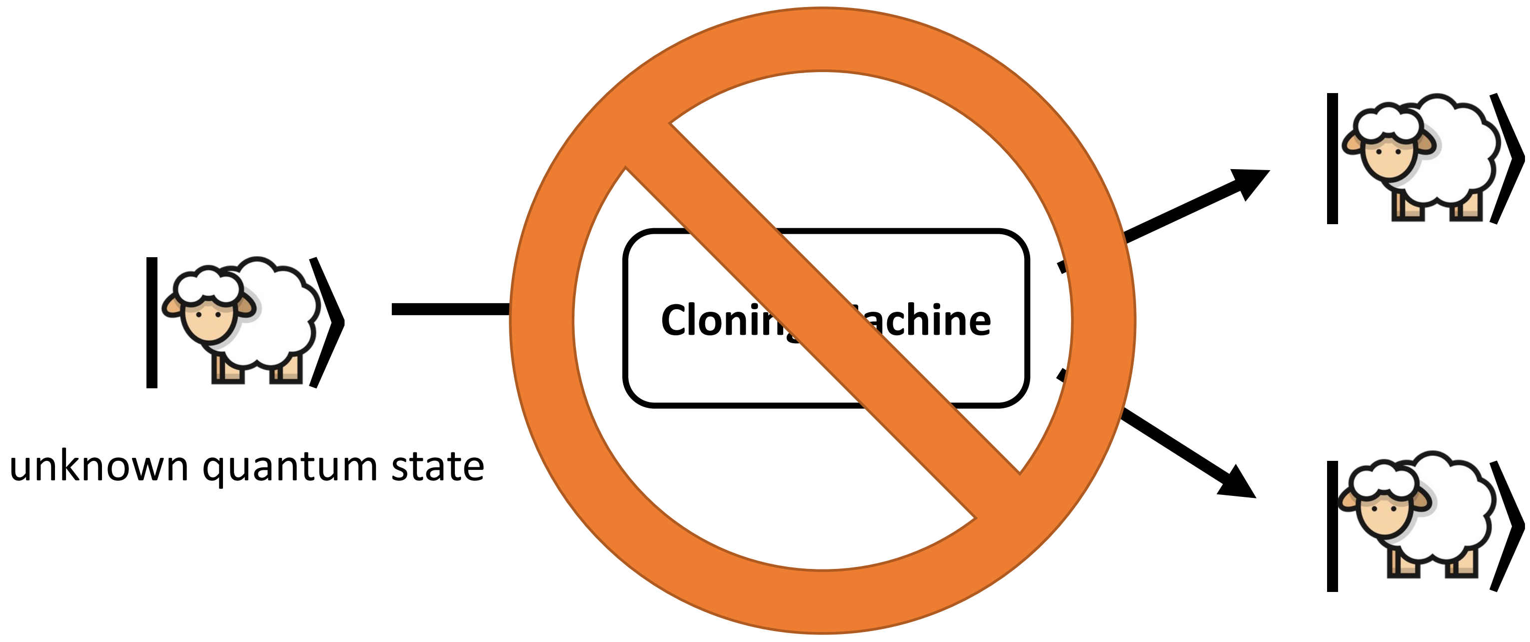
Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS-KYBER	CRYSTALS-Dilithium
	FALCON
	SPHINCS+

- hash functions (usually modeled as a random function)
  - $H(\cdot)$
  - encryption, digital signature, …
  - now becomes a much developed area, many tools

- ideal cipher (usually modeled as a keyed permutation, with forward and backward interface)
  - $E(k,\cdot)$ and $E^{-1}(k,\cdot)$
  - little techniques to analyze
  - tools wanted!

2. No-Cloning Principle



No-Cloning Principle

- challenges:
  - security proof requires to ``**rewind**'' a protocol to its previous stage
  - trivial with classical protocols
  - not immediately possible with quantum
  - now, we have many tools to do quantum rewinding [LZ'19,…]

- opportunities:
  - QKE
  - much more than that!

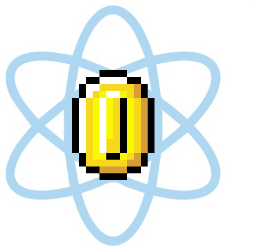
This Talk:

1. quantum properties, and challenges to post-quantum crypto

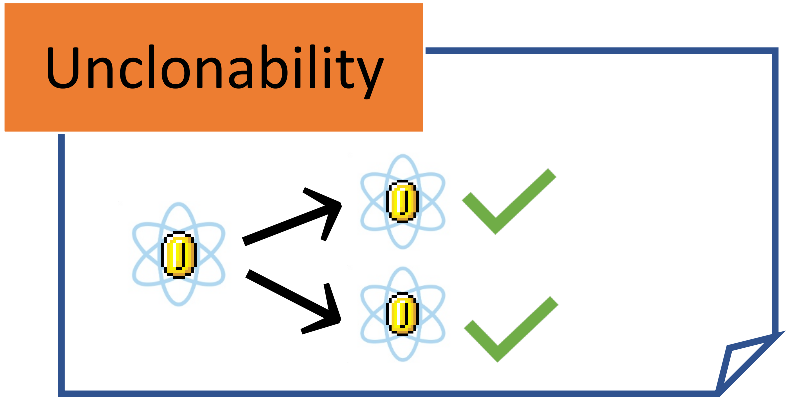
2. **opportunities** on new applications

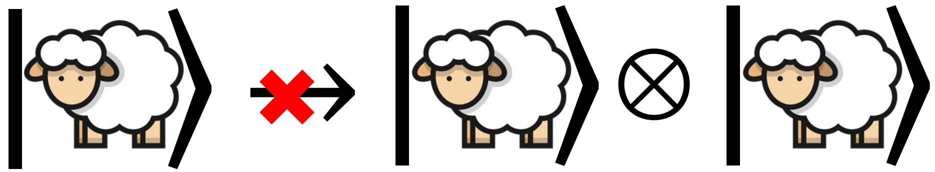
3. future

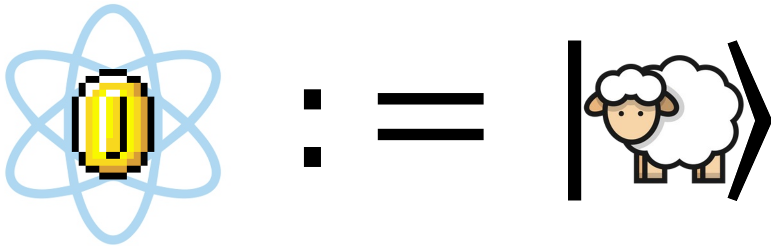
From No-cloning to Money



- Unclonability
- (Public) Verifiability







Public verifiability

Subspace states

[Aaronson-Christiano'12]

Beyond Quantum Money

quantum money

[AC'12] [Zhandry'18] …

subspace states

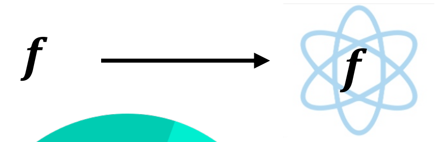
software copy-protection

[Aaronson-Liu-L-Zhandry-Zhang]

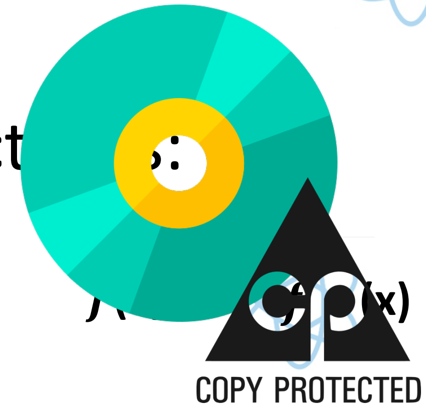
software copy-protection

[Aaronson'09]

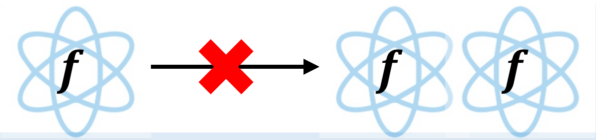
Compile:



Correct

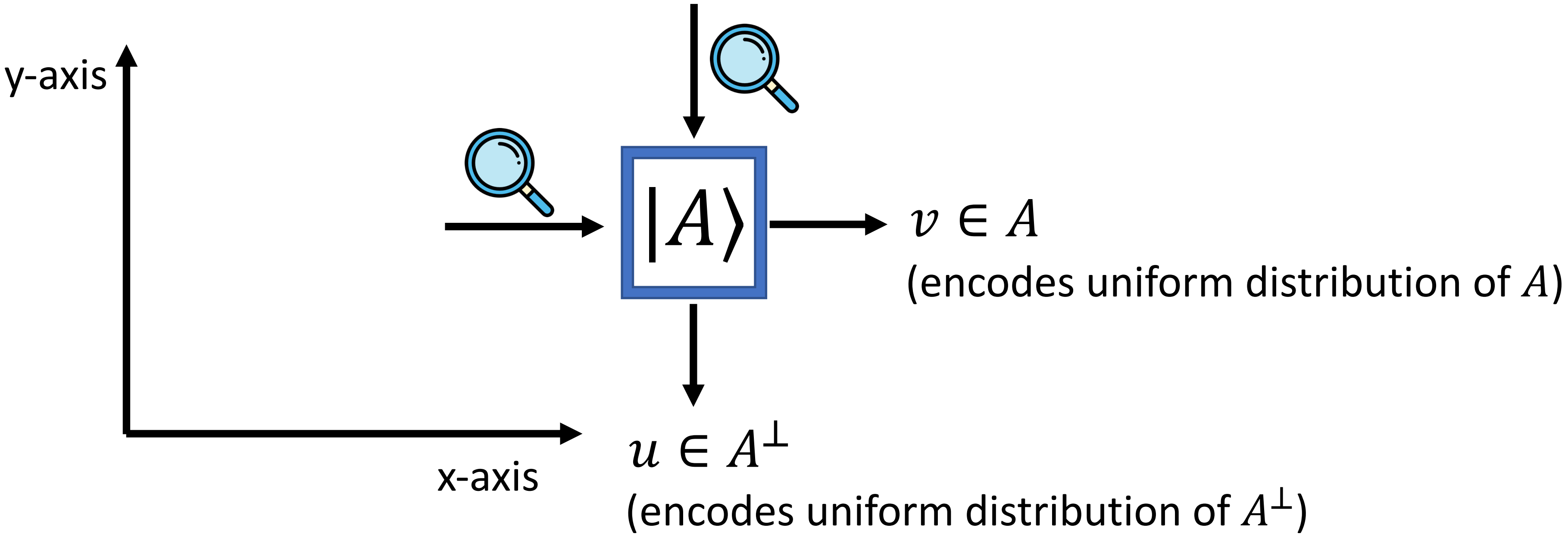


Security (Anti-piracy):



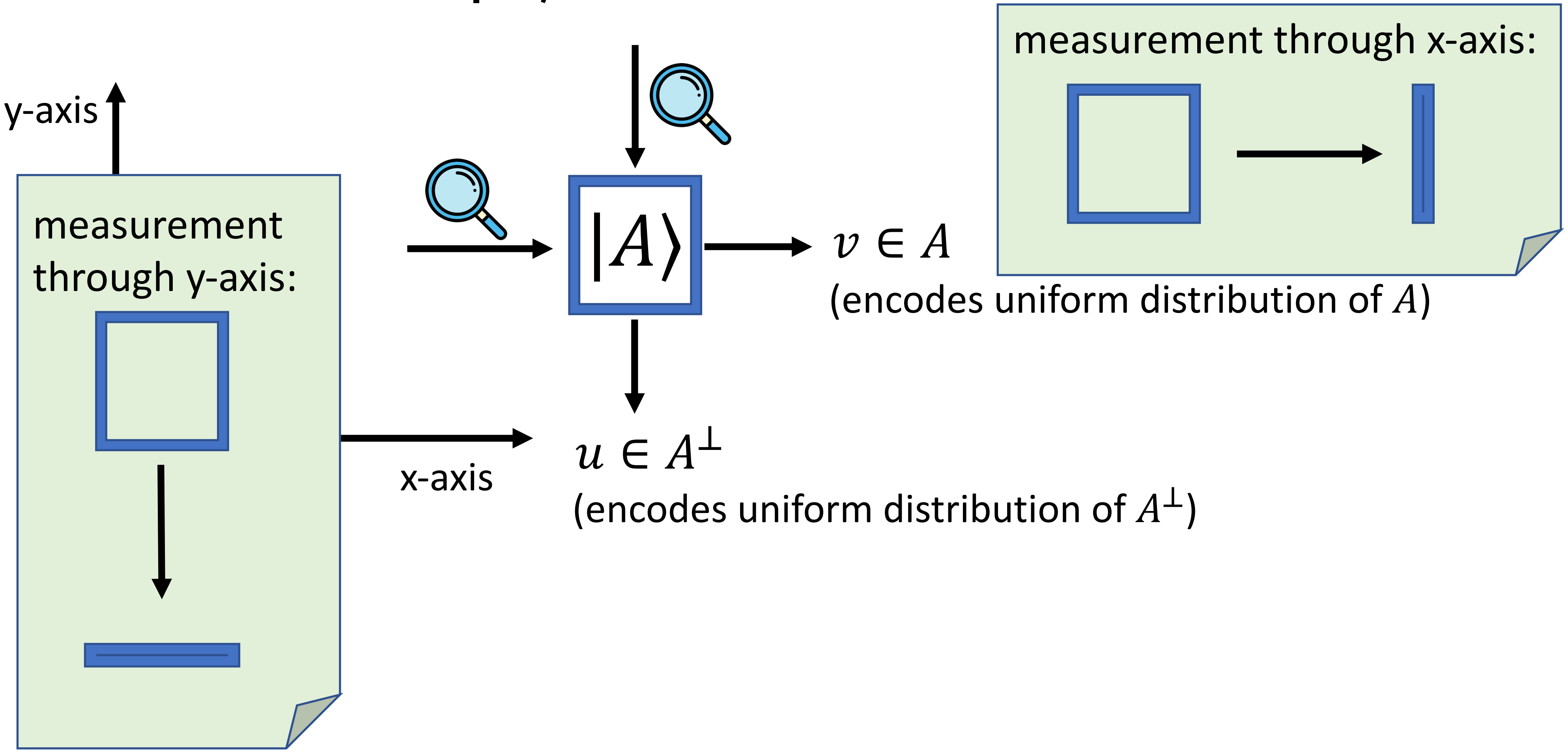
Subspace States

- Hidden subspace state $$|A\rangle = \sum_{v \in A} |v\rangle$$ for subspace A



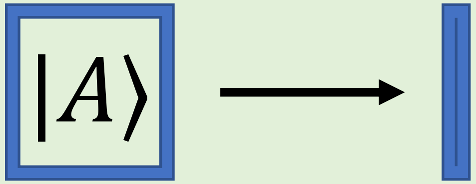
Subspace States

- Hidden subspace state $|A\rangle$ for subspace A



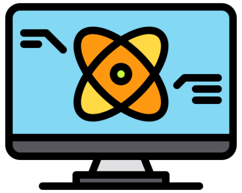
Unclonability of subspace states

measurement through x-axis:



Unclonability:

- No quantum algorithm can:

$|A\rangle \longrightarrow$  $\longrightarrow v \in A, u \in A^{\perp}$

(analogue) uncertainty principle:

One cannot know both the position and speed of a particle, with perfect accuracy.

Limitation

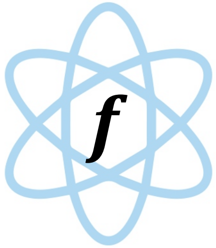
quantum money

[AC'12] [Zhandry'18] …

subspace states

software copy-protection

[ALLZZ'21]



$= \left(|A\rangle, O_A, O_{A^\perp} \right)$

limitations:

$O_A, O_{A^\perp}$ needs to be **obfuscated** in a very strong sense

Solution

quantum money

[AC'12] [Zhandry'18] …

↑

subspace states

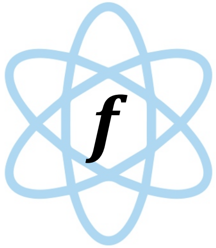
↓

software copy-protection

[ALLZZ'21]

use indistinguishability obfuscation

- practically inefficient
- no post-quantum candidate



$$f = \left(|A\rangle , O_A , O_{A^\perp} \right)$$

limitations:

$O_A, O_{A^\perp}$ needs to be **obfuscated** in a very strong sense

Questions

quantum money

[AC'12] [Zhandry'18] …

subspace states

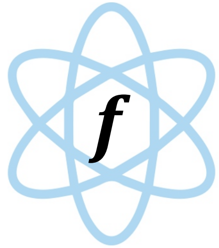
software copy-protection

[ALLZZ'21]

1. post-quantum candidate for program obfuscation

2. quantum states that possess more structures based on other mathematical structures?
   - unclonability, uncertainty principle
   - can be publicly verified

- some candidates: lattice, hash, isogeny, or any math objects you can name!



$$= \left(|\boldsymbol{A}\rangle\,, O_A\,, O_{A^\perp} \right)$$

limitations:

$O_A, O_{A^\perp}$ needs to be **obfuscated** in a very strong sense

This Talk:

1. quantum properties, and **challenges** to post-quantum crypto

2. **opportunities** on new applications

3. future

Quantum Cryptography: Prospects

post-quantum

understand post-quantum security and countermeasures

NISQ

applications

even with NISQ devices

full-scale quantum

classically-impossible

applications

post-quantum security, **better** understandings

- e.g., **beyond** hash functions
- e.g., connection to **theory**
- …

Thank you!

quantum power in the **NISQ** era

- e.g., performance with **bounded** resources?
- e.g., more applications
- …

classically impossible applications

- e.g., **practical** copy-protection
  rely on lattices?
- e.g., quantum lightning
- …

weaken assumptions

- e.g., quantum pseudorandomness
- …