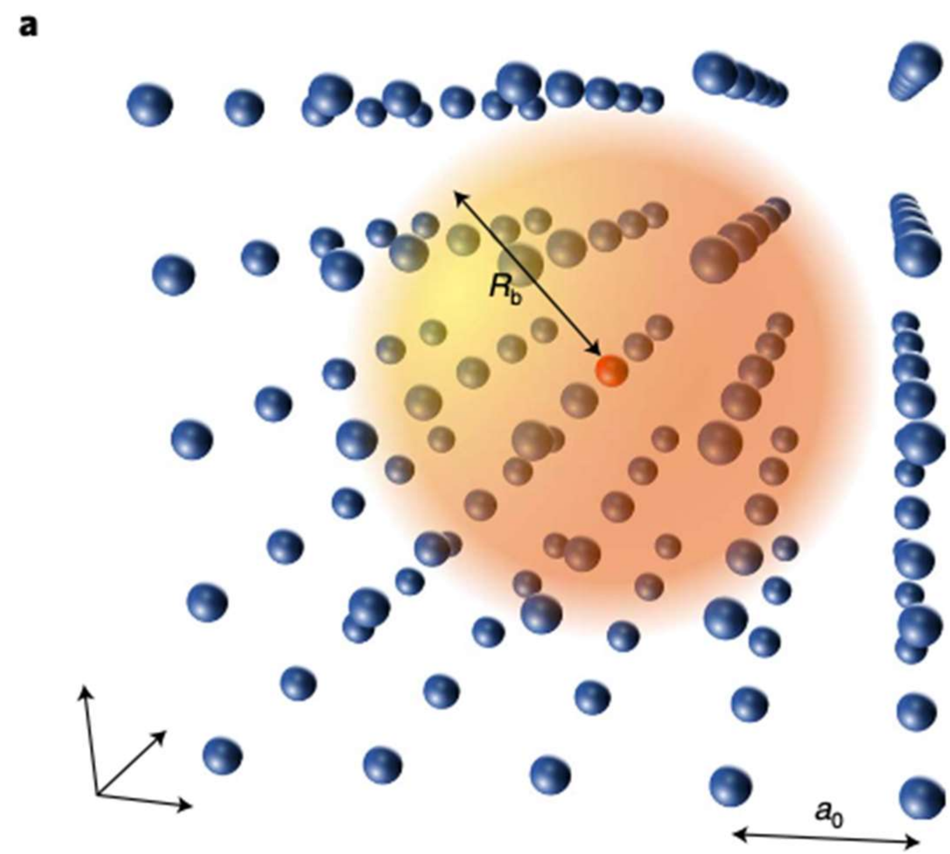
Classically verifiable quantum advantage from a computational Bell test

Group 1:
Aakash, Henry, Jayana & Preethi

https://doi.org/10.1038/s41567-022-01643-7



Background on the Paper and Authors

- Published August 1st, 2022 in *Nature Physics*
- Yao Group at UC Berkeley (Physics and EECS)
- Quantum computing and cryptography

ARTICLES
https://doi.org/10.1038/s41567-022-01643-7
nature physics
Check for updates

OPEN

Classically verifiable quantum advantage from a computational Bell test

Gregory D. Kahanamoku-Meyer[1], Soonwon Choi[1], Umesh V. Vazirani[2] and Norman Y. Yao[1]

What this paper does: an overview

1. This work relies on a class of cryptographic tools called trapdoor claw-free functions
2. Introduces independent innovations that improve the efficiency of algorithm implementation
3. Combining these results, describes a blueprint for implementing the protocol on Rydberg atom-based quantum devices

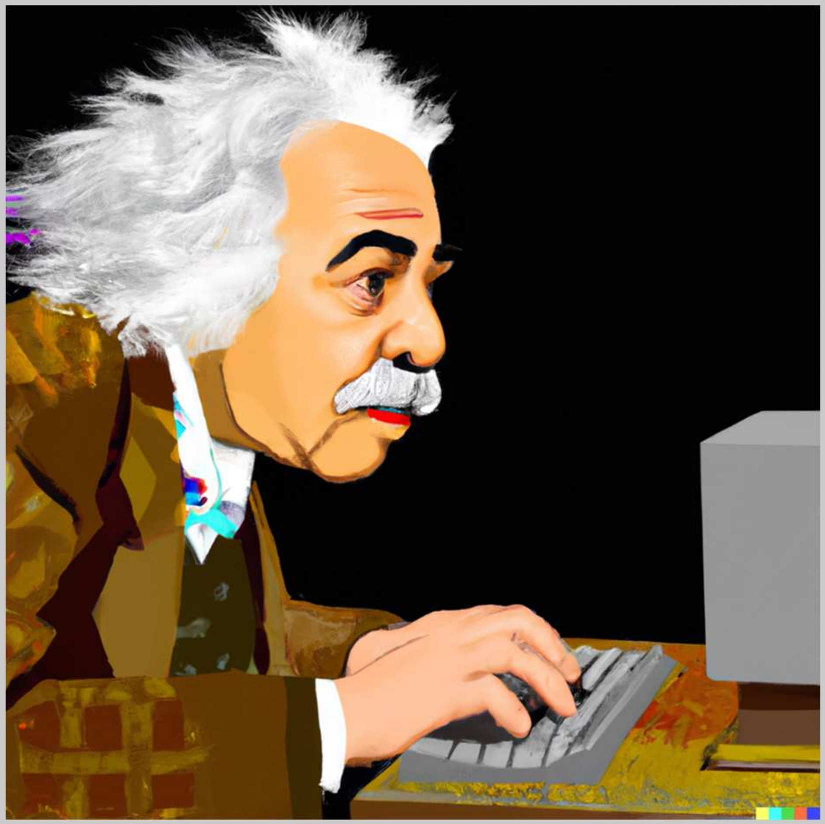


Image Source: DALL-E

Trapdoor Claw-Free Functions (TCF's)

- <u>One-way function:</u> Easy to compute, but hard to invert.
- <u>Trapdoor Function:</u> Hard to invert in general, with the knowledge of some secret data (the trapdoor key) inversion becomes easy.
- <u>Claw-Free:</u> has two inputs that map to each output, but it is computationally hard to implement without the trapdoor.

$$(f, t) = \textbf{Gen}(1^n)$$

$$f : D \rightarrow R$$

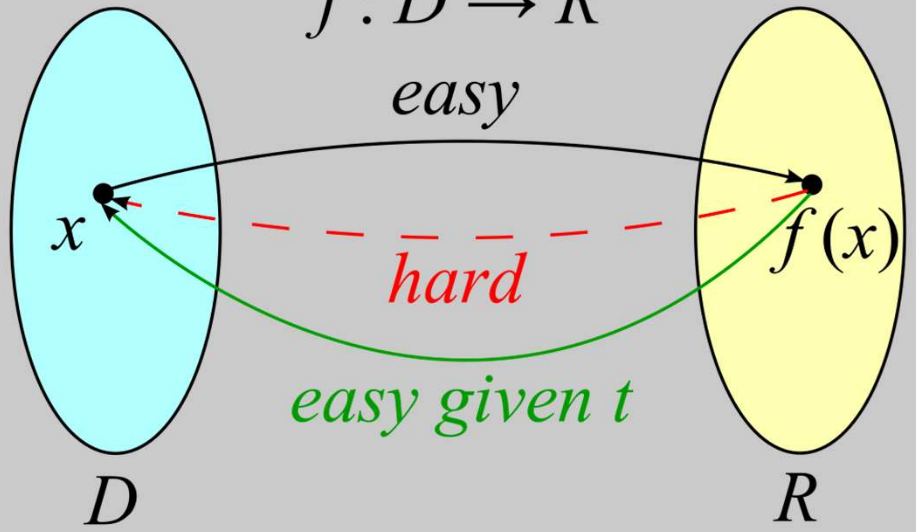
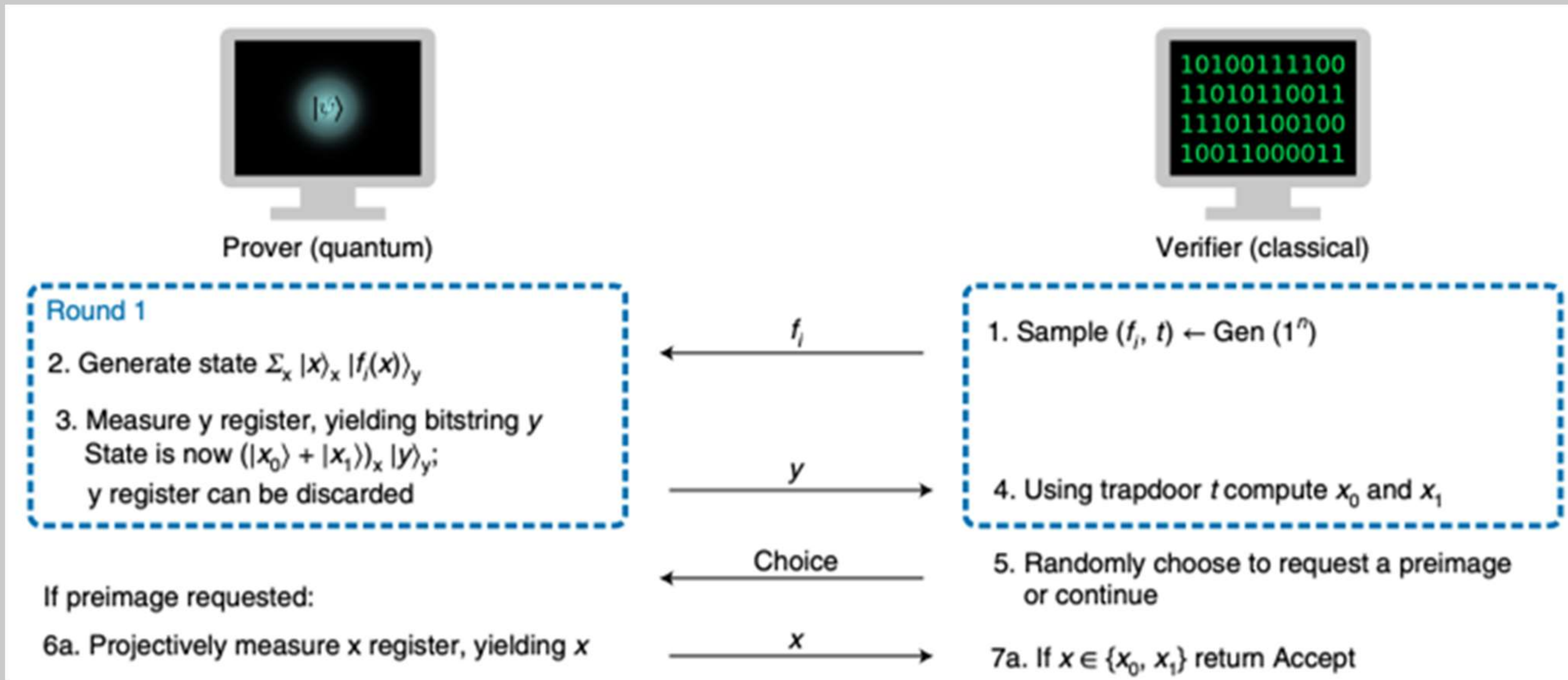
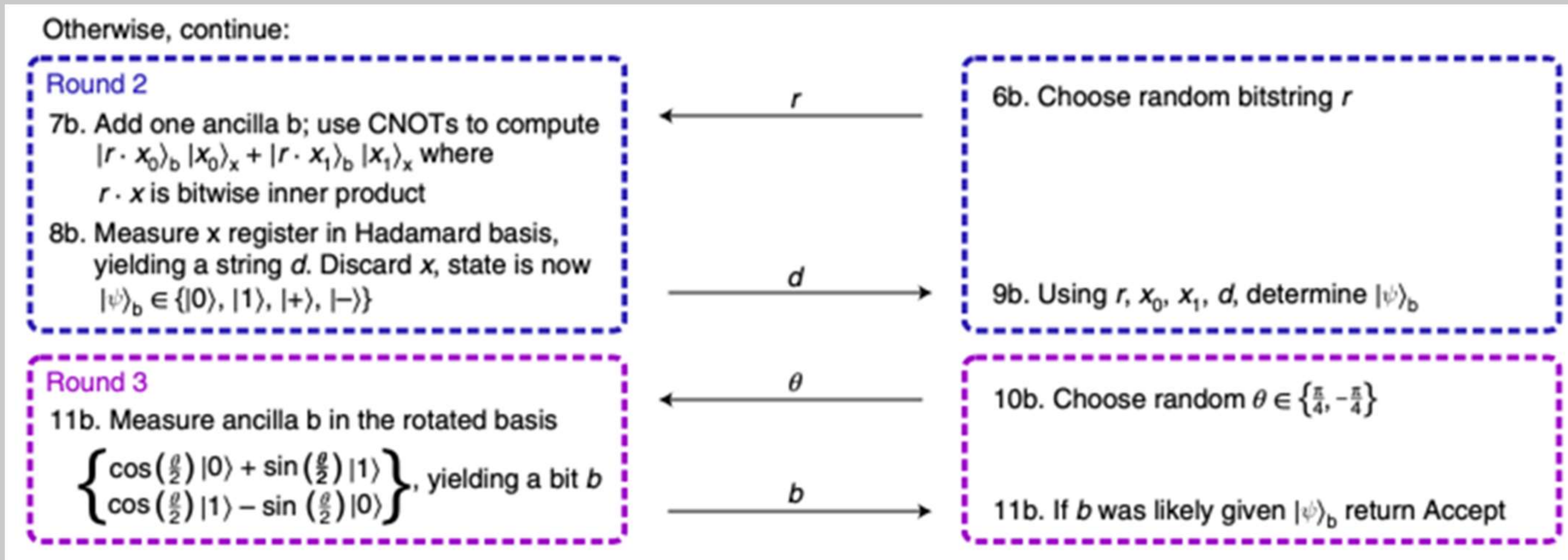


Image sources: DALL-E2, https://en.wikipedia.org/wiki/Trapdoor_function

Protocol - Round 1



Protocol - Rounds 2 and 3



Previous Works : Pioneers in the use of TCF for quantum cryptography tasks

Classical Homomorphic Encryption for Quantum Circuits

Urmila Mahadev*

September 14, 2018

https://doi.org/10.1137/18M1231055

- TCF as a verifier of quantum randomness
- Adaptive hardcore bit

A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device

Zvika Brakerski* Paul Christiano† Urmila Mahadev‡ Umesh Vazirani§ Thomas Vidick¶

https://doi.org/10.1145/3441309

Extension of the use of TCFs with adaptive hardcore bit: arbitrary calculations

Classical Verification of Quantum Computations

Urmila Mahadev*

September 14, 2018

10.1109/FOCS.2018.00033

Random Oracle Model - Non TCF-based proof

Simpler Proofs of Quantumness

Zvika Brakerski
Weizmann Institute of Science
zvika.brakerski@weizmann.ac.il*

Venkata Koppula
Weizmann Institute of Science
venkata.koppula@weizmann.ac.il†

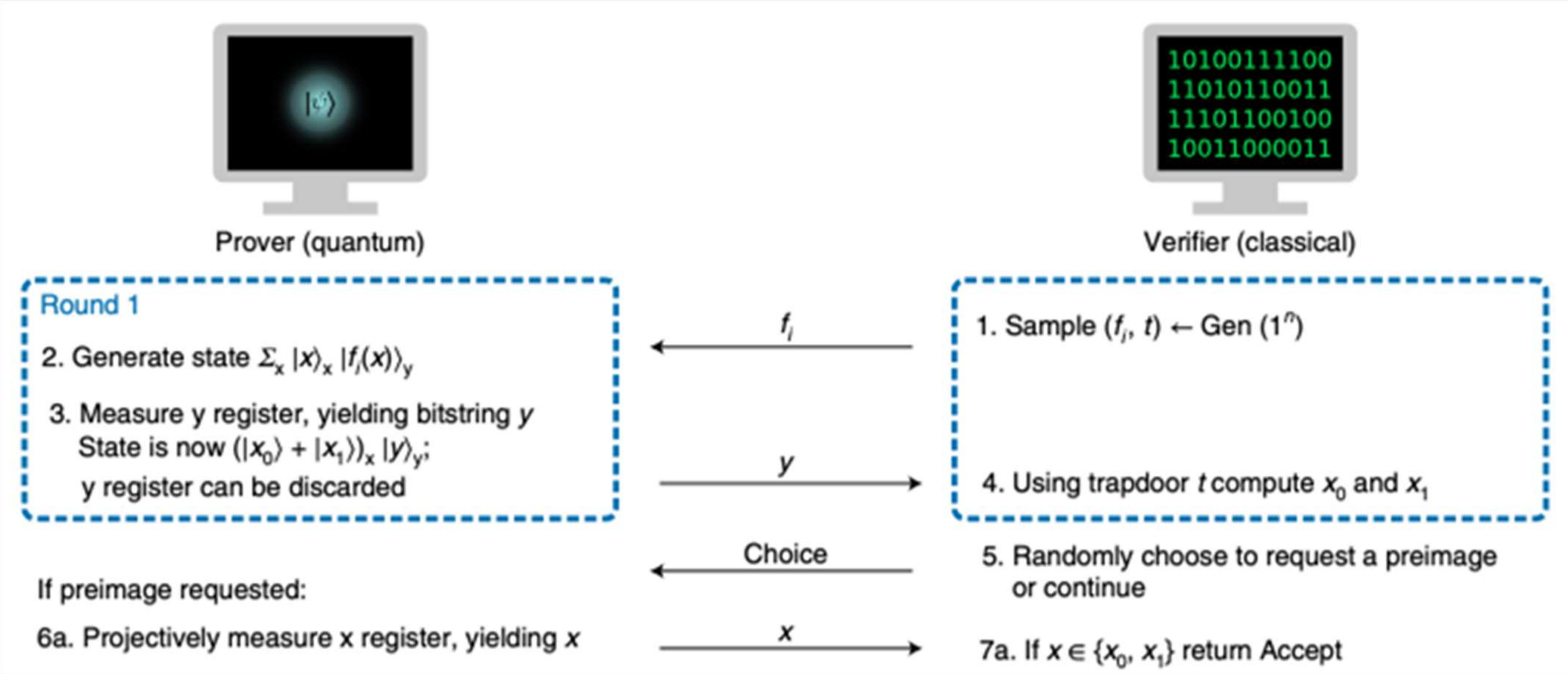
Umesh Vazirani
University of California Berkeley
vazirani@cs.berkeley.edu ‡

Thomas Vidick
California Institute of Technology
vidick@caltech.edu §

https://doi.org/10.48550/arXiv.2005.04826

https://www.pngwing.com/en/free-png-pvqpw
https://www.pngwing.com/en/free-png-yofrv

Interactive Protocol



Functions for the Protocol

Table 1 | Cryptographic constructions for interactive quantum advantage protocols

Problem	Trapdoor	Claw-free	Adaptive hardcore bit	Asymptotic complexity (gate count)
LWE[16]	✓	✓	✓	$n^2\log^2 n$
x^2 mod N	✓	✓	✗	$n\log n$
Ring-LWE[17]	✓	✓	✗	$n\log^2 n$
Diffie–Hellman	✓	✓	✗	$n^3\log^2 n$
Shor's algorithm	—	—	—	$n^2\log n$

n represents the number of bits in the function's input string. Big-$\mathcal{O}$ notation is implied and factors of log log$n$ and smaller are dropped. For references and derivations of the circuit complexities, see Supplementary Information.

Implementation of the Protocol

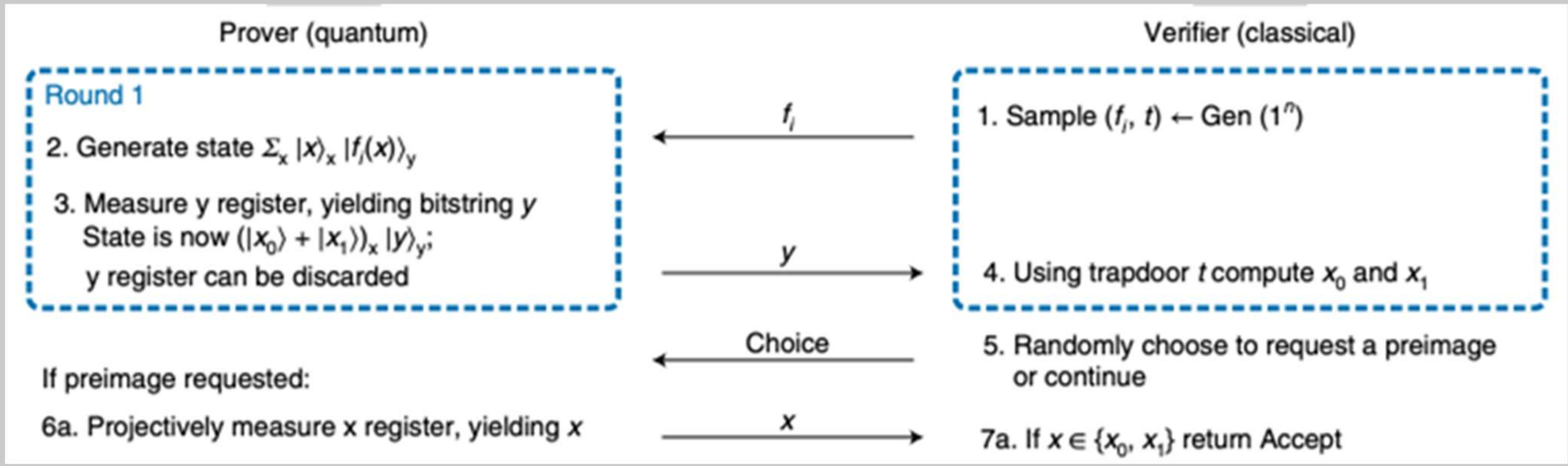
Two Key Innovations -

A) Post Selection Scheme - Reduces the Fidelity requirement

A) Measurement Based Circuit - Reduces the Quantum circuit overhead

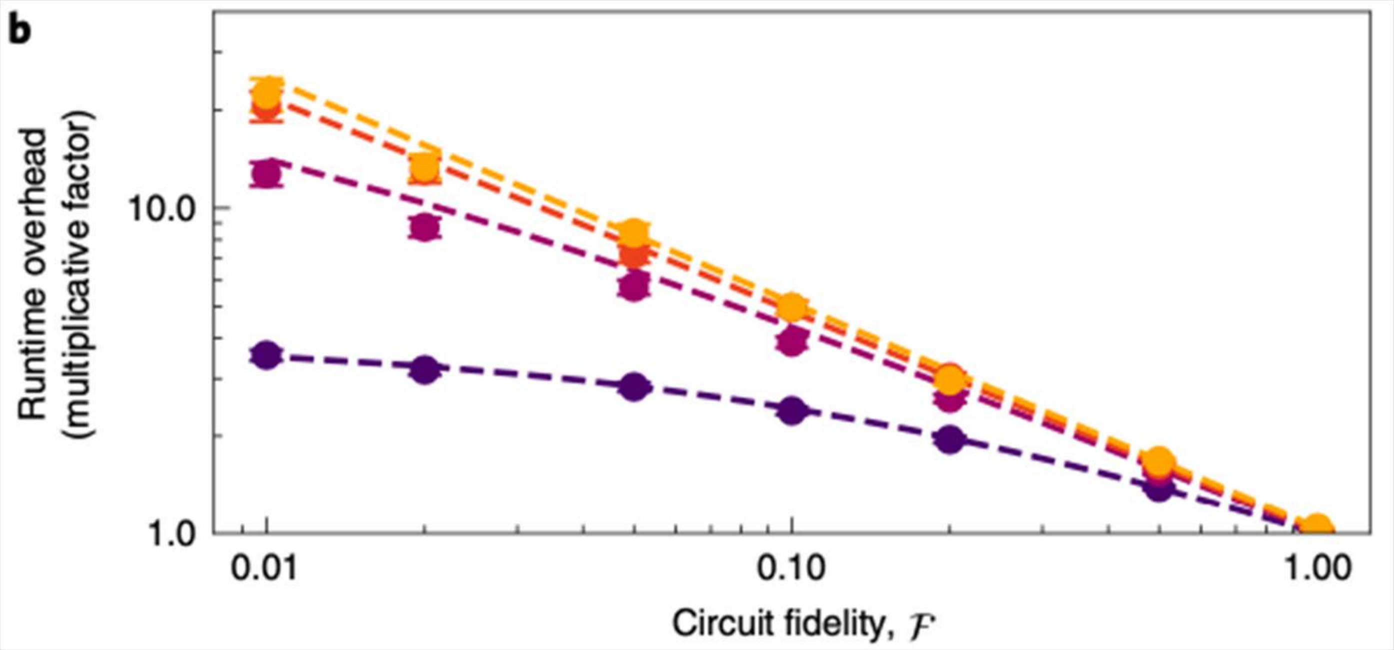
Post Selection Scheme

Discard Outputs which are not possible and Try Again



Low Fidelity Requirement

Postselection scheme increases a noisy device's probability of passing the test.

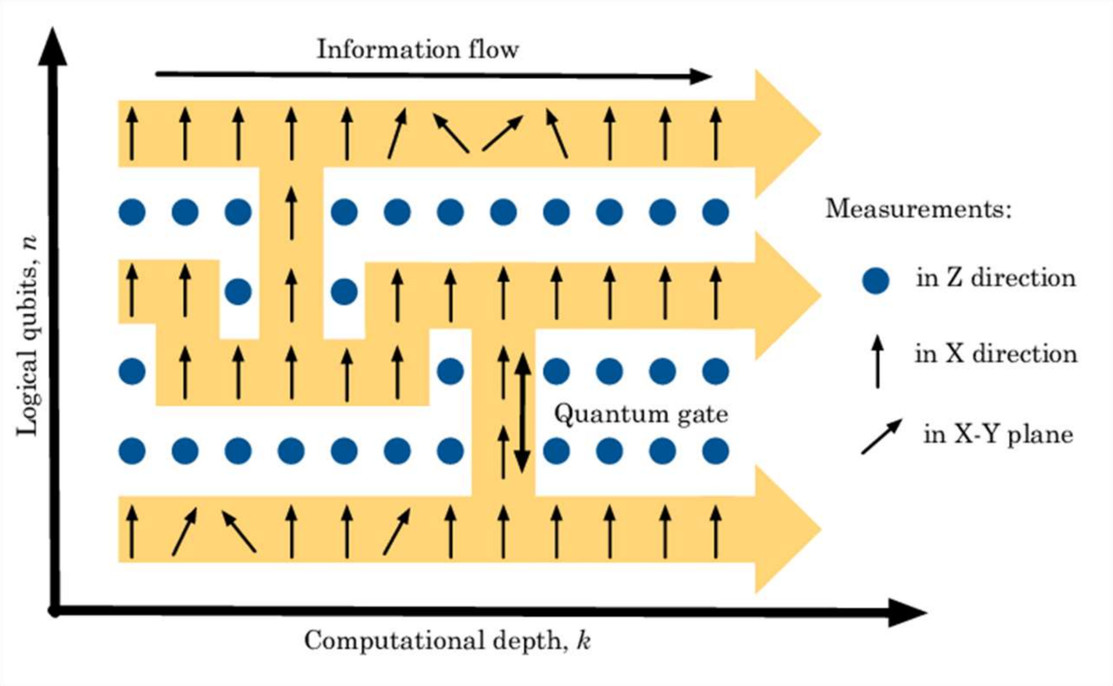


Measurement Based Circuit

Allows direct conversion from

Classical circuit to Quantum with

Zero Overhead



Quantum Circuit Implementation

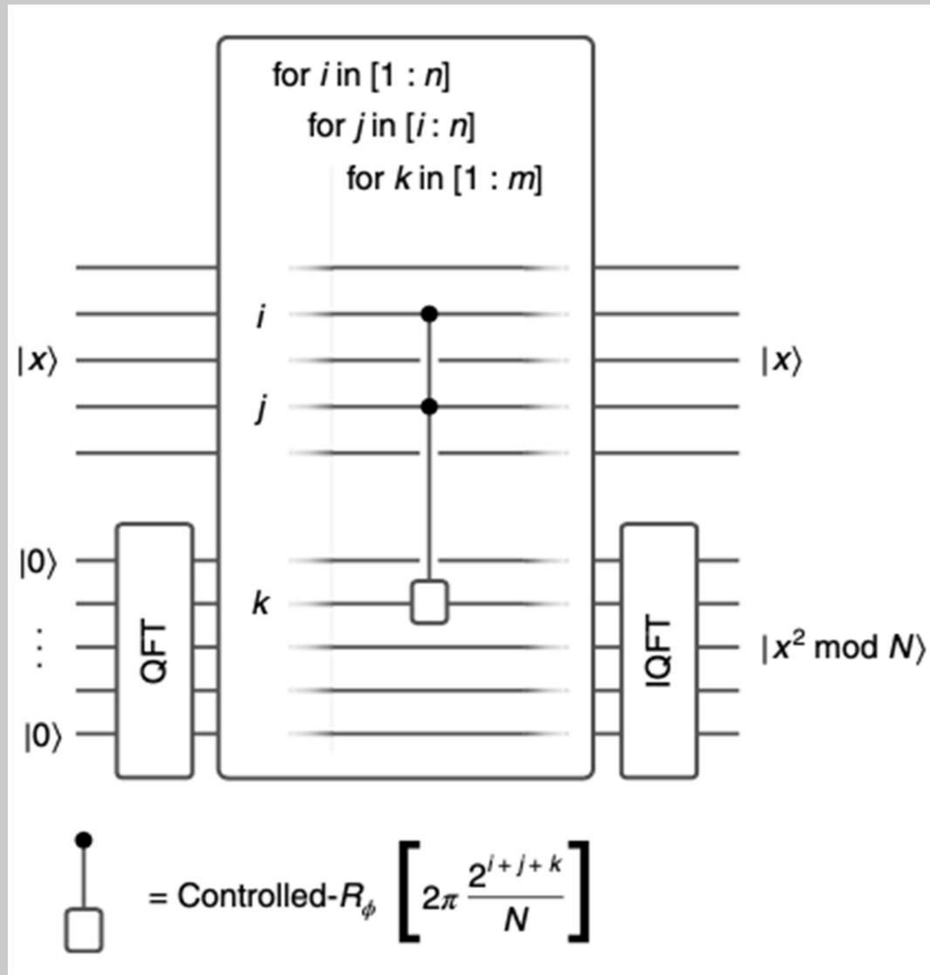
Quantum advantage can be achieved with

Qubits ~10^3

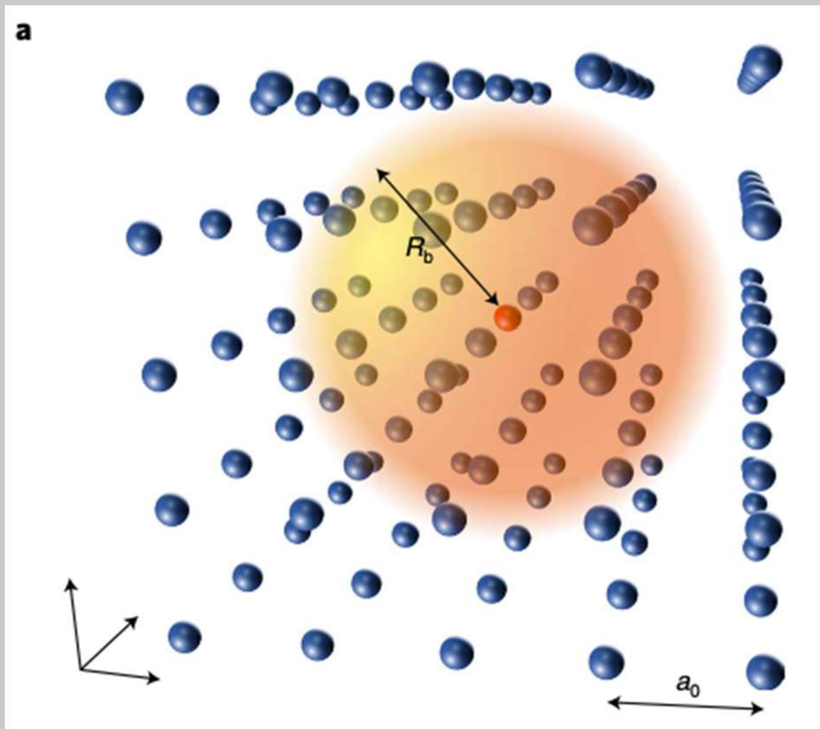
Gate depth ~10^5

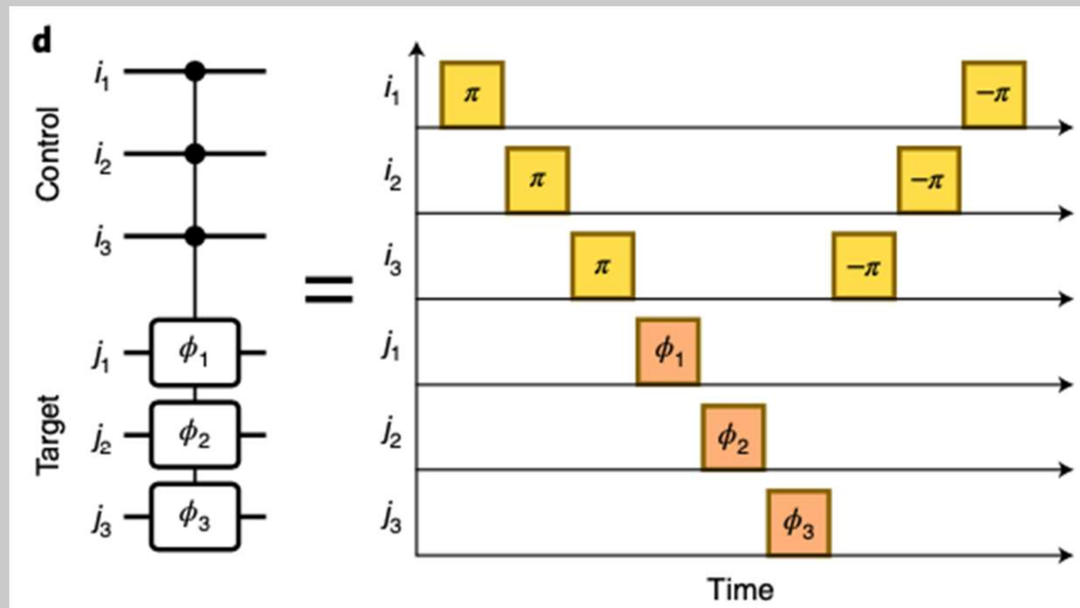
Importantly,

requires Low Circuit Fidelity

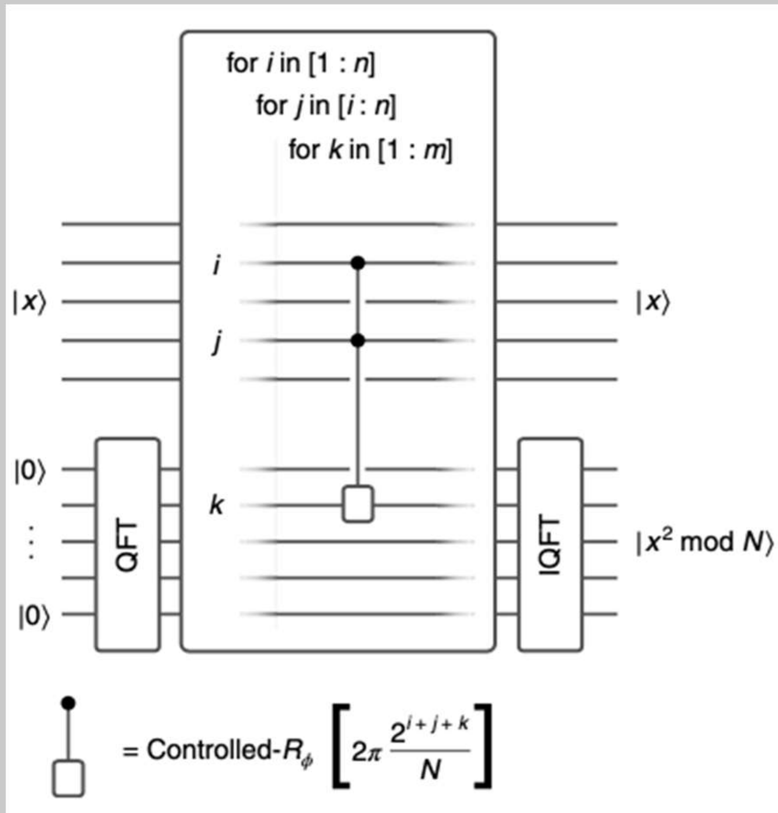


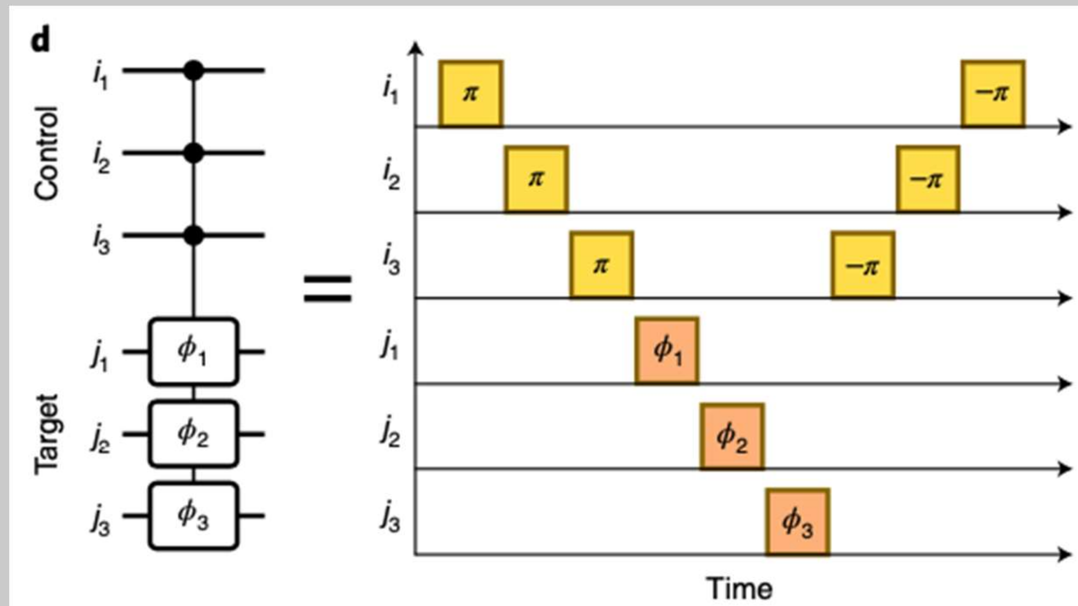
Natural implementation using Rydberg Atom





Natural implementation using Rydberg Atom





Summary of the paper

- The paper provides a way to experimentally test quantum advantage with current technology
- It does this by using a post selection scheme and a measurement-based circuit
- It also presents a methodology to implement in Rydberg atoms.

Summary of our analysis

- The paper is currently too inaccessible and requires the reader to be in the field to understand it.
- The paper does not justify why it is important well

Impact

- Relatively new paper so there is only one citation
- It is shown that this result is useful in showing proofs of quantumness in challenge-response protocols

Depth-efficient proofs of quantumness

Zhenning Liu[1] and Alexandru Gheorghiu[2]

[1]Department of Physics, ETH Zürich, Switzerland

[2]Institute for Theoretical Studies, ETH Zürich, Switzerland

A proof of quantumness is a type of challenge-response protocol in which a classical verifier can efficiently certify the *quantum advantage* of an untrusted prover. That is, a quantum prover can correctly answer the verifier's challenges and be accepted, while any polynomial-time classical prover will be rejected with high probability, based on plausible computational assumptions. To answer the verifier's challenges, existing proofs of quantumness typically require the quantum prover to perform a combination of polynomial-size quantum circuits and measurements.

Thank you!