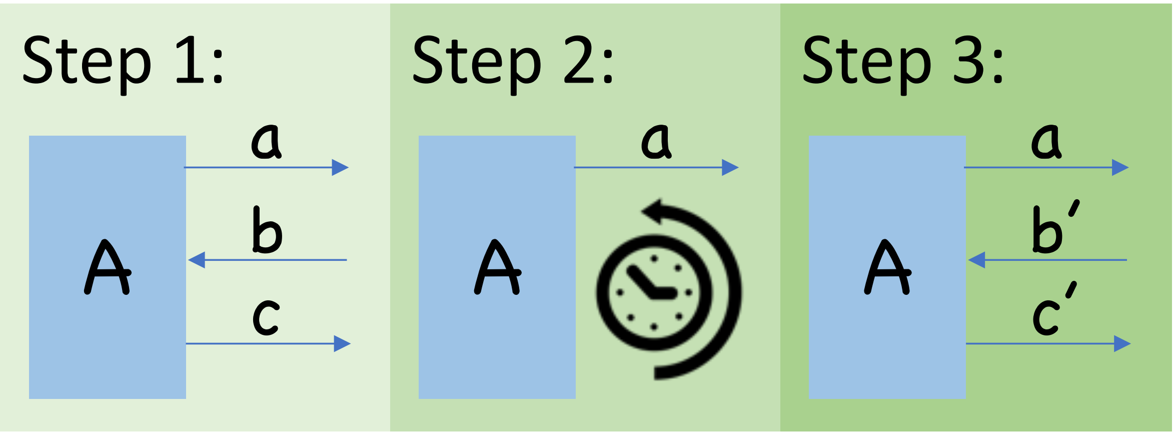
Quantum Rewinding

Mark Zhandry (Princeton & NTT Research)

Classical Rewinding

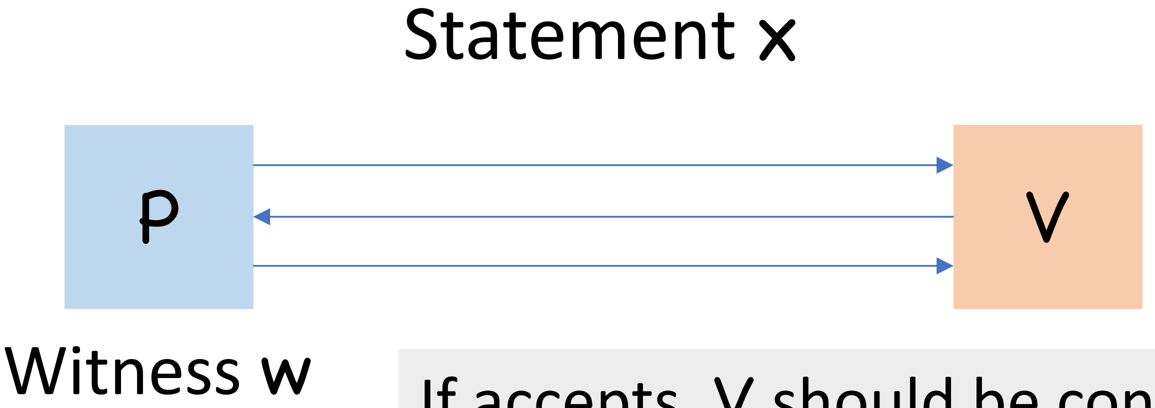


Zero knowledge

Commitments

Proofs of knowledge

Proof of Knowledge (PoK)



Statement x

P

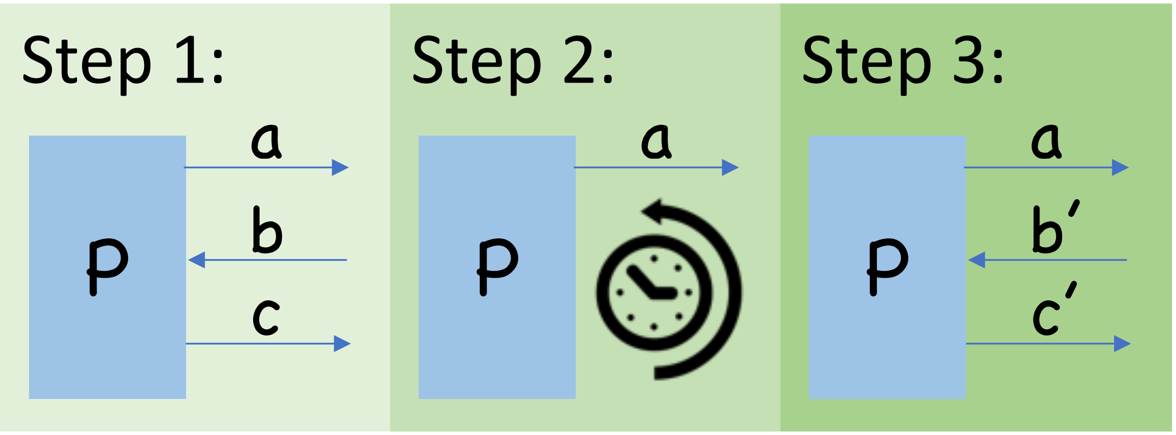
V

Witness w

If accepts, V should be convinced not only of x, but also that P “knows” witness

Usually combine with over properties like zero knowledge

Rewinding for PoK



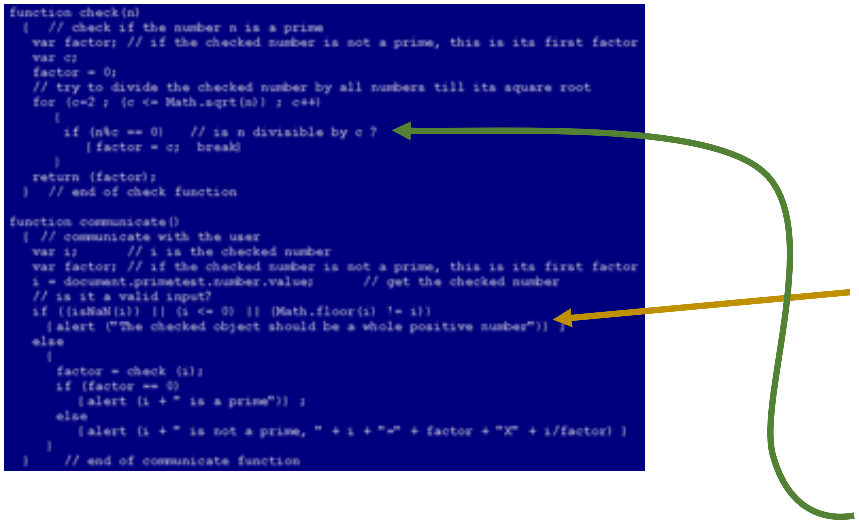
$(a,b,c,b',c'),\ b\neq b'$

$\Downarrow$

w

“special soundness”

What Does Rewinding *Really* Mean



```
function check(n)
  {   // check if the number n is a prime
    var factor; // if the checked number is not a prime, this is its first factor
    var c;
    factor = 0;
    // try to divide the checked number by all numbers till its square root
    for (c=2 ; (c <= Math.sqrt(n)) ; c++)
       {
        if (n%c == 0)    // is n divisible by c ?
           { factor = c;  break}
       }
    return (factor);
  }   // end of check function

function communicate()
  {  // communicate with the user
    var i;       // i is the checked number
    var factor; // if the checked number is not a prime, this is its first factor
    i = document.primetest.number.value;       // get the checked number
    // is it a valid input?
    if ((isNaN(i)) || (i <= 0) || (Math.floor(i) != i))
      { alert ("The checked object should be a whole positive number")} ;
    else
      {
       factor = check (i);
       if (factor == 0)
          { alert (i + " is a prime")} ;
       else
          { alert (i + " is not a prime, " + i + "=" + factor + "X" + i/factor) }
      }
  }    // end of communicate function
```

Given state here,

can we remember state here?

Classical programs not necessarily “reversible”

But can be *made* reversible by recording program trace

What Does Rewinding *Really* Mean

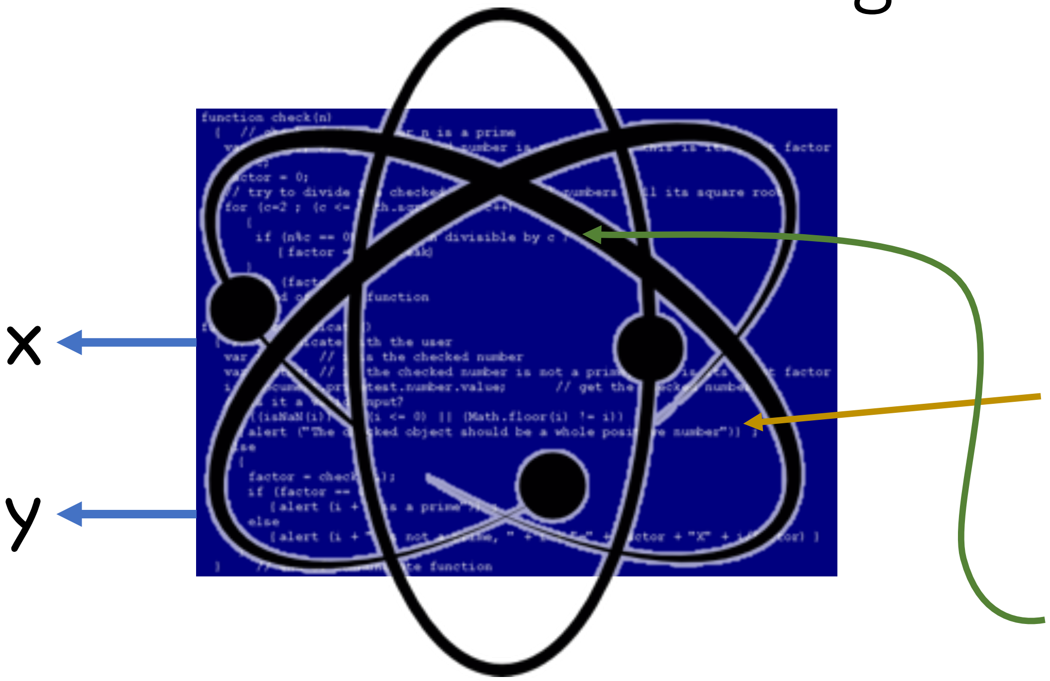
But isn’t quantum computing alrady reversible?

Only until a measurement…

Uncertainty Principle: once measurement is performed, quantum state irreversibly altered

No Cloning: can’t record program trace for later

What Does Rewinding *Really* Mean



Given state here,

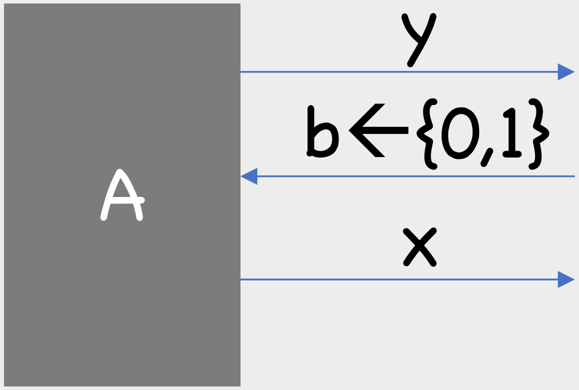
prior state un-recoverable

Interactive quantum programs *cannot* in general be made reversible

Impossibility of Quantum Rewinding

[Ambainis-Rosmanis-Unruh'14]

Coin flipping/commitment game



Win if

- $H(x)=y$
- $x_1 = b$

Classically:

$\Pr[A \text{ wins}] \geq \frac{1}{2}+\varepsilon$

+ Rewinding

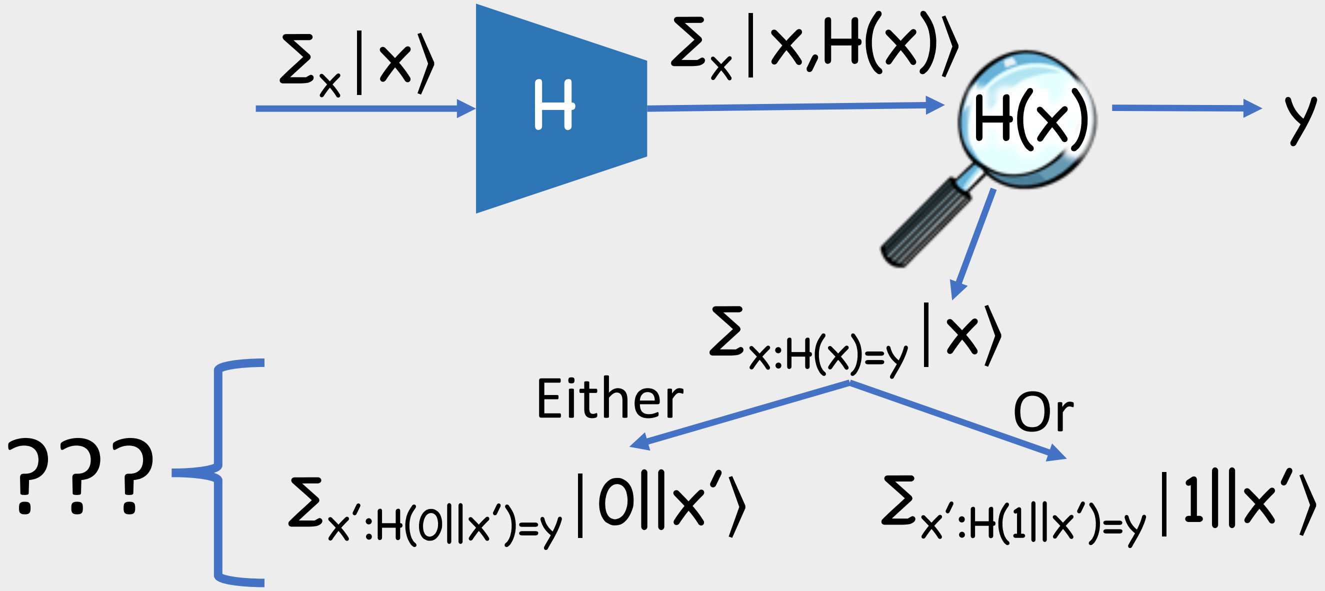
$= \Pr[\text{collision}] \geq \text{poly}(\varepsilon)$

Goal: devise *quantum* A and col. res. H where $\Pr[A \text{ wins}] \approx 1$

Impossibility of Quantum Rewinding

[Ambainis-Rosmanis-Unruh’14]

Idea:



$\Sigma_x|x\rangle$

H

$\Sigma_x|x,H(x)\rangle$

H(x)

y

$\Sigma_{x:H(x)=y}|x\rangle$

Either

Or

???

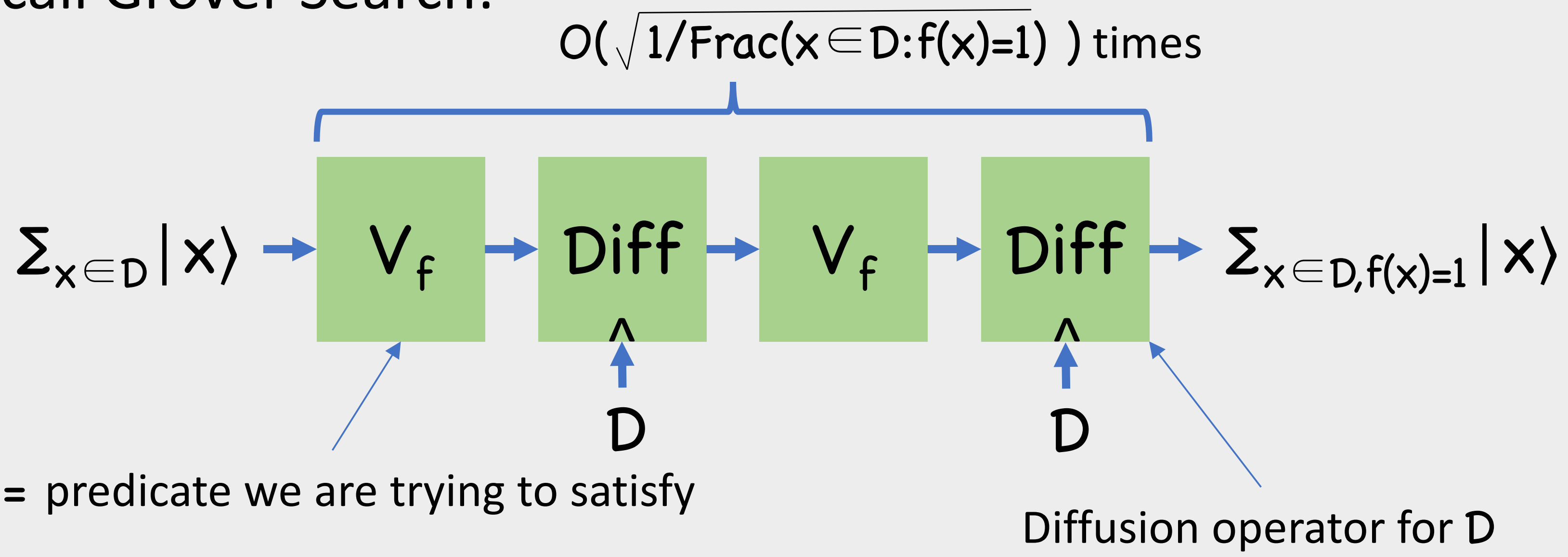
$\Sigma_{x':H(0||x')=y}|0||x'\rangle$

$\Sigma_{x':H(1||x')=y}|1||x'\rangle$

Impossibility of Quantum Rewinding

[Ambainis-Rosmanis-Unruh'14]

Recall Grover Search:



$O(\sqrt{1/\text{Frac}(x \in D : f(x)=1)})$ times

$\Sigma_{x \in D}|x\rangle$ → V_f → Diff → V_f → Diff → $\Sigma_{x \in D, f(x)=1}|x\rangle$

^ D

^ D

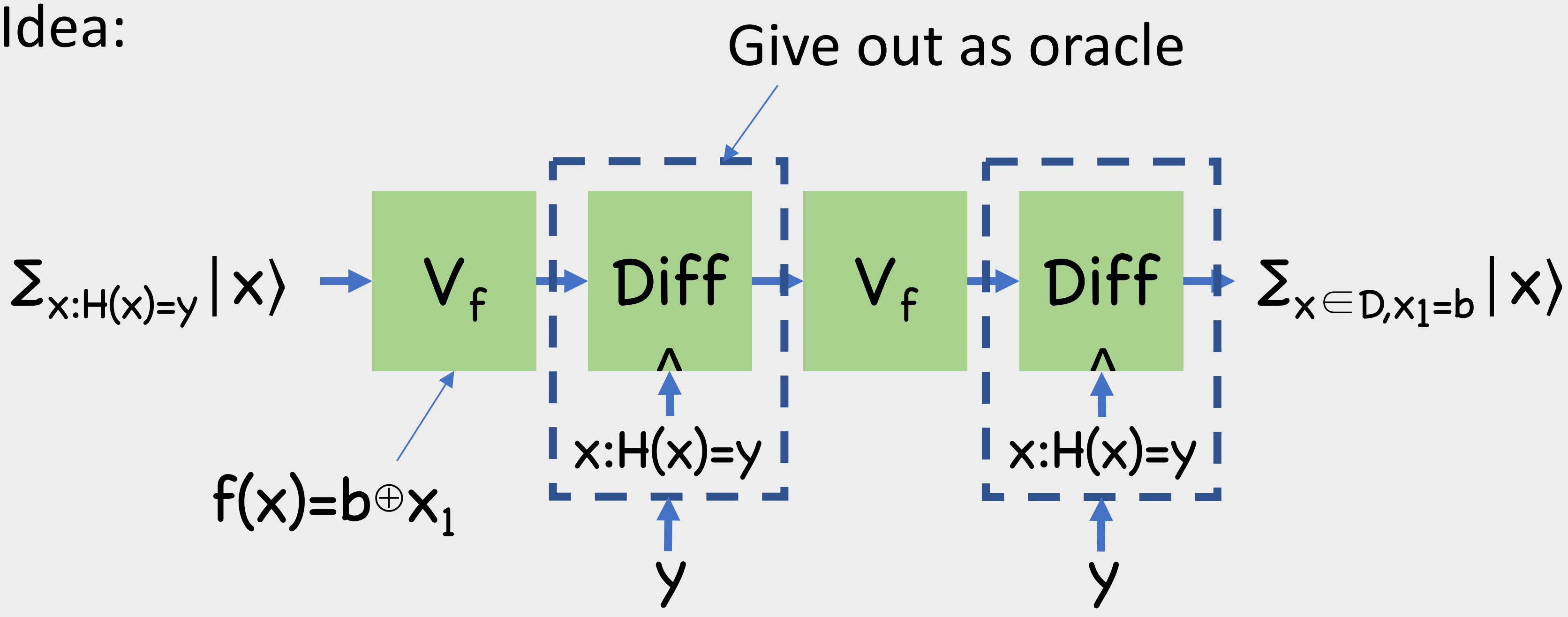
f = predicate we are trying to satisfy

Diffusion operator for D

Impossibility of Quantum Rewinding

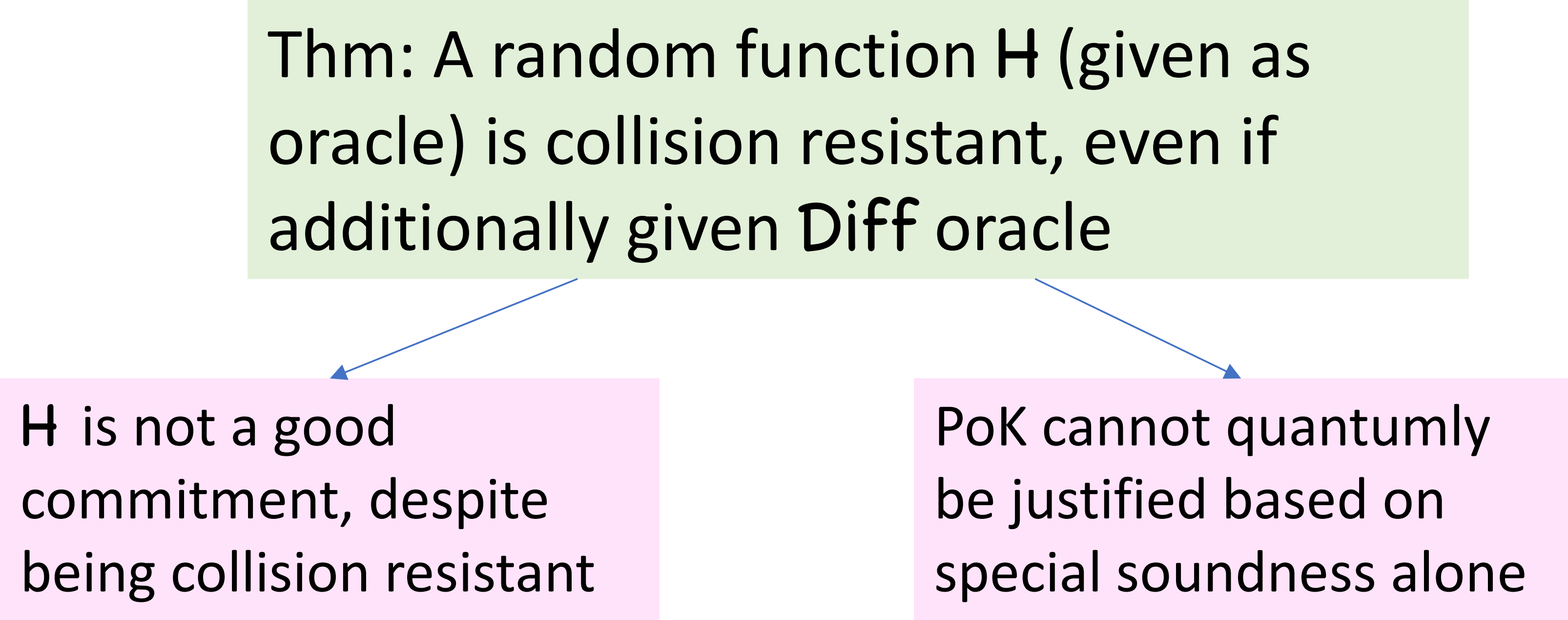
[Ambainis-Rosmanis-Unruh'14]

Idea:



Impossibility of Quantum Rewinding

[Ambainis-Rosmanis-Unruh'14]



Thm: A random function H (given as oracle) is collision resistant, even if additionally given Diff oracle

H is not a good commitment, despite being collision resistant

PoK cannot quantumly be justified based on special soundness alone

Ingredient 1: Rewinding Lemma

Lemma [Unruh'10]:

Suppose: (1) c is a single bit

(2) Defer all measurements except c

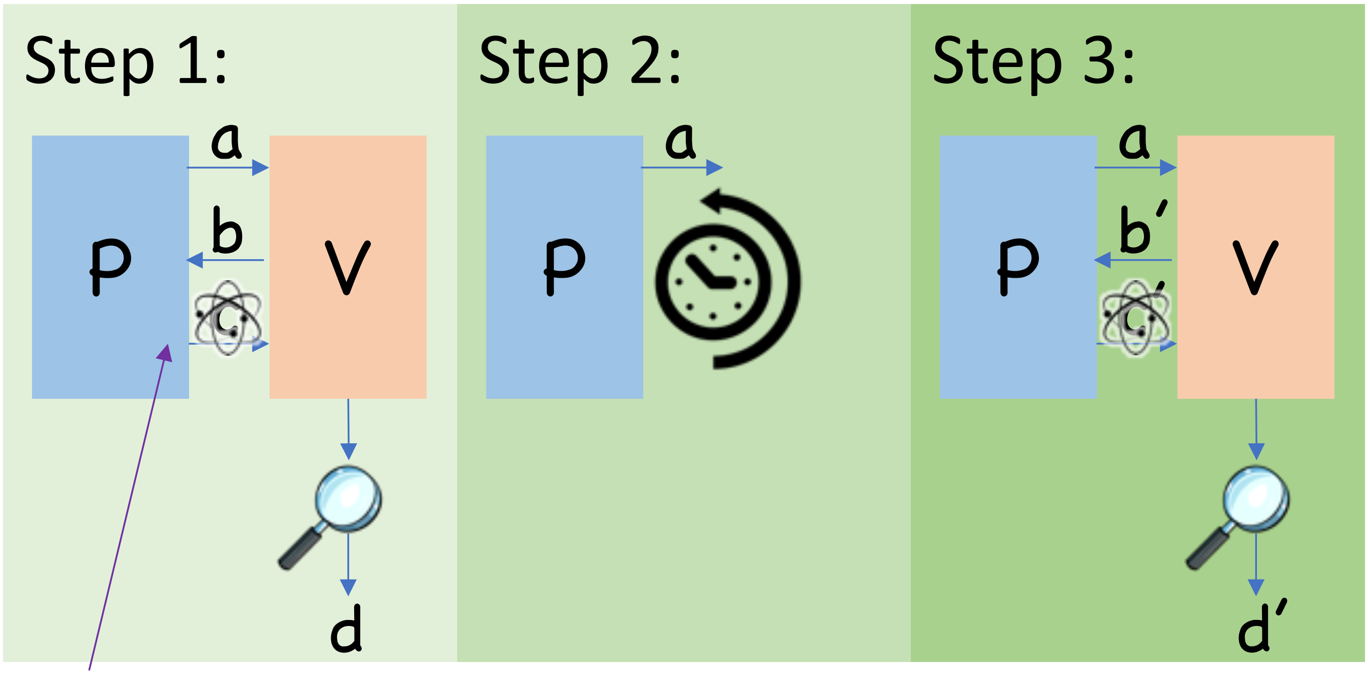
(3) $\Pr[c=1 \mid a]=\varepsilon$

Then: $\Pr[c=c'=1 \mid a]\geq\varepsilon^3$

Compare to ε^2 classically

Really need $\Pr[c=c'=1 \mid (b\neq b'),\ a]$, Unruh gives better bound

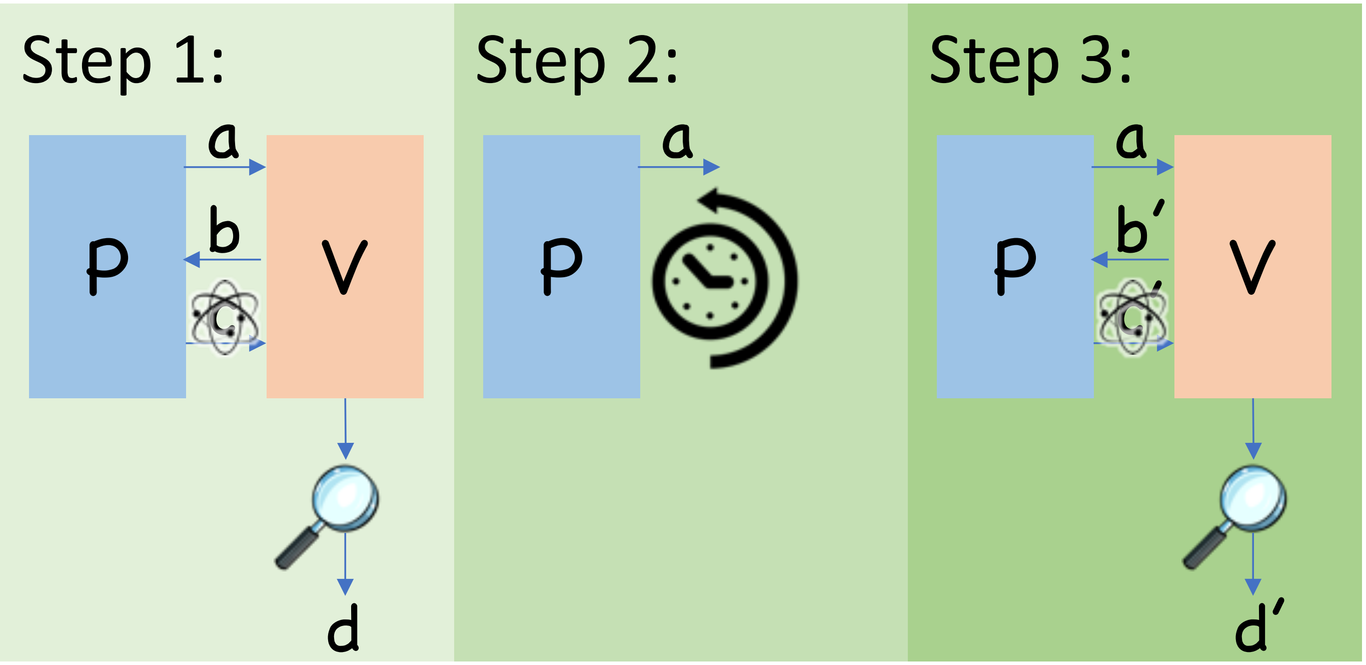
Applying Rewinding Lemma



No measurement after b!

Rewinding Lemma: Pr[d=d′=1]$\geq \varepsilon^3$

Applying Rewinding Lemma



Problem: Can’t extract c,c′ without changing d,d′

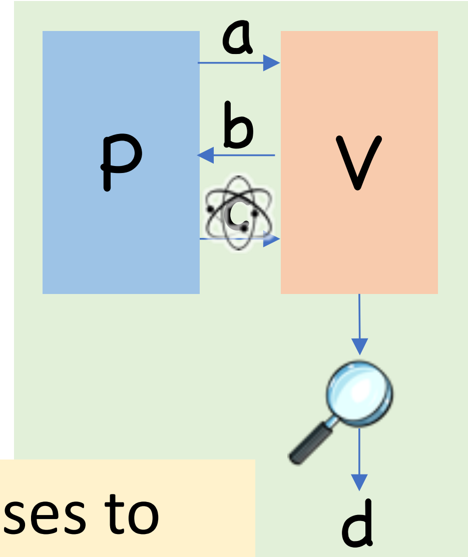
Ingredient 2: Additional Security Promises

Option 1: **Injective H** → Unique “opening” x, can measure without any collapse

Ingredient 2: Additional Security Promises

Option 1 [Unruh'10]: **Strict Soundness:**

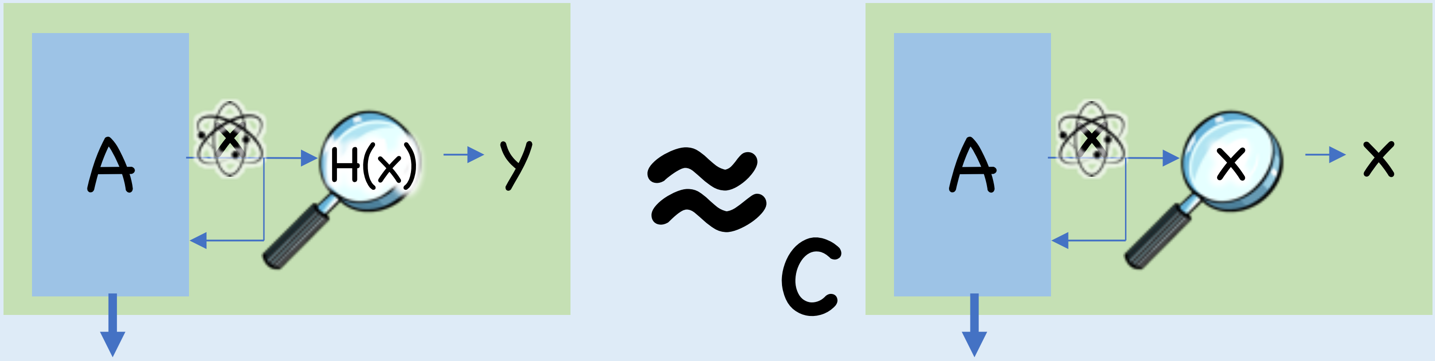
$\forall$ a,b, $\exists$ unique c s.t. V(a,b,c)=1



If d=1, c collapses to classical value anyway

Ingredient 2: Additional Security Promises

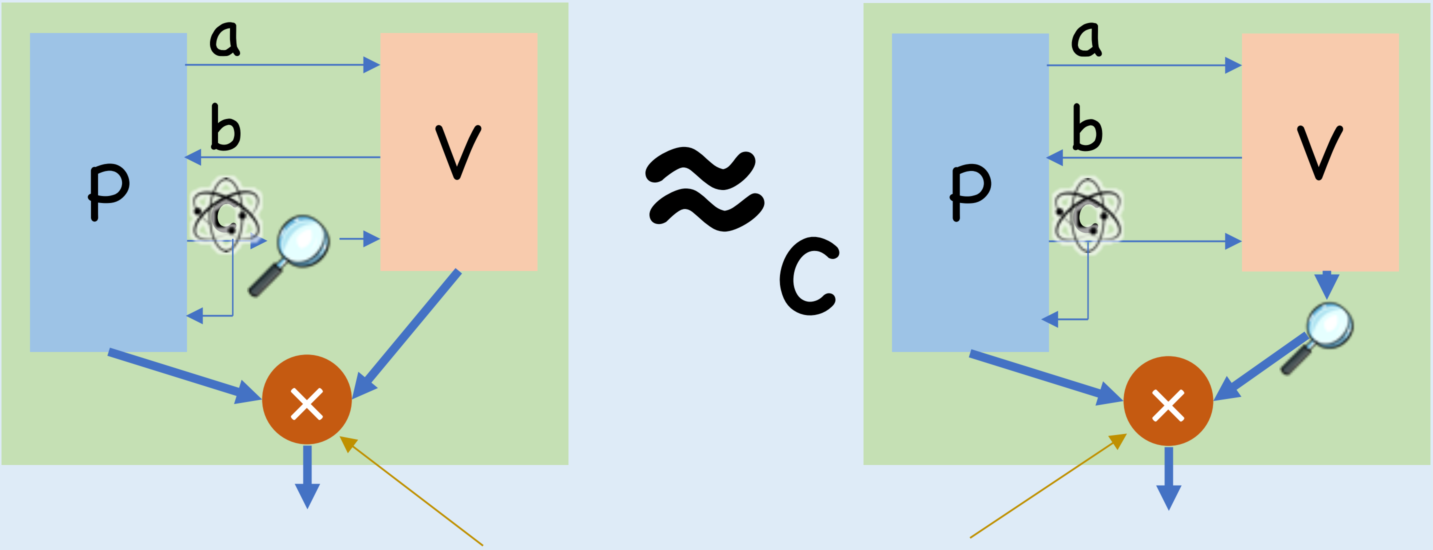
Option 2 [Unruh’16]: **Collapsing Hashes:**



Ingredient 2: Additional Security Promises

Option 2 [Liu-Z’19,Don-Fehr-Majenz-Schaffner’19]:

Collapsing:



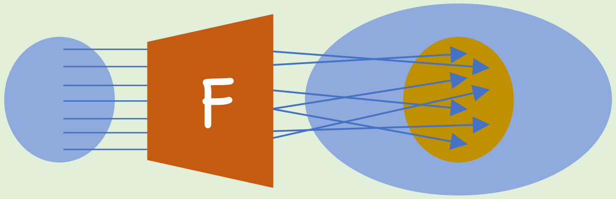
(Means condition on verifier accepting)

Justify Collapsing: Lossy Functions

[Unruh'16]

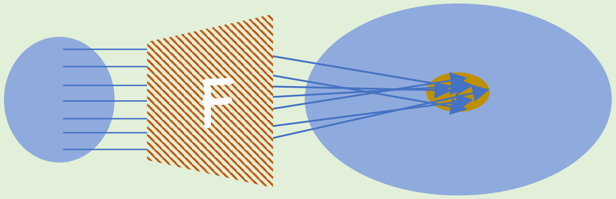
Lossy functions:

Injective Mode:



$\approx_c$

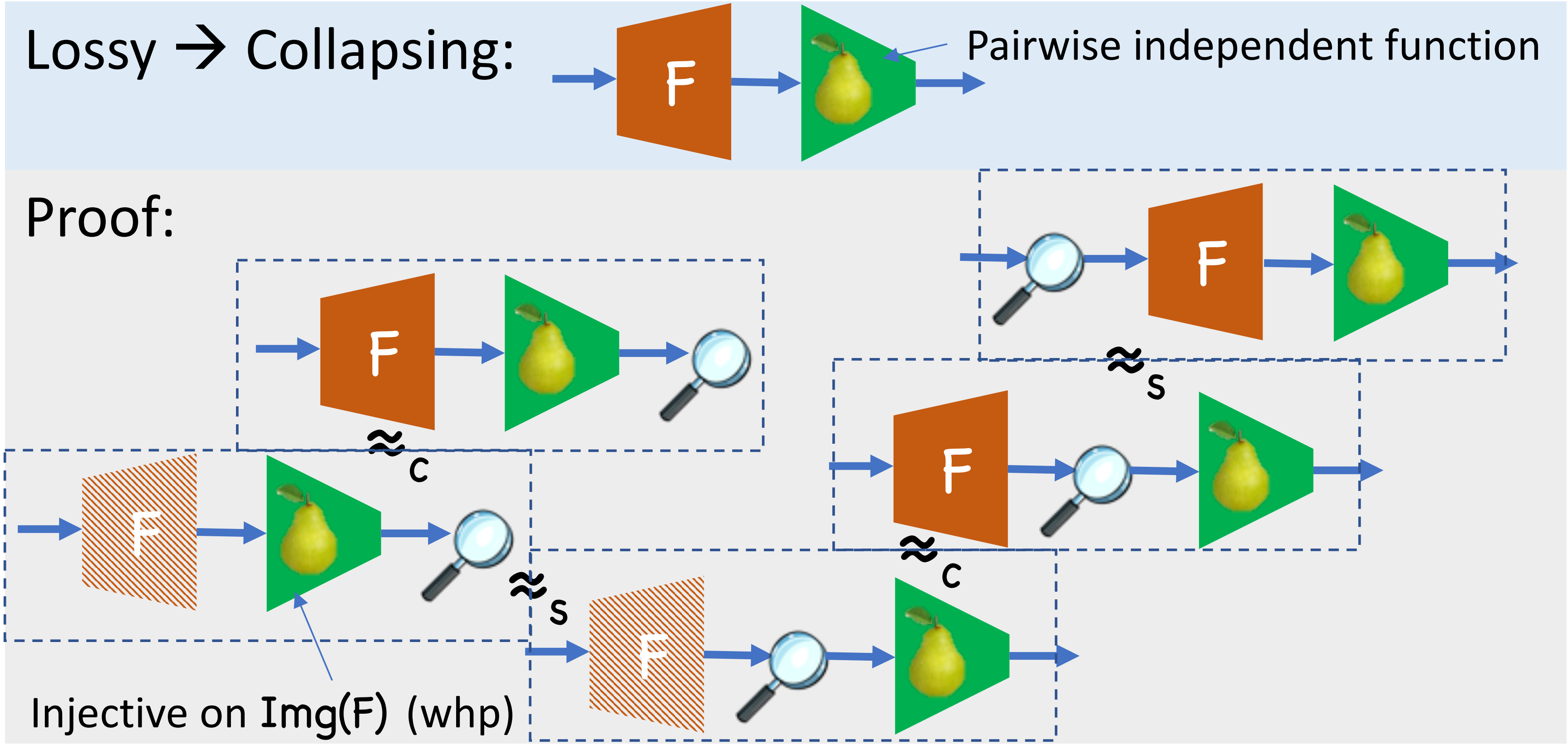
Lossy Mode:



Can construct from LWE

Justify Collapsing: Lossy Functions

[Unruh'16]



Lossy → Collapsing:

Pairwise independent function

Proof:

Injective on Img(F) (whp)

Limitations

For PoK’s, applying 🍐 destroys structure, makes verification impossible

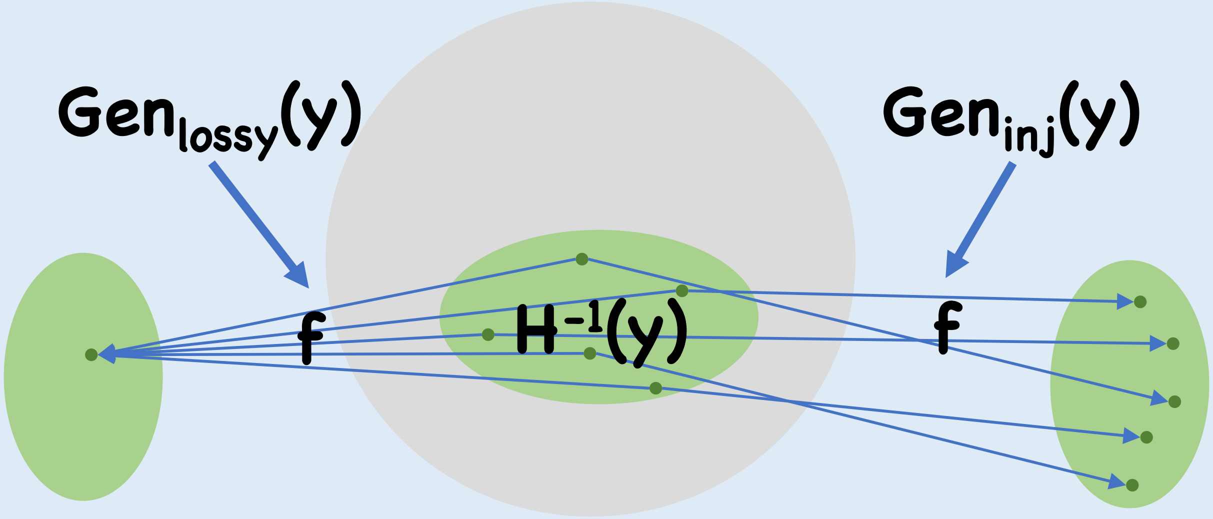
Can remove 🍐, but then **c** is large; bad for some application (e.g. signatures)

May be inefficient (large intermediate computation)

Improvement: Associated Lossy Funcs

[Liu-Z'19]

Def:



$$\text{Gen}_{\text{lossy}}(y) \approx_c \text{Gen}_{\text{inj}}(y)$$

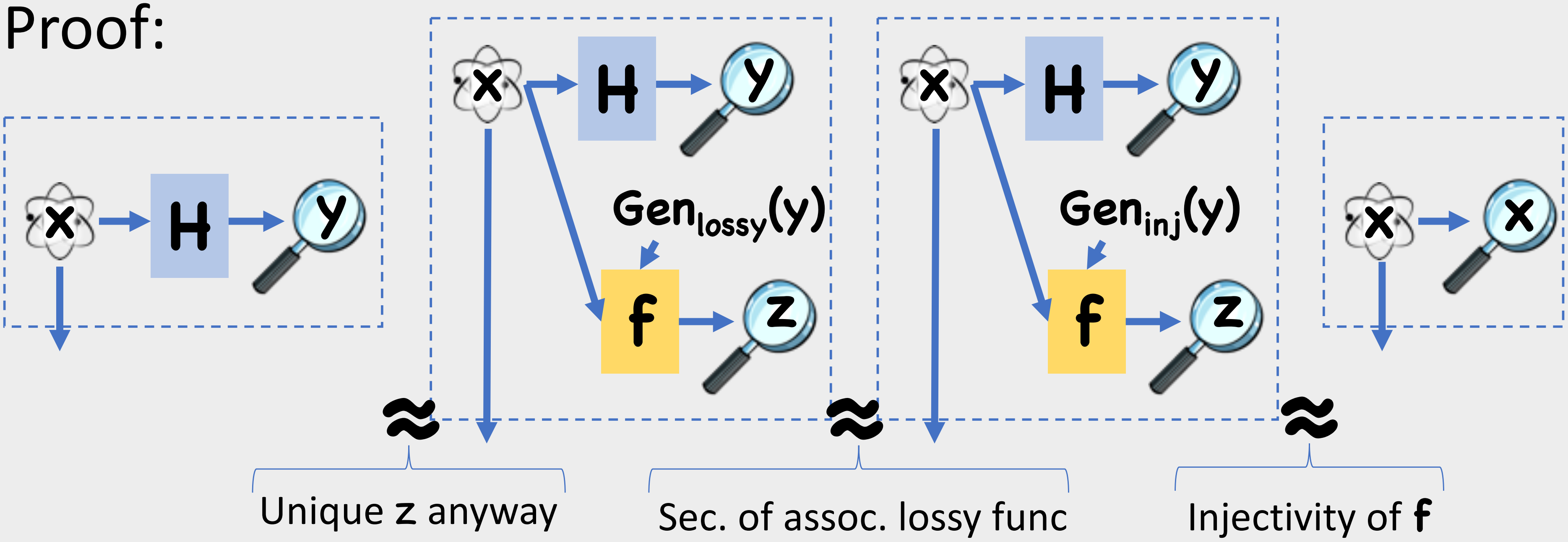
Improvement: Associated Lossy Funcs

[Liu-Z'19]

Thm:

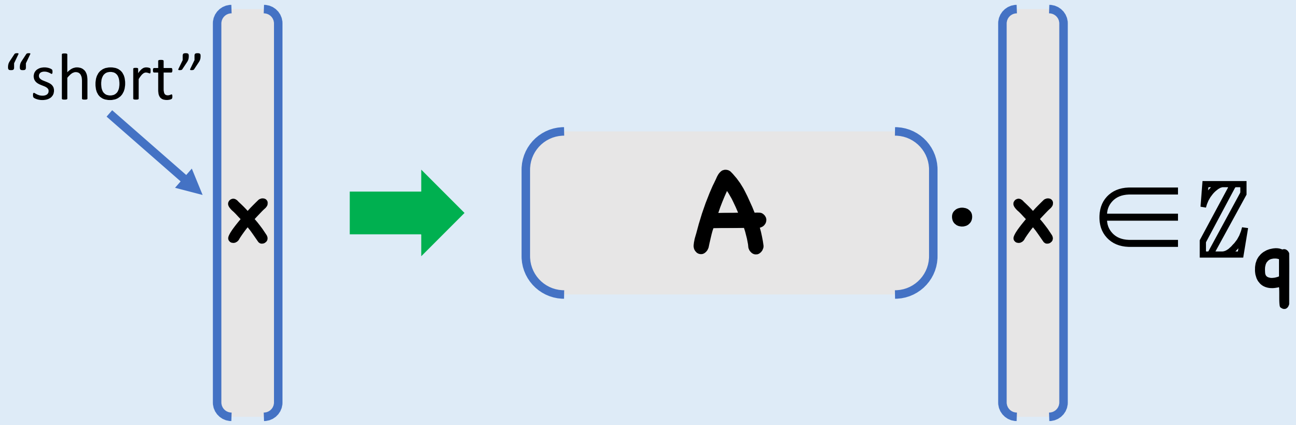
H has associated lossy func ➡ **H** is collapsing

Proof:


x
H
y
x
H
y
$\text{Gen}_{\text{lossy}}(y)$
f
z
≈
x
H
y
$\text{Gen}_{\text{inj}}(y)$
f
z
≈
x
x
≈
Unique z anyway
Sec. of assoc. lossy func
Injectivity of f

Consequences

SIS is Collapsing



[Lyubashevsky’11] Is a PoK for SIS

Associated Lossy Functions for SIS

$\mathrm{Gen}_{\mathrm{lossy}}(y)$:

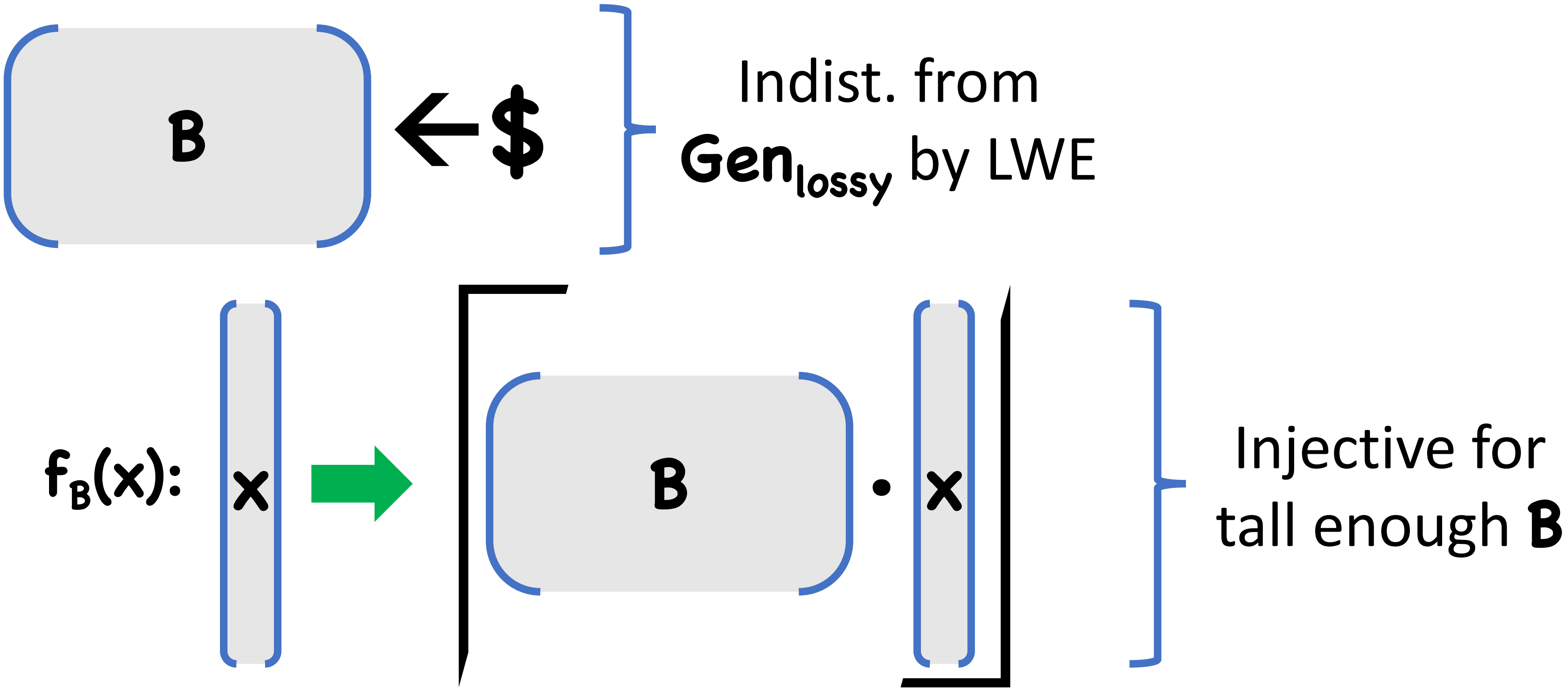
$$B = u \cdot A + \underset{\text{“short”}}{e}$$

$f_B(x)$:

$$x \rightarrow \lceil B \cdot x \rfloor = \lceil u \cdot y \rfloor$$

Associated Lossy Functions for SIS

Gen$_{inj}$(y):



$\mathbf{B} \leftarrow \$$

Indist. from **Gen$_{lossy}$** by LWE

$f_{\mathbf{B}}(\mathbf{x})$: $\mathbf{x} \rightarrow \lceil \mathbf{B} \cdot \mathbf{x} \rfloor$

Injective for tall enough **B**

The Silver Lining…

Proofs of Quantumness

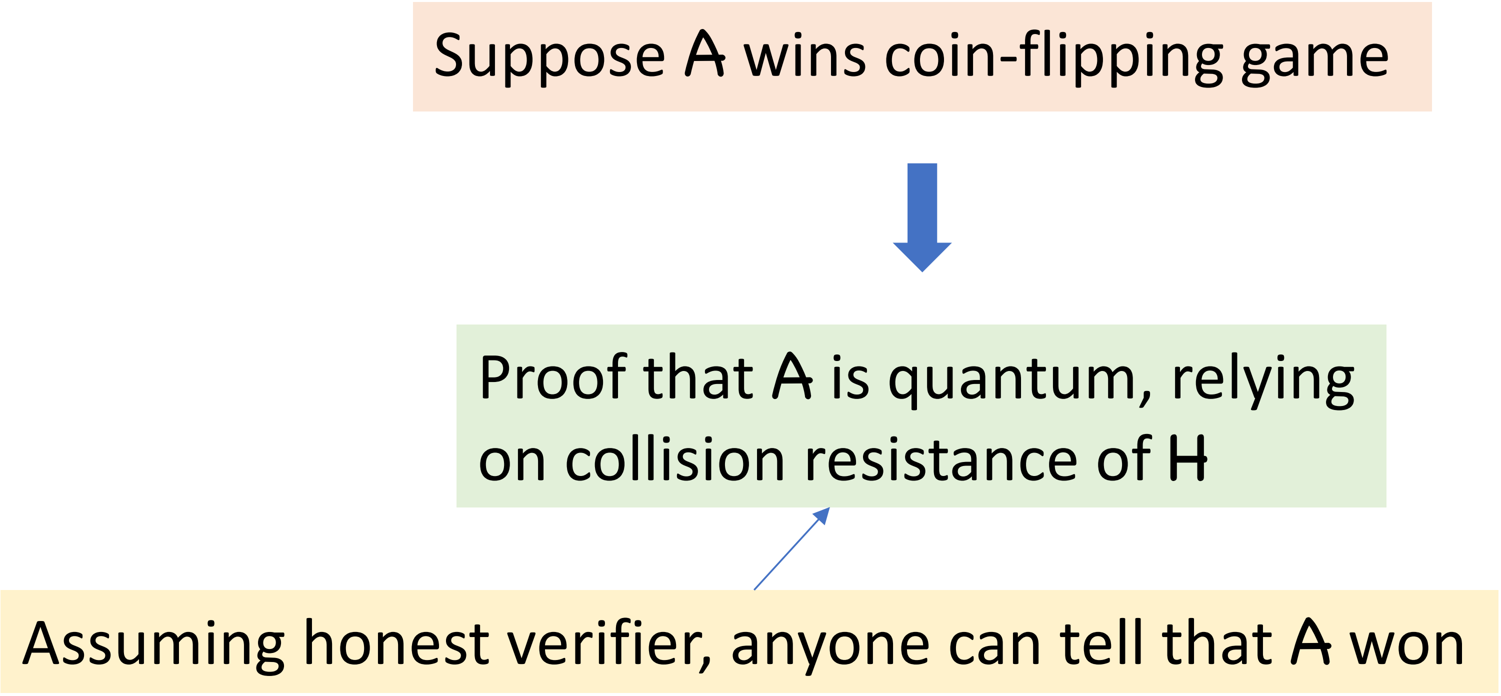
But, can’t be verified by others

Thm [Brakerski-Christiano-Mahadev-Vazirani-Vidick’18]:

LWE → Designated verifier (privately verifiable) proof of quantumness

Doesn’t require quantum-easy assumptions

Proofs of Quantumness

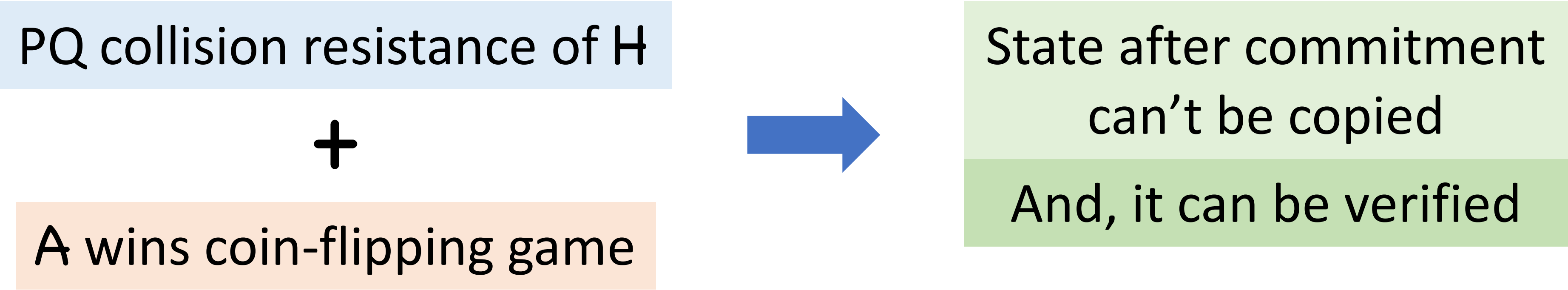


Suppose A wins coin-flipping game

Proof that A is quantum, relying on collision resistance of H

Assuming honest verifier, anyone can tell that A won

Proofs of Unclonable State



PQ collision resistance of H

+

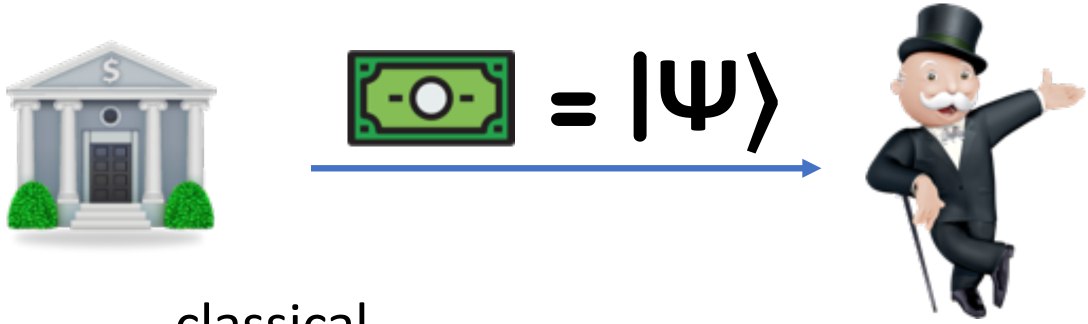
A wins coin-flipping game

State after commitment can't be copied

And, it can be verified

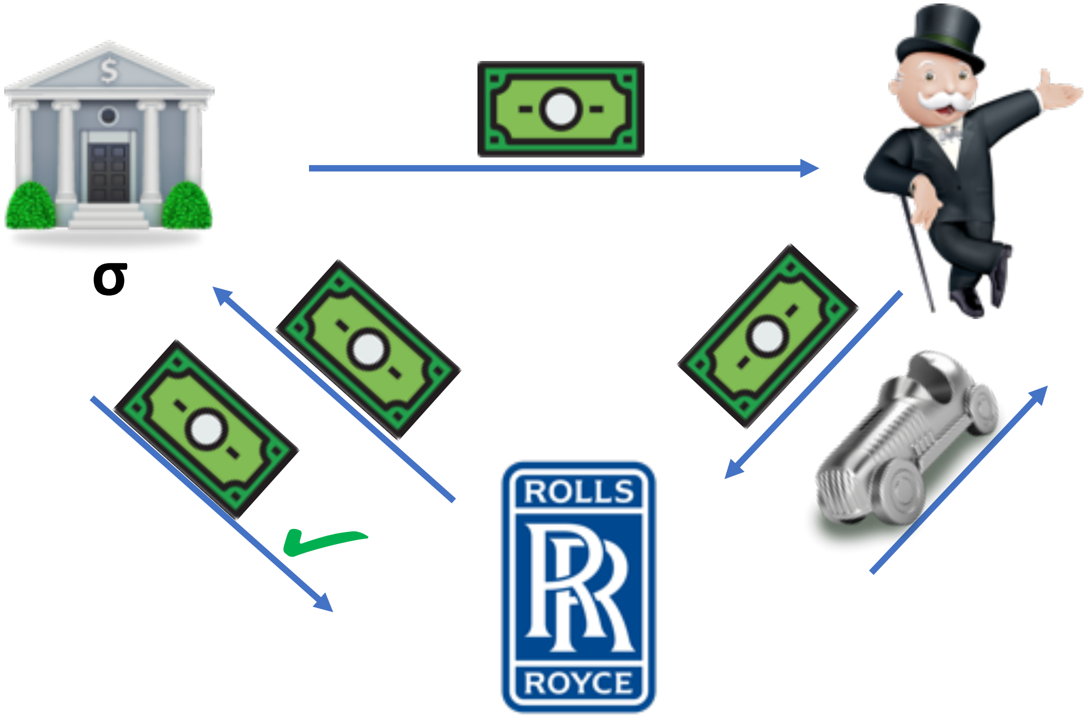
No-Cloning = Quantum Money

[Wiesner’70]



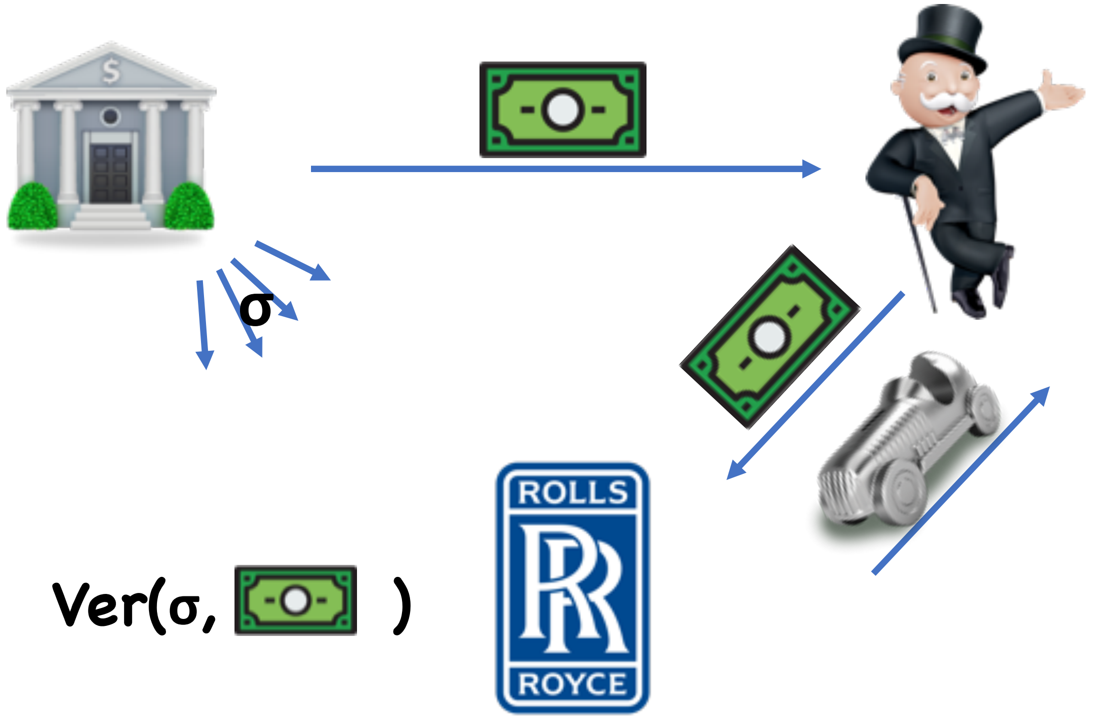
$$\underbrace{\text{Serial \# = classical description}}_{\text{Kept secret}}$$

Limits of (Plain) Quantum Money



Public Key Quantum Money

[Aaronson'09]

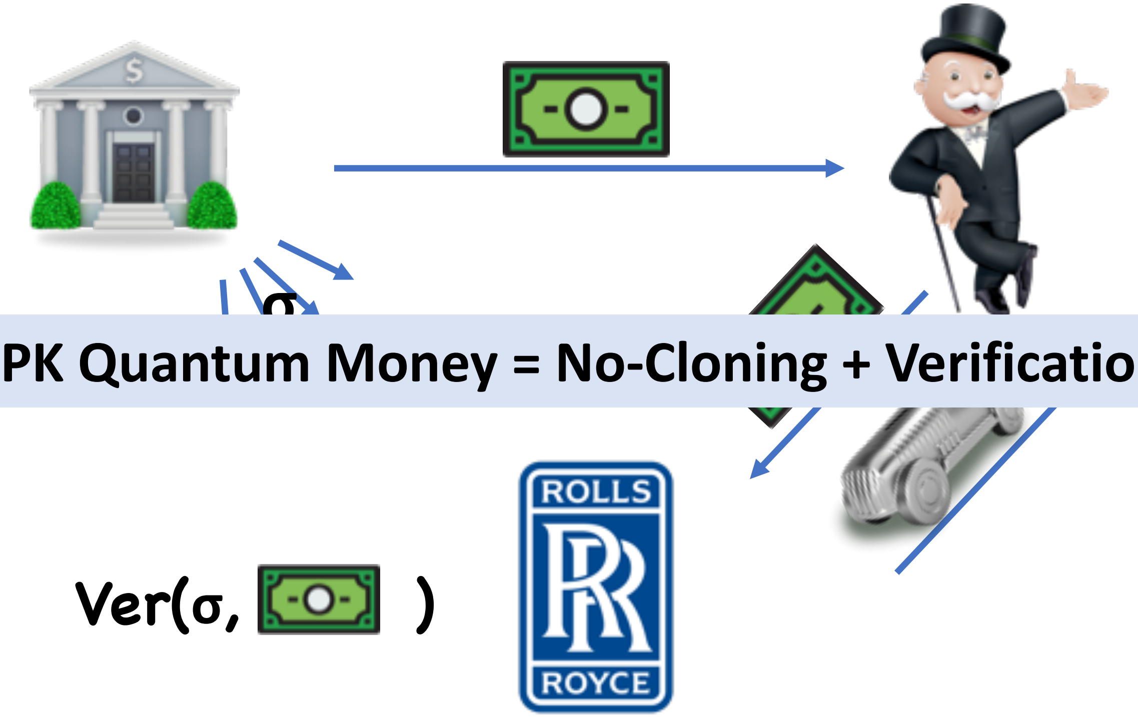


σ

Ver(σ, 💵)

Public Key Quantum Money

[Aaronson'09]

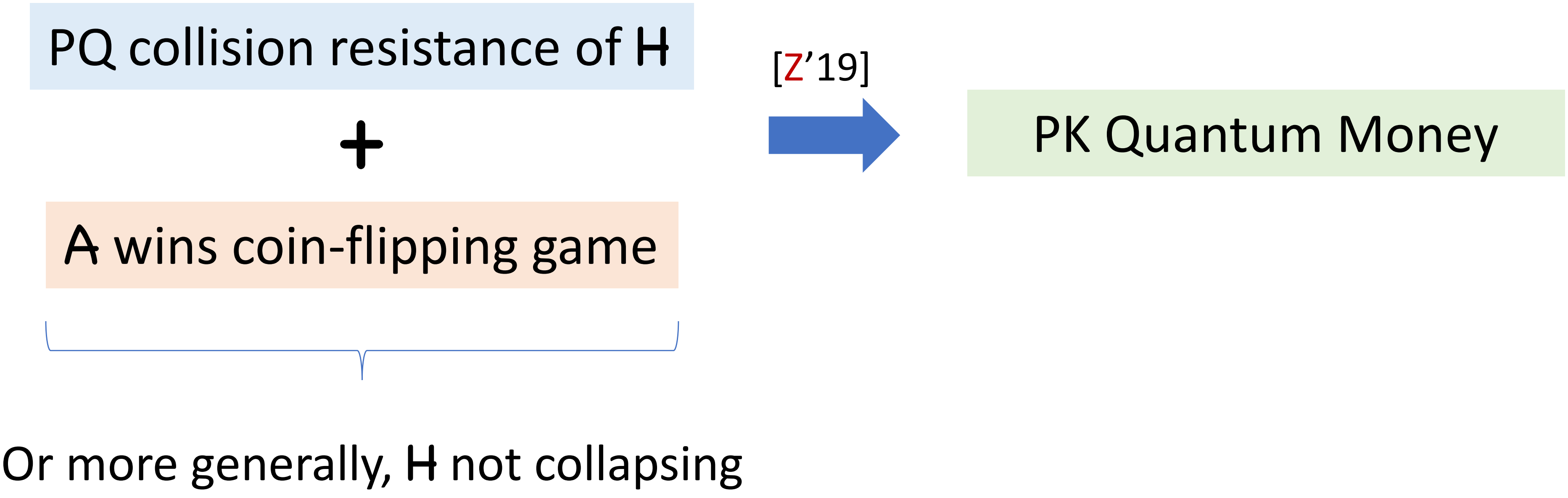


PK Quantum Money = No-Cloning + Verification

Ver(σ, 💵)

Constructing PK quantum money is a major goal in quantum cryptography

Public Key Quantum Money



PQ collision resistance of H

+

A wins coin-flipping game

[Z'19]

PK Quantum Money

Or more generally, H not collapsing

Takeaway: whenever post-quantum proofs fail, look for interesting quantum crypto applications