The NISQ Complexity of Collision Finding

Yassine Hamoudi, Qipeng Liu, Makrand Sinha

CNRS, LaBRI   UC San Diego   U. of Illinois

arXiv:2211.12954 + work in progress

Noisy Intermediate-Scale Quantum

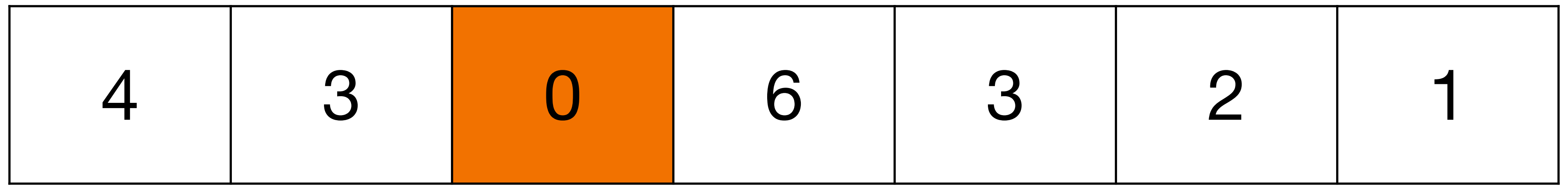
Limitations of short-term quantum computers:

- limited error correction
- small coherence time
- few logical qubits
- …

NISQ complexity: understand what cannot be done with NISQ computers

Toy problems

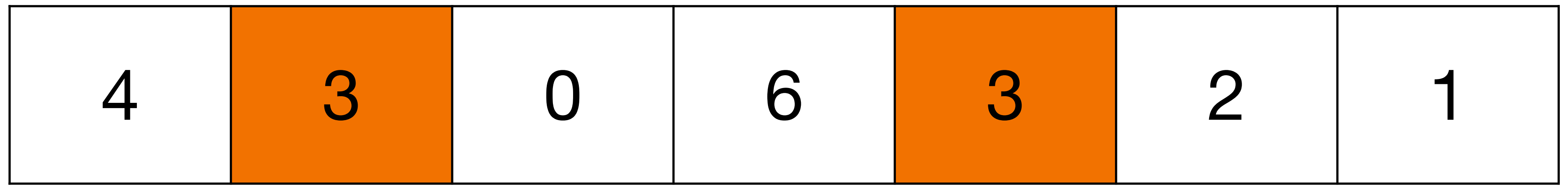
Search problem



4	3	0	6	3	2	1

Find a 0

Collision problem



4	3	0	6	3	2	1

Find a pair of equal values

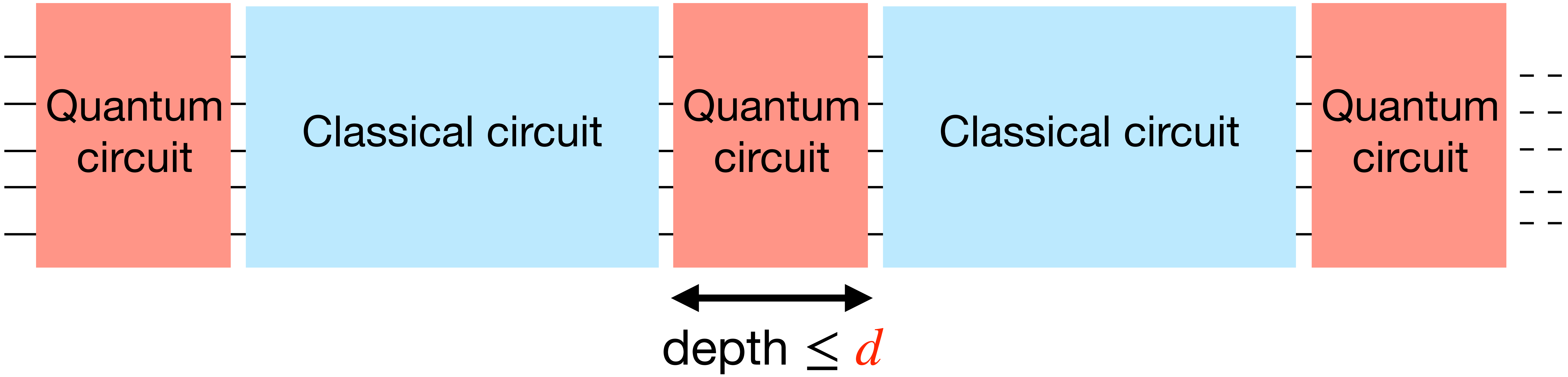
- Subroutines of many quantum algorithms and crypto. attacks
- Amenable to query complexity analysis
- Current algorithms (Grover, BHT, …) are not considered NISQ

Can we get quantum speedups for these problems in NISQ era?

How to model NISQ complexity?

Model 1

Shallow quantum circuits



Quantum circuit

Classical circuit

Quantum circuit

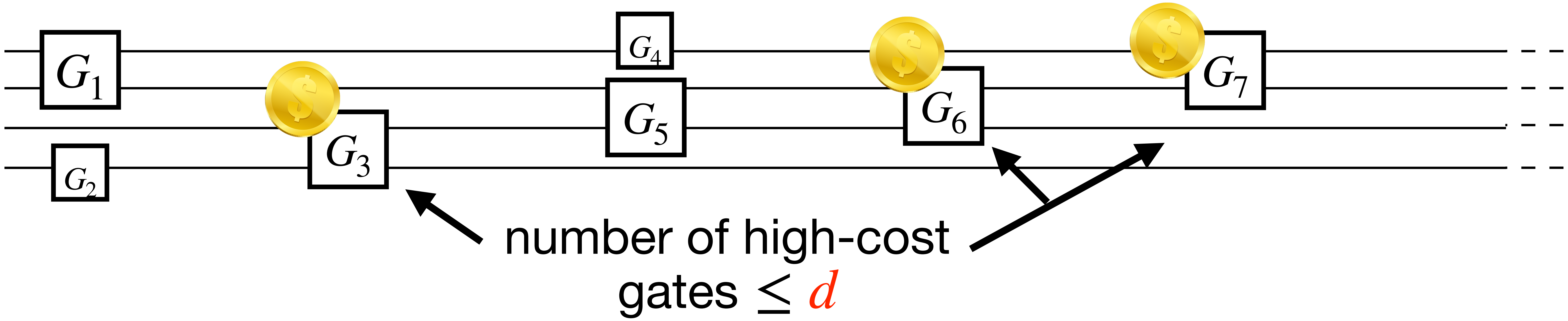
Classical circuit

Quantum circuit

depth $\leq d$

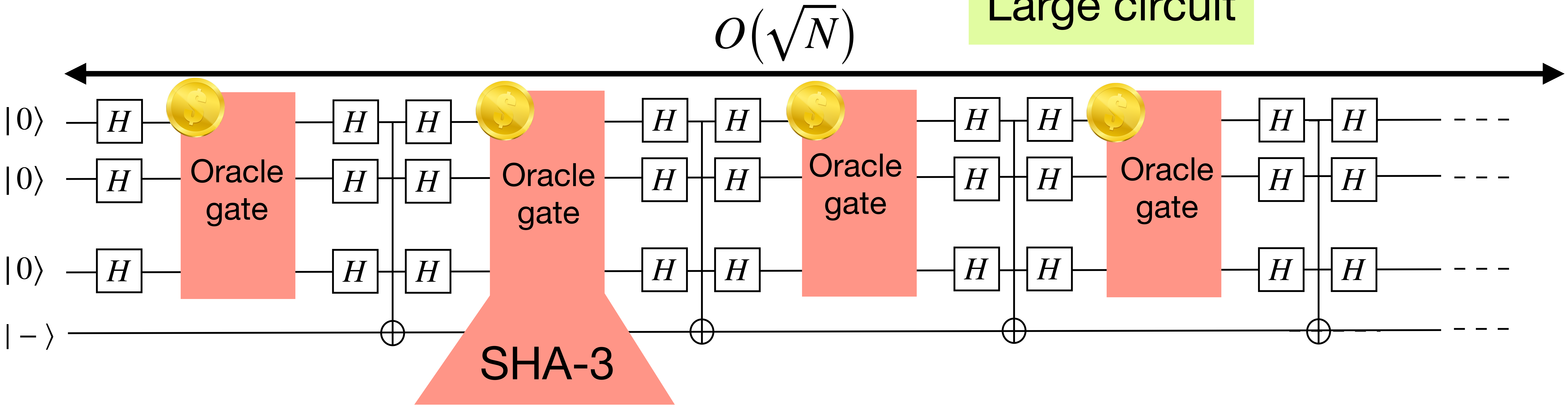
Model 2

Costly gates



number of high-cost gates $\leq d$

Grover is not a NISQ algorithm

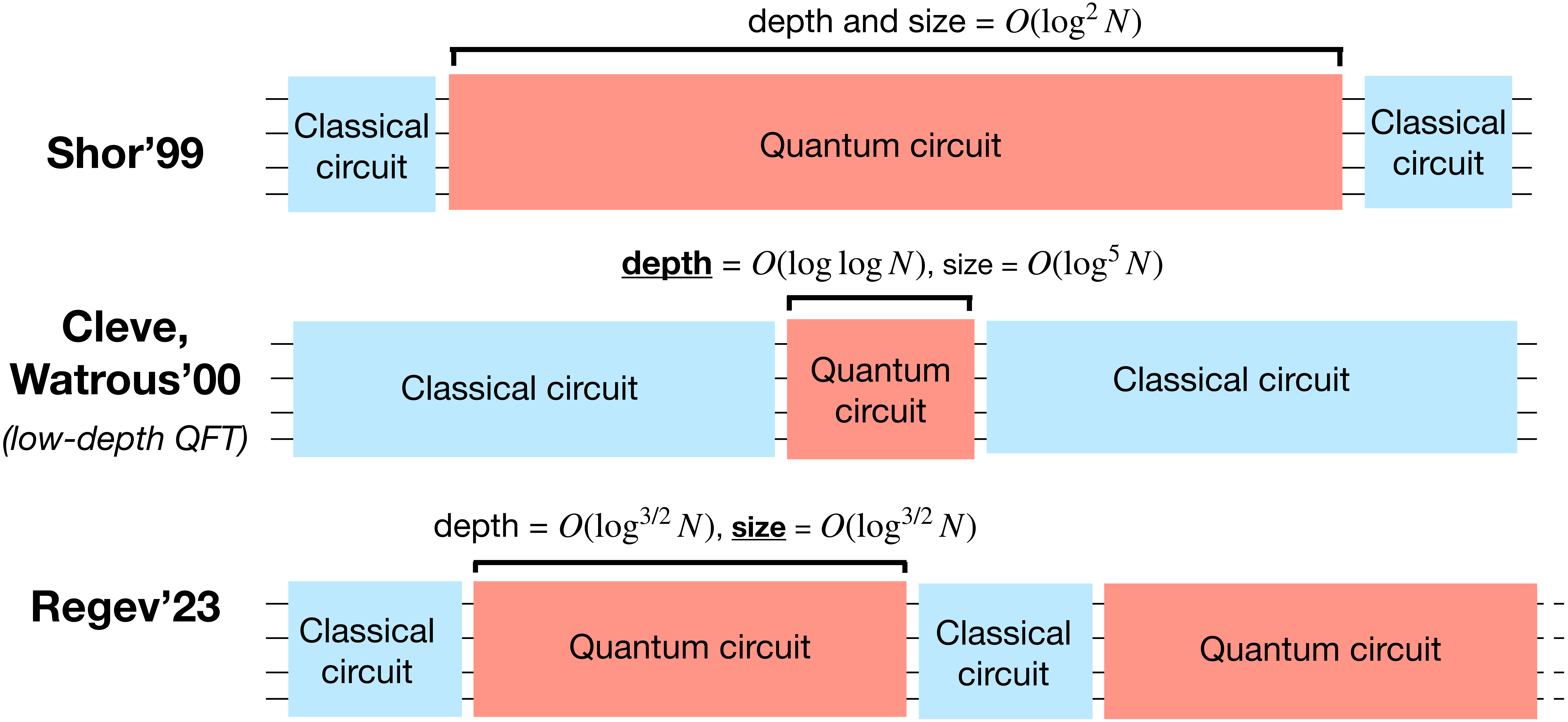


Large circuit

Depth of reversible circuit

Oracle gates are extremely costly

“NISQ-ier” Shor’s factoring



Shor’99

depth and size = $O(\log^2 N)$

Classical circuit

Quantum circuit

Classical circuit

Cleve, Watrous’00

(low-depth QFT)

<u>depth</u> = $O(\log\log N)$, size = $O(\log^5 N)$

Classical circuit

Quantum circuit

Classical circuit

Regev’23

depth = $O(\log^{3/2} N)$, **<u>size</u>** = $O(\log^{3/2} N)$

Classical circuit

Quantum circuit

Classical circuit

Quantum circuit

“NISQ-ier” algorithms for Search/Collision?

Search with constant-depth quantum sub circuits + $\sqrt{N}$ queries?

Search with $o\left(\sqrt{N}\right)$-depth quantum sub circuits + $o\left(N\right)$ queries?

Search with 1 quantum query + $\sqrt{N}$ classical queries?

Search with $o\left(\sqrt{N}\right)$ quantum query + $o(N)$ classical queries?

… and for Collision?

Main results

1/ No quantum speedups for Search and Collision problems in NISQ models

2/ Tight characterization of optimal speedups for Search and Collision in all “super-NISQ” models

For all $0 \leq d \leq \infty$

3/ New framework for analyzing NISQ complexity

Previous work on Search:
[Sun, Zheng’19] (model 1), [Chen, Cotler, Huang, Li’22] (model 1),
[Rosmanis’22] (model 2), [Rosmanis’23] (model 1)

Relaxations of NISQ models

First relaxation: query complexity

Idea: focus the analysis on oracle gates only

Motivations:

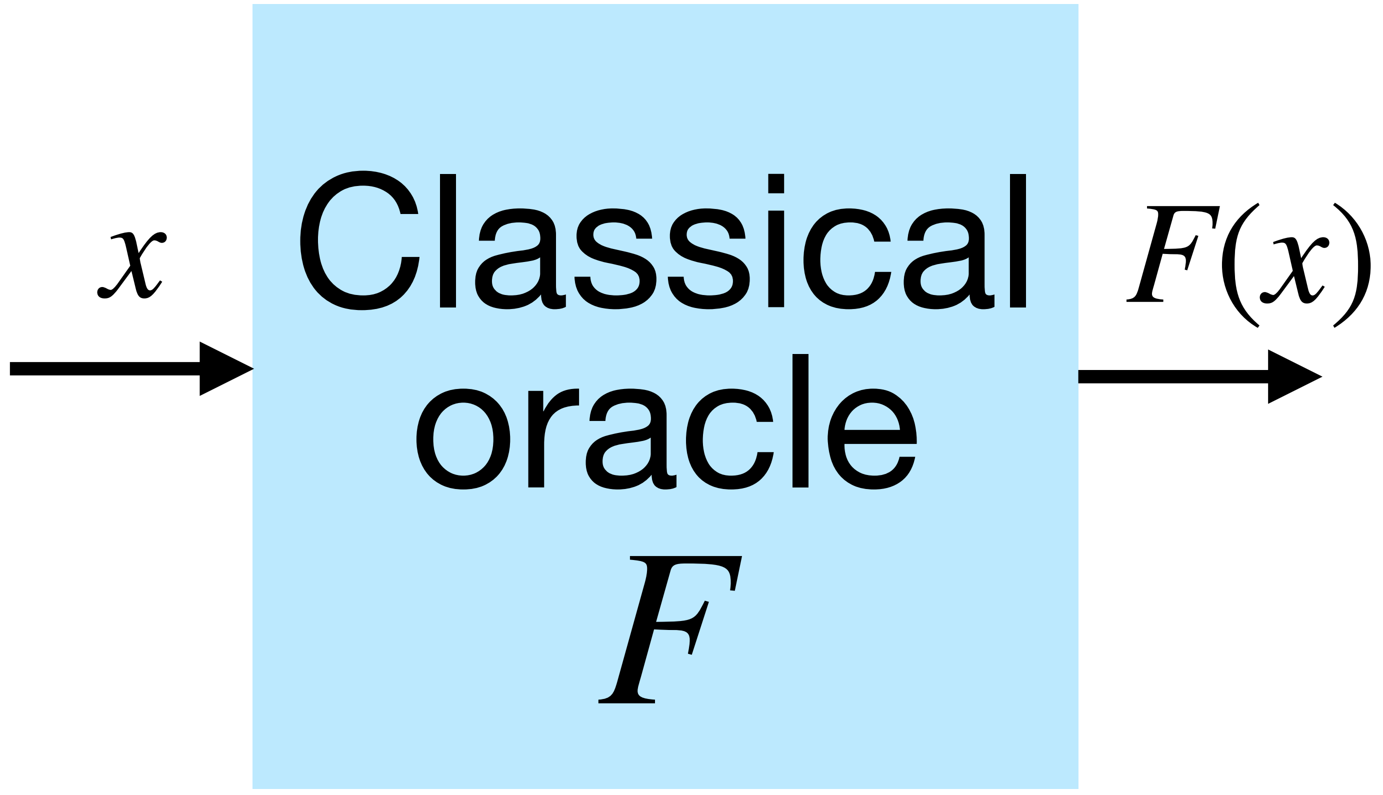
- Often the most time-consuming part of the circuit
- Toy model for analyzing crypto. protocols that require hash functions (random oracle model)
- Efficient lower bound methods on number of oracle gates (= query complexity)

First relaxation: query complexity

The input is represented as a (random) function

$F(0)$	$F(1)$		$\cdots$			$F(N-1)$
4	3	0	6	3	2	1

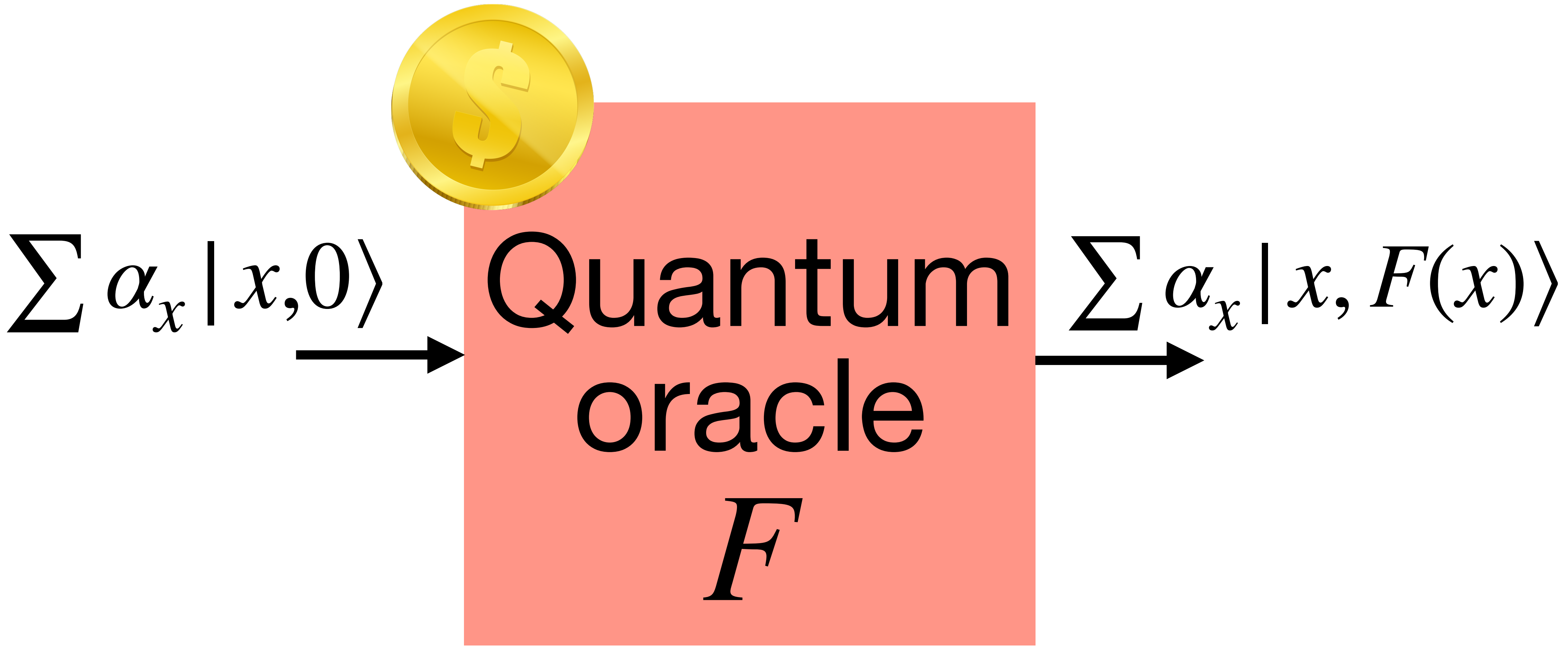
$F : [N] \rightarrow [N]$ accessible via an oracle (= query operator)



x

Classical oracle F

$F(x)$



$\sum \alpha_x | x,0 \rangle$

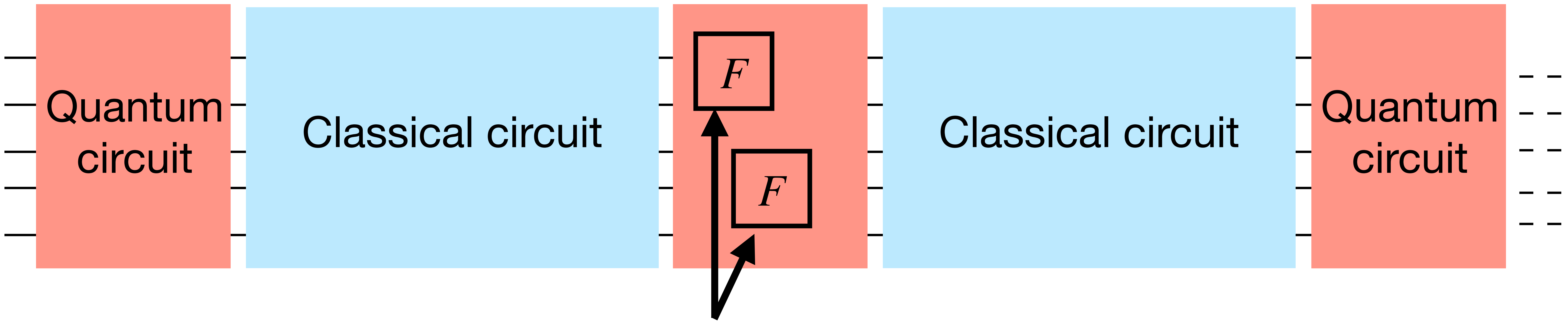
Quantum oracle F

$\sum \alpha_x | x, F(x) \rangle$

First relaxation: query complexity

Model 1

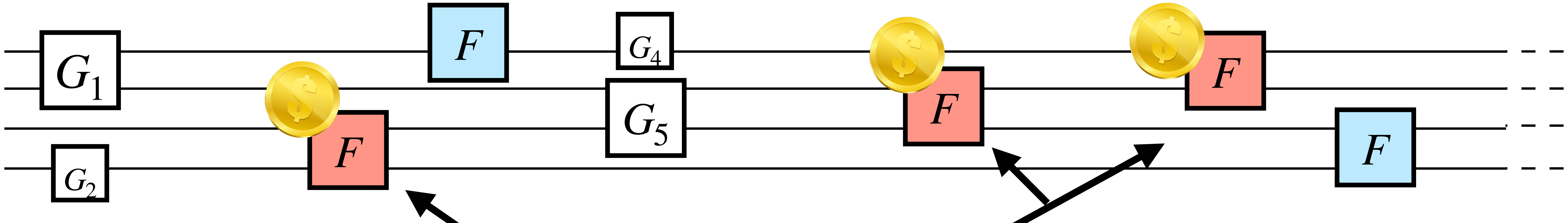
Shallow quantum circuits



number of quantum oracle gates $\leq d$

Model 2

Costly gates



number of quantum oracle gates $\leq d$

Second relaxation: dephasing noise

Idea: substitute the depth constraint (model 1) with dephasing noise

Motivations:

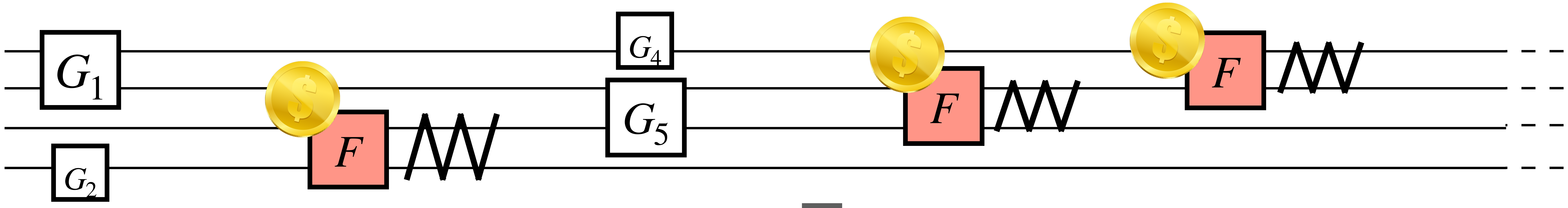
- Local decoherence is easier to analyze than global decoherence
- Dephasing noise commutes with quantum oracle gates

Second relaxation: dephasing noise

$$\rho \xmapsto{\text{W}} \varepsilon \sum_i \langle i|\rho|i\rangle\, |i\rangle\langle i| \otimes |0\rangle\langle 0| + (1-\varepsilon)\rho \otimes |1\rangle\langle 1|$$

Model 3

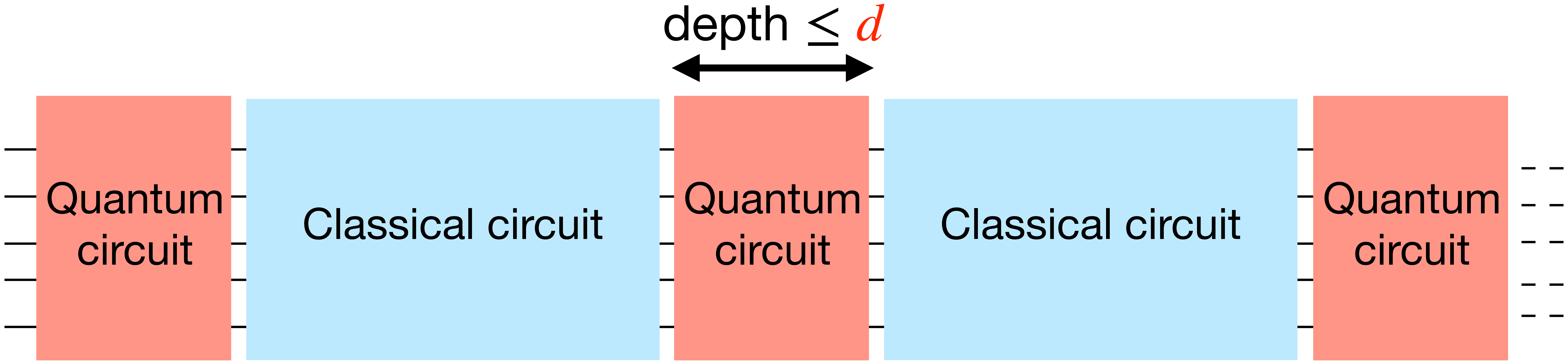
Dephasing noise



Efficient simulation when $\varepsilon \leq 1/d$

Model 1

Shallow quantum circuits


depth $\leq d$

Quantum circuit

Classical circuit

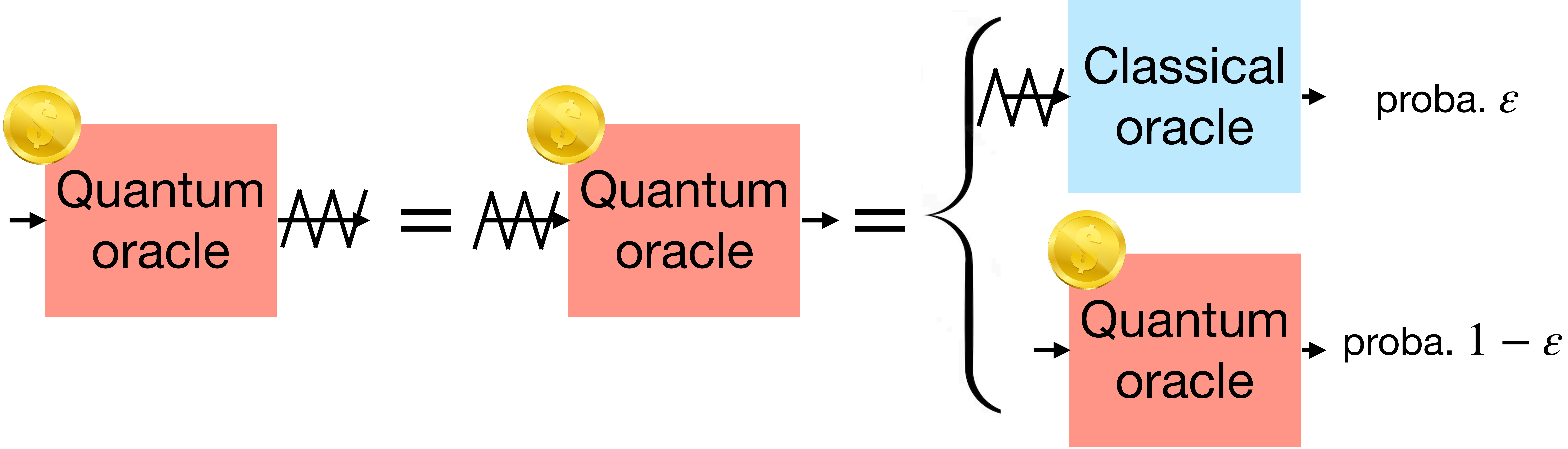
Quantum circuit

Classical circuit

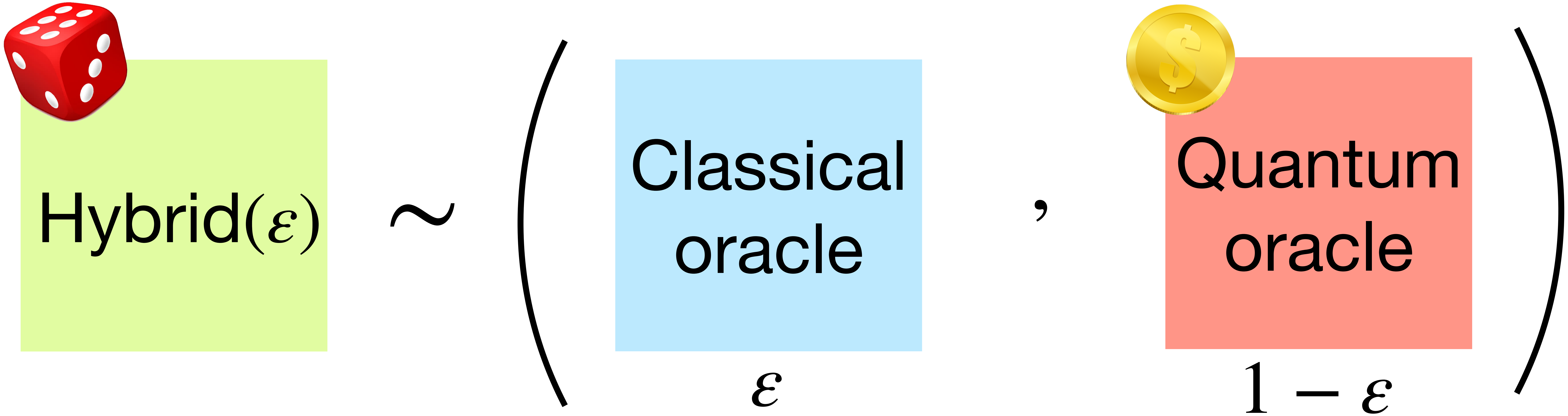
Quantum circuit

Second relaxation: dephasing noise

Observation: depolarizing channel commutes with quantum oracle



Hybrid oracle



Hybrid(ε) $\sim$ (Classical oracle ε , Quantum oracle $1-\varepsilon$)

Equivalently: quantum oracle collapses into classical oracle with proba. ε

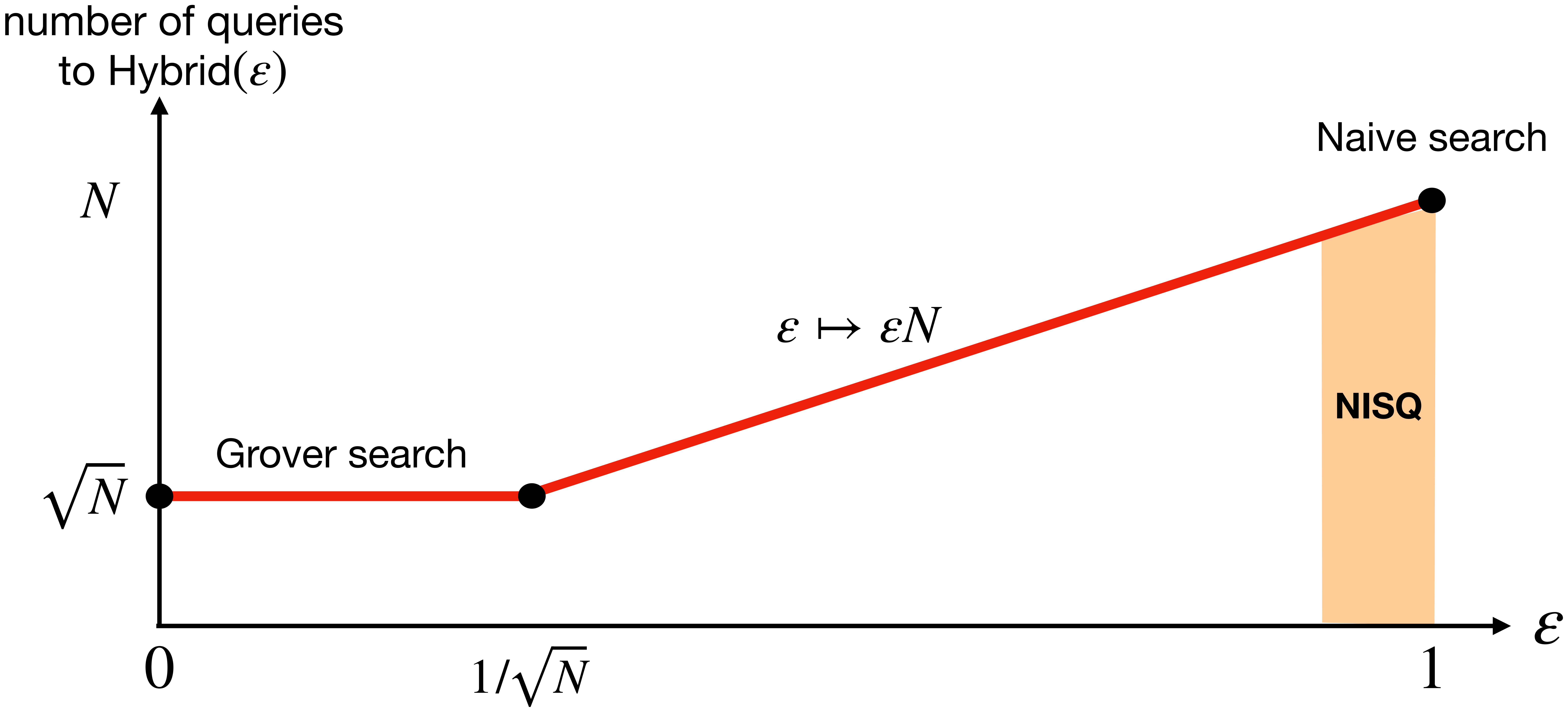
Relaxations: NISQ hardness can be deduced from query complexity with Hybrid(0) + Hybrid(1) (model 2) or Hybrid(ε) (models 1, 3)

Contribution: first generic method for analyzing such combinations of oracles

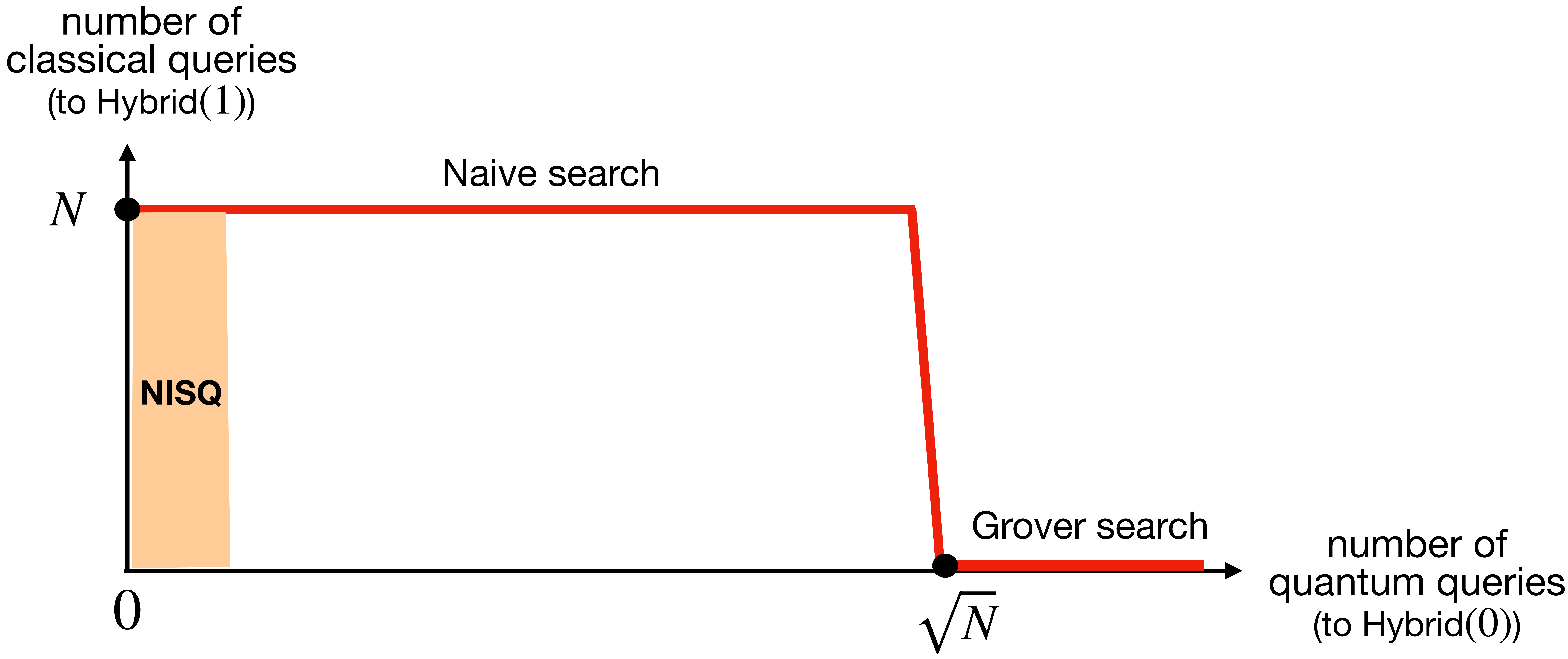
Technical overview:

NISQ hardness of Search

Find x such that $F(x) = 0$
when $F : [N] \to [N]$ is random



Find x such that $F(x) = 0$
when $F : [N] \to [N]$ is random



Classical transcript $(\varepsilon = 1)$

x_1	$F(x_1)$
x_2	$F(x_2)$
x_3	$F(x_3)$
…	

List of (query, answer)
made by a classical algorithm

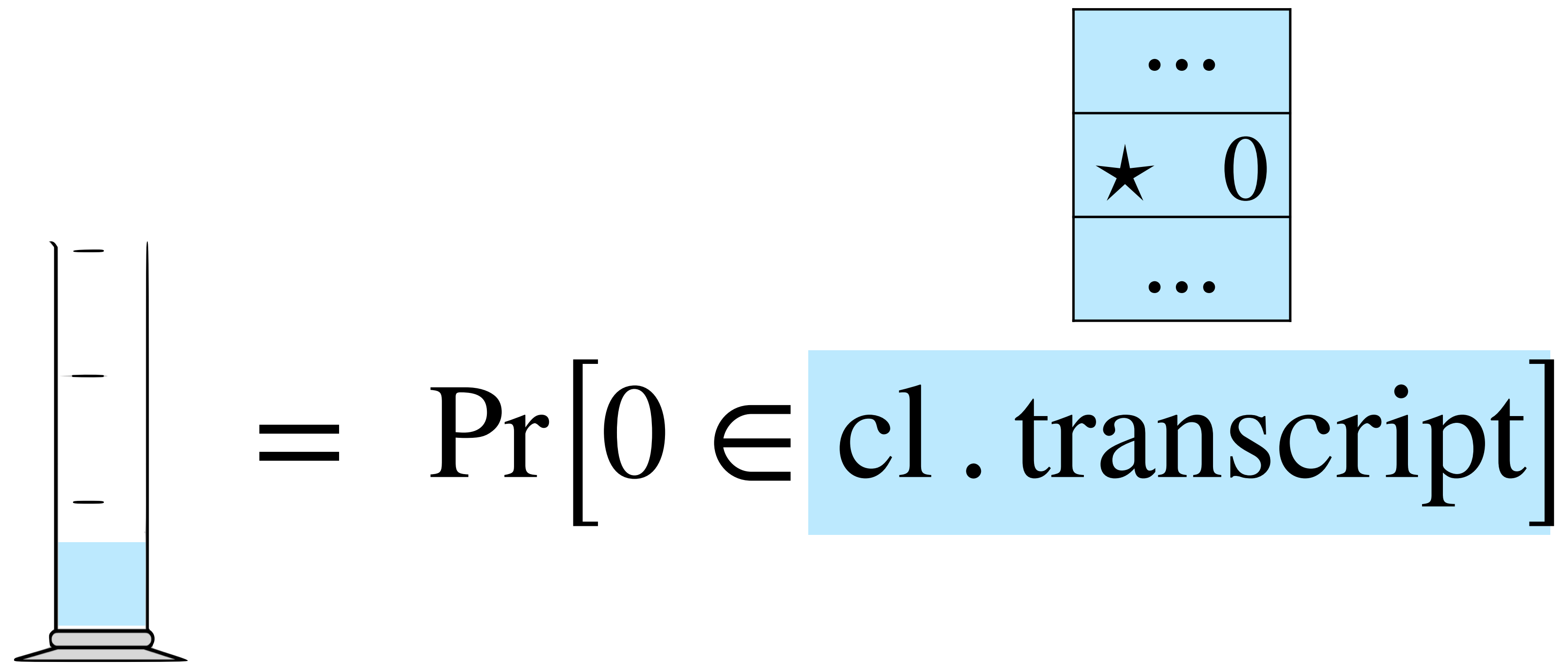
Conditioning on the transcript state

Ex: $\Pr\left[F(x) = 0 \,|\, \text{transcript}\right] =$

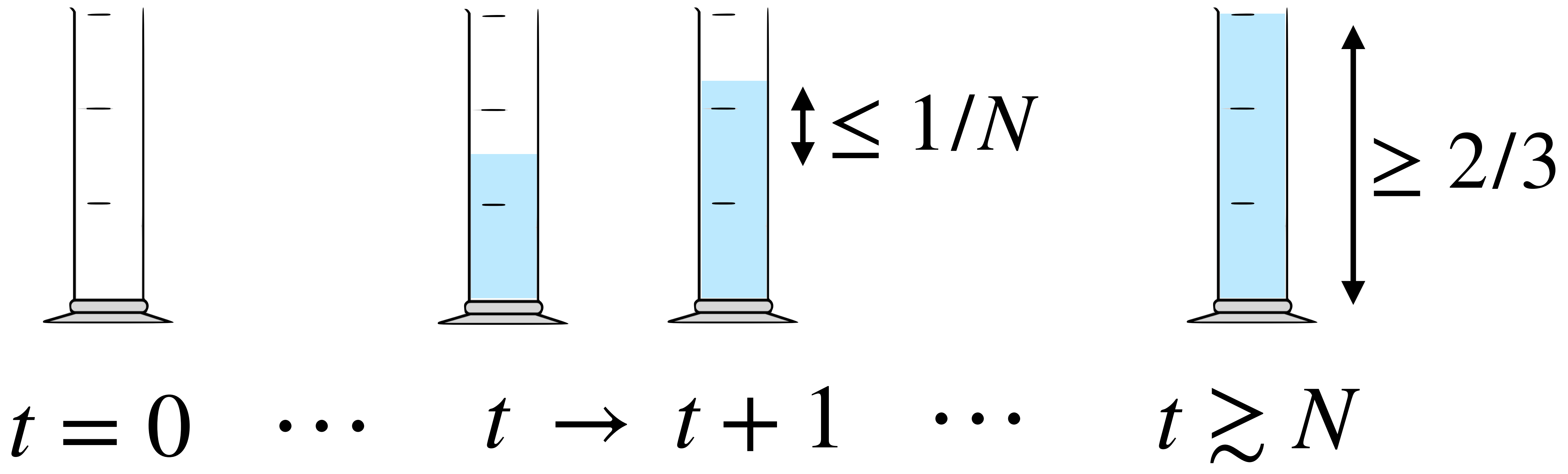
$$\begin{cases} 1 & \text{if } (x, 0) \in \text{transcript} \\ 0 & \text{if } (x, y) \in \text{transcript and } y \neq 0 \\ 1/N & \text{otherwise} \end{cases}$$

$(\varepsilon = 1)$

Classical lower bound



$$= \Pr\left[0 \in \mathrm{cl\,.\,transcript}\right]$$



$(\varepsilon = 0)$

Quantum lower bound

Quantum transcript?

Quantum transcript $(\varepsilon = 0)$

[Zhandry'19]

Step 1: purify the input F

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

Quantum transcript

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

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

$F(x)$ looks random to the algorithm

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

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

Quantum transcript $(\varepsilon = 0)$

Initial state: $|0\rangle \otimes \frac{1}{N^{N/2}} \sum_F \left| \begin{array}{|c|}\hline F(0) \\ \hline F(1) \\ \hline F(2) \\ \hline \cdots \\ \hline F(N-1) \\ \hline \end{array} \right\rangle \xmapsto{\text{Compress}} |0\rangle \otimes \left| \begin{array}{|c|}\hline \varnothing \\ \hline \varnothing \\ \hline \varnothing \\ \hline \cdots \\ \hline \varnothing \\ \hline \end{array} \right\rangle$

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 $\neq \varnothing$

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

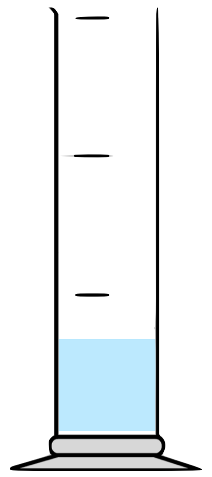
(Oracle basis) *(Transcript basis)*

($\varnothing$ = unif. distribution)

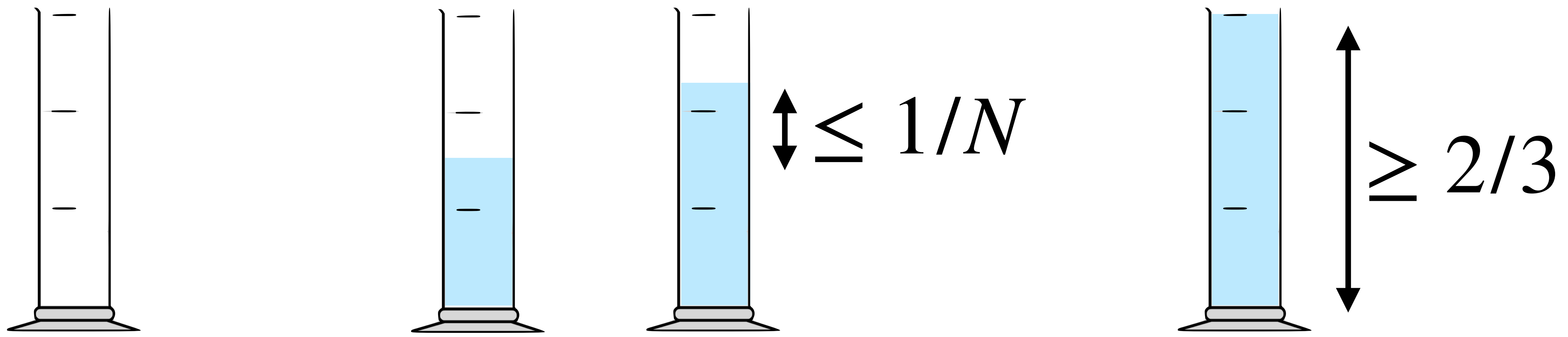
$(\varepsilon = 1)$

Classical lower bound

…
★ 0
…



$= \Pr[0 \in \mathrm{cl\,.\,transcript}]$

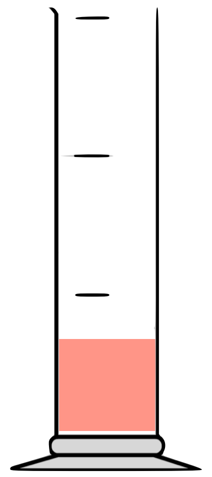


$t = 0 \quad \cdots \quad t \;\to\; t+1 \quad \cdots \quad t \gtrsim N$

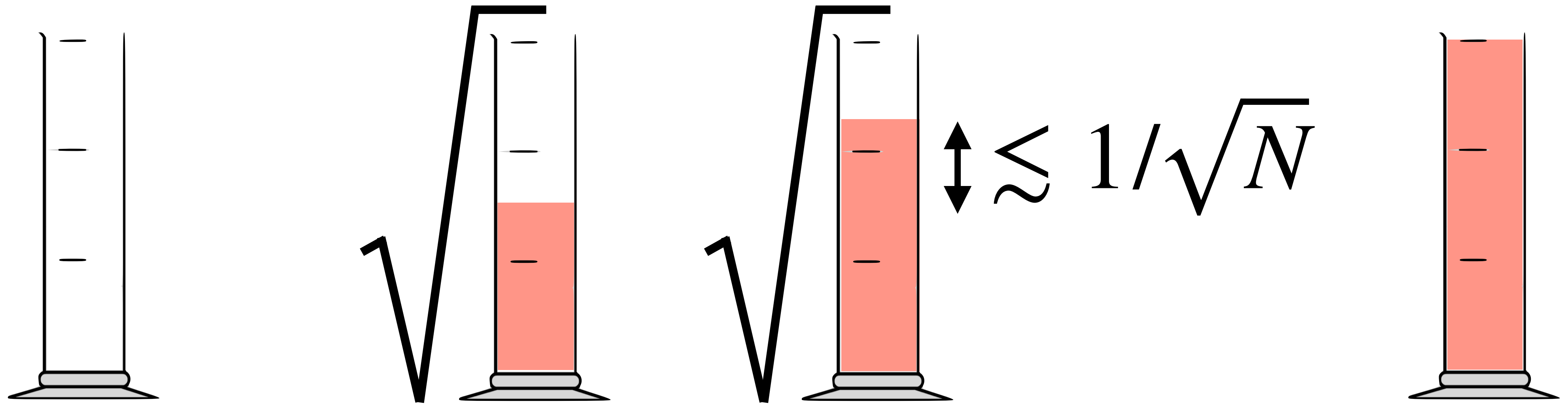
$(\varepsilon = 0)$

Quantum lower bound

…
0
…



$= \Pr[0 \in \mathrm{qu\,.\,transcript}]$



$t = 0 \quad \cdots \quad t \;\to\; t+1 \quad \cdots \quad t \gtrsim \sqrt{N}$

Amplitude increase

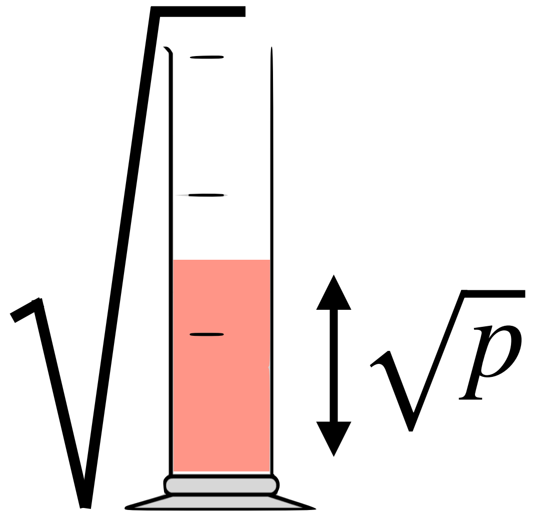
Why is the quantum progress faster?

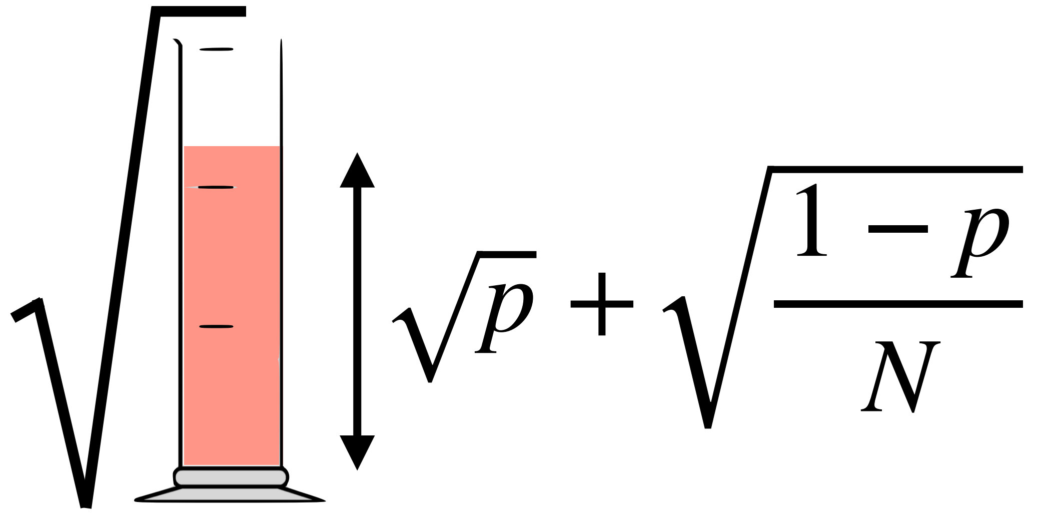
Transcript interference:

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

Quantum query x

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





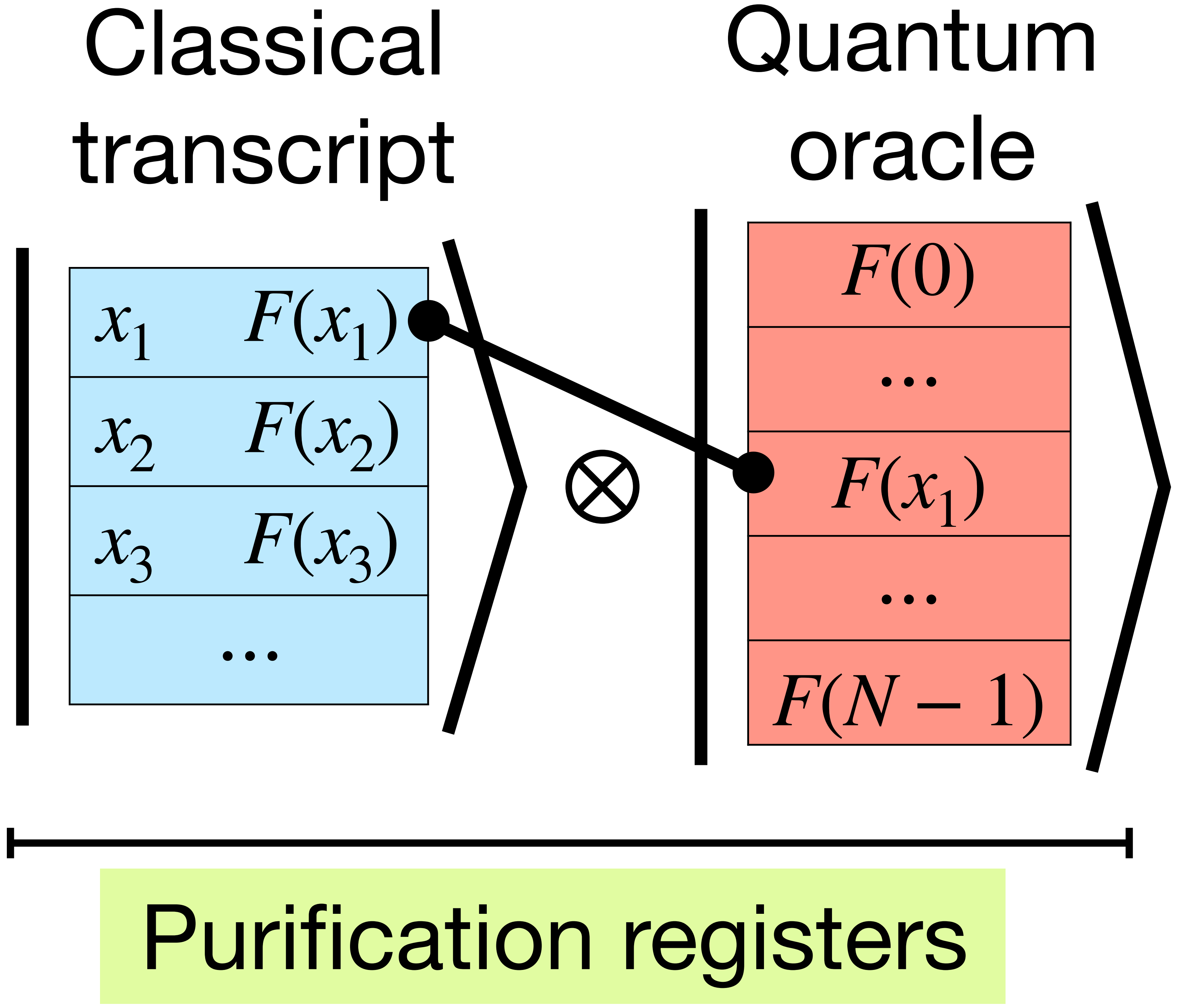
No such phenomenon for classical transcript (*time-stamped recording*)

Hybrid transcript

$(0 \leq \varepsilon \leq 1)$

Step 1:

$$\sum \alpha_{x,u,F,x_1,x_2,\ldots} |x, u\rangle \otimes$$



Classical transcript

Quantum oracle

x_1 $F(x_1)$

x_2 $F(x_2)$

x_3 $F(x_3)$

$\ldots$

$\otimes$

$F(0)$

$\ldots$

$F(x_1)$

$\ldots$

$F(N-1)$

Purification registers

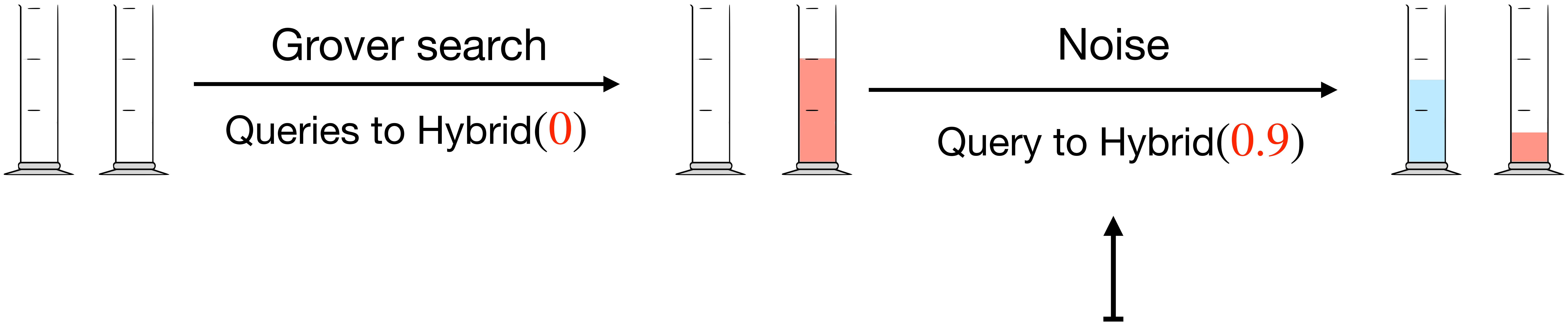
Step 2: compress $\frac{1}{\sqrt{N}} \sum_y |F(x) = y\rangle \mapsto |D(x) = \emptyset\rangle$ if $(x, \cdot\,) \notin$ cl . transcript

$|F(x) = y\rangle \mapsto |D(x) = \emptyset\rangle$ if $(x, y) \in$ cl . transcript

Hybrid lower bound

Classical-Quantum progress:

Example:



Grover search

Queries to Hybrid(0)

Noise

Query to Hybrid(0.9)

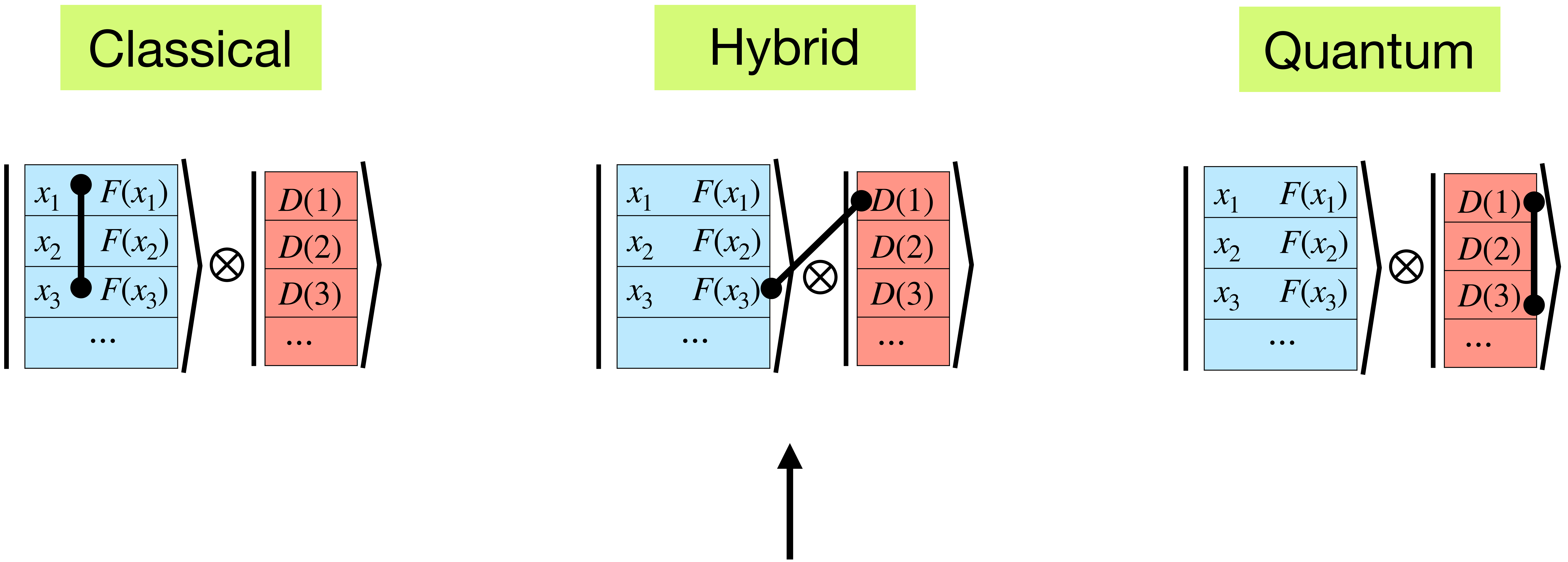
Classical progress increases

… but interference effects are lost

	Classical query $t \longrightarrow t+1$	Quantum query $t \longrightarrow t+1$	Hybrid(ε) query $t \longrightarrow t+1$
$\Pr\left[0 \in \mathrm{cl.transcript}\right]$	$\leq 2h$ $\lesssim \frac{1}{N}$	$=$	$\leq 2\varepsilon h$ $\lesssim \frac{\varepsilon}{N}$
$\Pr\left[0 \in \mathrm{qu.transcript}\right]$	$\geq$ $-h$	$\lesssim \sqrt{\frac{h}{N}} + \frac{1}{N}$	$\lesssim -\varepsilon h + (1-\varepsilon)\sqrt{\frac{h}{N}} + \frac{(1-\varepsilon)}{N}$
$= \quad + 3$			$\lesssim \frac{1}{\varepsilon N}$

NISQ hardness of Collision

3 types of collisions



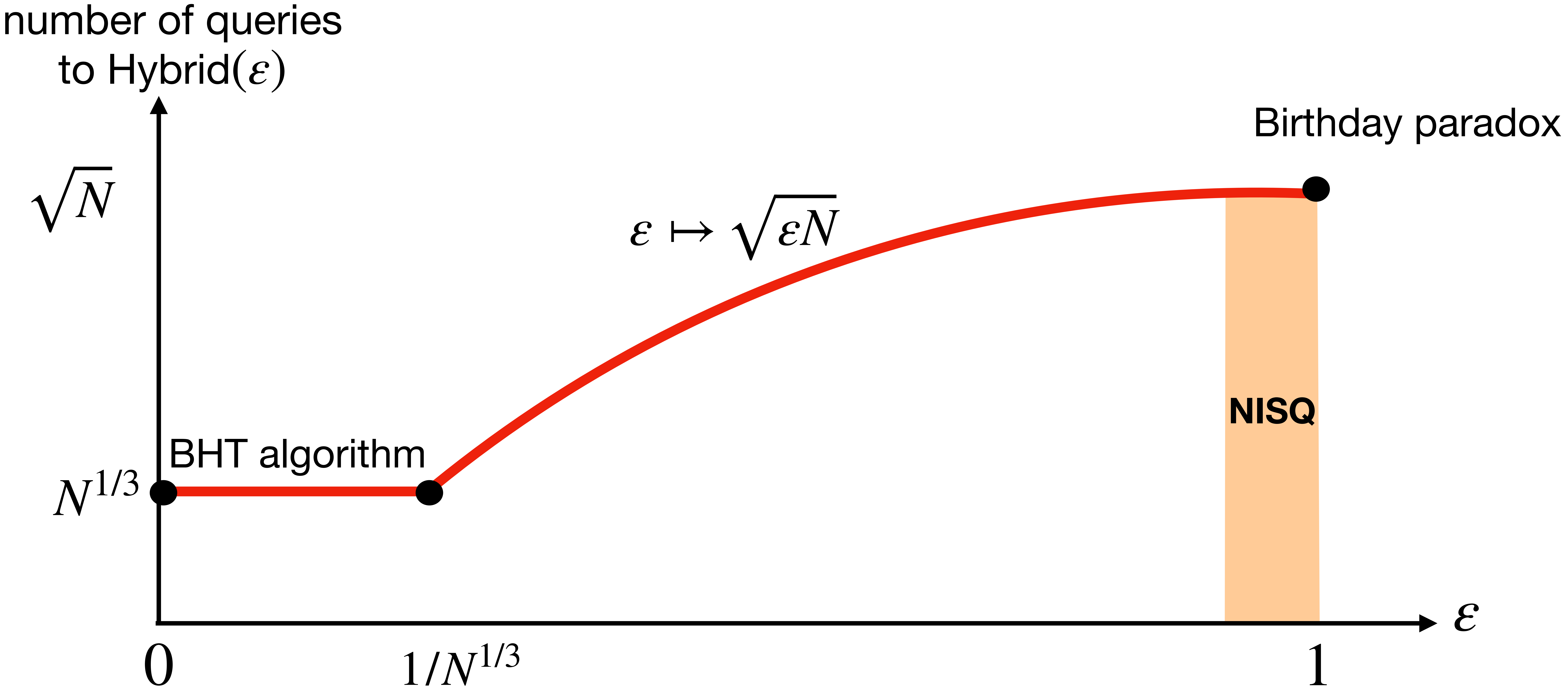
Classical

Hybrid

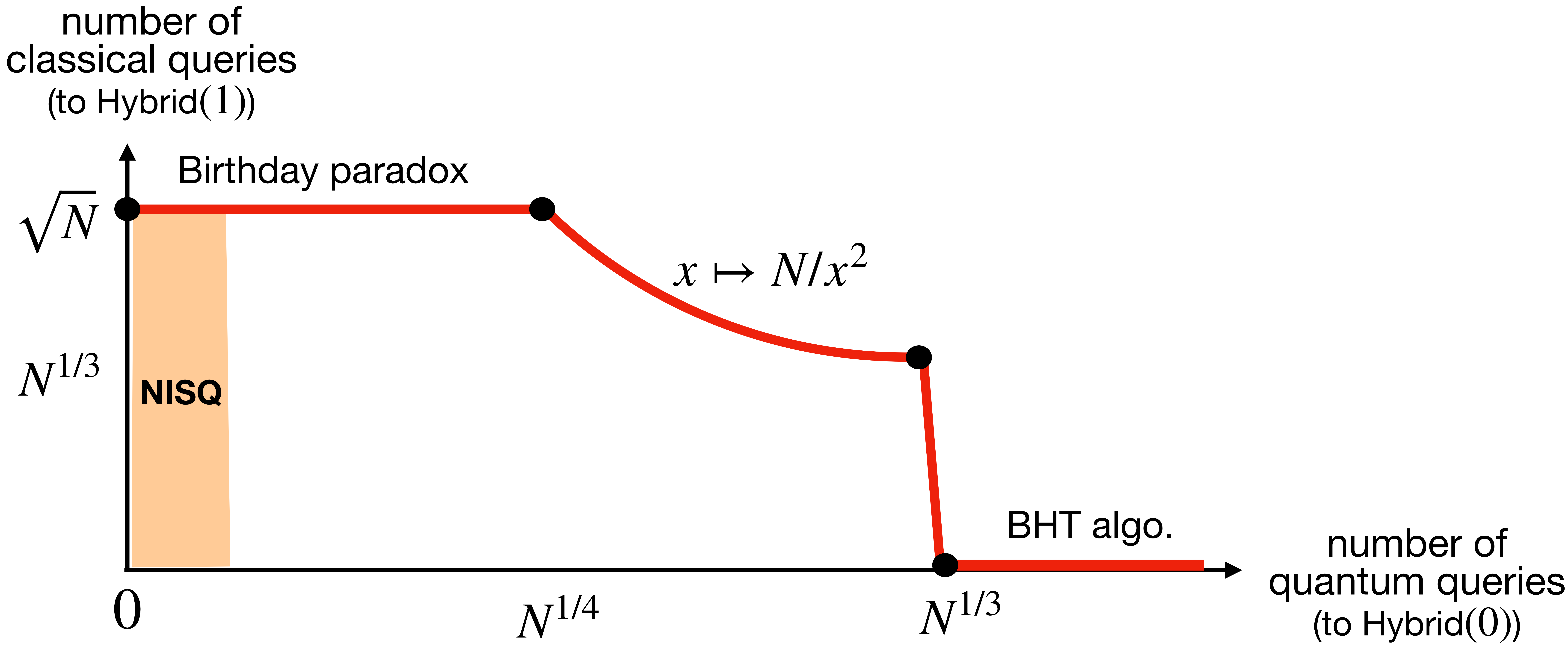
Quantum

Unlike for Search, not all interference effects are lost by classical queries!

Find x, y such that $F(x) = F(y)$ when $F : [N] \to [N]$ is random



Find x, y such that $F(x) = F(y)$ when $F : [N] \to [N]$ is random


number of classical queries (to Hybrid(1))
Birthday paradox
$\sqrt{N}$
$N^{1/3}$
NISQ
$x \mapsto N/x^2$
BHT algo.
$N^{1/4}$
$N^{1/3}$
number of quantum queries (to Hybrid(0))