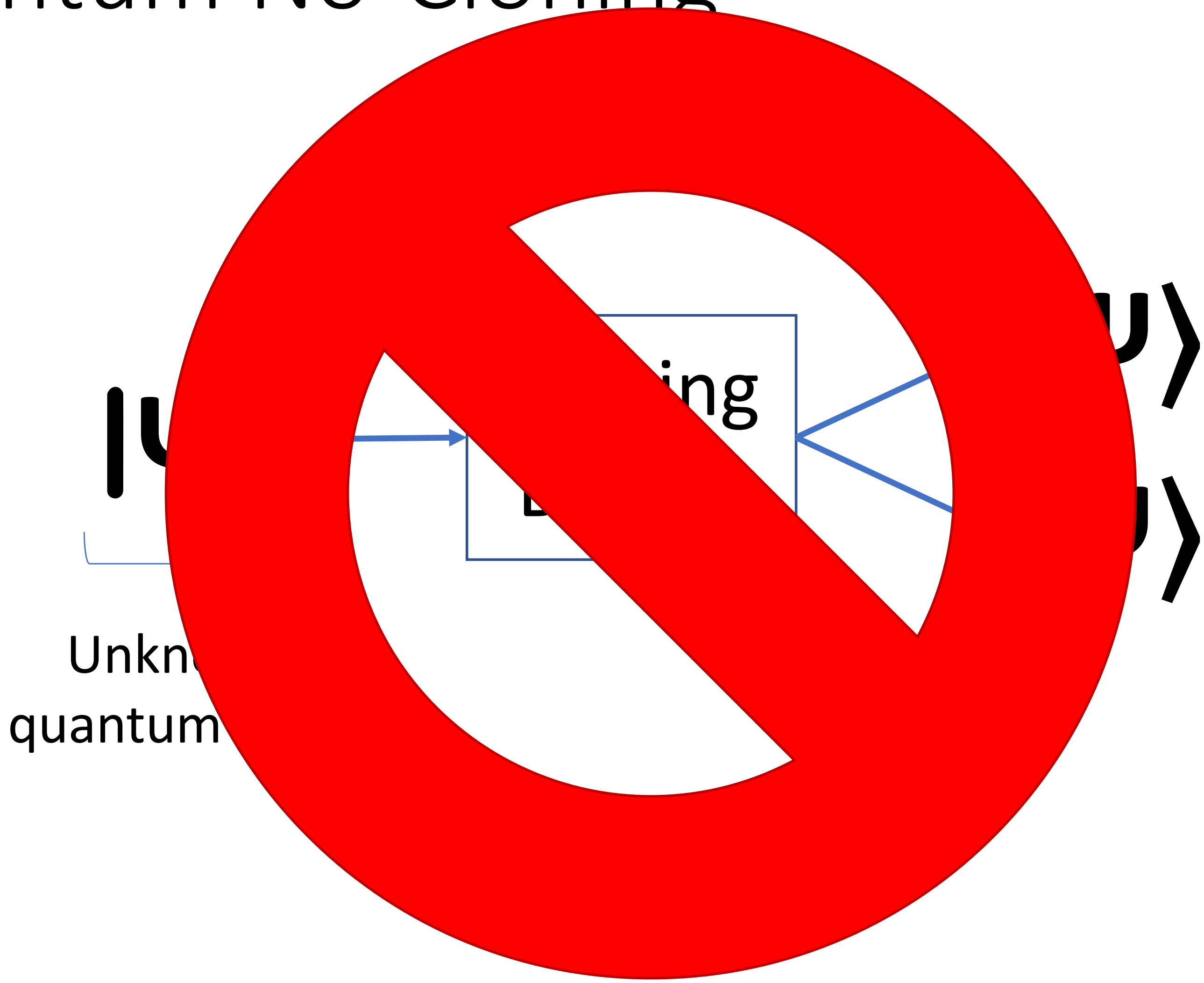
Quantum Lightning Never Strikes the Same State Twice

Mark Zhandry

Princeton University

Quantum No-Cloning

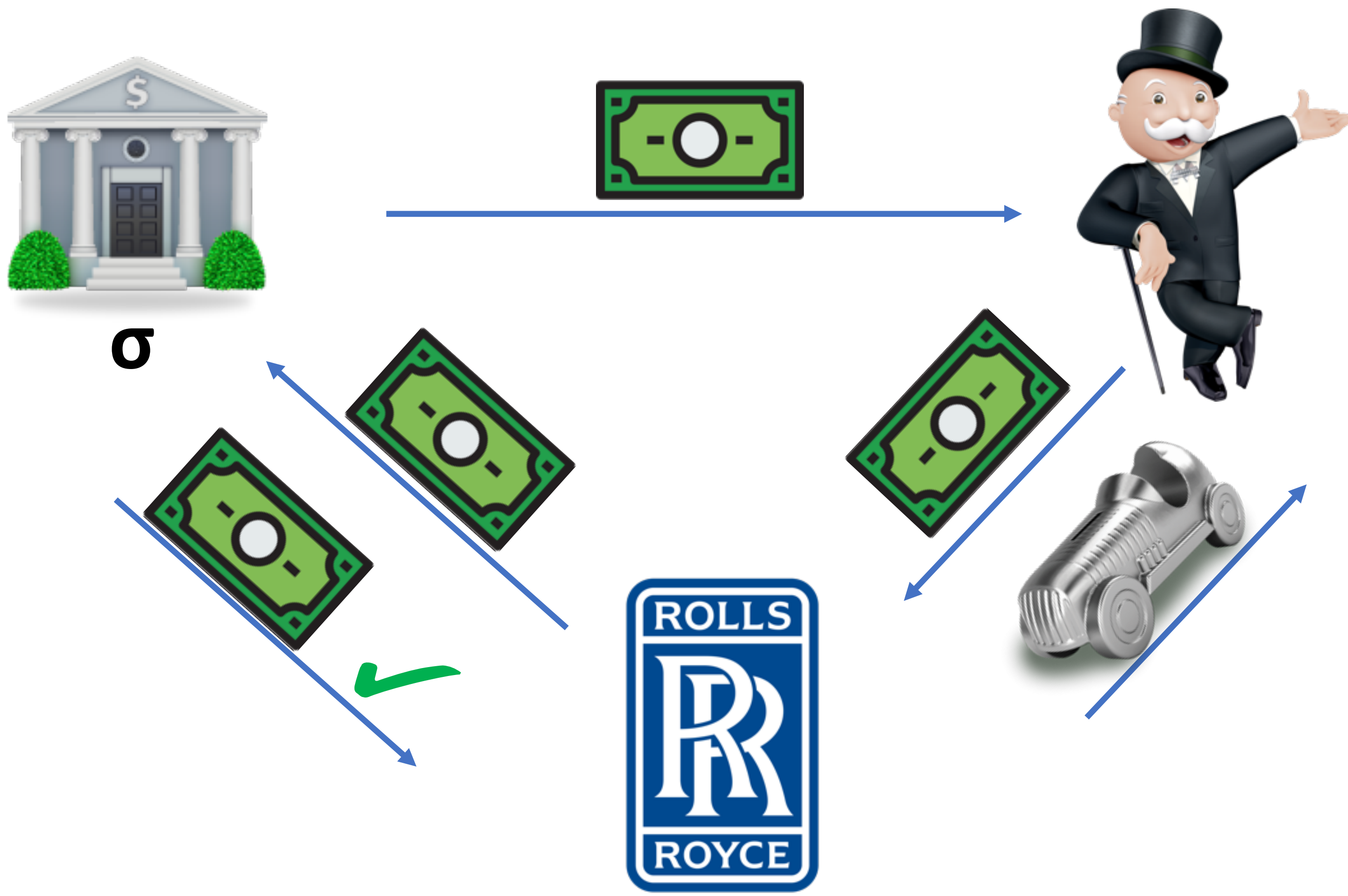


No-Cloning = Quantum Money [Wiesner'70]

 $= |\Psi\rangle$

$\underbrace{\text{Serial \#} = \text{classical description}}_{\text{Kept secret}}$

Limits of (Plain) Quantum Money



Limits of (Plain) Quantum Money

Mint must be involved in verification

- Requires merchant and Mint to have quantum channel

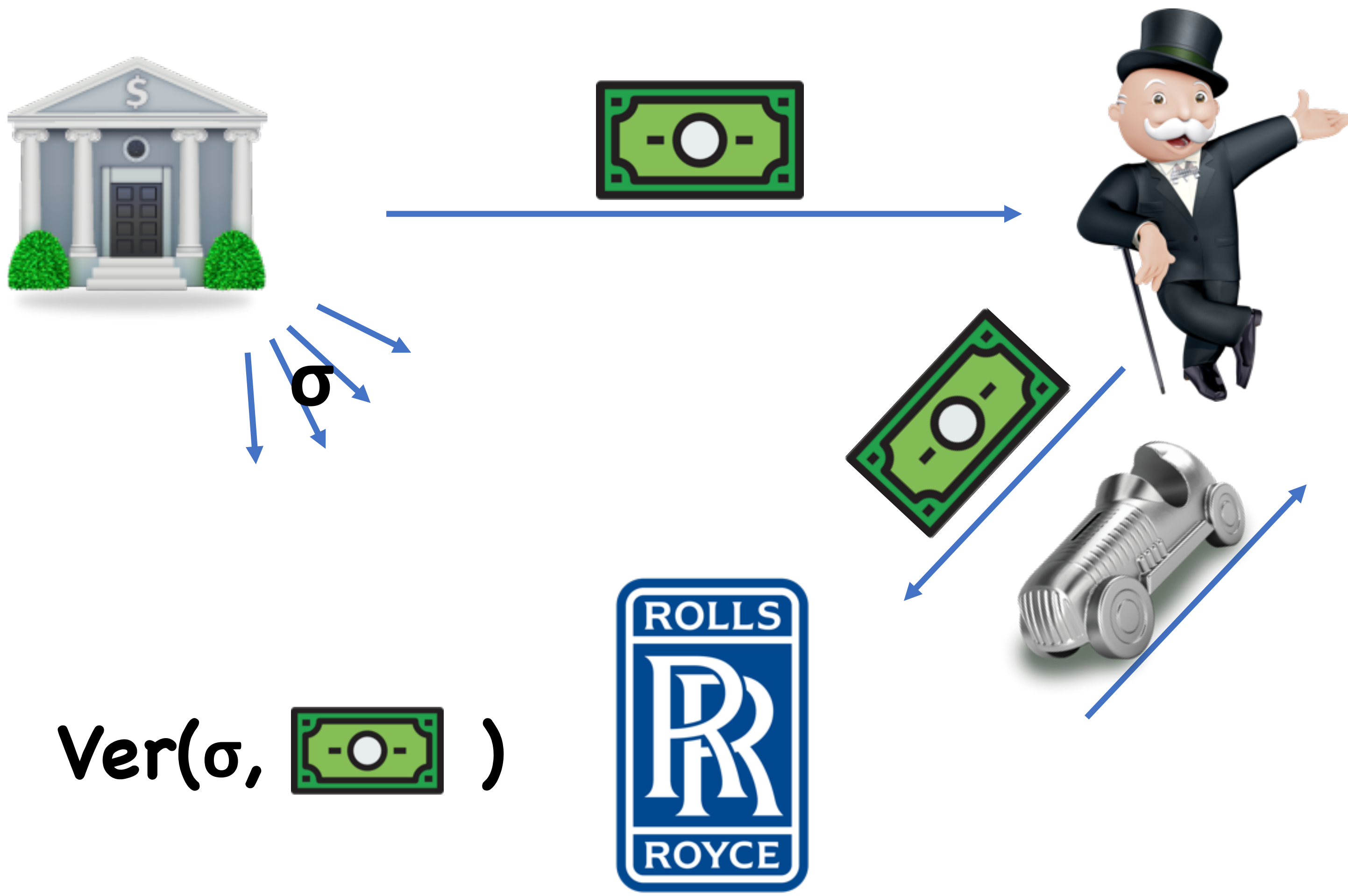
Moreover, having verification oracle can break security [Lutomirski'10]

- Can fix by replacing note with new bill every time

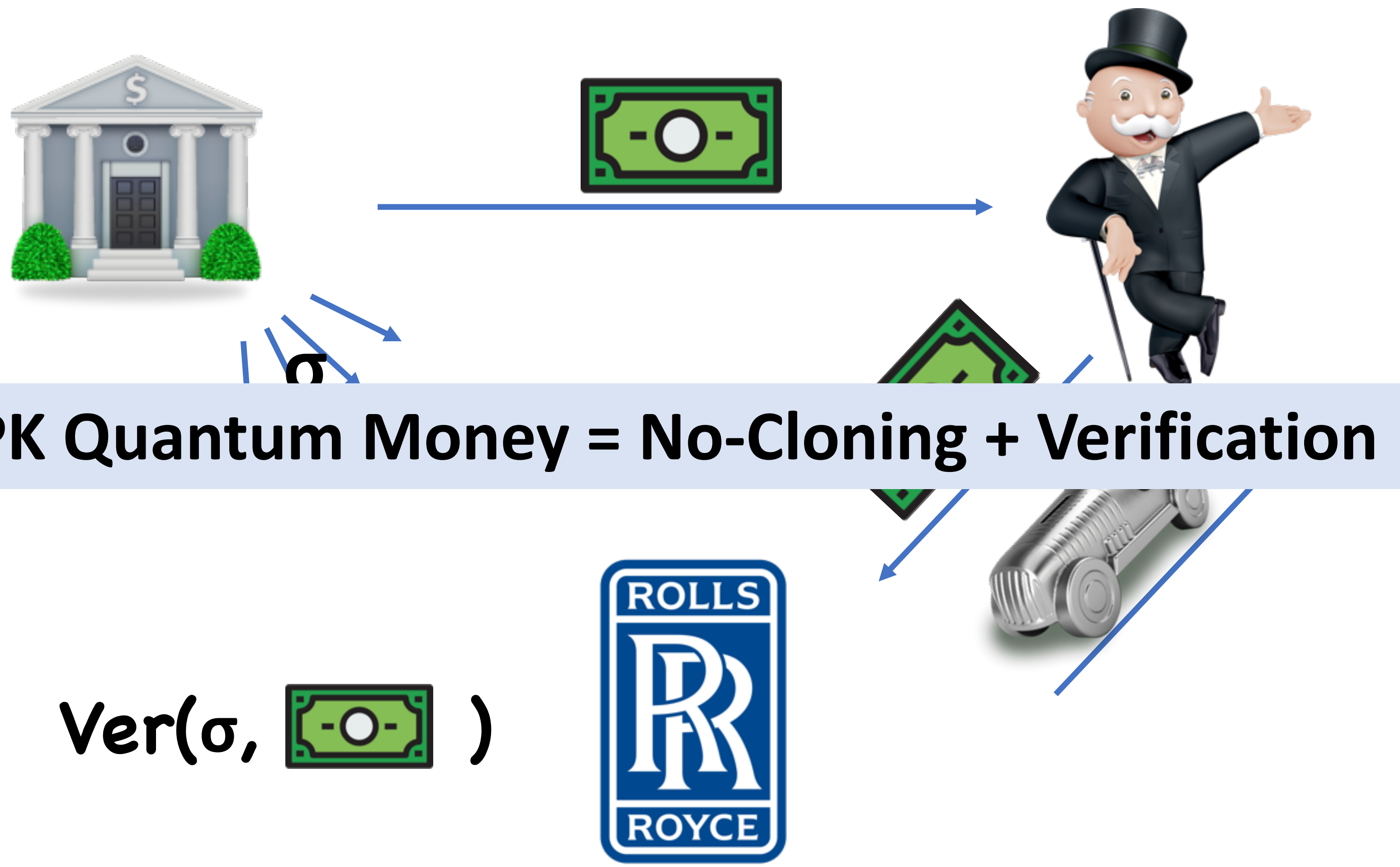
(Some proposals to circumvent difficulties [Mosca-Stebila'10, Gavinsky'10])

Decoherence?

Public Key Quantum Money [Aaronson'09]

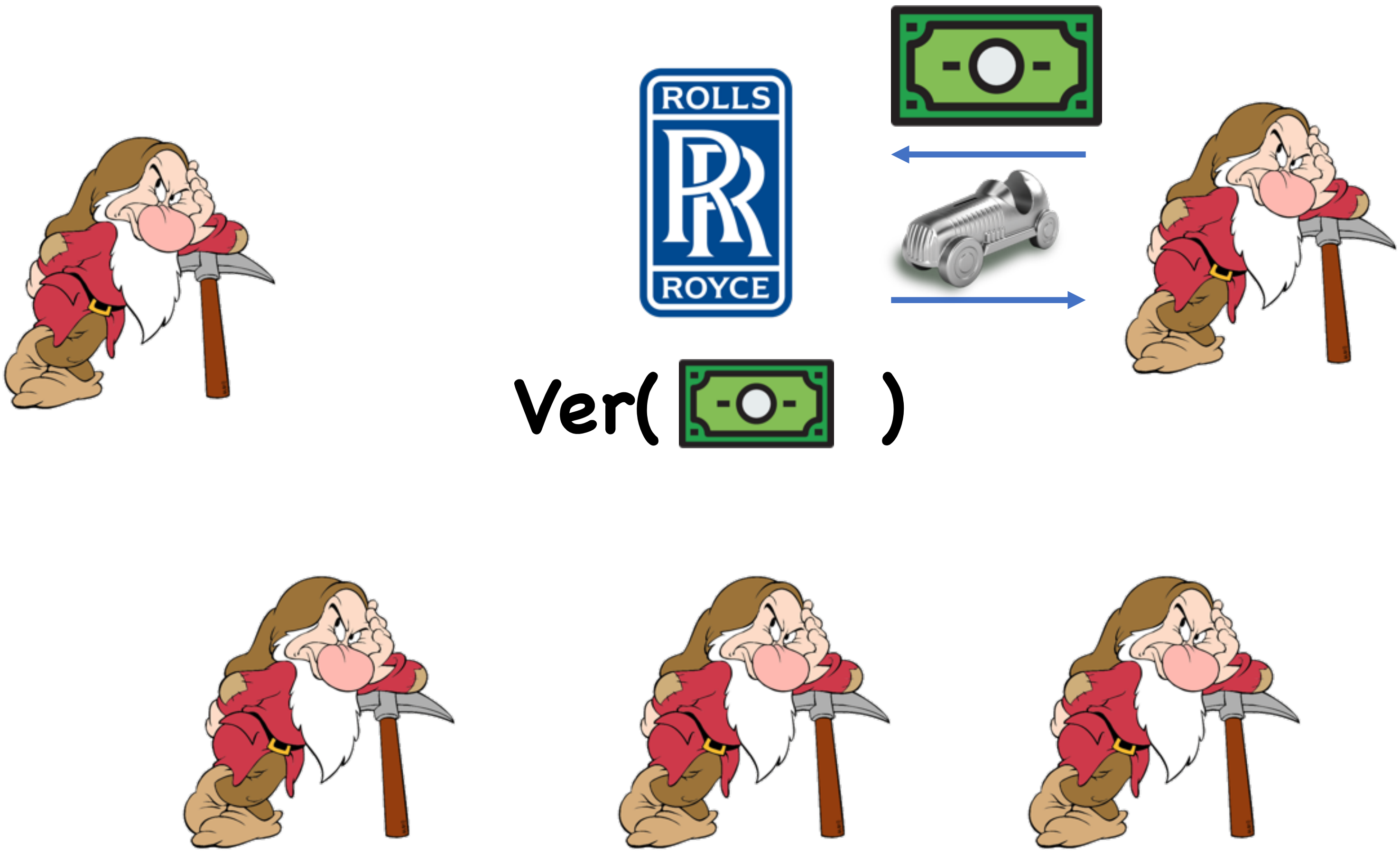


Public Key Quantum Money [Aaronson'09]



PK Quantum Money = No-Cloning + Verification

Bitcoin sans blockchain?



Quantum Lightning

Let’s pretend old adage is true of lightning in nature

Of course, can erect lightning rod to tamper with nature




Quantum lightning = secure “digital” lightning immune to adversarial generation (aka lightning rods)

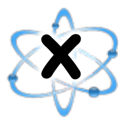
- Impossible classically: can always reset to same initial conditions

This work: study strong variants of no cloning

- **New constructions**
- **Connections to post-quantum security**

Quantum Background

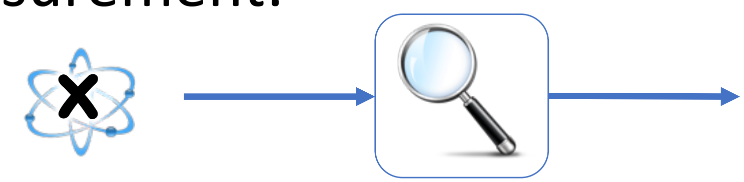
Quantum states:



= superposition of **all** messages

$= \Sigma\alpha_x|x\rangle \qquad (\Sigma|\alpha_x|^2 = 1)$

Measurement:



x with probability $|\alpha_x|^2$

Operations: Unitary transformations on amplitude vectors

Quantum Background

Example Operations:

- Simulate classical ops in superposition:

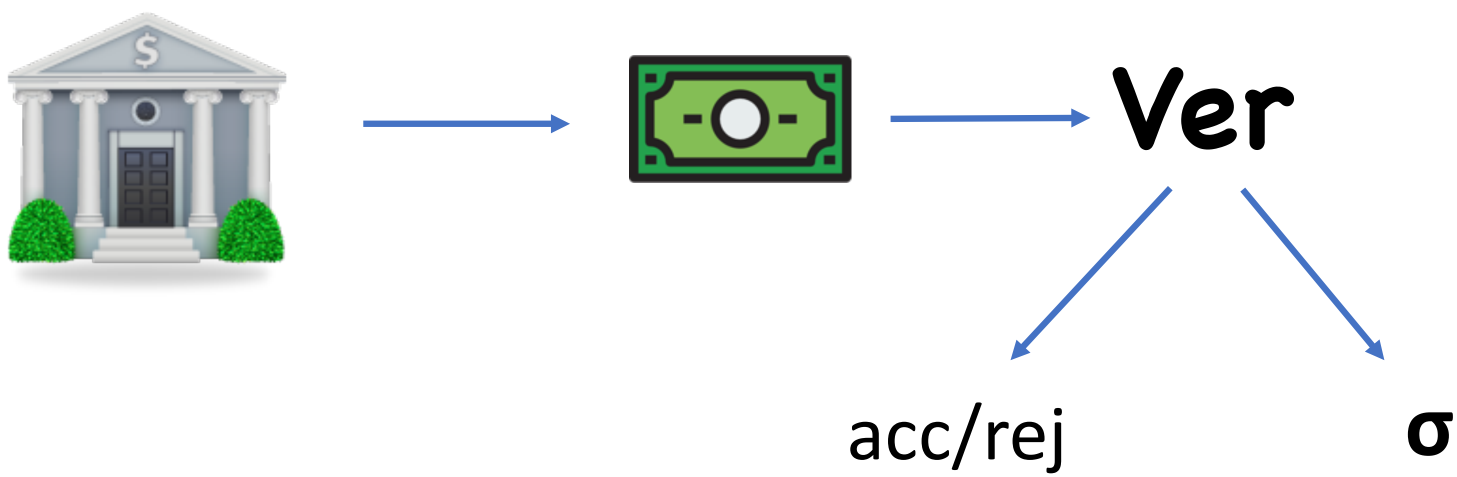
$$x,y \longrightarrow \boxed{O} \longrightarrow x,y+O(x) \;=\; \Sigma\alpha_{x,y}|x,y+O(x)\rangle$$

- Quantum Fourier Transform:

$$x = \Sigma\alpha_x|x\rangle \longrightarrow \boxed{\text{QFT}} \longrightarrow y = \Sigma\hat{a}_y|y\rangle$$

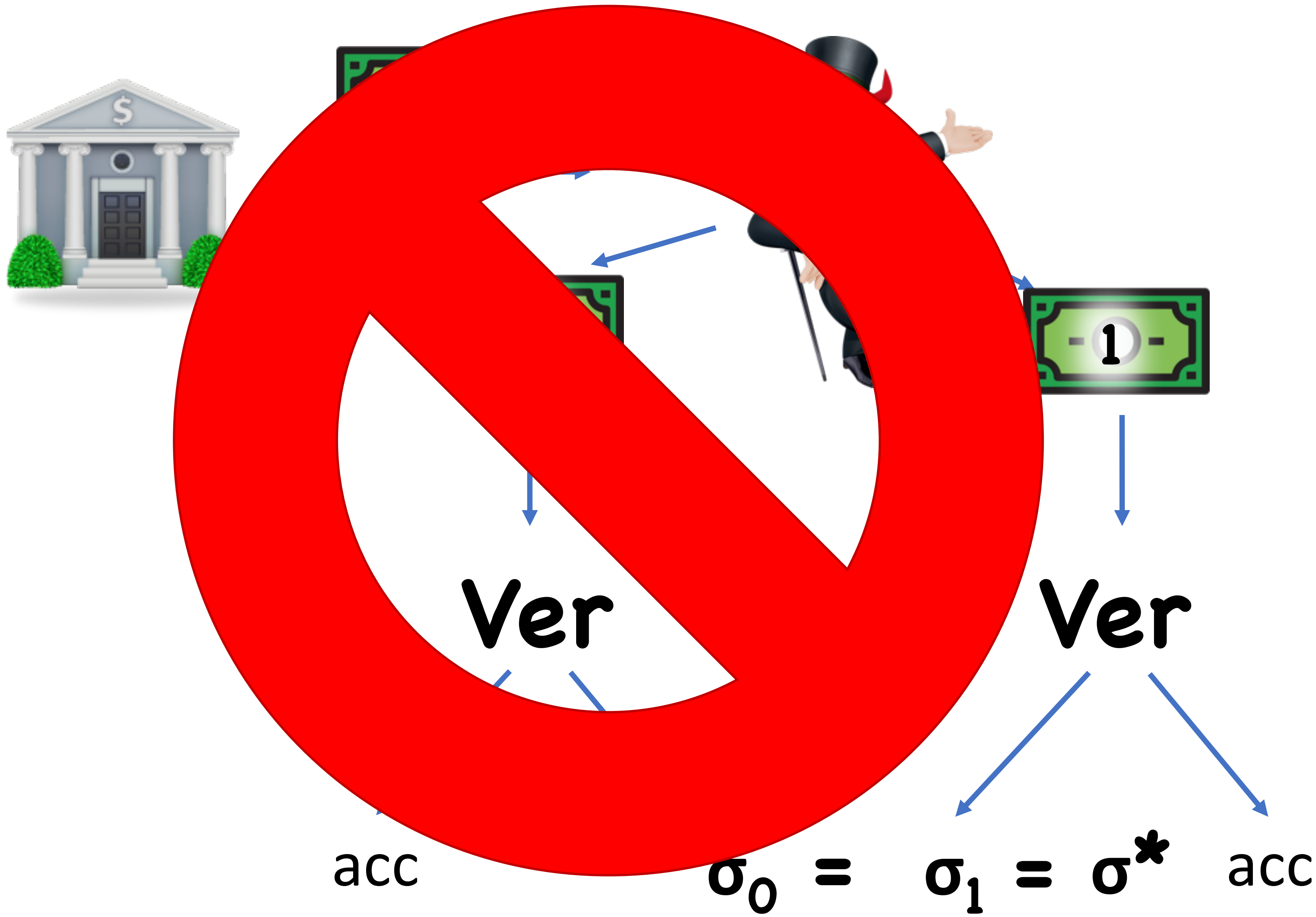
$$\hat{a}_y = (\Sigma\alpha_x\omega^{xy})/C$$

Public Key Quantum Money



- Verification accepts honest banknotes
- Verification leaves honest banknotes intact
- Repeated verification on honest banknotes results in same **σ**

Public Key Quantum Money

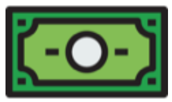


Constructions of PK Quantum Money

- [Aaronson’09]: (1) relative to **Quantum** oracle, (2) concrete candidate instantiation
  - (2) broken by [Lutomirski-Aaronson-Farhi-Gosset-Kelner-Hassidim-Shor’10]
- [Farhi-Gosset-Hassidim-Lutomirski-Shor’12]: from knots
- [Aaronson-Christiano’12]: (1) relative to **Classical** oracle, (2) concrete candidate instantiation
  - (2) broken by [Pena-Faugère-Perret’15]

[Aaronson-Christiano’12]

Let **S** be a **d/2**-dimemsional subspace of $\mathbb{Z}_p^{d}$



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

Ver:

$$\to \boxed{S} \to \boxed{QFT} \to \boxed{S^{\perp}} \to \boxed{QFT} \to$$

✓ ✓

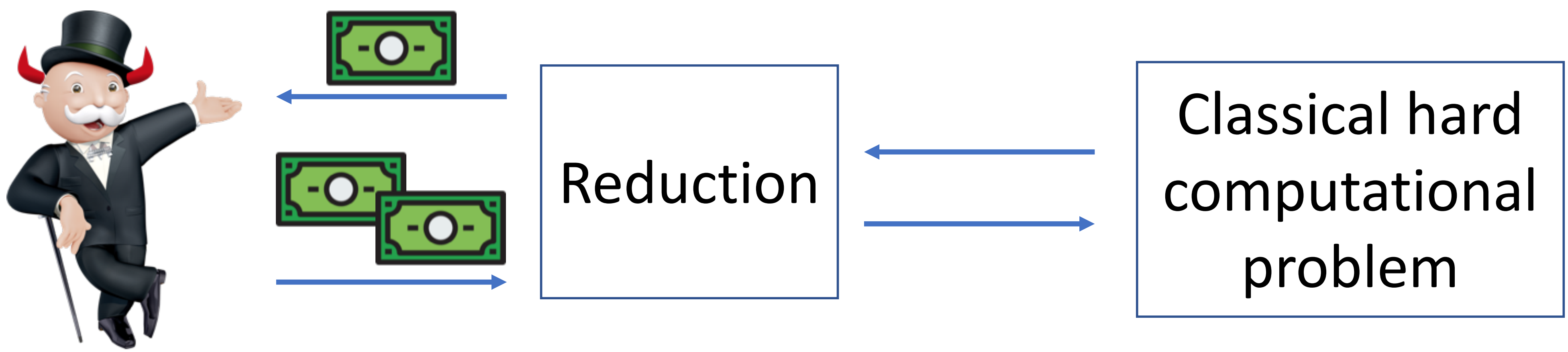
[Aaronson-Christiano’12]

Thm [Aaronson-Christiano’12**]:** If $\mathbf{S},\mathbf{S}^{\perp}$ given as oracles, no efficient quantum adversary can copy

Additionally provide candidate *obfuscator* for subspaces

- Serial number = obfuscations of $\mathbf{S},\mathbf{S}^{\perp}$
- Proof relative to non-standard assumption
- Scheme/assumption broken by [Pena-Faugère-Perret’15]

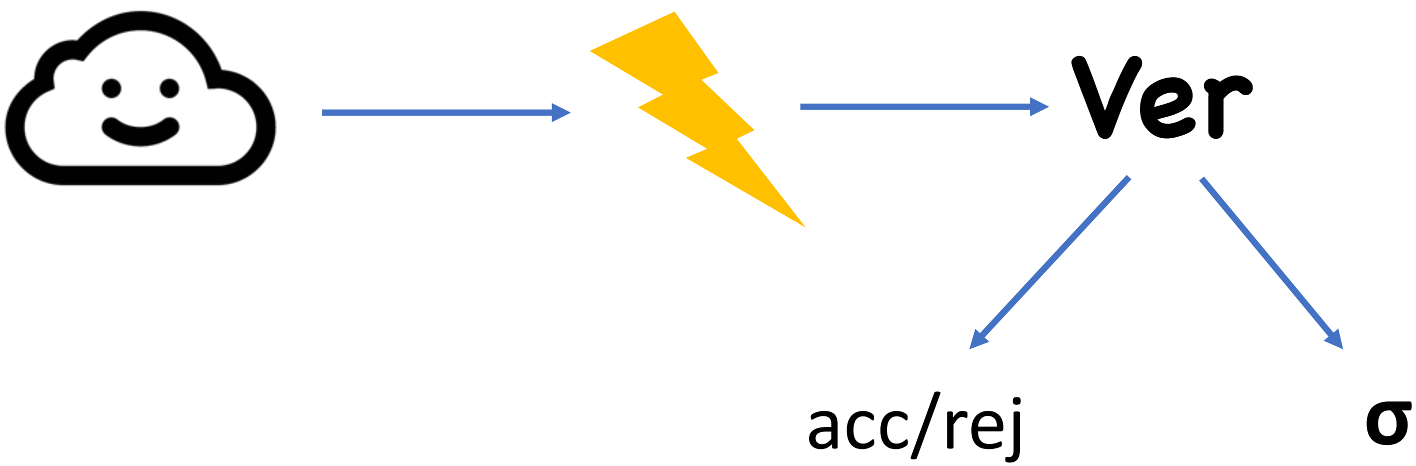
Barrier to Proving Quantum Money



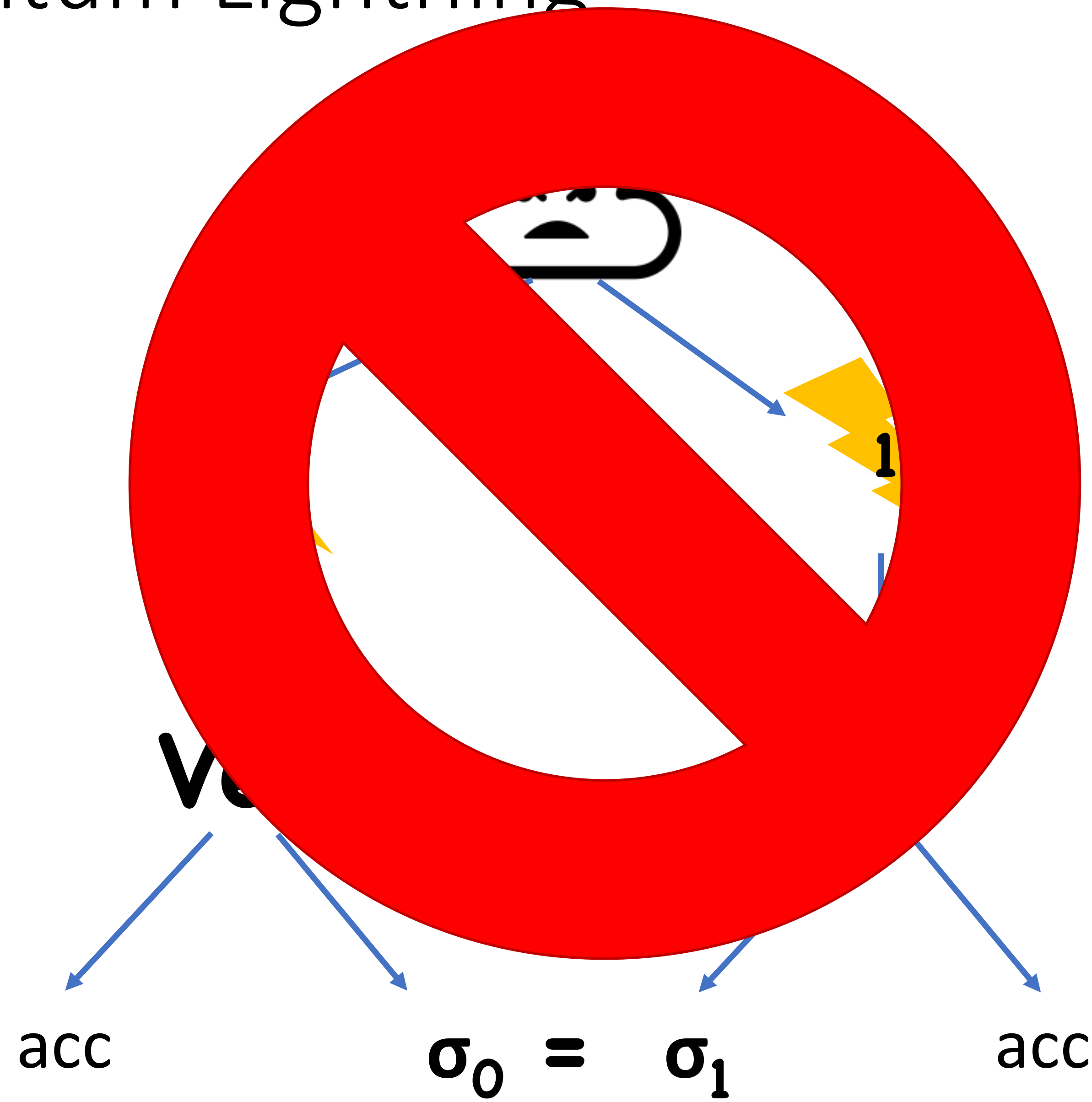
If adversary can produce a single banknote, why can't it produce two?

Quantum Lightning

Aka "collision-free" quantum money
[Lutomirski-Aaronson-Farhi-Gosset-Kelner-Hassidim-Shor'10]



Quantum Lightning

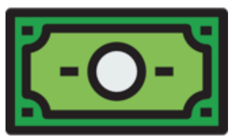
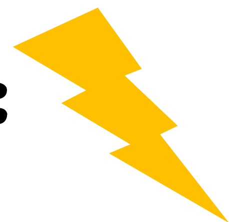


Quantum Lightning

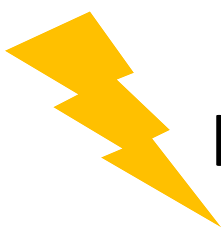
Applications:

- PK Quantum money

- Decentralized currency

 =  s.t. $H(\sigma)=0^n\{0,1\}^*$

- Provable min-entropy

 proves that **σ** has min-entropy

Detour:
Classical crypto in a quantum world

(Bit) Commitment Schemes

Hiding

Commit
Phase

$m \in \{0,1\}$

?

Binding

Limitation

Security goal: once Alice commits, there is a unique message she can de-commit to

Actual security notion: once Alice commits, she cannot simultaneously de-commit to both $\mathbf{0}$ and $\mathbf{1}$

Classically, these two goals are the same (use rewinding), but quantumly, they may not be

Limitation: Quantum Rewinding

Intuition:

- Alice may keep a state that allows her to decommit to either $\mathbf{0}$ or $\mathbf{1}$

- Once she decommits to, say, $\mathbf{0}$, she must measure to get classical decommitment $\Rightarrow$ state collapses

- Cannot no longer rewind to evaluate on $\mathbf{1}$

Solution: Collapse-Binding [Unruh'16]

Commit Phase

$\Sigma\alpha_m$ $|$**m,**Reveal **m**$\rangle$

$|\Psi\rangle$

Measured?

- Verify
- W/ prob ½, measure **m**

Is this really a problem?

Thm [Ambainis-Rosmanis-Unruh'14**]:** Relative to a quantum oracle, there exists a commitment scheme that is classically binding, but an efficient quantum adversary can de-commit to either **0** or **1**

What's this got to do with no-cloning?

Either/Or Results

Thm (Informal): A **binding** commitment is either **collapse binding**, or can be used to build public key quantum money.

Thm (Informal): A *non-interactive* **binding** commitment is either **collapse binding**, or can be used to build quantum lightning.

Also show analogous statements for digital signatures, hash functions

Intuition

Thm (Informal): A **binding** commitment is either **collapse binding**, or can be used to build public key quantum money.

What if we could clone adversary's post-commitment state?
- Then no need to rewind, definitions equivalent

So any separation inherently uses no-cloning
- Banknote/bolt = adversary's state
- For verification, check that adversary breaks collapse-binding

Proof (Non-Interactive Case)

Assume:

$\downarrow$

m measured?

comm $\longrightarrow$

$\Sigma\alpha_m$ $|$**m**$,$Reveal **m**$\rangle$ $\longrightarrow$

$\longleftarrow$ $|\Psi\rangle$

- Verify
- W/ prob ½, measure **m**

Proof (Non-Interactive Case)

Assume:

state

m measured?

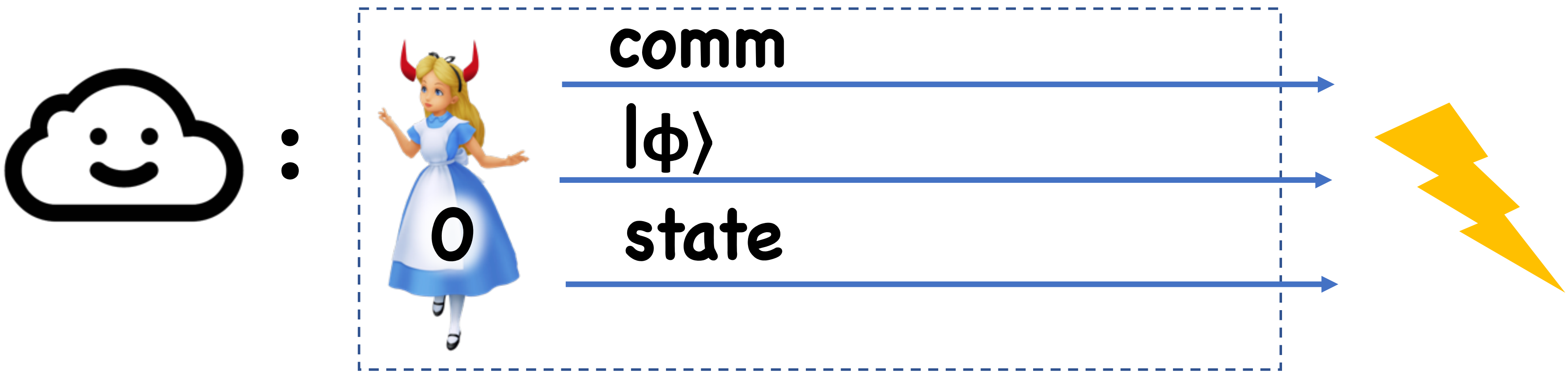
comm

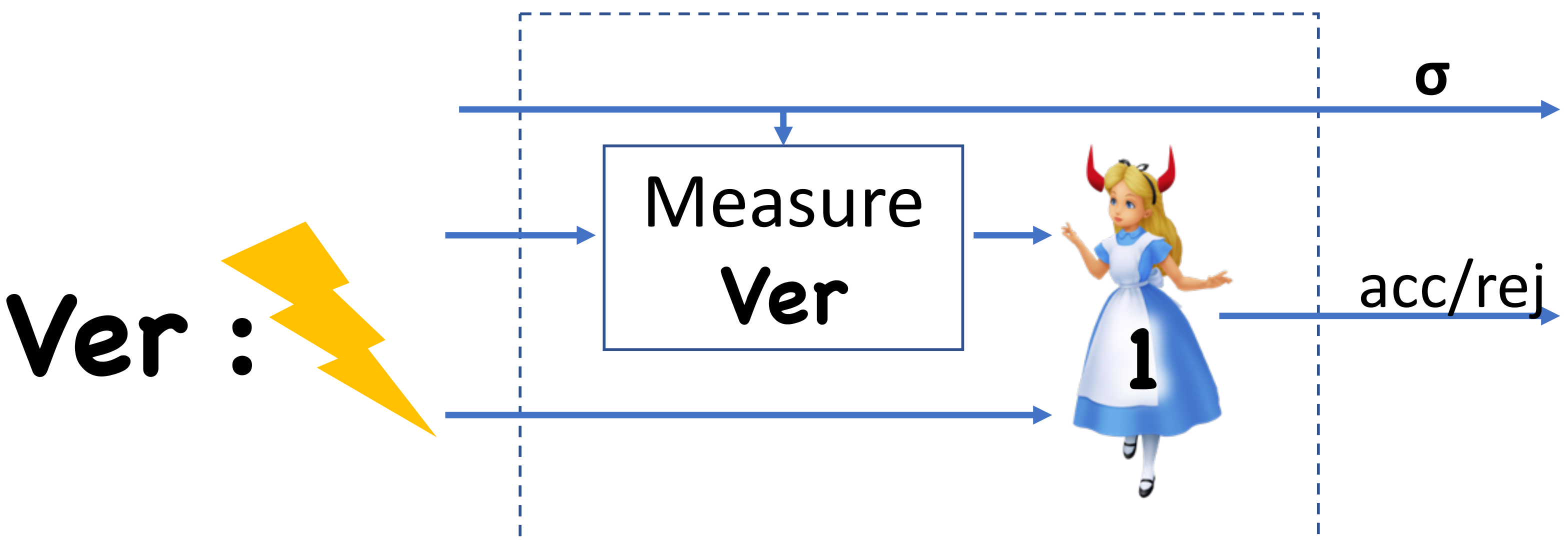
$|\phi\rangle = \Sigma\alpha_m\ |m, \text{Reveal } \mathbf{m}\rangle$

$|\psi\rangle$

- Verify
- W/ prob ½, measure **m**

Proof (Non-Interactive Case)





Proof (Non-Interactive Case)

Given two valid bolts with same serial number **σ=comm**,

- Both $|\phi\rangle$ contain only openings valid wrt **comm**

- Both $|\phi\rangle$ are in superposition

Therefore, if we measure both bolts, we will get openings to both 0 and 1 with reasonable probability

Proof Difficulties

- Alice may not be a perfect distinguisher
- Bolt may contain state that didn't come from Alice
- Need to rule out small success probabilities
- Verifier may not be able to rewind Alice perfectly

  $\Longrightarrow$ Hard to simultaneously guarantee in superposition and contains only valid pre-images

Takeaways

Two possible interpretations:

(1) Quantum money is hard, so probably don't have to worry about these quantum security issues

(2) Possible route toward building quantum money/lightning

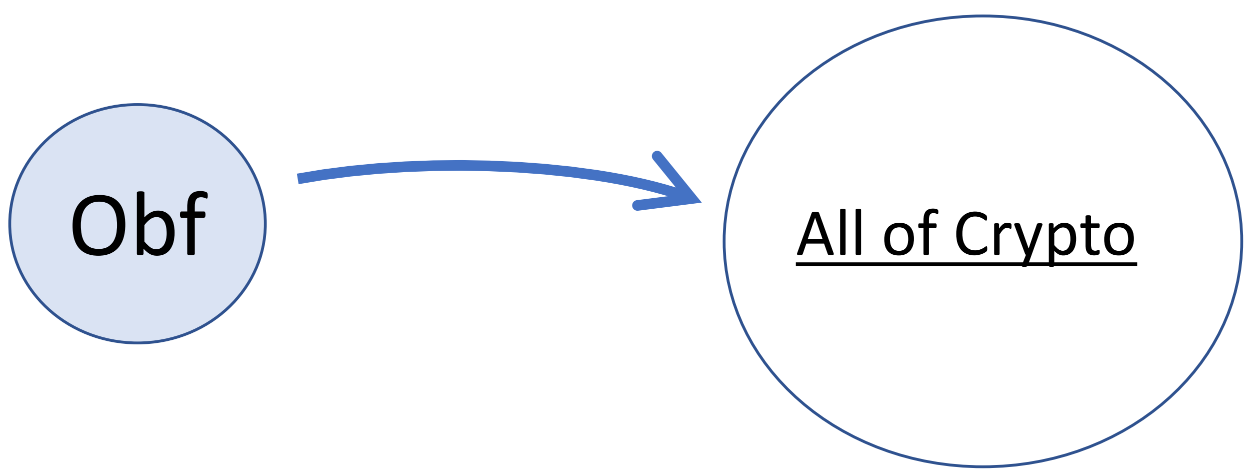
New Constructions of Quantum Money/Lightning

Program Obfuscation

"Scramble" a program

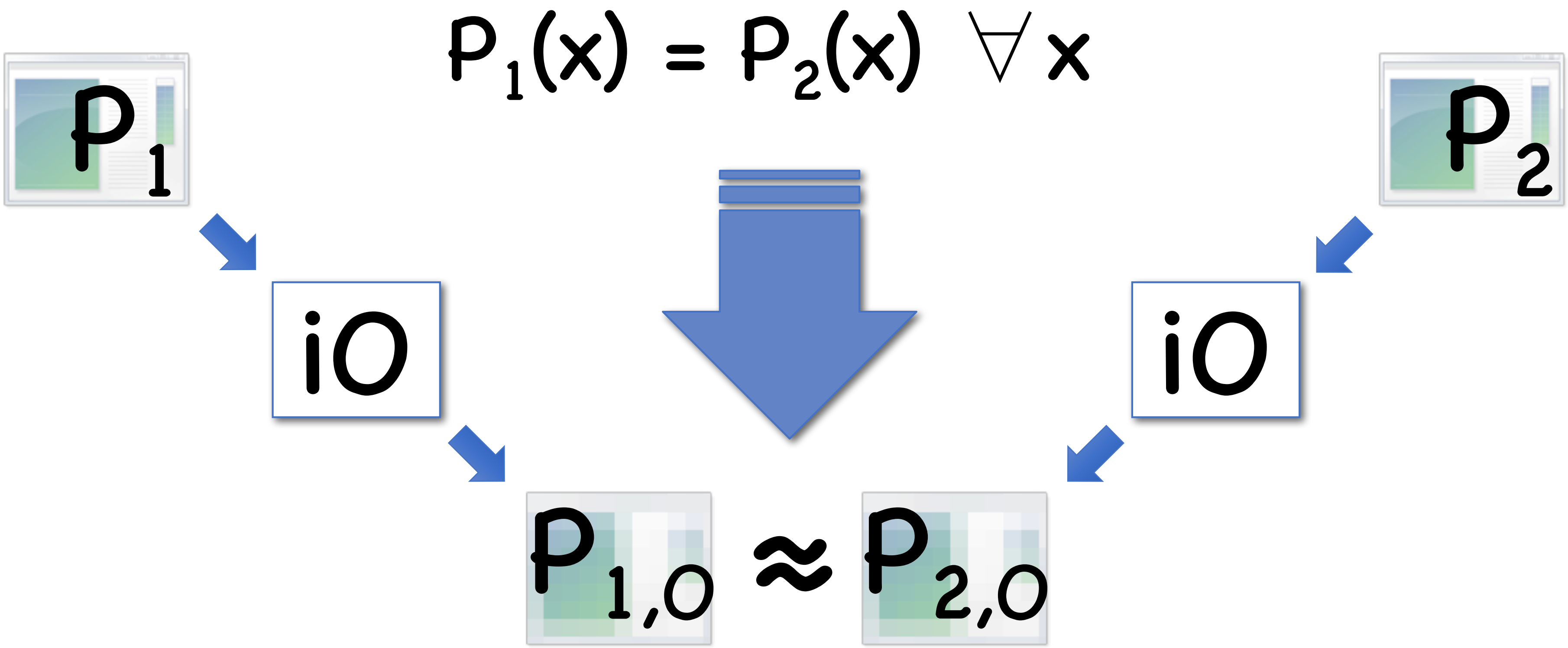
- Hide implementation details
- Maintain functionality

Golden goose of crypto, believed by many to be "crypto complete"



Indistinguishability Obfuscation (iO)

[Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang'01]



Candidate Constructions

First: [Garg-Gentry-Halevi-Raykova-Sahai-Waters'13]
- Based on "multilinear maps" from [Garg-Gentry-Halevi'12]

Many subsequent proposals, and attacks
- [Coron-Lepoint-Tibouchi'13, Cheon-Han-Lee-Ryu-Stehle'14,Boneh-Wu-Zimmerman'14, Brakerski-Rothblum'14, Barak-Garg-Kalai-Paneth-Sahai'14, Ananth-Gupta-Ishai-Sahai'14, Coron-Gentry-Halevi-Lepoint-Maji-Miles-Raykova-Sahai-Tibouchi'15,Hu-Jia'15, Brakerski-Gentry-Halevi-Lepoint-Sahai-Tibouchi'15,Coron-Lepoint-Tibouchi'15, Cheon-Lee-Ryu'15, Minaud-Fouque'15, Badrinarayanan-Miles-Sahai-Z'15, Miles-Sahai-Z'16, Garg-Miles-Mukherjee-Sahai-Srinivasan-Z'16,Chen-Gentry-Halevi'16,…]

Quantum security unclear, but I strongly believe a construction exists

Folklore PK Quantum Money

Simply obfuscate oracles $\mathbf{S},\mathbf{S}^{\perp}$ in [AC'12] using iO

Unfortunately, not so simple…

- Proving security for most tasks using iO is already hard (not uncommon to have 60+ page papers)

- Plus, difficulty discussed earlier

Security Proof for QM from iO

Thm: If injective OWFs exist, then [Aaronson-Christiano'12] instantiated with iO is secure

Security Proof for QM from iO

Proof idea:

- Don’t use iO to directly prove cloning is hard
- Instead, use iO to convert adversary into information-theoretic cloner
- Then use information-theoretic techniques to rule out such a cloner

Security Proof for QM from iO

Let **T** be a random super-space of **S** of dimension **¾d**

Let **T'** be a random super-space of $\mathbf{S}^{\perp}$ of dimension **¾d**

What if we instead obfuscate **T,T'**?

Lemma: By iO (plus injective OWFs), even if adversary knows **S** (but not **T,T'**), can't tell difference between **iO(S),iO($\mathbf{S}^{\perp}$)** and **iO(T),iO(T')**

Actually, suffices to have a good "subspace-hiding" obfuscator

Security Proof for QM from iO

Equivalent way to generate $\mathbf{S},\mathbf{T},\mathbf{T'}$:

- Choose random $\mathbf{T},\mathbf{T'}$ such that $\mathbf{T}^\perp \subseteq \mathbf{T'}$
- Then choose random $\mathbf{S}$ s.t. $\mathbf{T}^\perp \subseteq \mathbf{S} \subseteq \mathbf{T'}$

Security Proof for QM from iO

Suppose we obfuscate **T,T′**

Let $|\Psi_S\rangle = \Sigma_{x \in S} |x\rangle$

Now adversary duplicates $|\Psi_S\rangle$ for unknown **S**

Lemma: Even if adversary knows **T,T′**, cannot clone $|\Psi_S\rangle$

Follows from a new quantitative version of no-cloning theorem

Constructing Quantum Lightning

Apparently really hard (at least for me)

No known constructions from any existing tools

- Using [ARU'14] + obfuscator for *quantum* circuits + Either/Or result, may get *candidate*
- But no good candidates for quantum obfuscation

Instead, I devise a new assumption…

Failed Approach to Quantum Lightning

The SIS hash function:

- Fix integers $\mathbf{n,m,q,B}$, $\mathbf{m \gg n}$, $\mathbf{B \ll q}$
- Let $\mathbf{A}$ be a random matrix in $\mathbb{Z}_q^{n\times m}$

$$H_A: [-B,B]^m \rightarrow \mathbb{Z}_q^n$$
$$H_A(x) = A\cdot x$$

Collision resistant based on worst-case lattice problems

Maybe non-collapsing?

Failed Approach to Quantum Lightning

Idea to show non-collapsing:

- Prepare state $\Sigma_x \ N_\sigma(x) \ |x\rangle$
- If we apply H_A and measure, will get state

$$|\Psi_y\rangle = \Sigma_{x:A\cdot x=y} \ N_\sigma(x) \ |x\rangle \ = \ \Sigma_x \ J_y(x) N_\sigma(x) \ |x\rangle$$

$J_y(x)$ indicator for $A\cdot x=y$

- QFT of this state:

$$|\Psi'_y\rangle \ = \ \Sigma_{r,e} \ \omega^{y\cdot e} \ N_{q/\sigma}(e) \ |r\cdot A+e\rangle$$

- Superposition of LWE samples!

Quantum Lightning from Lattices?

Turns out SIS for random $\mathbf{A}$ is collapsing* [Liu-Z'19]

But maybe we can break SIS in such a way to allow decisional LWE to be easy?

- Obvious choice: give a short vector ($\ll \sigma$) in kernel of $\mathbf{A}$. But then $\mathbf{H}_\mathbf{A}$ is not collision resistant!

Open question: Devise distribution over $\mathbf{A}$ such that:

(1) SIS hard (2) dec. LWE easy (3) search LWE hard

* for super-poly modulus, weaker notion for poly modulus

Abstracted Construction

SIS is an example of a domain-constrained linear function

- Linear functions are easily cryptanalyzed by quantum

Maybe other domain restrictions are useful?

- Need to behave nicely with QFT

In paper, give candidate construction

- Interpret input as a matrix
- Domain constraint: low-rank matrix
- Show trapdoor that doesn't trivially break security
- Lots of annoying details

Future Directions

Construct quantum lightning from iO (+LWE etc)

Verifiable Entropy
- Quantum lightning gives quantum non-interactive proof of min-entropy
- [Brakerski-Christiano-Mahadev-Vazirani-Vidick'18] interactive privately verifiable classical proof of uniform randomness from LWE
- Goal: classical non-interactive proof?

Other applications of no-cloning
- Un-clonable programs
- Various one-shot primitives (one-time memory, etc)

Thanks!