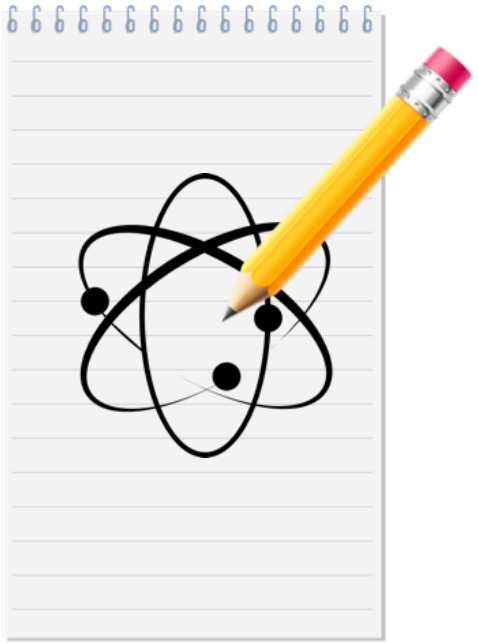
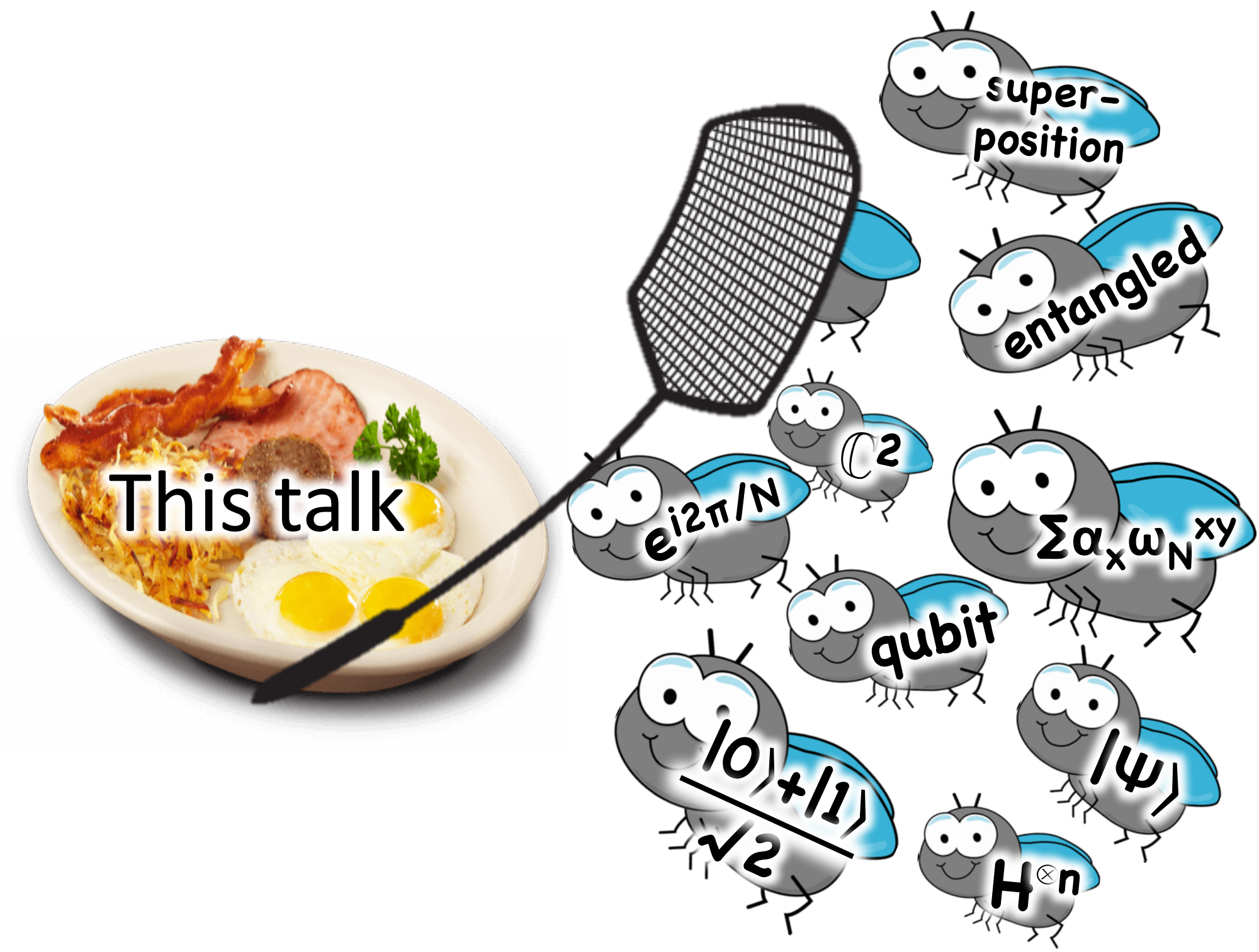
How to Record Quantum Queries

and Applications to Quantum Indifferentiability

Mark Zhandry

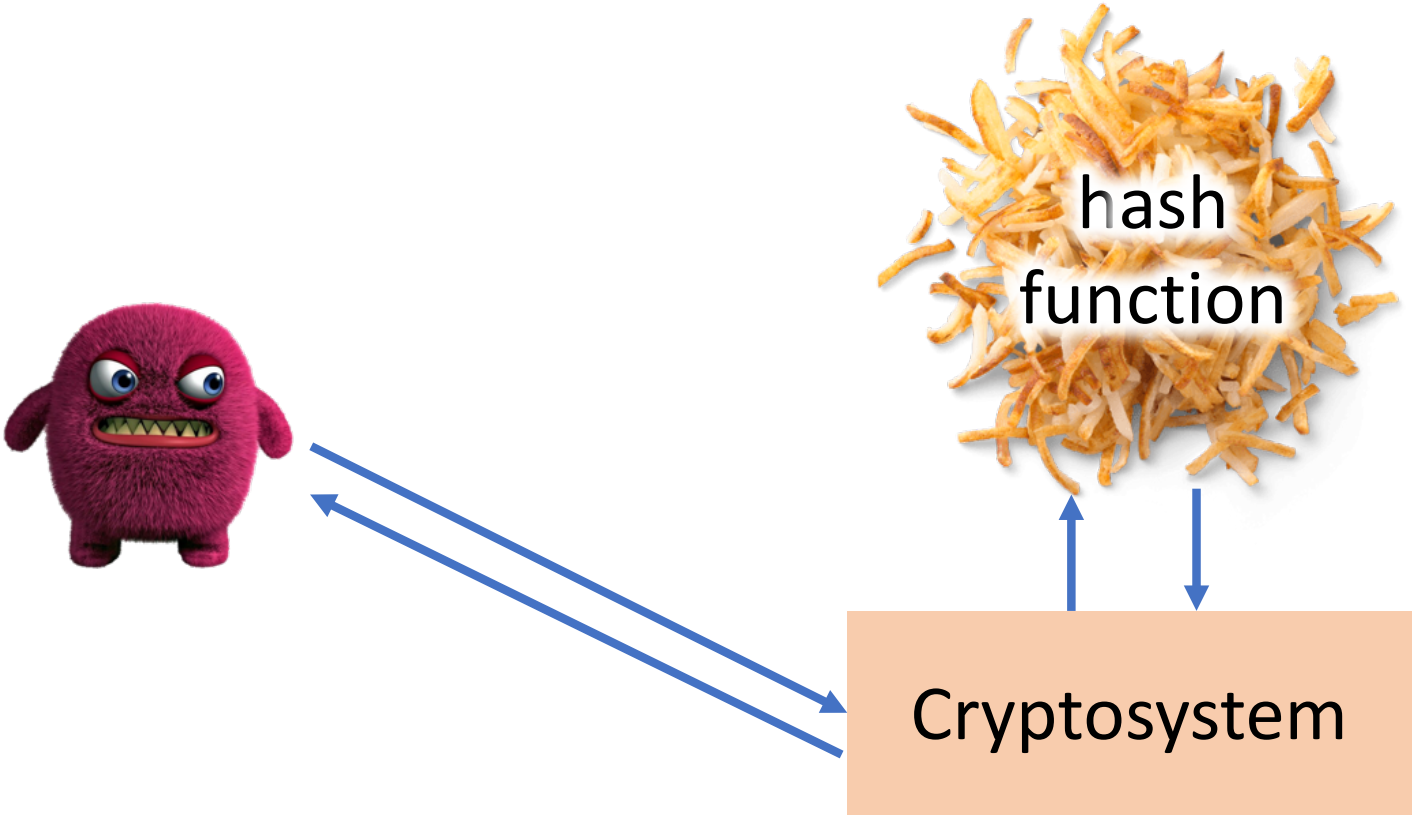
Princeton University & NTT Research




This talk
super-
position
entangled
$\mathbb{C}^2$
$e^{i2\pi/N}$
$\Sigma\alpha_x\omega_N{}^{xy}$
qubit
$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
$|\psi\rangle$
$H^{\otimes n}$

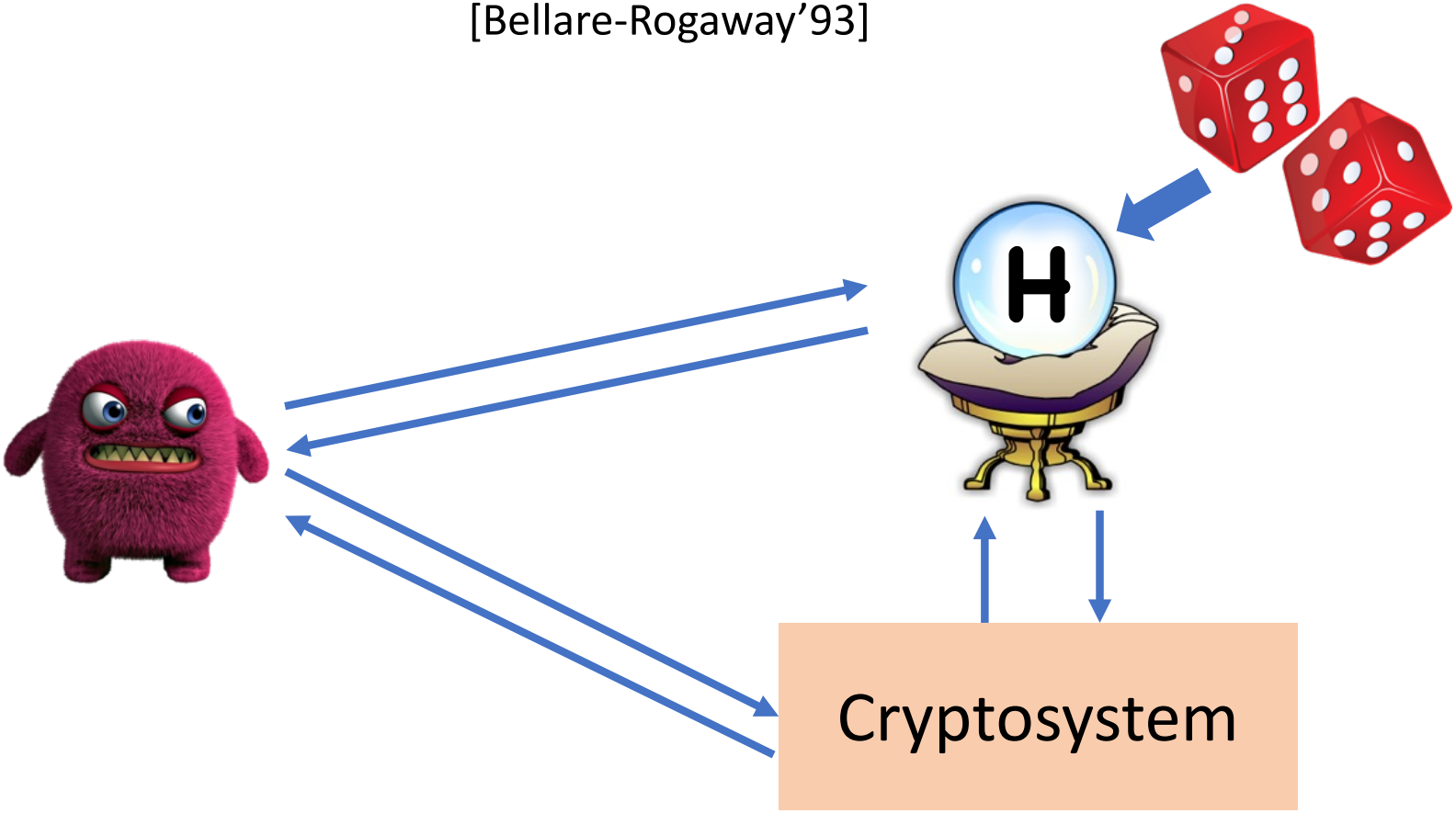
The (Classical) Random Oracle Model (ROM)

[Bellare-Rogaway'93]

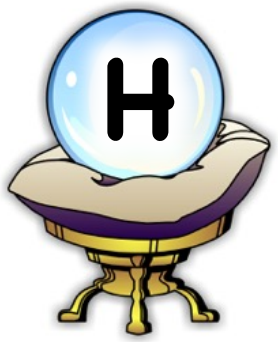


The (Classical) Random Oracle Model (ROM)

[Bellare-Rogaway'93]



Typical 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:

$y \leftarrow\$ Y$

$D' = D+(x,y)$

Return(y,D')

Typical ROM Proof: On-the-fly Simulation

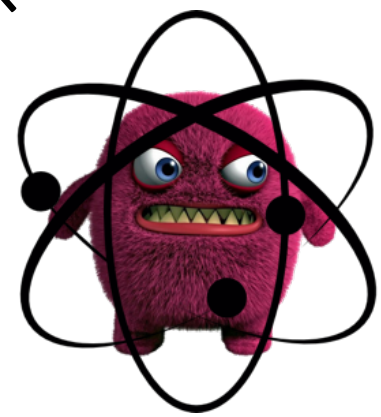
Allows us to:

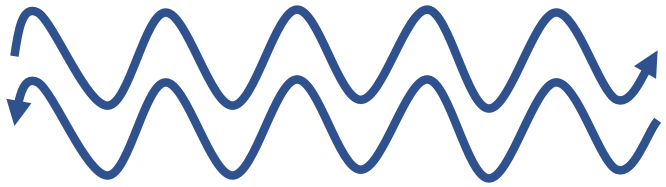
- Know the inputs adversary cares about ✓
- Know the corresponding outputs ✓
- (Adaptively) program the outputs ✓
- Easy analysis of bad events (e.g. collisions) ✓

The Quantum Random Oracle Model (QROM)

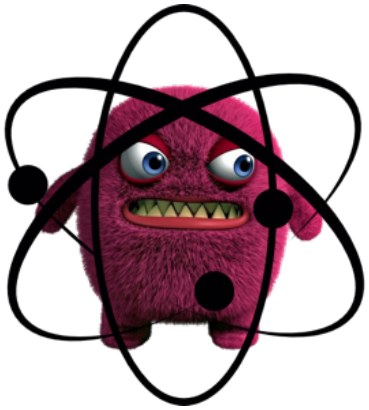
[Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Z'11]

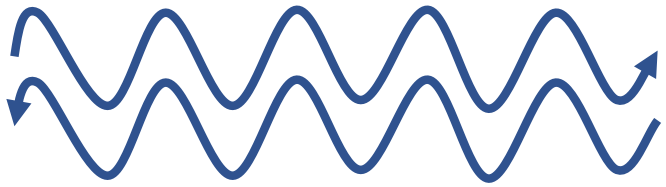
Real World





ROM

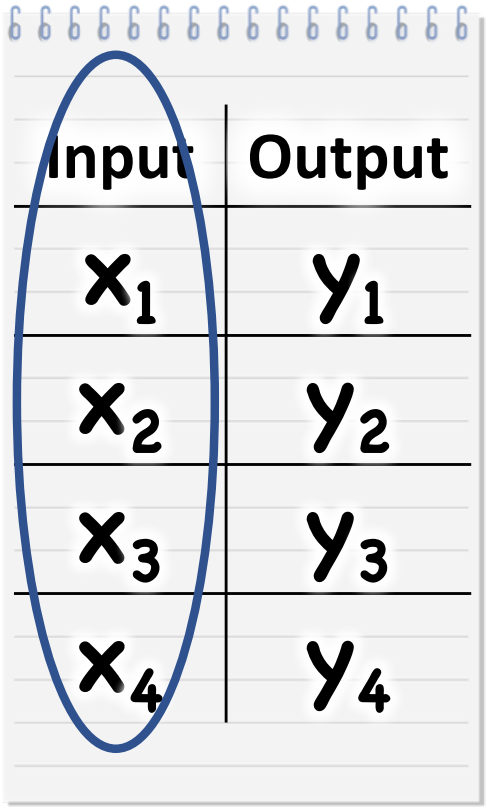




Now standard in post-quantum crypto

Problem with Classical Proofs in QROM

How do we record the x values?



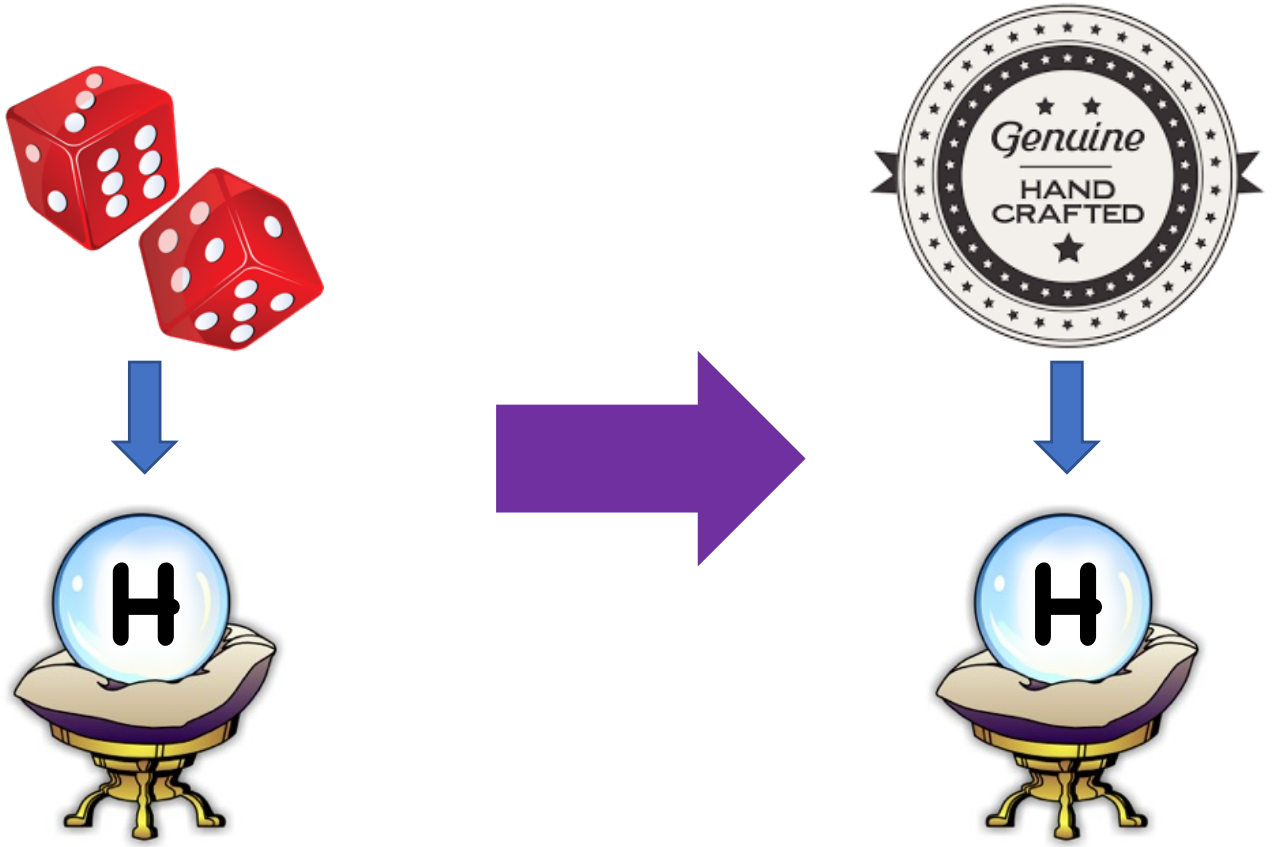
Problem with Classical Proofs in QROM

Observer Effect:
Learning anything about quantum system disturbs it

answers obliviously, so no disturbance

Reduction must answer obliviously, too?

Typical QROM Proof



H fixed once and for all at beginning

Limitations

Allows us to:

- Know the inputs adversary cares about?
- Know the corresponding outputs?
- (Adaptively) program the outputs?
- Easy analysis of bad events (e.g. collisions)?

Limitations

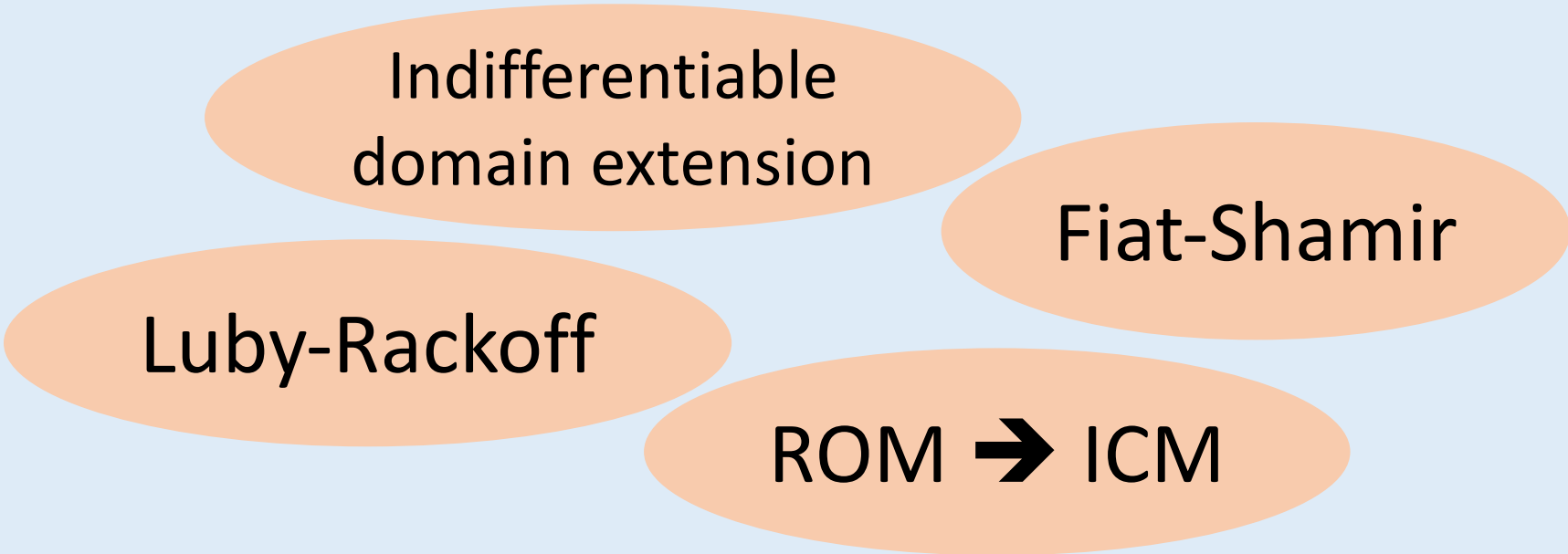
Allows us to:

- ~~Know the inputs adversary cares about?~~ ✘
- ~~Know the corresponding outputs?~~ ✘
- ~~(Adaptively)~~ program the outputs? ✓ / ✘
- ~~Easy analysis of bad events (e.g. collisions)?~~ ✘

Limitations

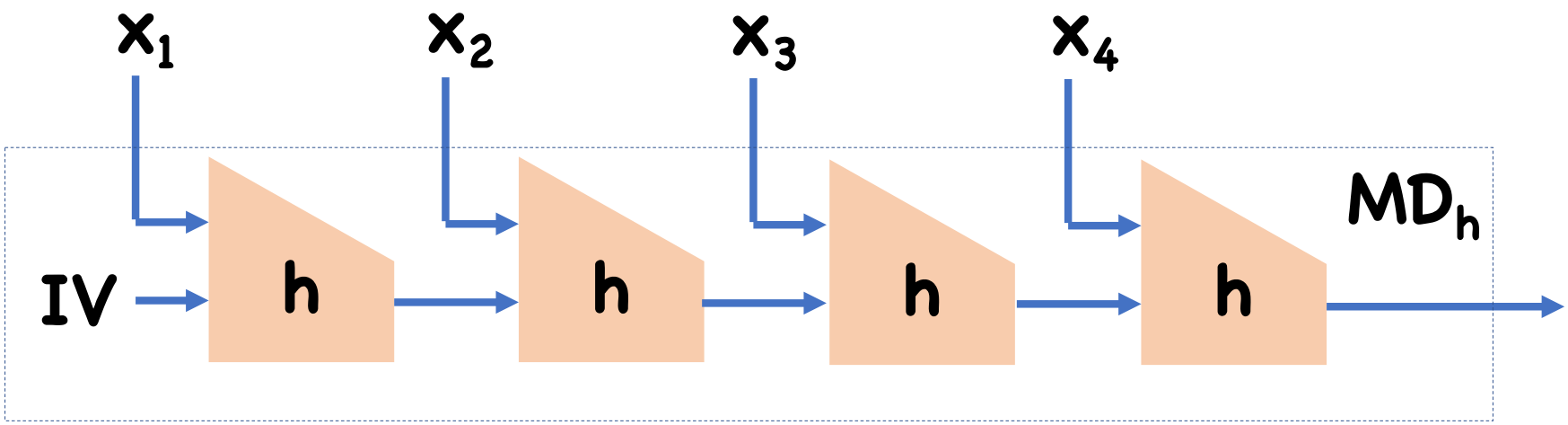
Good News: Numerous positive results (30+ papers)

Bad News: Still some major holdouts



Example: Domain Extension for Random Oracles

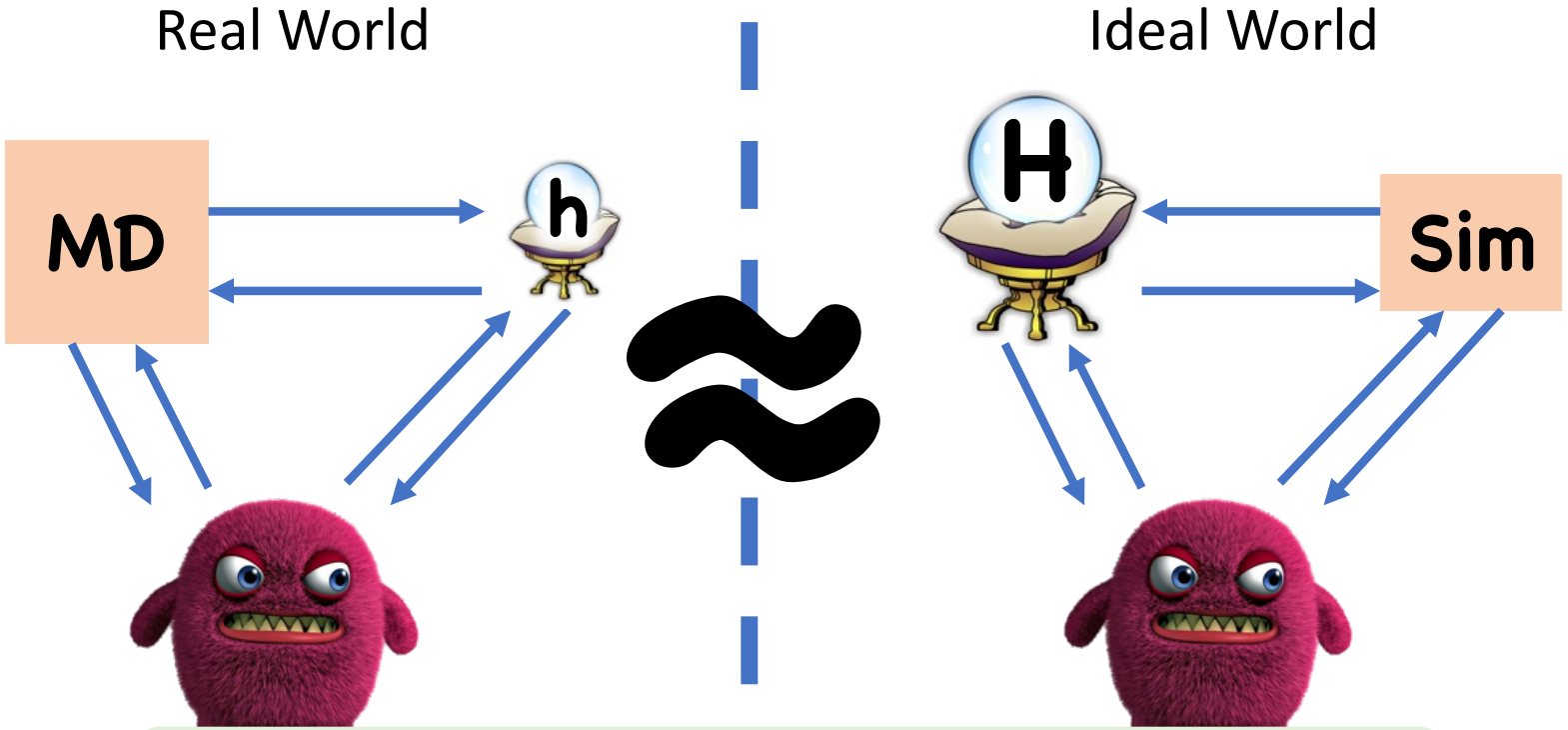
Q: Does Merkle-Damgård preserve random oracle-ness?



Example: Domain Extension for Random Oracles

A: Yes(ish) [Coron-Dodis-Malinaud-Puniya'05]

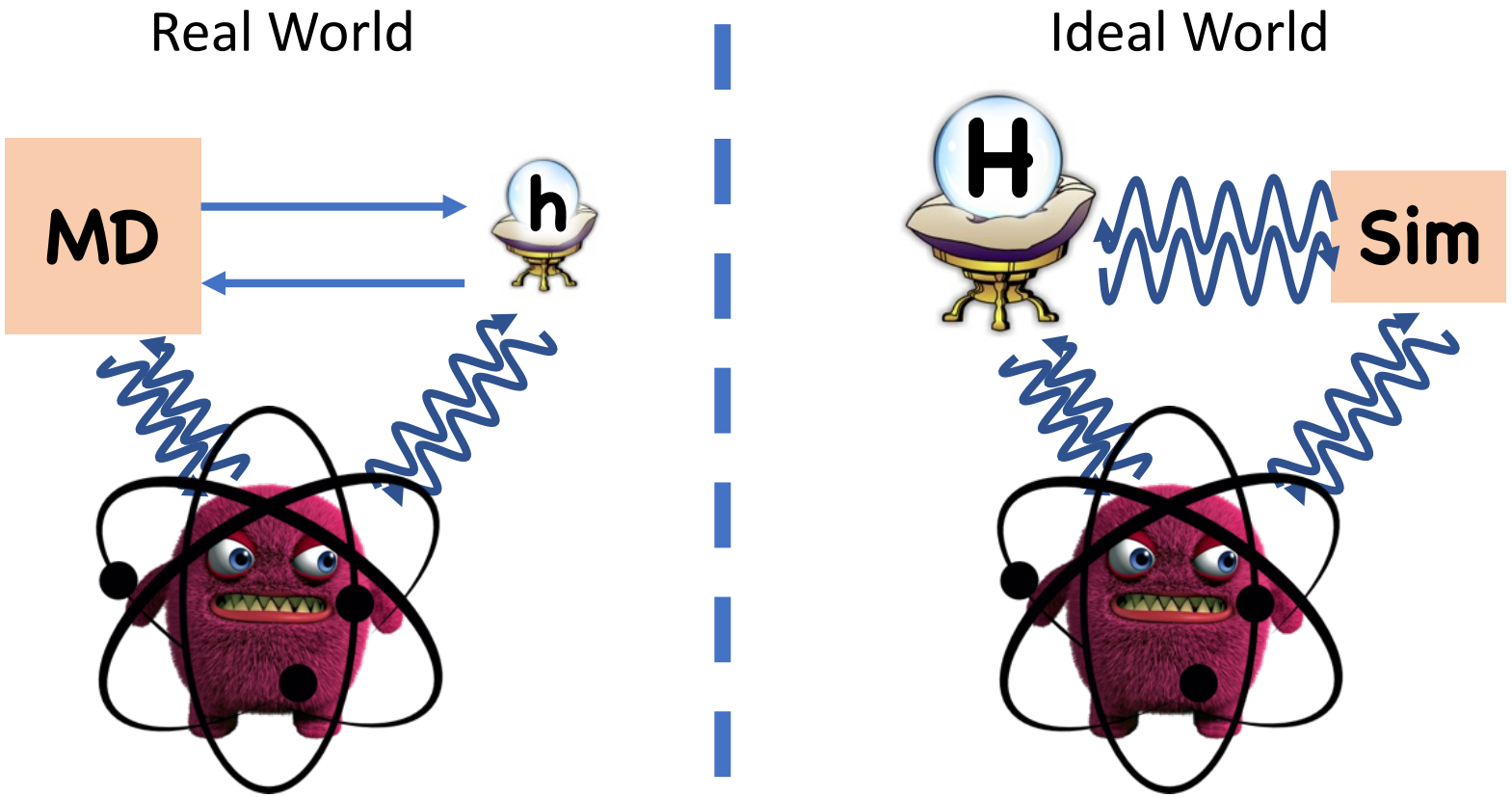
How? *Indifferentiability* [Maurer-Renner-Holenstein'04]



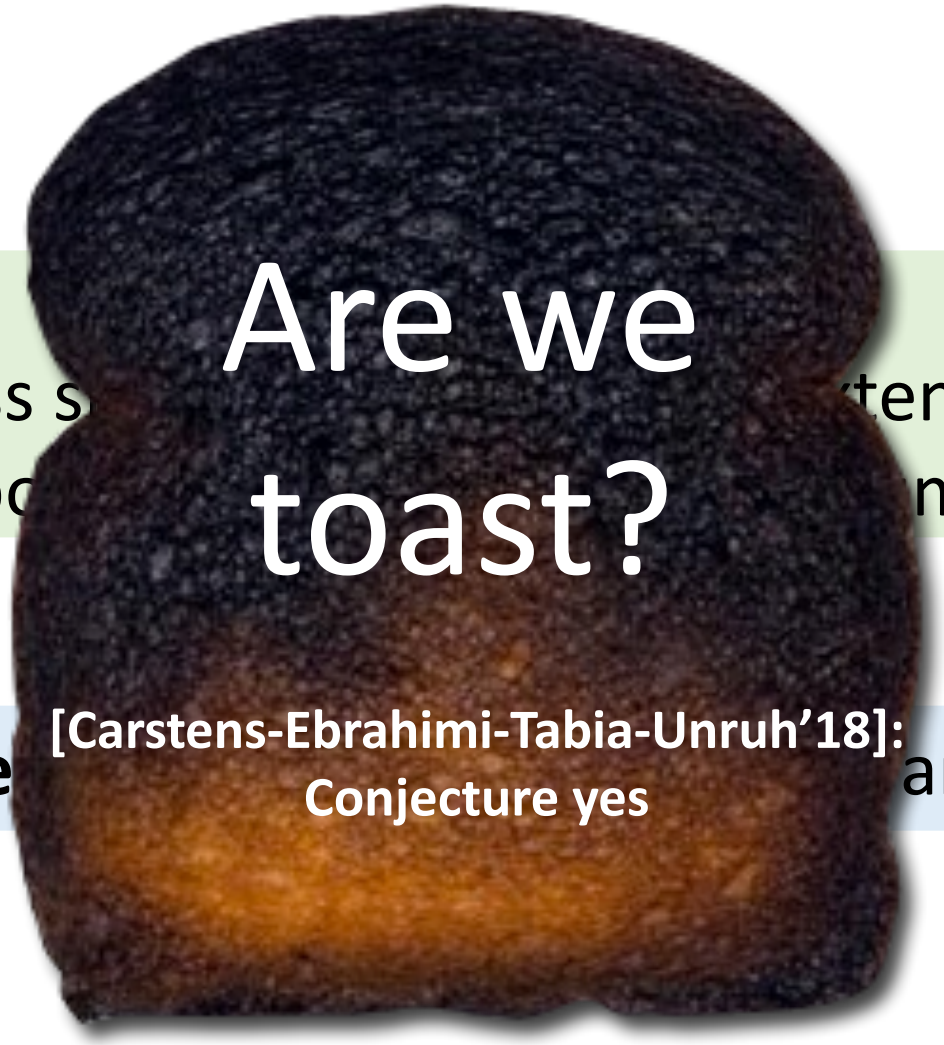
Thm [Ristenpart-Shacham-Shrimpton'11]:
Indifferentiability ⇒ as good as RO for "single stage games"

Quantum Indifferentiability?

Concurrently considered by [Carstens-Ebrahimi-Tabia-Unruh'18]



Quantum Indifferentiability?



Stateless s tension is
impo mly

Proof ide andom **H**

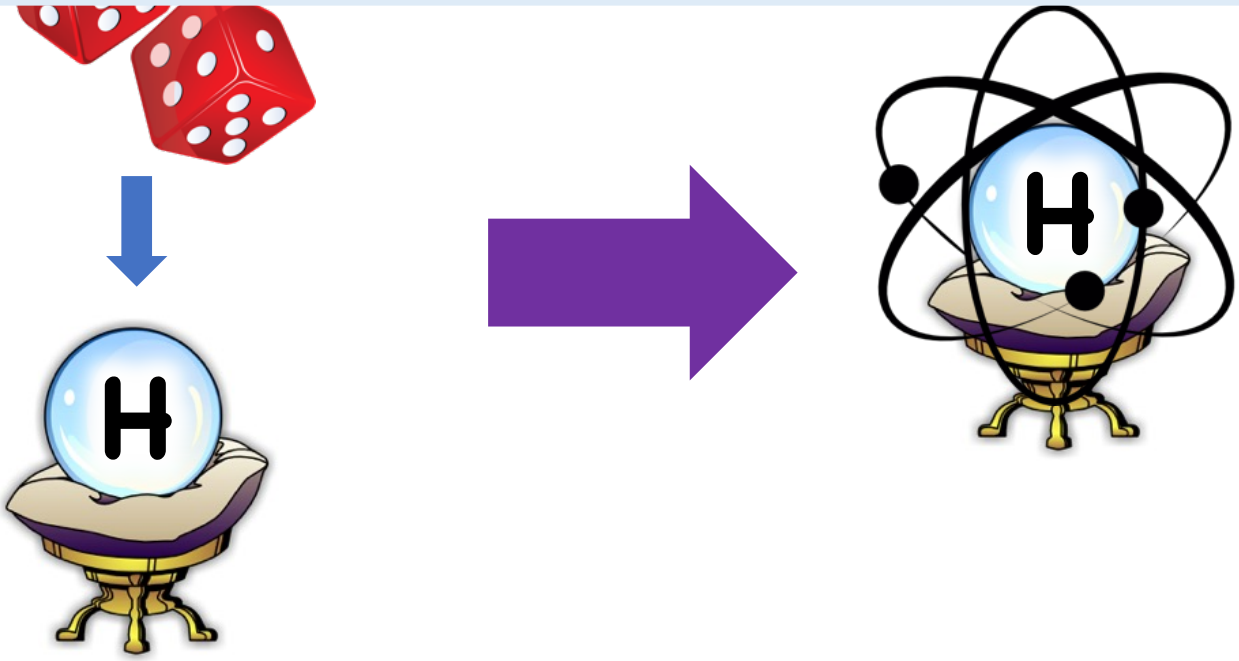
[Carstens-Ebrahimi-Tabia-Unruh'18]:
Conjecture yes

This Work:
On-the-fly simulation of quantum random oracles
(aka Compressed Oracles)

Step 1: Quantum-ify (aka Purify)

Quantum-ifying (aka purifying) random oracle:

now single quantum system



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

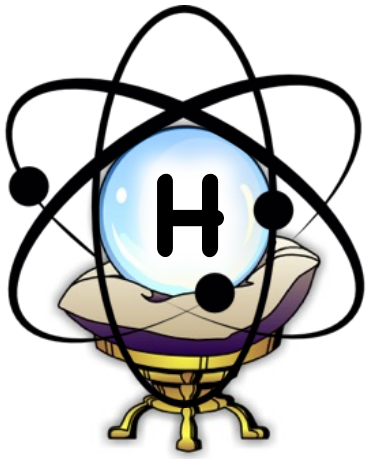
Step 1: Superposition of Oracles

Initial oracle state: 

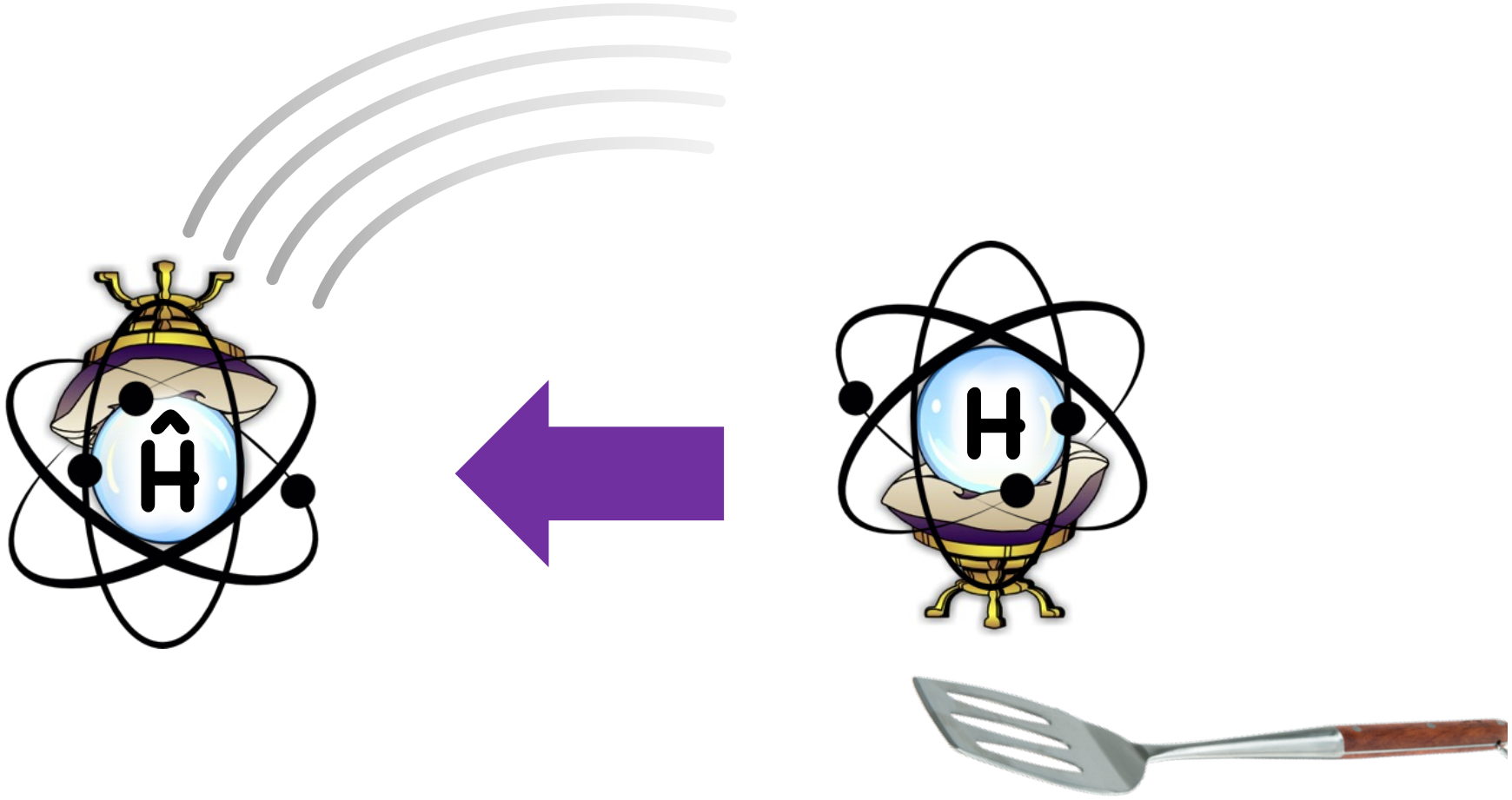
Query(x, y, H): y = y⊕H(x)

Adversary's query

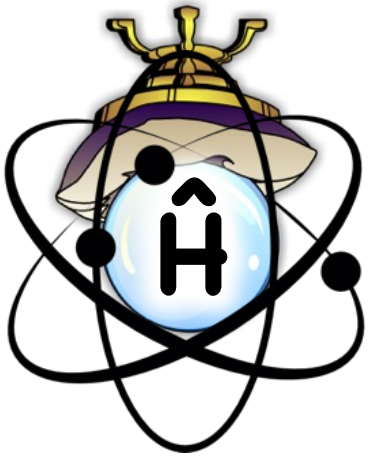
Oracle's state



Step 2: Look at Fourier Domain



Step 2: Look at Fourier Domain

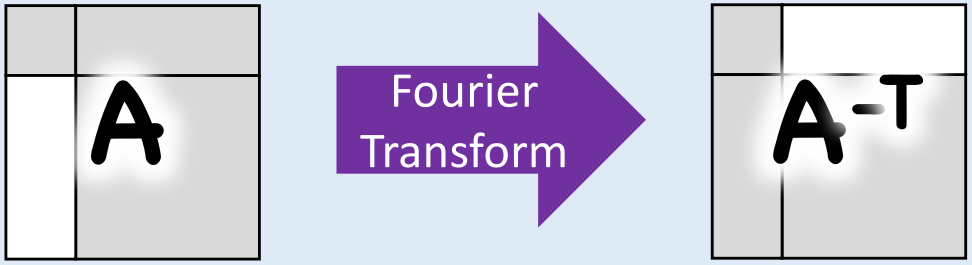


Initial oracle state: $Z(x) = 0$

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

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

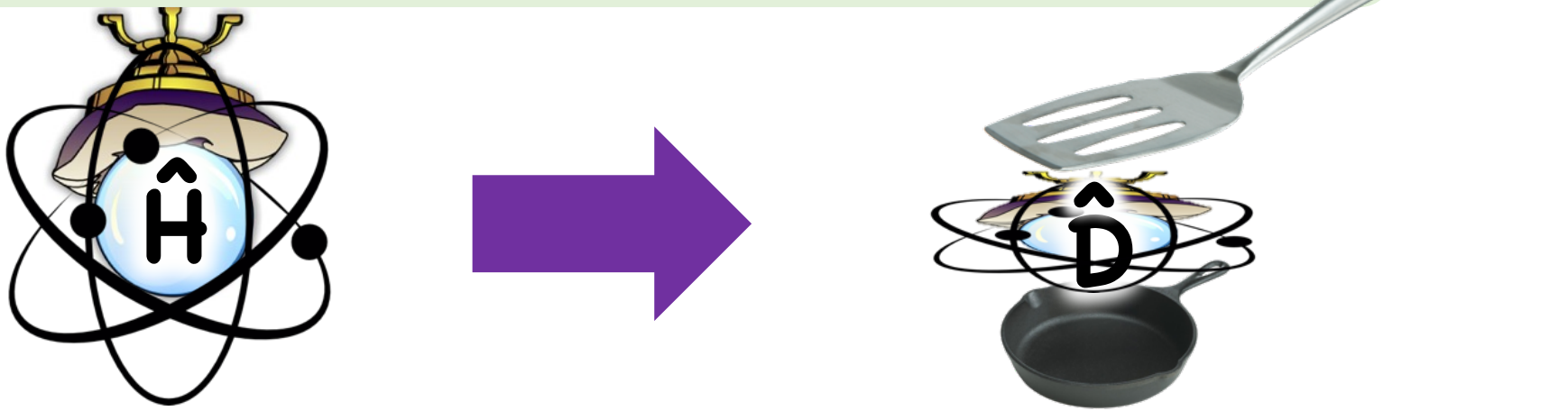
Proof:



Step 3: Compress

Observation:

After **q** queries, $\hat{H}$ is non-zero on at most **q** points



Step 3: Compress

Initial oracle state: **{}**

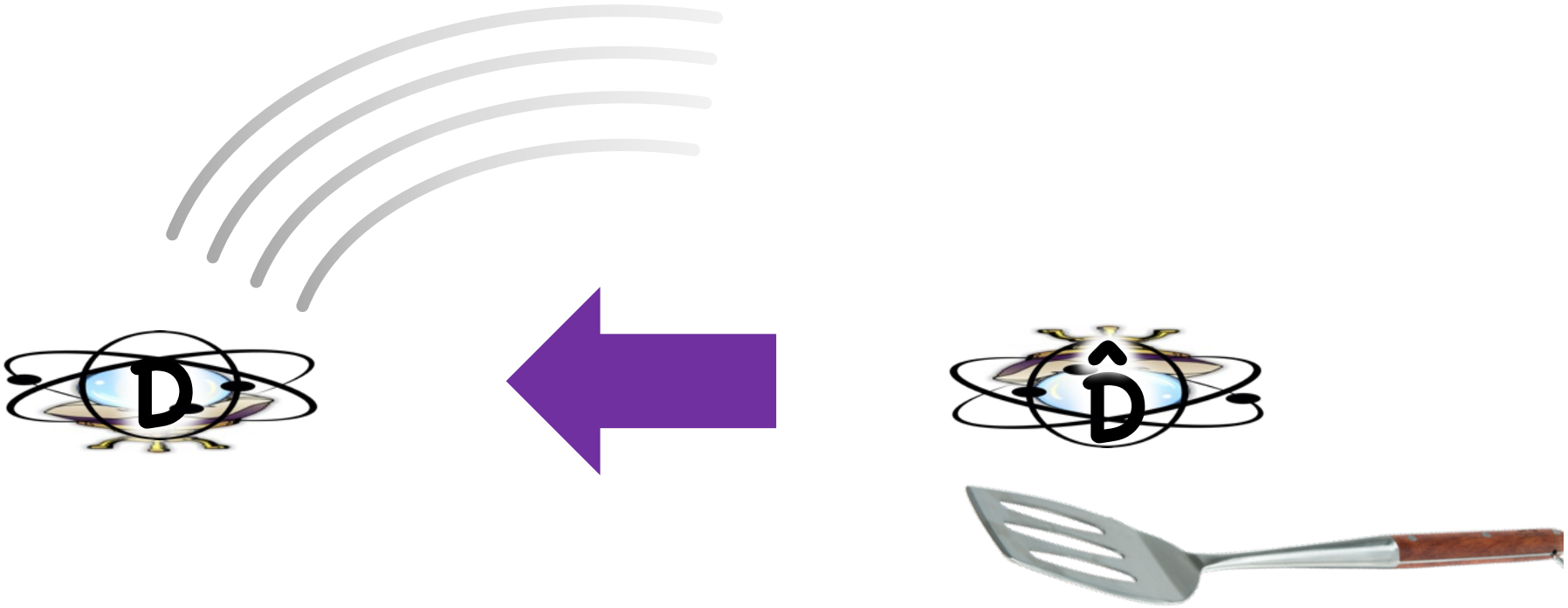
Query(x, y, $\hat{D}$):

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

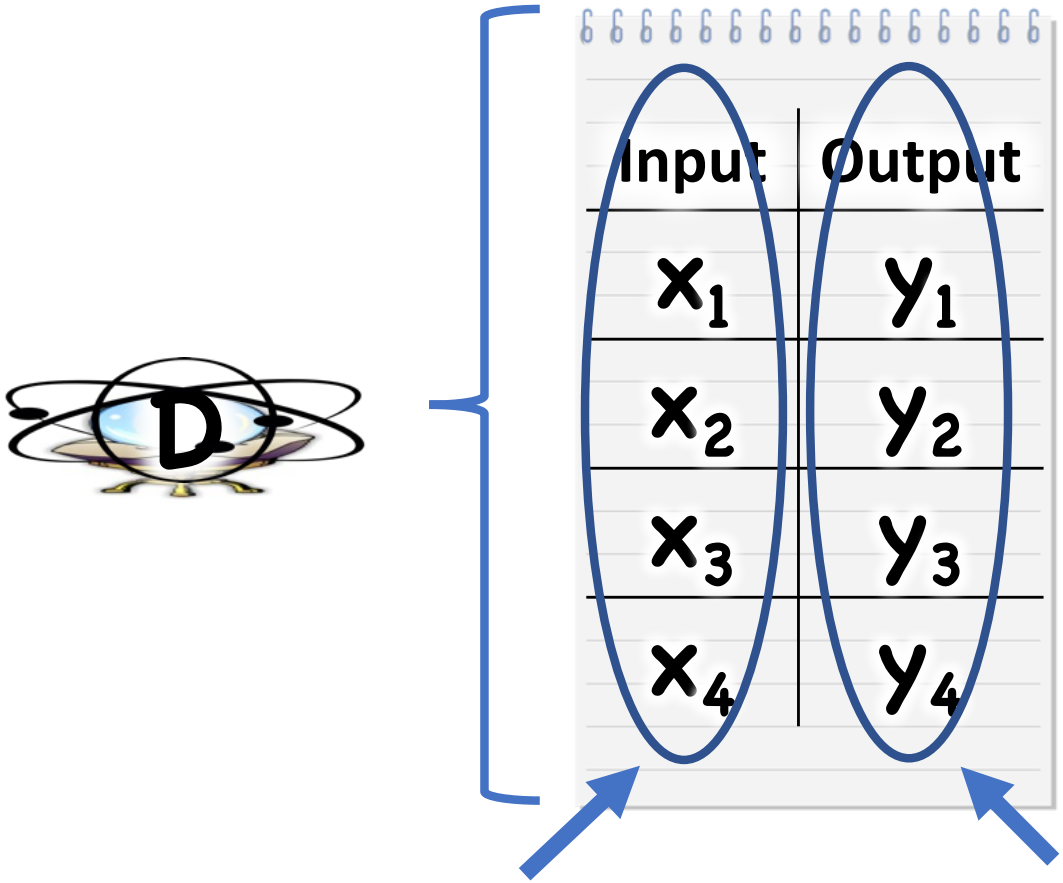
(2) Replace $(x,y') \in \hat{D}$ with $(x, y' \oplus y)$

(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:

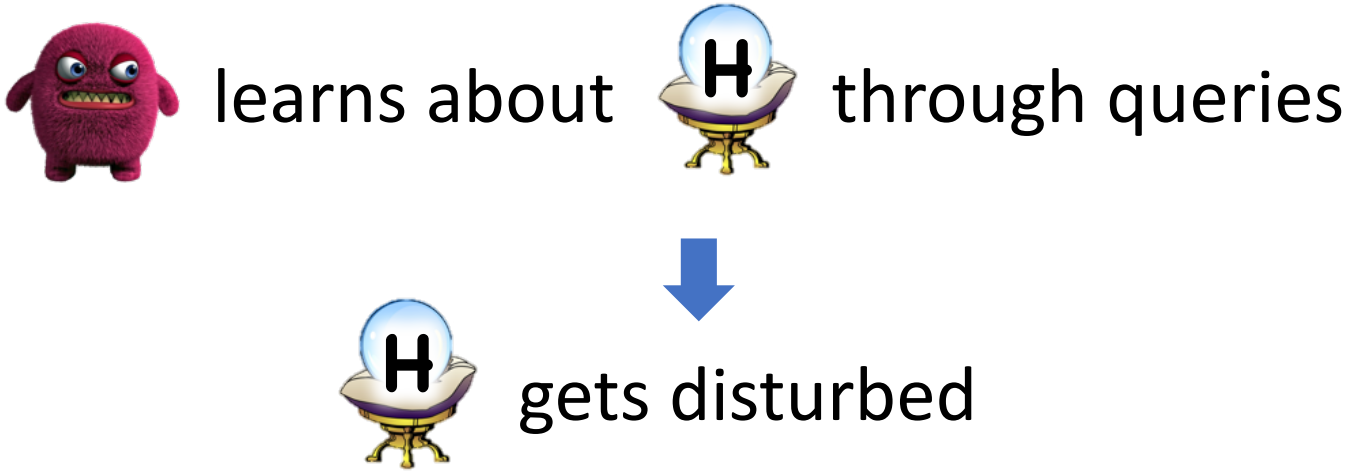
- Know the inputs adversary cares about? ✓
- Know the corresponding outputs? ✓
- ~~(Adaptively) program the outputs?~~ ✗

  Fixed by [Don-Fehr-Majenz-Schaffner'19,Liu-Z'19], later this session!
- Easy analysis of bad events (e.g. collisions)? ✓

So, what happened?

Recall…

Observer Effect:
Learning anything about quantum system disturbs it



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…

Applications In This Work

Quantum Indiff. of Merkle-Damgård

Easily re-prove quantum lower bounds:

$\Omega(N^{1/2})$ queries needed for Grover search

$\Omega(N^{1/3})$ queries needed for collision finding

$\Omega(N^{1/(k+1)})$ queries needed for **k**-SUM

CCA-security of plain Fujisaki-Okamoto

Further Applications

[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)

[Czajkowski-Majenz-Schaffner-Zur'19]:
Indifferentiability of Sponge

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

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

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

Lessons Learned

Always purify your oracles!