The NISQ Complexity of Collision Finding

Yassine Hamoudi, Qipeng Liu, Makrand Sinha

CNRS, LaBRI UC San Diego U. of Illinois

arXiv:2211.12954

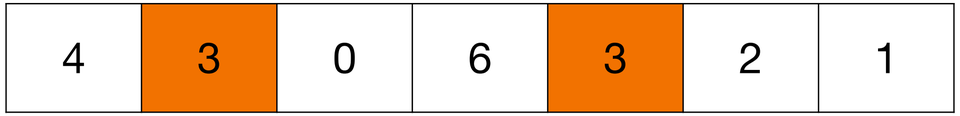
Noisy Intermediate-Scale Quantum

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

Collision finding



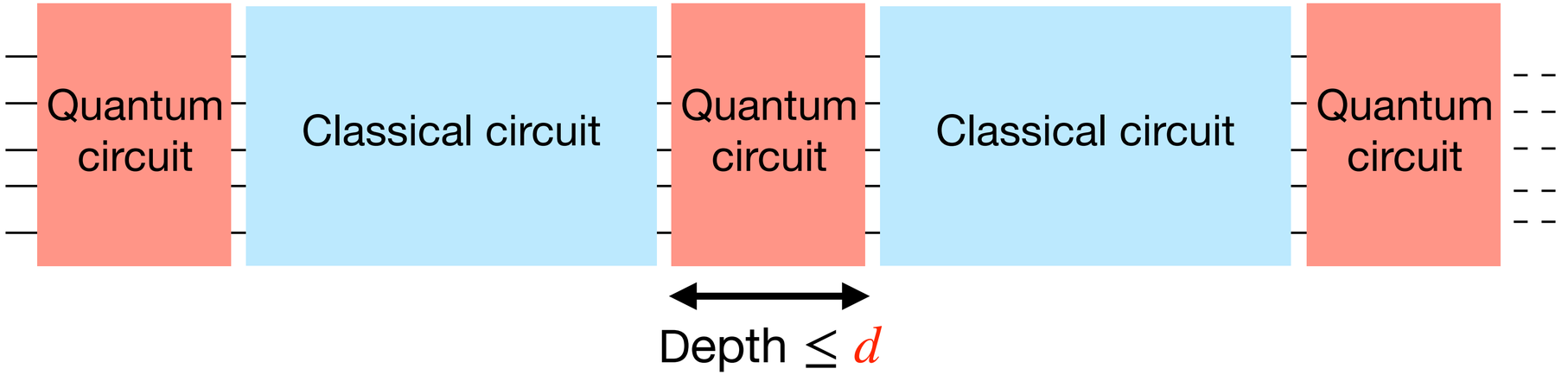
Find x, y *with* $H(x) = H(y)$ *in a function* $H : [N] \to [N]$

- Subroutines of many quantum algorithms and crypto. attacks
- Current speedups (BHT, Ambainis' quantum walk…) are not NISQ

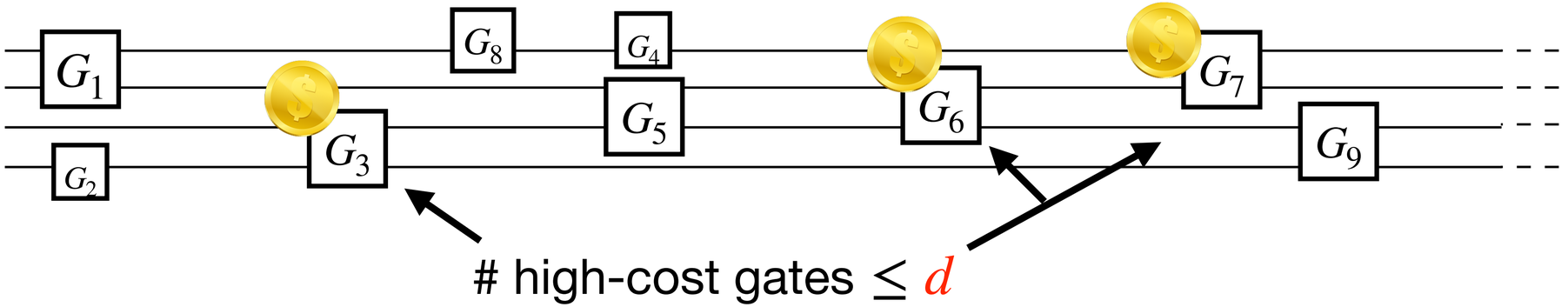
Can we get quantum speedups for Collision finding in NISQ era?

How to model NISQ complexity?

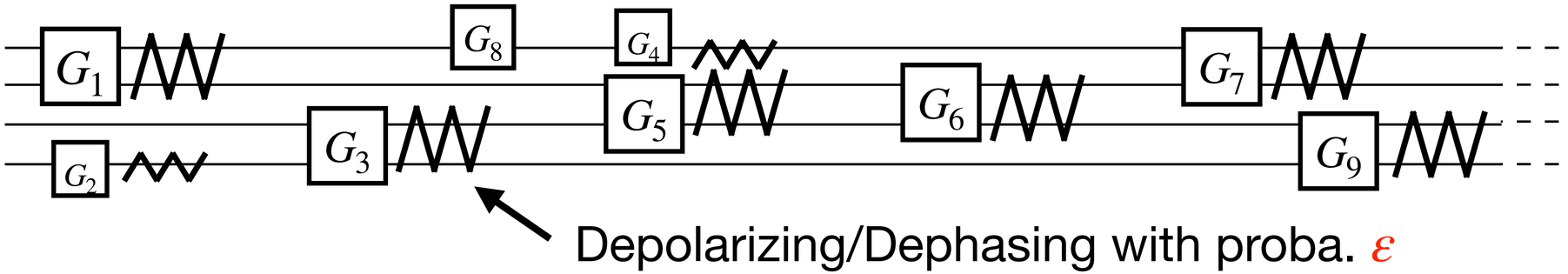
Model 1
Shallow quantum circuits



Model 2
Costly gates

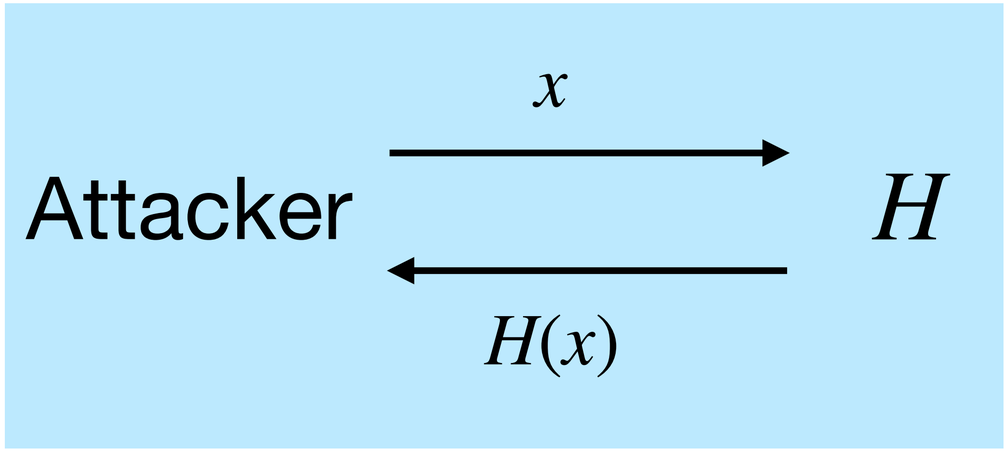


Model 3
Noisy gates

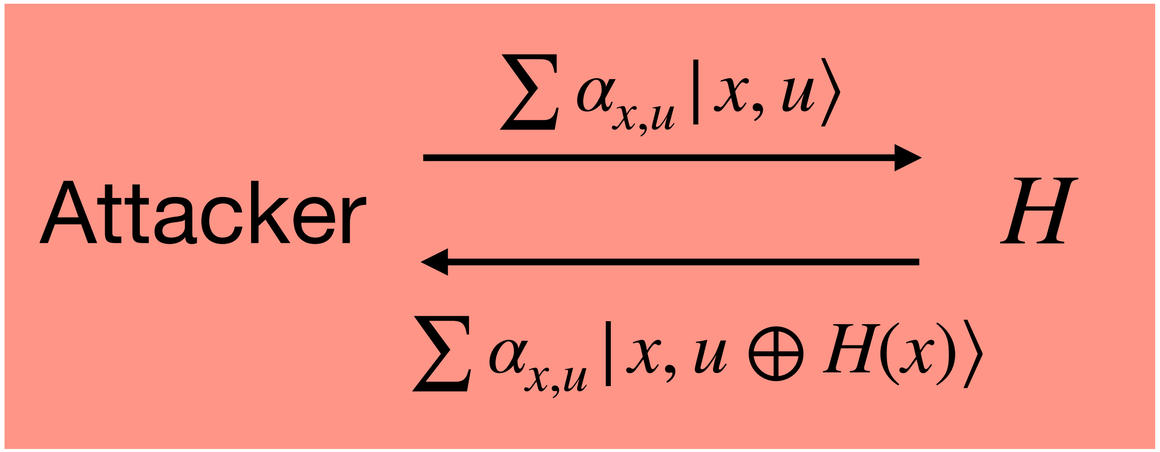


Random oracle model

Classical query



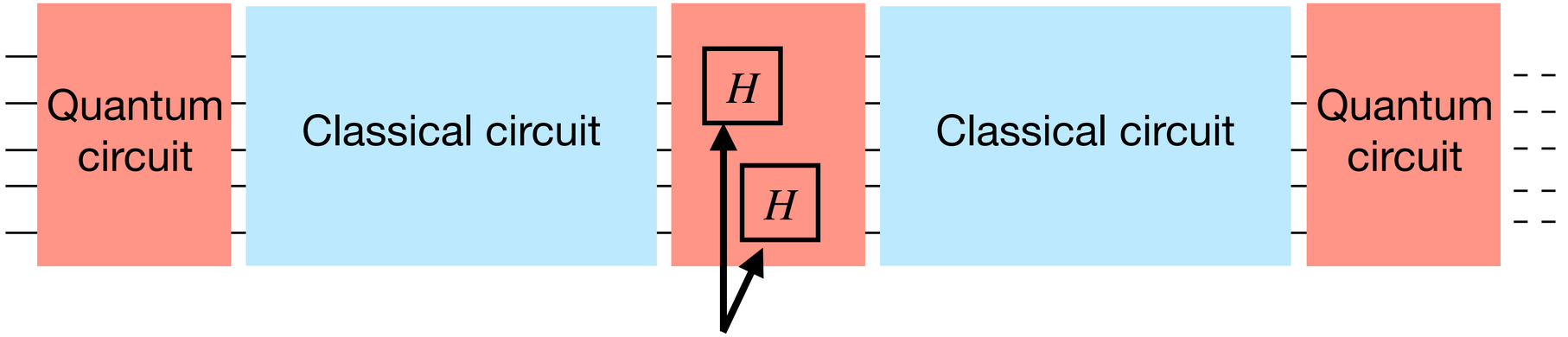
Quantum query



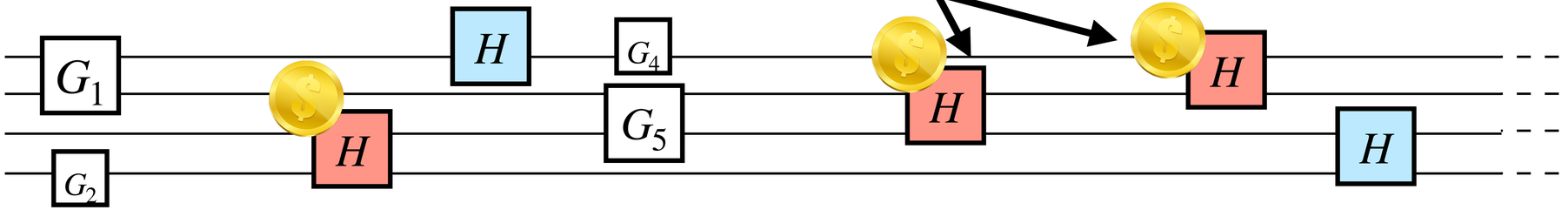
Black-box interface to an “ideal” hash function

- Existing quantum attacks are designed in this model
- Quantum queries are often the most time-consuming part

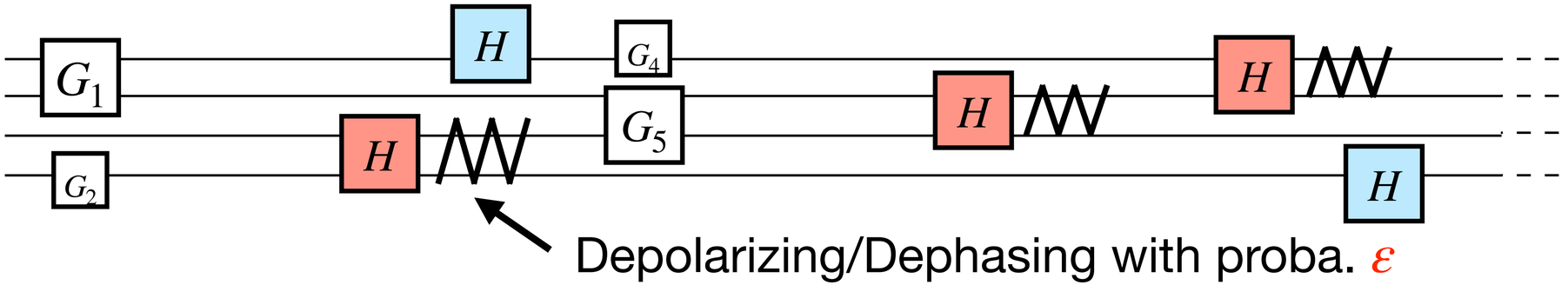
Model 1
Shallow quantum circuits



Model 2
Costly gates



Model 3
Noisy gates



Main results

Main results

1/ No significant speedup for Collision finding in NISQ models

2/ Tight characterization of optimal speedups in “super-NISQ” models

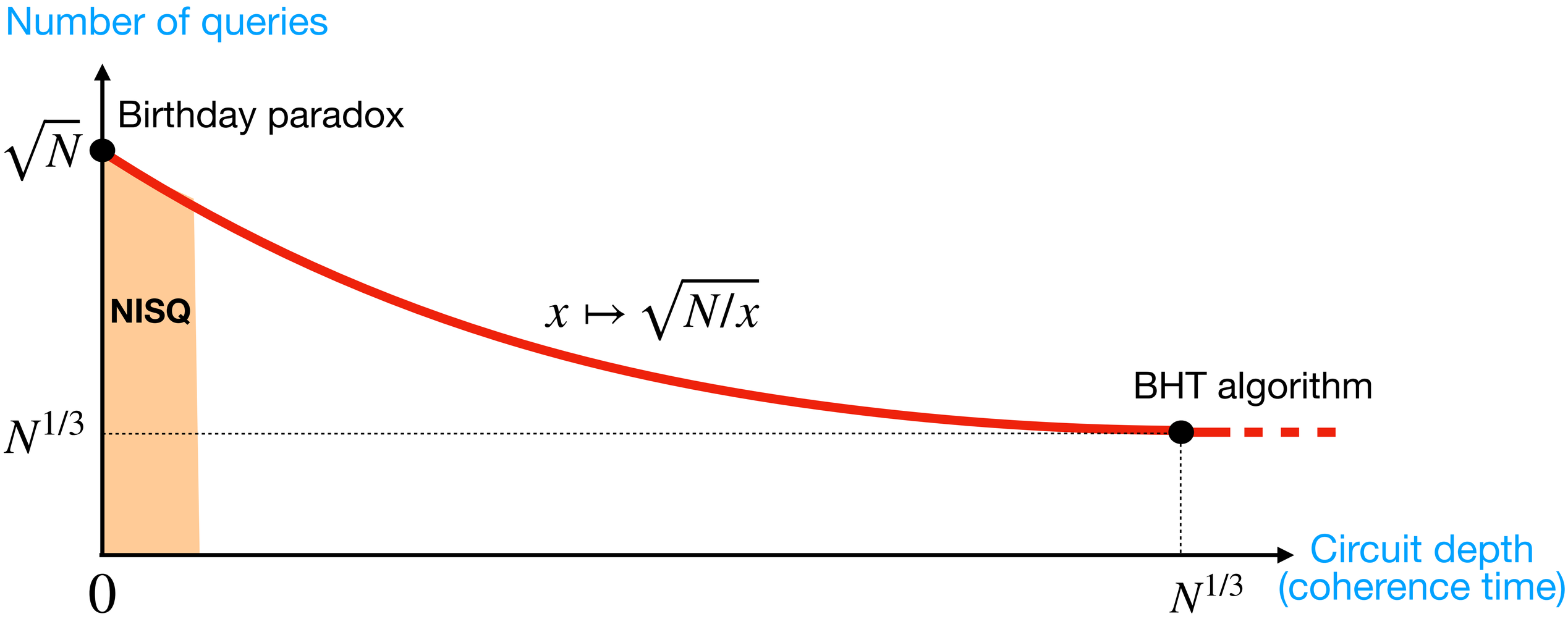
3/ New framework and techniques for analyzing NISQ complexity

4/ Similar results for Preimage search

Extends to QROM: [Sun, Zheng’19], [Chen, Cotler, Huang, Li’22], [Rosmanis’22’23]

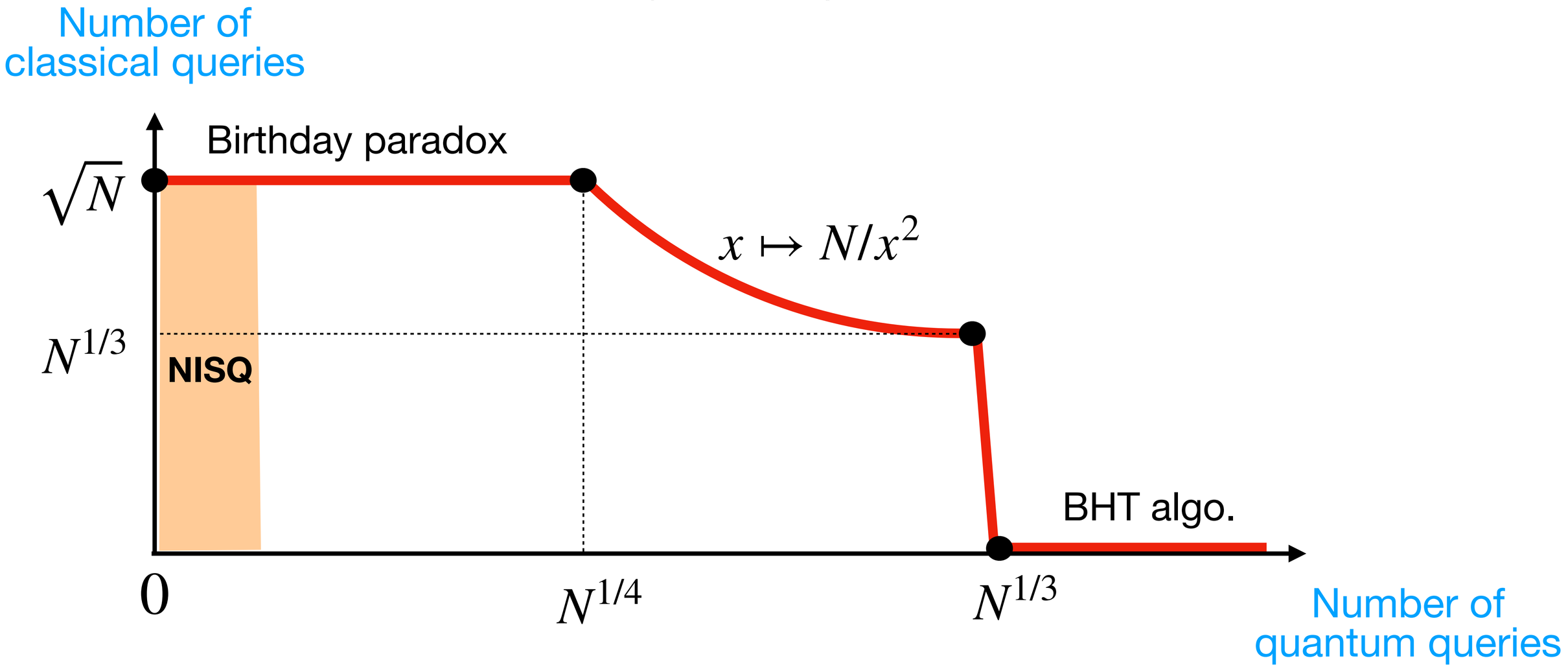
Depth vs Quantum queries

(Model 1)



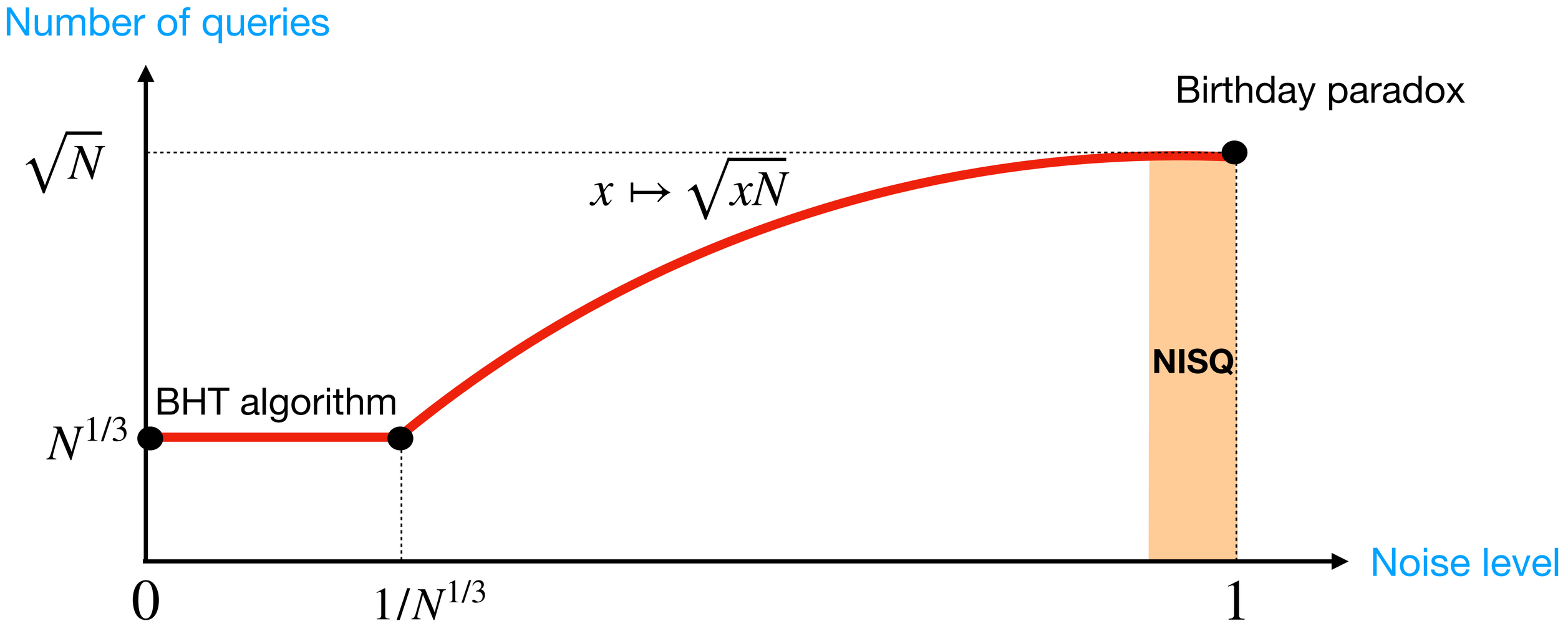
Classical queries vs Quantum queries

(Model 2)



Noise vs Quantum queries

(Model 3)

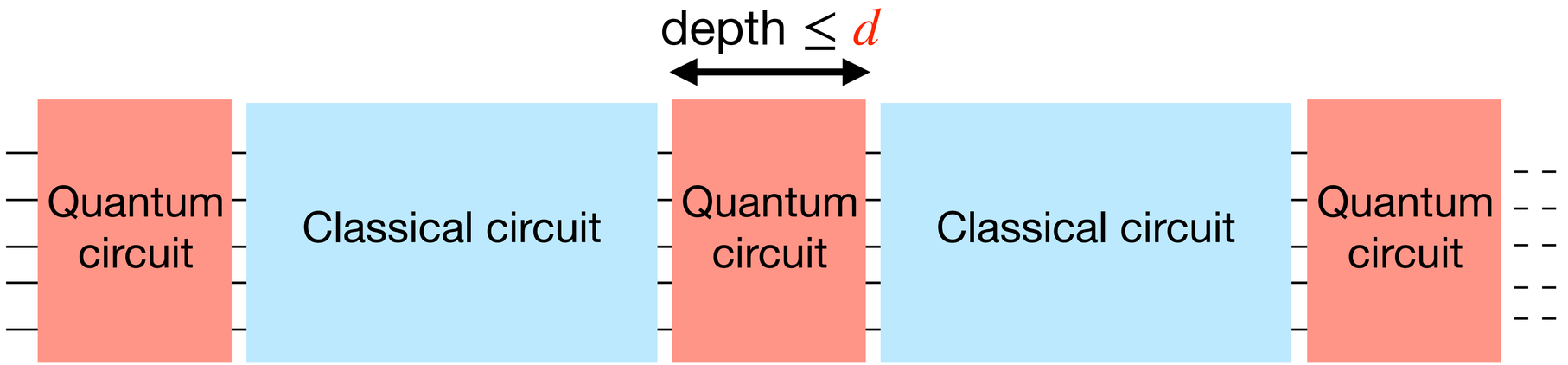


Proof methods

Idea 1: Dropping the depth constraint

Model 1

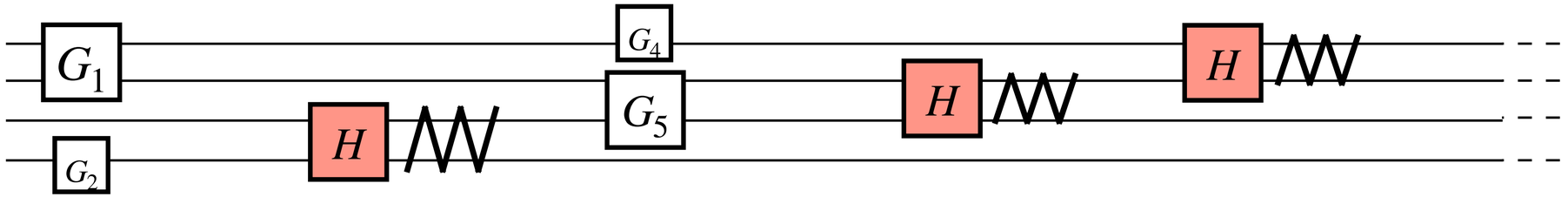
Shallow quantum circuits



Shallow circuits can be simulated if noise $\varepsilon \leq 1/d$

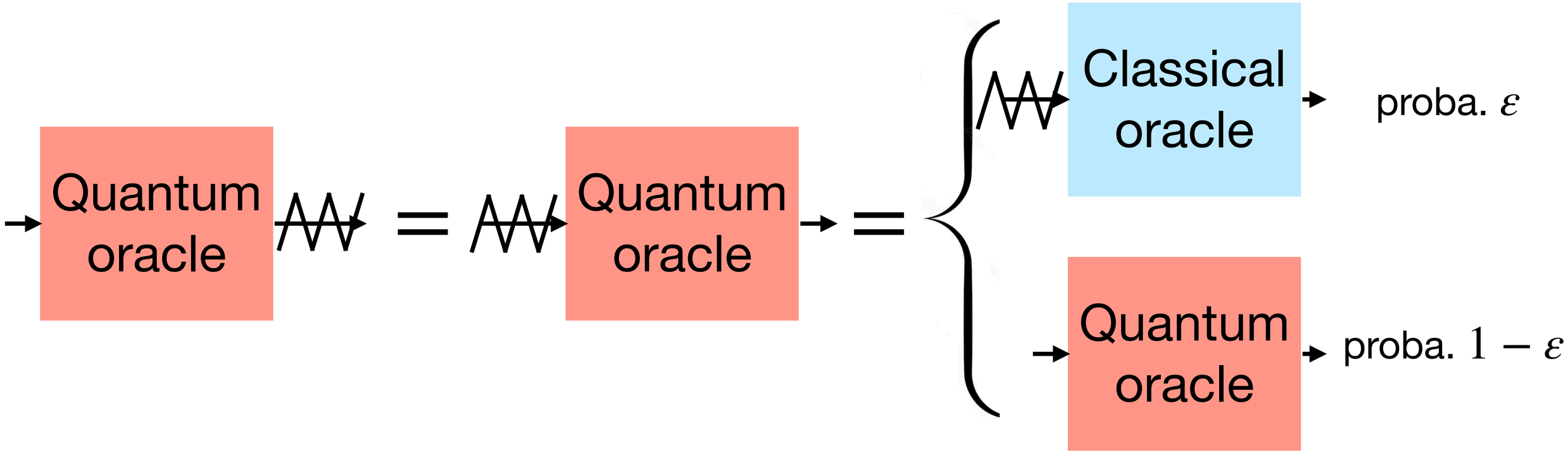
Model 3

Dephasing noise



Idea 2: Hybrid oracles

Observation: (dephasing) noise commutes with quantum oracle



Idea 2: Hybrid oracles

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

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

Idea 3: Hybrid *compressed* oracles

Extend the oracle purification technique of [Zhandry, CRYPTO'19] to hybrid oracles

1/ We devise a way of simultaneously recording classical and quantum queries into a classical-quantum database

2/ We relate the probability of finding a collision to some progress measure on this database