Quantum Random Oracle Model, Part 3

Mark Zhandry (Princeton & NTT Research)

Recall: Typical Classical ROM Proof: On-the-fly Simulation

Input	Output
x_1	y_1
x_2	y_2
x_3	y_3
x_4	y_4

Query(x, D):

If **(x,y)$\in$D**:

Return(y,D)

Else:

y ←$ Y

D' = D+(x,y)

Return(y,D')

Recall: Typical Classical ROM Proof: On-the-fly Simulation

Allows us to:

- Know the inputs adversary cares about ✓
- Know the corresponding outputs ✓
- (Adaptively) program the outputs ✓

CPReds?

Allows us to:

- Know the inputs adversary cares about ✘
- Know the corresponding outputs ✘
- (Adaptively) program the outputs ✓ / ✘

Beyond Committed Programming

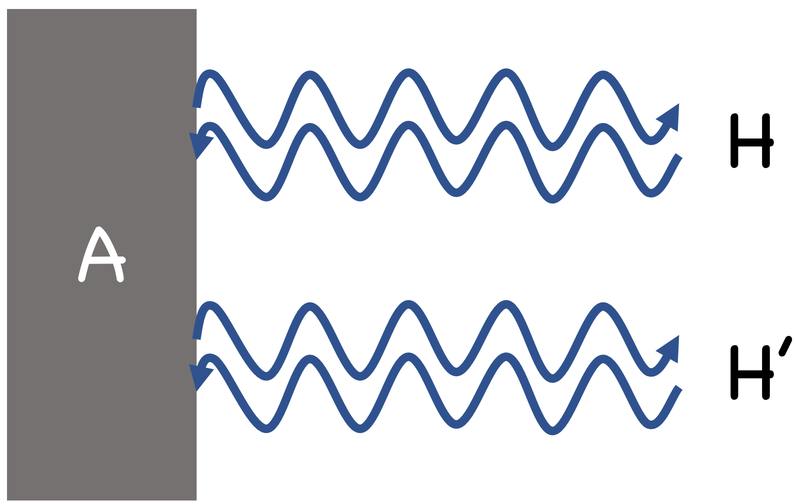
How do we change oracle without detection?

Problem: repeated queries?

Problem: distinguishing attack

$\sum|x,0\rangle \rightarrow$ / $\leftarrow \sum|x,V_1\rangle$ VS $\sum|x,0\rangle \rightarrow$ / $\leftarrow \sum|x,O(x)\rangle$

Random points



$a \leftarrow \$$

$H'(x)=H(x)\ \forall\ x \neq a$

Negligible query mass on a, so change undetectable

Used, e.g. for NIZKs [Unruh'16]

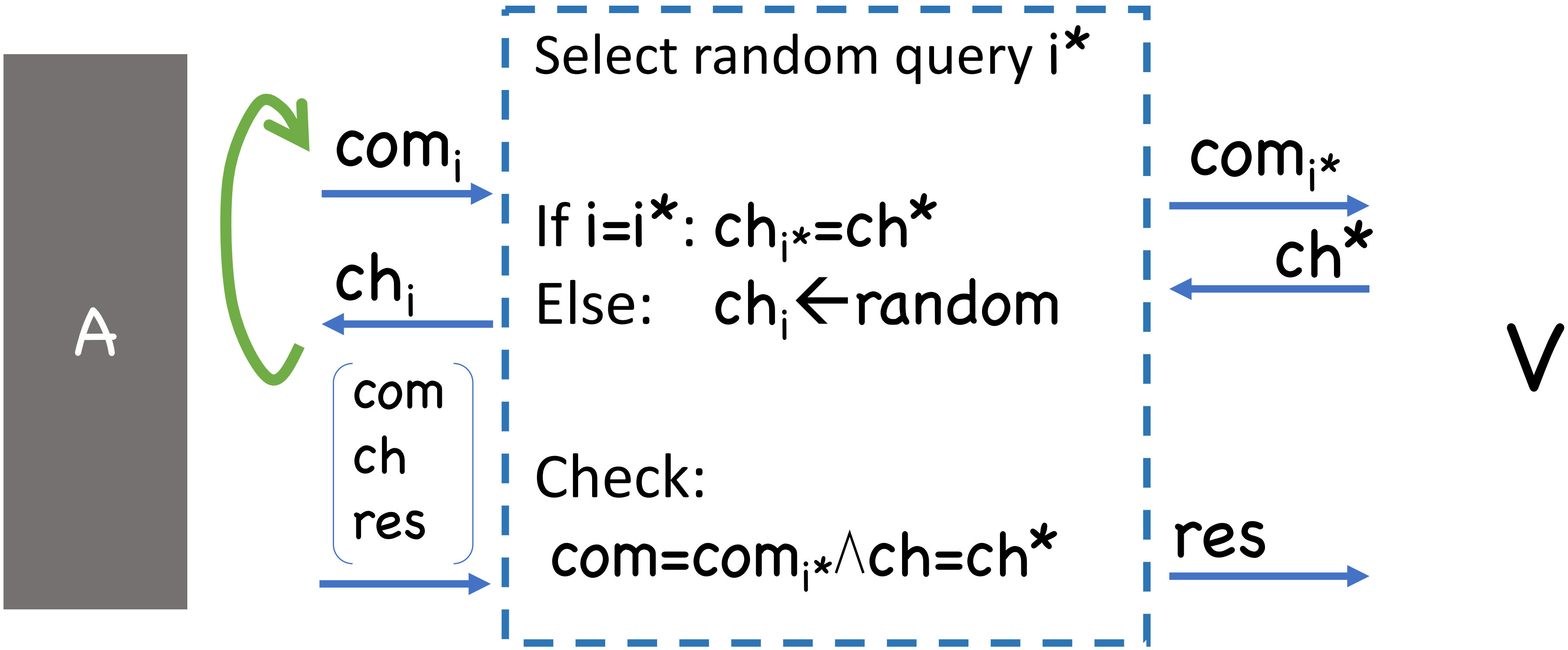
Newer Techniques

Very recently (last 2 years), new techniques have emerged that allow for better programming

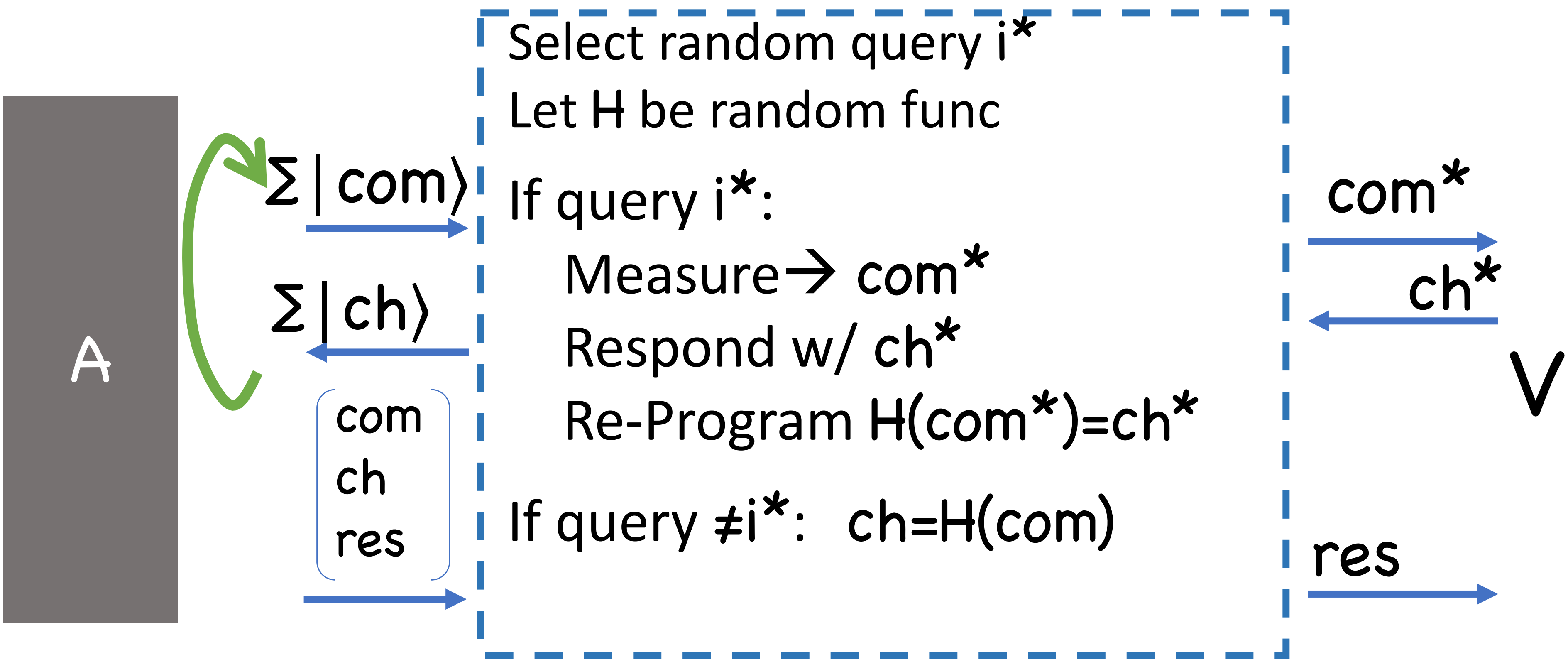
Will highlight some techniques

Fiat Shamir

Recall: Classical Fiat-Shamir Proof

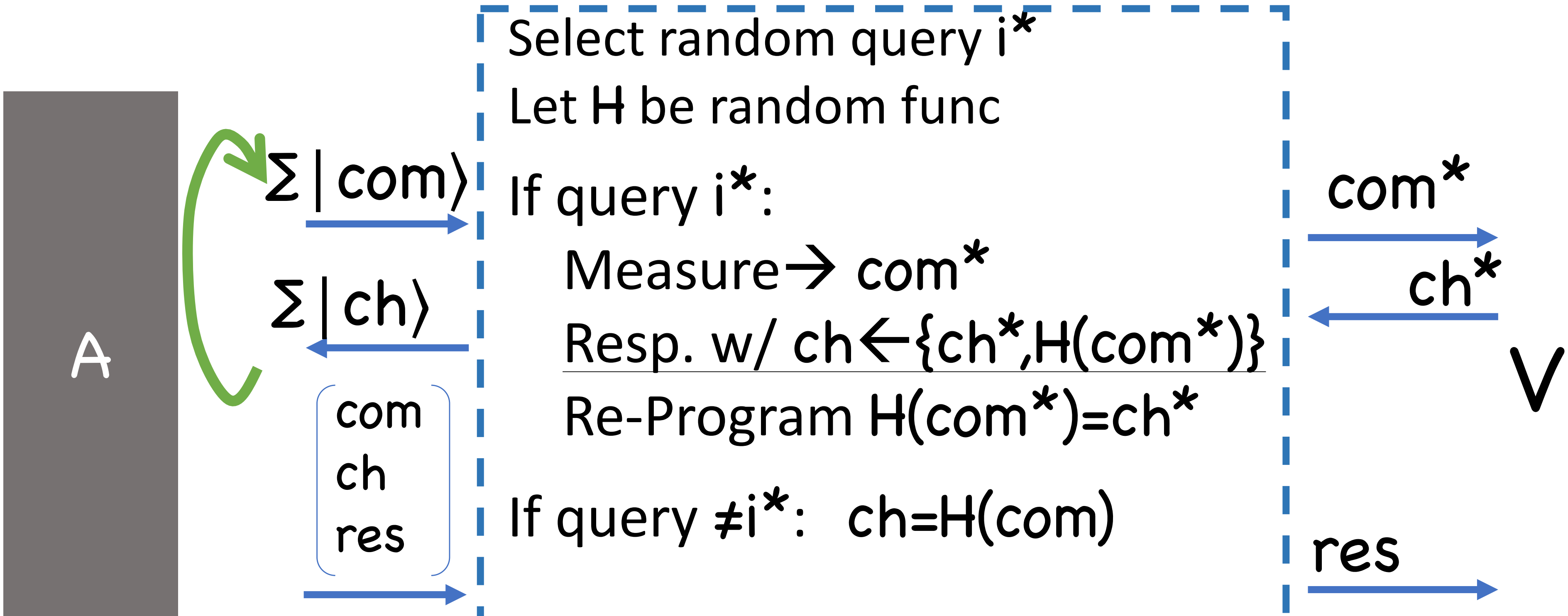


Failed Quantum Fiat-Shamir Proof



Unfortunately, doesn’t work

Fixed Quantum Fiat-Shamir Proof



[Don-Fehr-Majenz-Schaffner’19]: Amazingly works

Other Applications

[Don-Fehr-Majenz'20]: Multi-round Fiat-Shamir

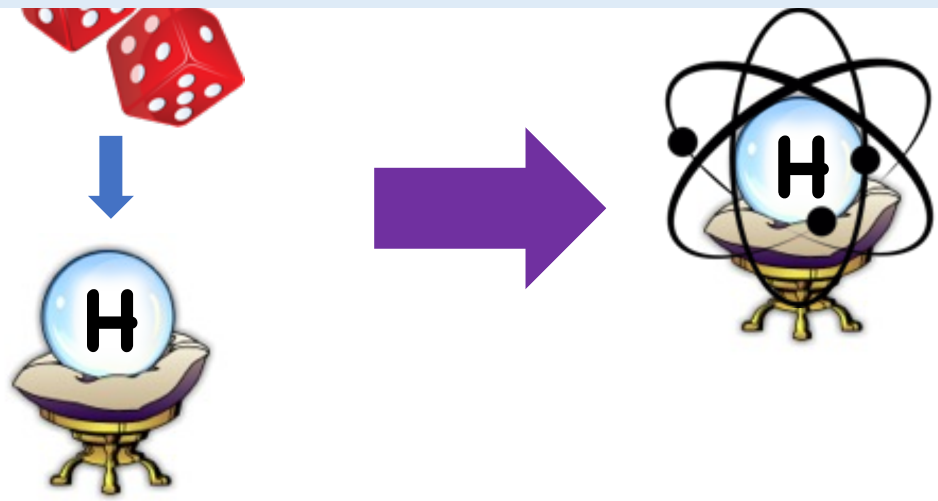
"Lifting Theorem" [Yamakawa-Z'20]:
If *search-type* game, and challenger makes *constant* number of queries to RO, classical ROM proof → QROM proof (w/ polynomial security loss)

Compressed Oracles

Step 1: Quantum-ify (aka Purify)

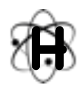
Quantum-ifying (aka purifying) random oracle:

→ A +  now single quantum system

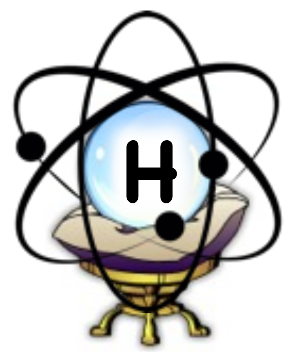


Reminiscent of old impossibilities for unconditional quantum protocols [Lo'97,Lo-Chau'97,Mayers'97,Nayak'99]

Step 1: Superposition of Oracles

Initial oracle state: 

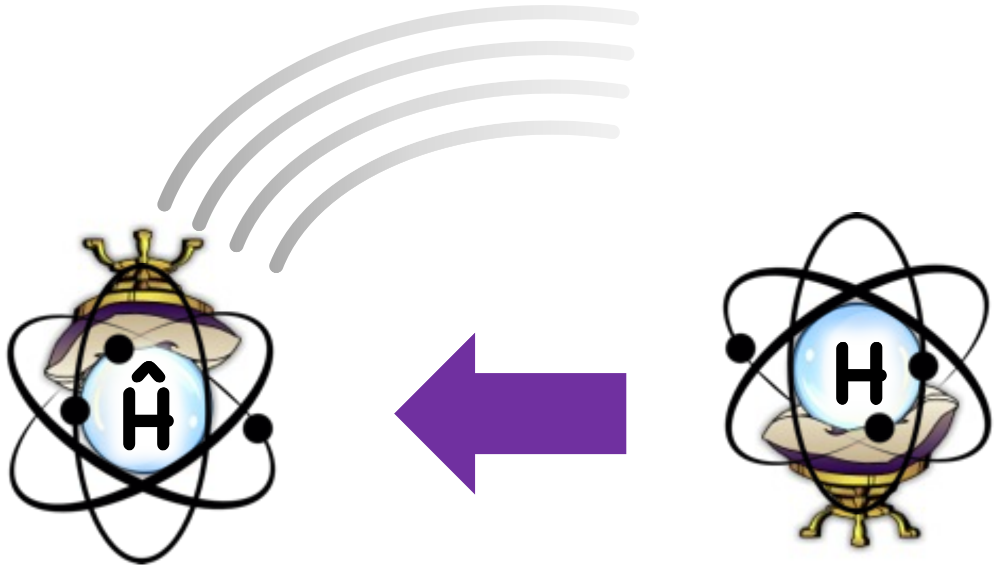
Query(x, y, H): y = y⊕H(x)



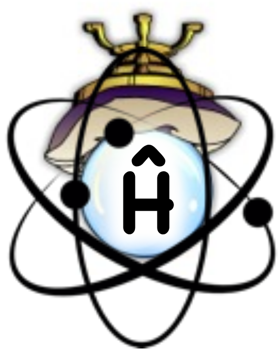
Adversary's query

Oracle's state

Step 2: Look at Fourier Domain



Step 2: Look at Fourier Domain

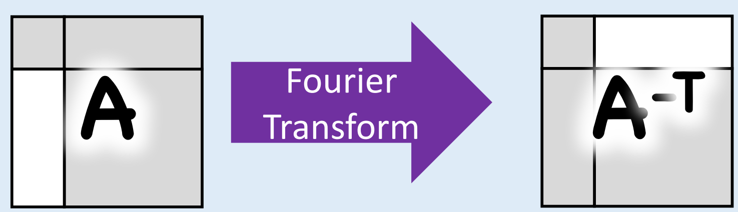


Initial oracle state: $Z(x) = 0$

Query$(x, y, \hat{H})$: $\hat{H} = \hat{H} \oplus P_{x,y}$

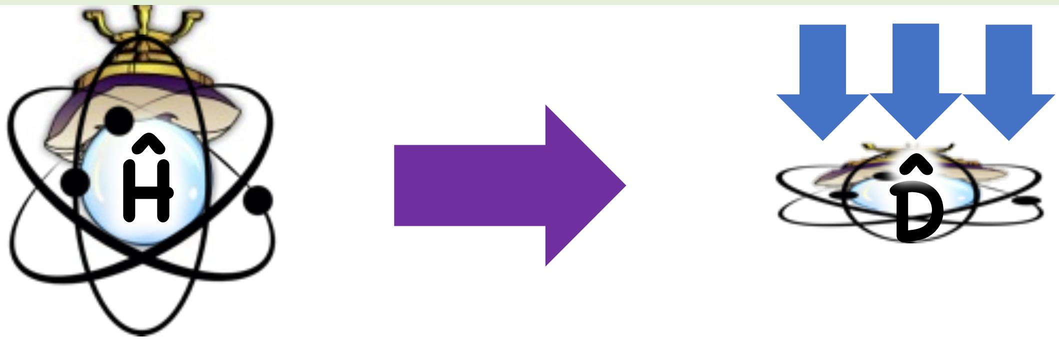
$$P_{x,y}(x') = \begin{cases} y \text{ if } x=x' \\ 0 \text{ else} \end{cases}$$

Proof:



Step 3: Compress

Observation:
After **q** queries, **Ĥ** is non-zero on at most **q** points



Step 3: Compress

Initial oracle state: **{}**

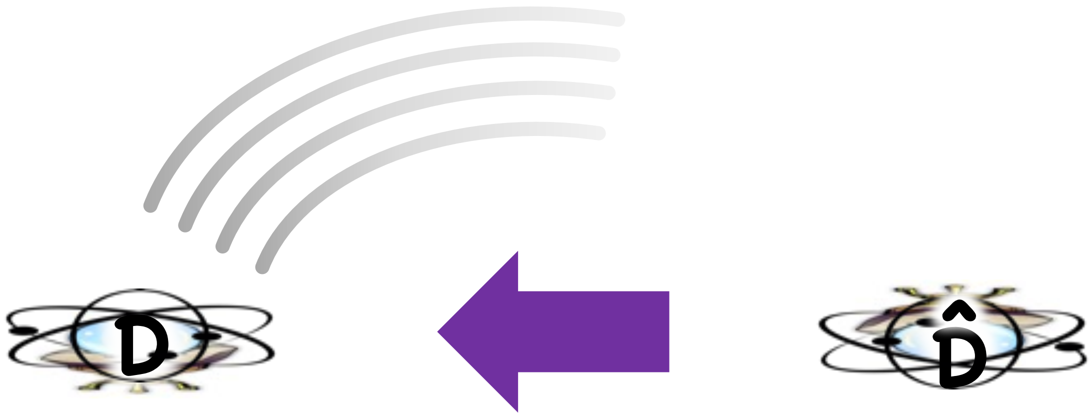
Query(x, y, $\hat{D}$):

(1) If $\nexists$**(x,y')**$\in$**$\hat{D}$: $\hat{D}$ = $\hat{D}$+(x,0)**

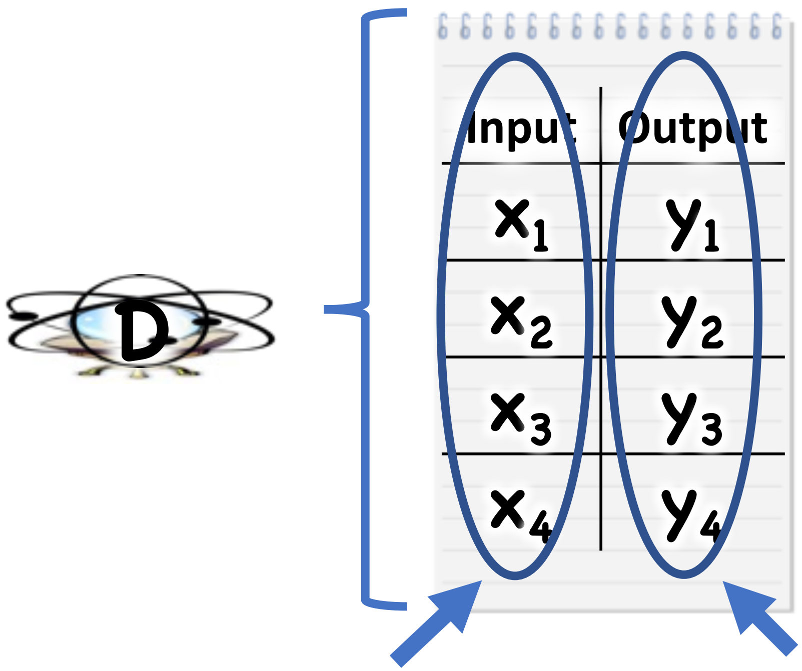
(2) Replace **(x,y')**$\in$**$\hat{D}$**
with **(x,y'$\oplus$y)**

(3) If **(x,0)**$\in$**$\hat{D}$:** remove it

Step 4: Revert back to Primal Domain



Step 4: Revert back to Primal Domain



Roughly analogous to classical on-the-fly simulation

Points adversary cares about

≈Corresponding outputs

Compressed Oracles

Allows us to:

- Know the inputs adversary cares about? ✓
- Know the corresponding outputs? ✓
- (Adaptively) program the outputs? ✓ (with some work)

So, what happened?

Observer Effect:
Learning anything about quantum system disturbs it

<u>Motivation for CPReds:</u>

answers obliviously,
so no disturbance

Reduction must answer obliviously, too?

<u>Beyond CPReds:</u>

A learns about 

through queries

gets disturbed

Compressed oracles decode such disturbance

Caveats

Outputs in database **≠0** in Fourier domain
➡ **y** values aren't exactly query outputs

Examining **x,y** values perturbs state
➡ Still must be careful about how we use them

But, still good enough for many applications…

Some Applications

[Z'19]: Indifferentiability of MD

[Alagic-Majenz-Russell-Song'18]: Quantum-secure signature separation

[Liu-Z'19a]: Tight bounds for multi-collision problem

[Liu-Z'19b]: Fiat-Shamir

([Don-Fehr-Majenz-Schaffner'19]: direct proof)

[Hosoyamada-Iwata'19]: 4-round Luby-Rackoff

[Unruh'21]: Collision resistance of Sponge

[Chiesa-Manohar-Spooner'19]: zk-SNARKs

[Bindel-Hamburg-Hülsing-Persichetti'19]: Tighter CCA security proofs

Summary

- Now have numerous techniques for proving QROM security
- Many schemes of interest now have QROM proof
- Major lingering issues:
  - Tightness of reductions
  - Indifferentiability (Sponge, ideal ciphers from RO)
  - Constant-query lifting theorem for indistinguishability?
  - Still various missing pieces