Quantum-Classical Tradeoffs in the Random Oracle Model

Yassine Hamoudi, Qipeng Liu, Makrand Sinha

UC Berkeley

Hash functions

Real world: SHA-3

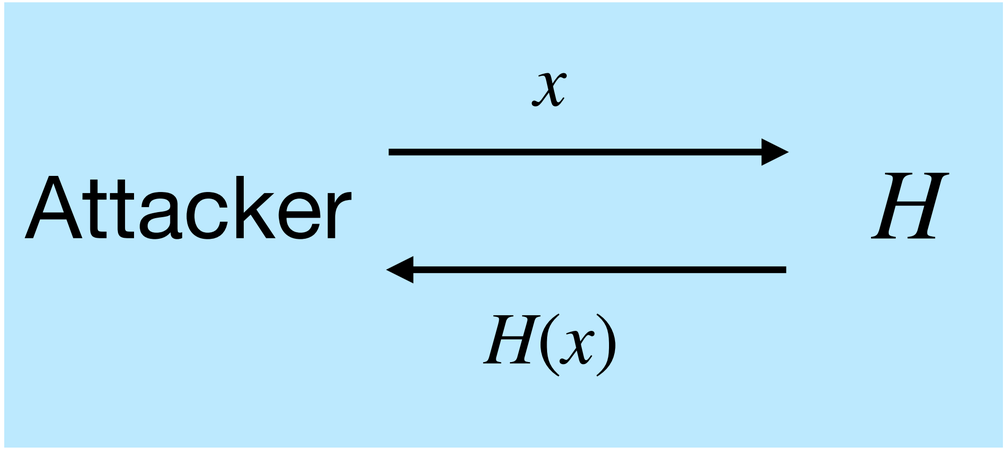
Ideal world: random $H : [N] \to [N]$
+ interface for querying H

⟶ Amenable to security proofs

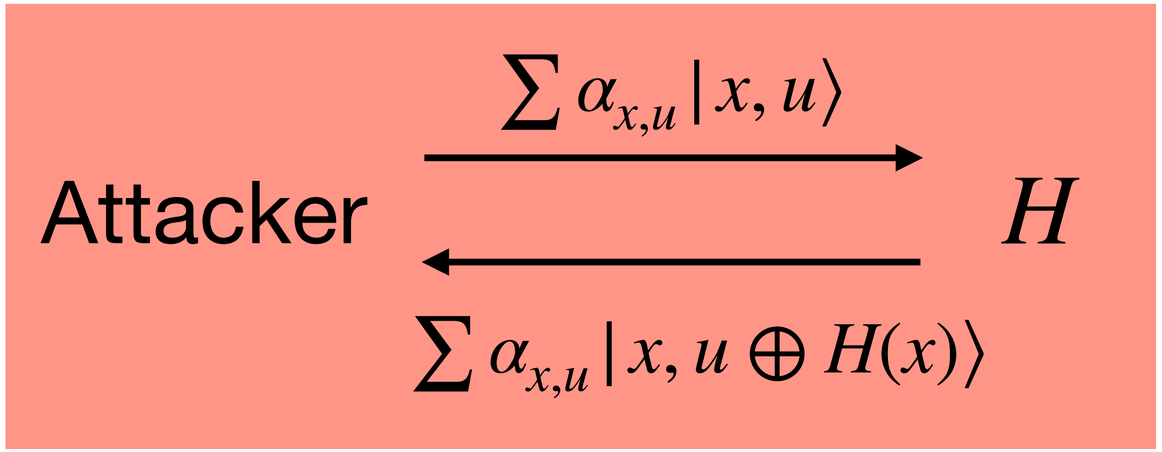
⟶ Focus on # of queries

Random oracle model

Classical



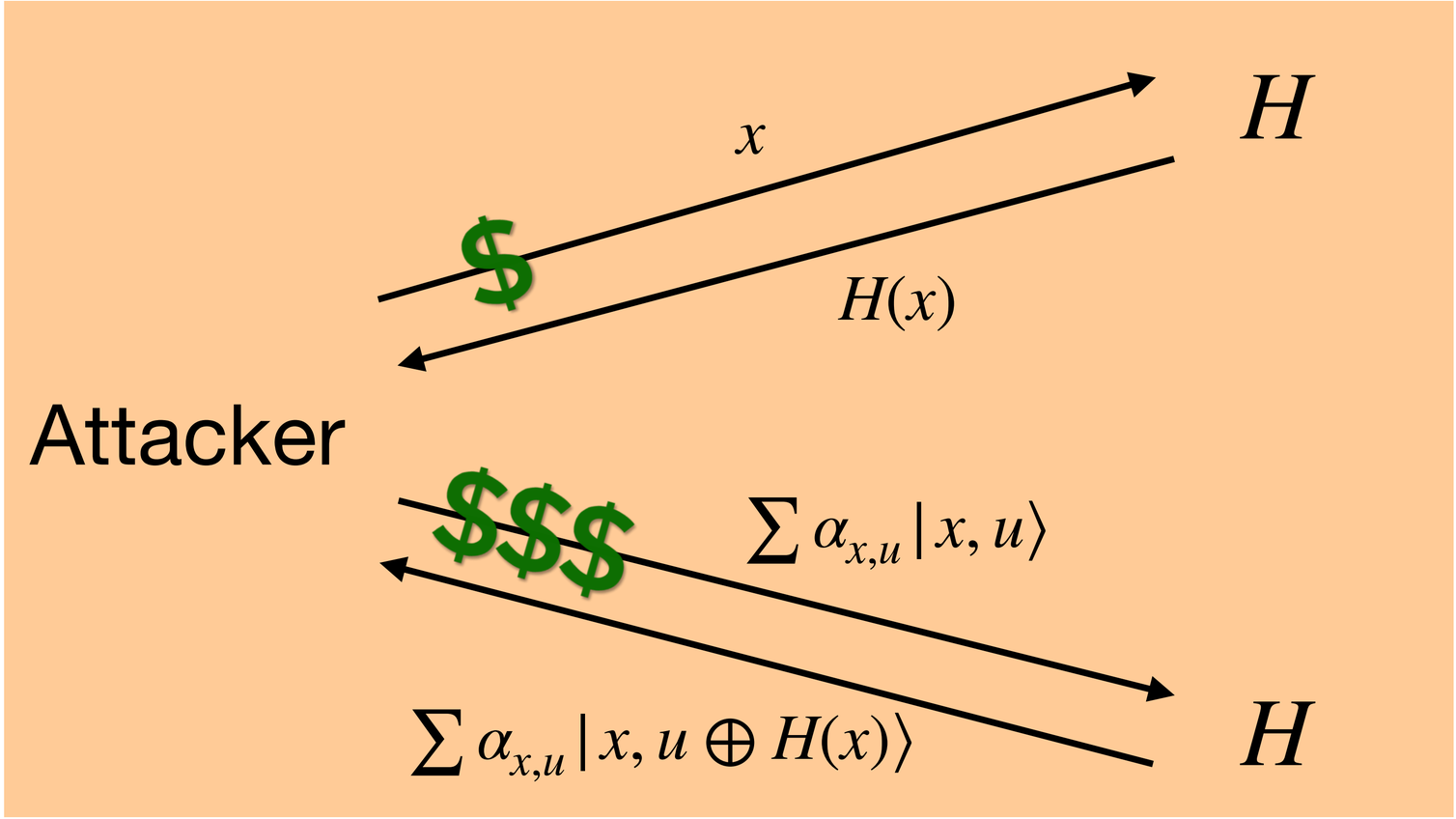
Quantum



+ More powerful
  (⇒ stronger security proofs)

- Hide larger implementation cost/query
  (⇒ exaggerated security parameters)

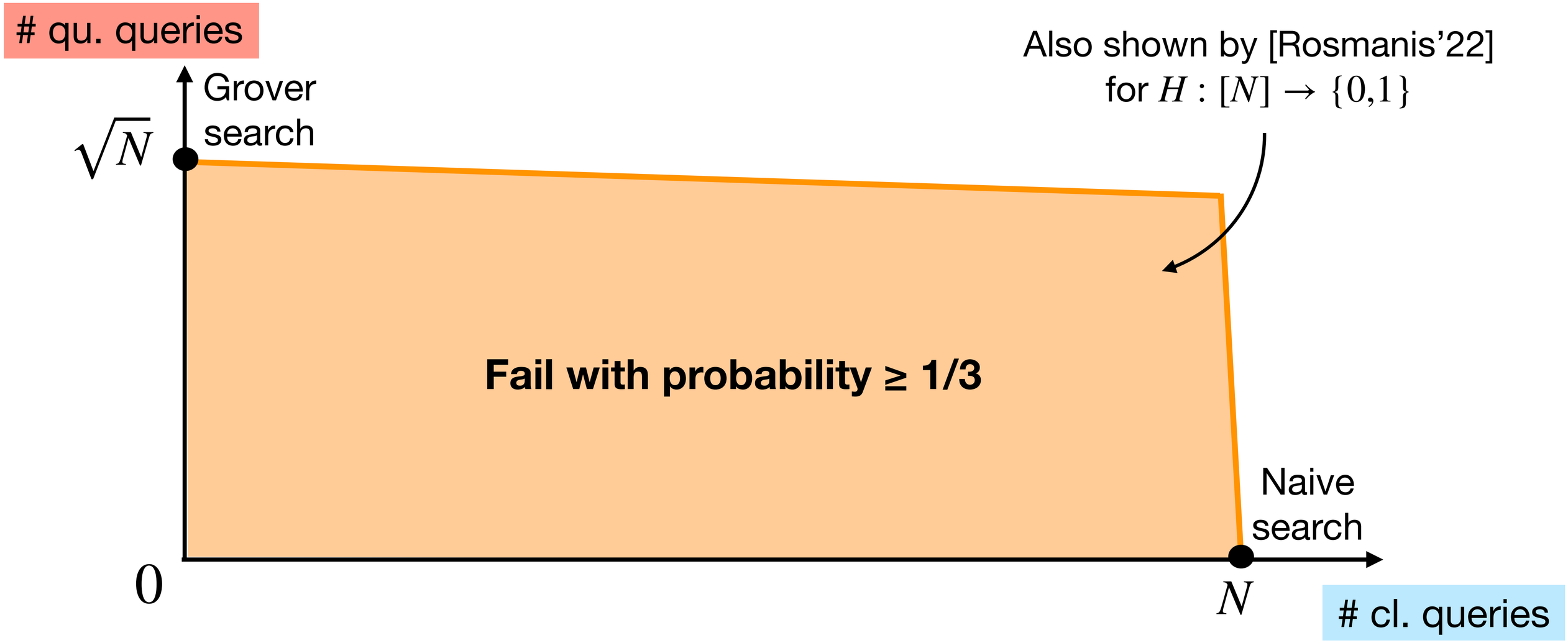
“Hybrid” random oracle



Classical and quantum queries are counted separately

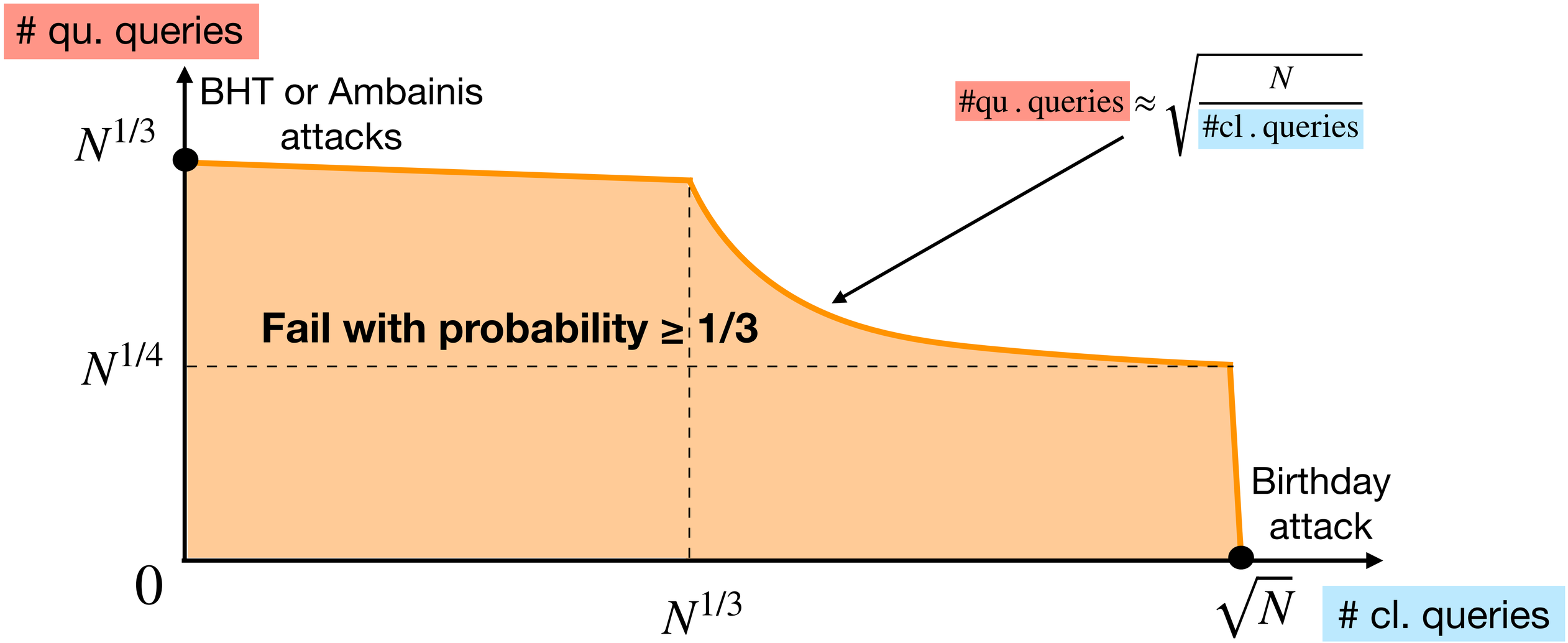
Preimage search:

Find x such that $H(x) = 0$



Collision finding:

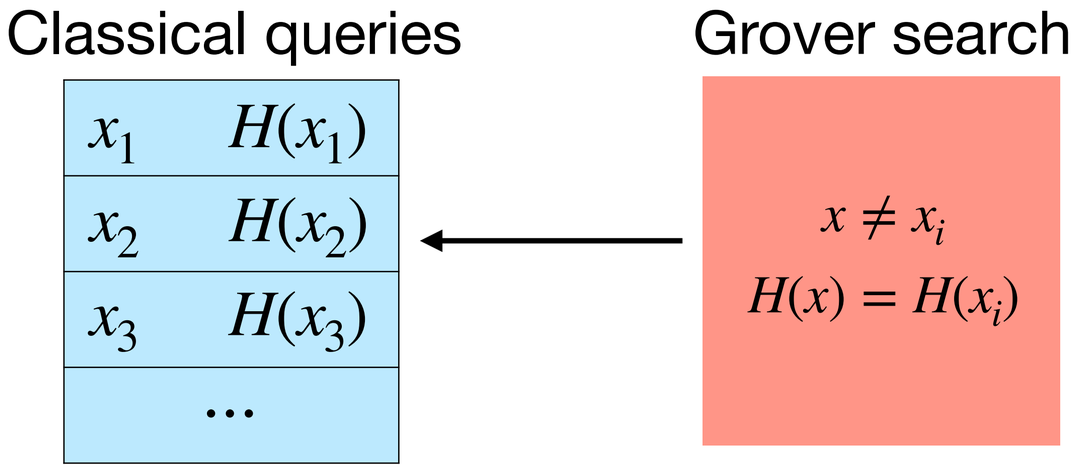
Find $x_1 \neq x_2$ such that $H(x_1) = H(x_2)$



Hybrid BHT attack

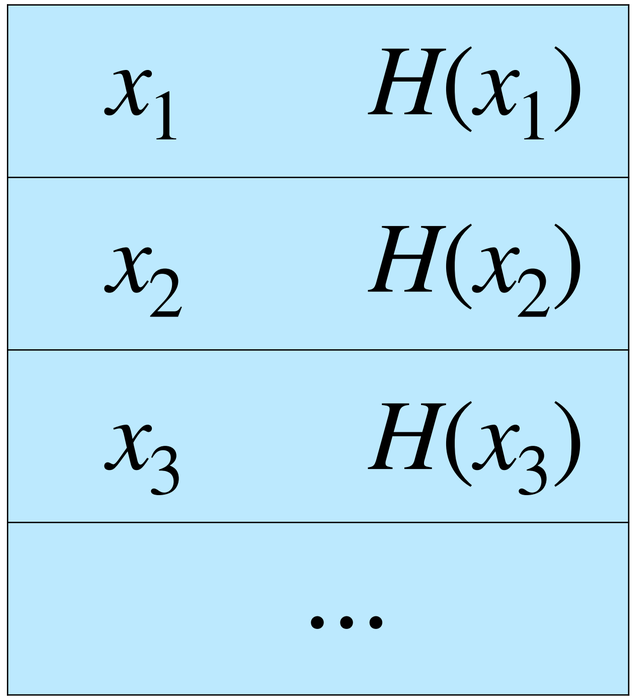
Example: $\#\text{qu . queries} \approx N^{0.27} \ll$ BHT or Ambainis attacks

$\#\text{cl . queries} \approx N^{0.46} \ll$ Birthday attack



Hybrid compressed oracle

Classical transcript



List of (query, answer) obtained by the attacker

Conditioning on the transcript state

Ex: $\Pr\left[H(x) = y \,|\, \text{transcript}\right] =$

$$\begin{cases} 1/N & \text{if } (x, \cdot\,) \notin \text{transcript} \\ 1 & \text{if } (x, y) \in \text{transcript} \\ 0 & \text{otherwise} \end{cases}$$

Quantum transcript

Step 1: purify the oracle H

$$\sum \alpha_{x,u,H} |x,u\rangle \otimes \left| \begin{array}{|c|} \hline H(0) \\ \hline H(1) \\ \hline H(2) \\ \hline \dots \\ \hline H(N-1) \\ \hline \end{array} \right\rangle$$

Step 2: compress $|H(x)\rangle \mapsto |D(x)\rangle$

$$\begin{cases} \dfrac{1}{\sqrt{N}} \displaystyle\sum_{y \in [N]} |y\rangle \longmapsto |\emptyset\rangle \\ \text{Identity elsewhere} \end{cases}$$

$H(x)$ looks random to the attacker

$$\sum \alpha'_{x,u,D} |x,u\rangle \otimes \left| \begin{array}{|c|} \hline D(0) \\ \hline D(1) \\ \hline D(2) \\ \hline \dots \\ \hline D(N-1) \\ \hline \end{array} \right\rangle$$

$$\in \{\emptyset, 0, \dots, N-1\}$$

Quantum transcript

Initial state: $|0\rangle \otimes \frac{1}{N^{N/2}} \sum_H \left| \begin{array}{|c|}\hline H(0) \\ \hline H(1) \\ \hline H(2) \\ \hline \cdots \\ \hline H(N-1) \\ \hline \end{array} \right\rangle = \begin{array}{l} \otimes \frac{1}{\sqrt{N}} \sum_y |y\rangle \\ |0\rangle \ \vdots \\ \otimes \frac{1}{\sqrt{N}} \sum_y |y\rangle \end{array}$ Compress $\longmapsto |0\rangle \otimes \left| \begin{array}{|c|}\hline \emptyset \\ \hline \emptyset \\ \hline \emptyset \\ \hline \cdots \\ \hline \emptyset \\ \hline \end{array} \right\rangle$

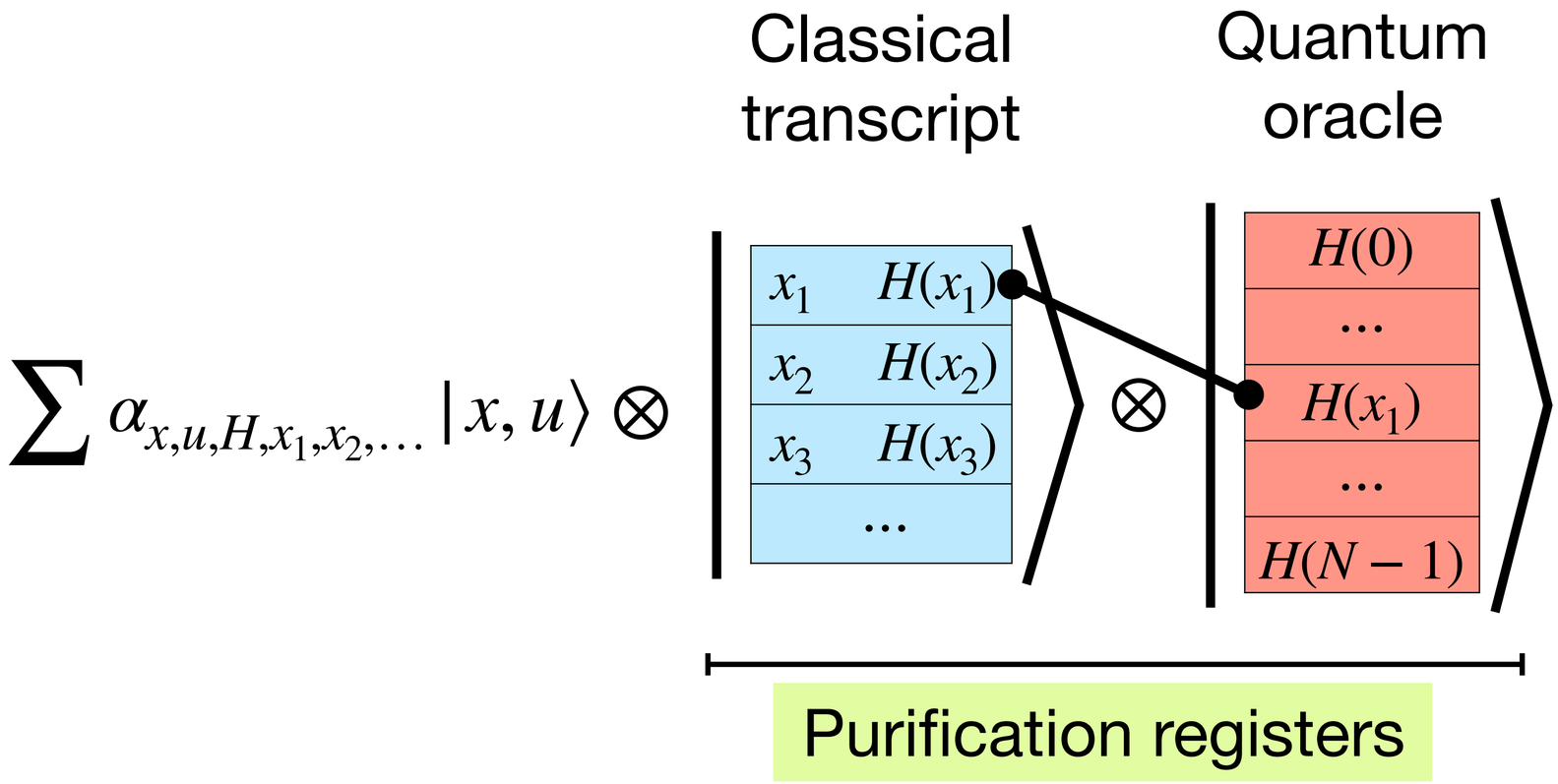
After t queries: $\sum \alpha'_{x,u,D} |x, u\rangle \otimes \left| \begin{array}{|c|}\hline D(0) \\ \hline D(1) \\ \hline D(2) \\ \hline \cdots \\ \hline D(N-1) \\ \hline \end{array} \right\rangle$ $\vdots$ at most t entries $\neq \emptyset$

Disturbance: $\left\| \text{Measure}(|H(x)\rangle) - \text{Measure}(|D(x)\rangle) \right\|_\infty \lesssim 1/N$

(Oracle basis) *(Transcript basis)* ($\emptyset$ = unif. distribution)

Hybrid transcript

Step 1:



Step 2: compression?

Hybrid transcript

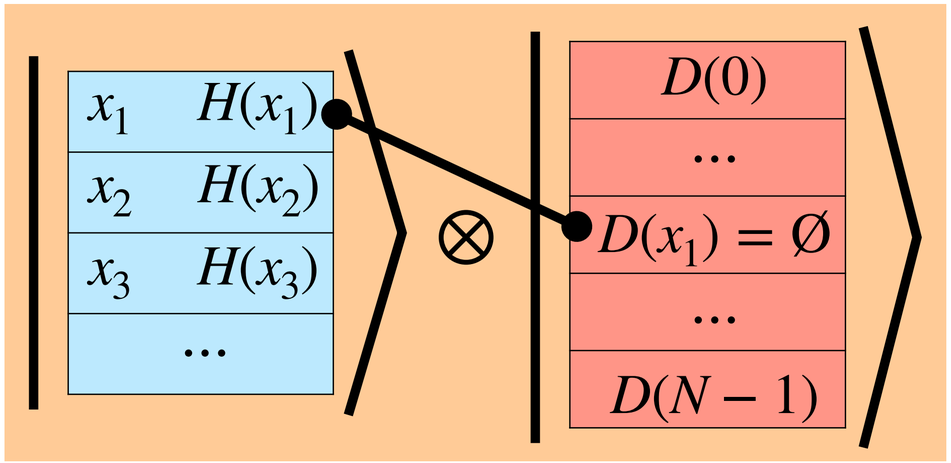
New compression:

Conditioned on $\mathrm{cl}\,.\,\mathrm{transcript}$

$$\begin{cases} |H(x)=y\rangle \mapsto |\emptyset\rangle & \text{if } (x,y) \in \mathrm{cl}\,.\,\mathrm{transcript} \\ \text{Compress as before otherwise: } \frac{1}{\sqrt{N}}\sum_y |H(x)=y\rangle \mapsto |\emptyset\rangle \end{cases}$$

$$\sum \alpha''_{x,u,H,D,x_1,x_2,\ldots} |x,u\rangle \otimes$$

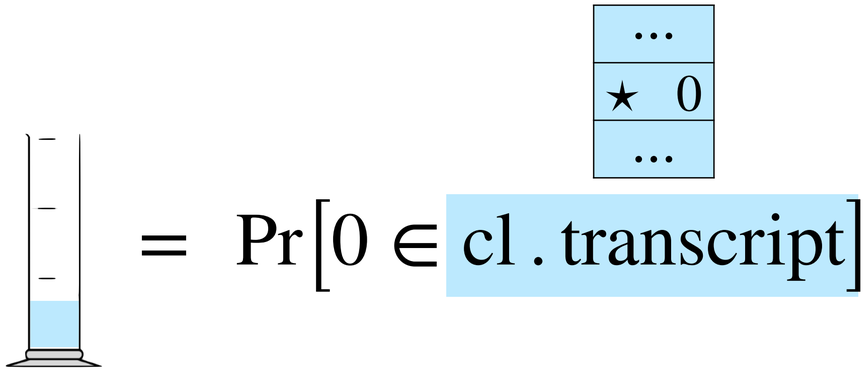
Hybrid transcript

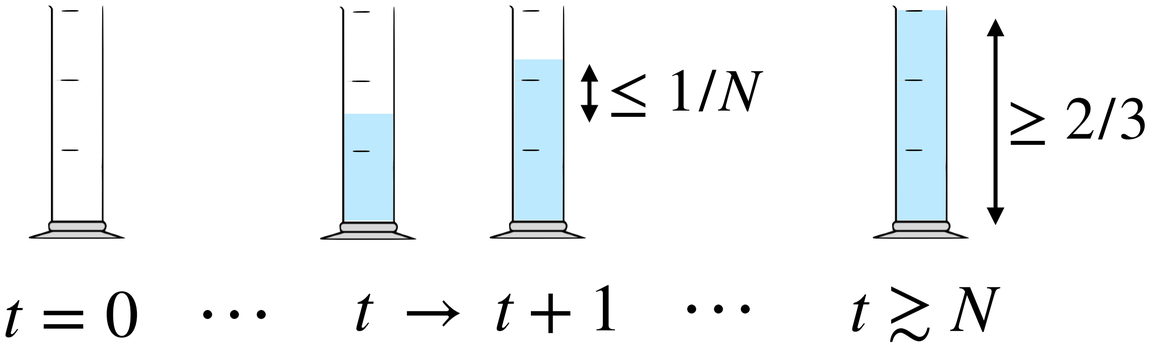


Application 1:

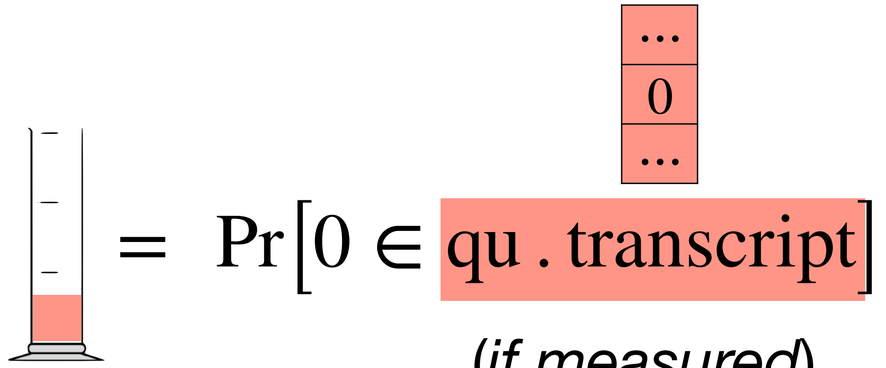
Preimage search

Classical lower bound

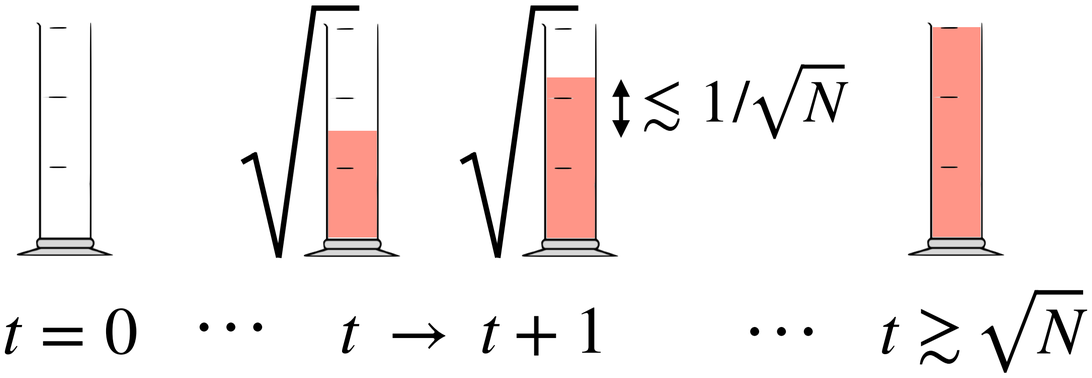




Quantum lower bound



(*if measured*)

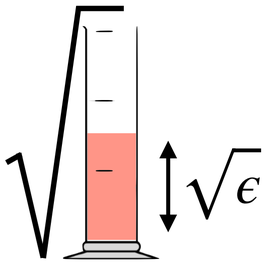


Norm increase

Why is the quantum progress faster?

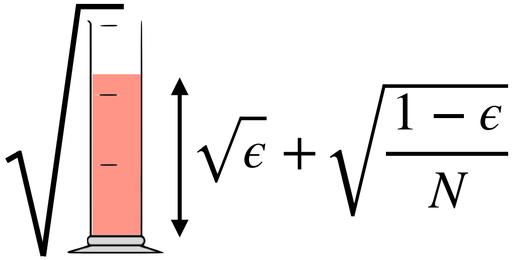
Transcript interference:

$$\sqrt{\epsilon}\,|D(x)=0\rangle \;+\; \sqrt{1-\epsilon}\,|D(x)=\emptyset\rangle$$



Quantum query x

$$\sim \sqrt{\epsilon}\,|D(x)=0\rangle \;+\; \sqrt{\frac{1-\epsilon}{N}}\,|D(x)=0\rangle \;+\; \dots$$

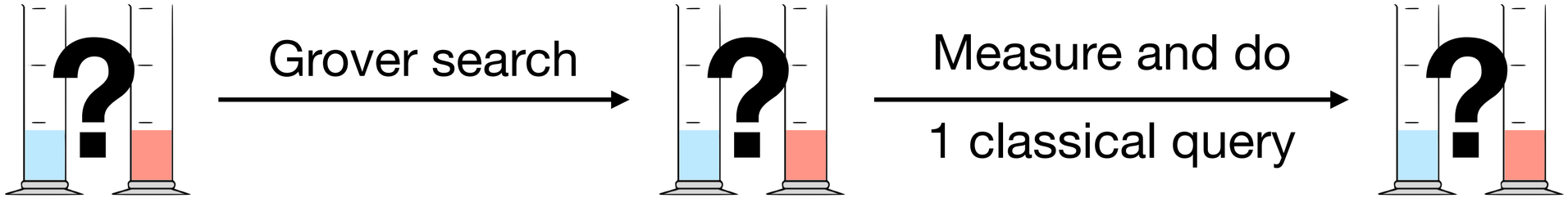


No such phenomenon for classical transcript (*time-stamped recording*)

Hybrid lower bound

Classical-Quantum progress:

Example:



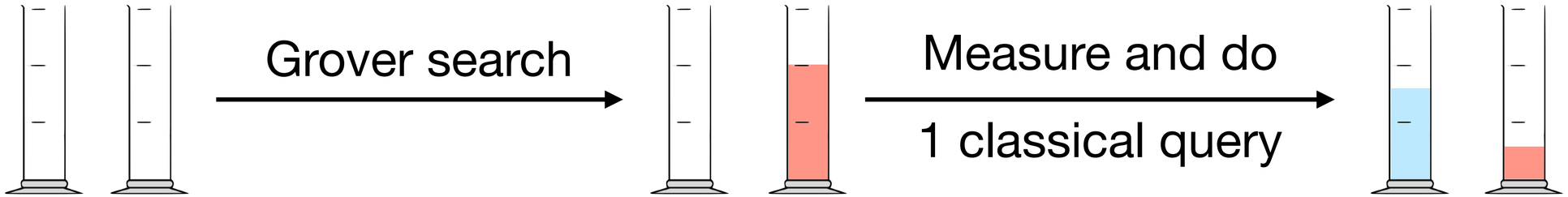
Classical query succeeds
with probability $\gg 1/N$

… but interference effects are lost

Hybrid lower bound

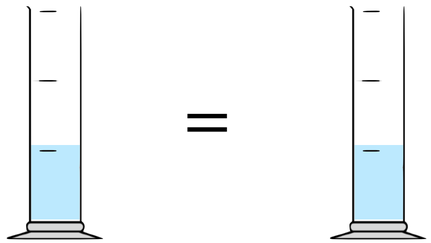
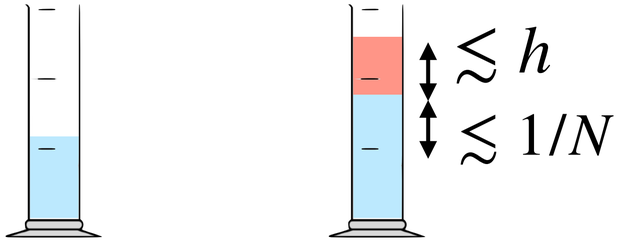
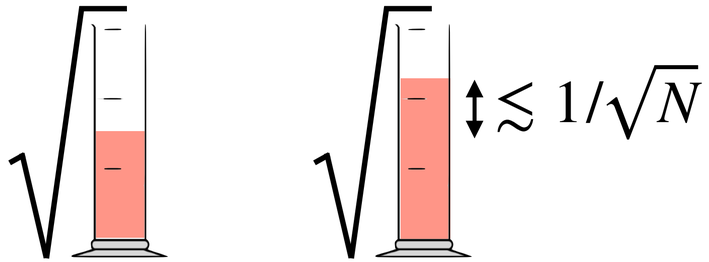
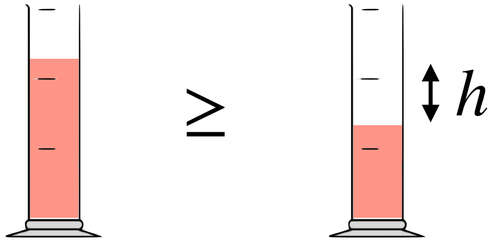
Classical-Quantum progress:

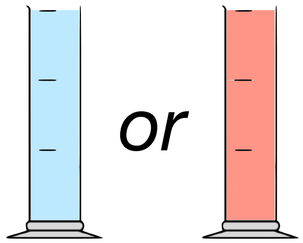
Example:



Classical query succeeds
with probability $\gg 1/N$

… but interference effects are lost

	Quantum query $t \longrightarrow t+1$	Classical query $t \longrightarrow t+1$
$\Pr[0 \in \text{cl . transcript}]$		
$\Pr[0 \in \text{qu . transcript}]$		

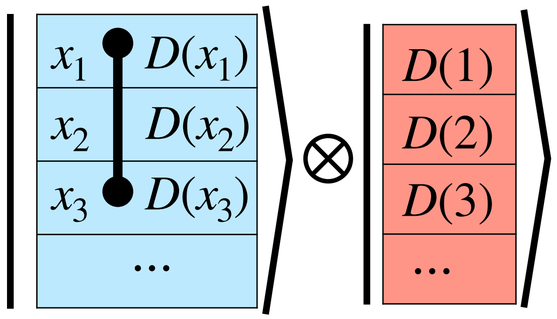
 *or* $\Rightarrow$ # qu. queries $\geq \Omega\left(\sqrt{N}\right)$ or # cl. queries $\geq \Omega(N)$

Application 2:

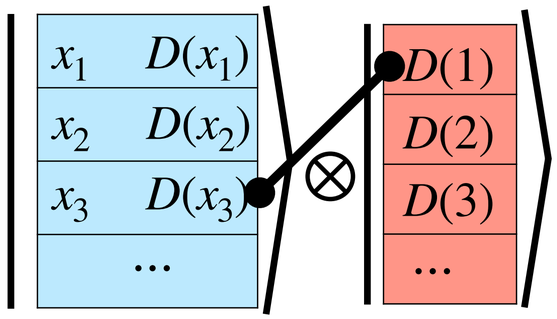
Collision finding

3 types of collisions

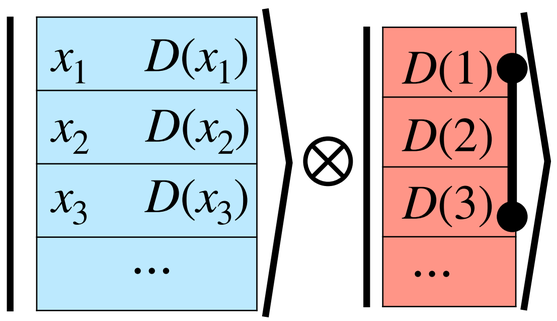
Classical



Hybrid



Quantum



Not all interference effects
are lost by classical queries

Conclusion

New method for analyzing hybrid oracles

⟶ Extension of Zhandry's compressed oracle

Application 1: Preimage search

⟶ Optimal success probability: $\sim \frac{t_c + t_q^2}{N}$

t_q = # qu. queries

t_c = # cl. queries

Application 2: Collision finding

⟶ Optimal success probability: $\sim \frac{t_c^2 + t_q^3 + t_c \cdot t_q^2}{N}$