‹ WOMANIUM | QUANTUM ›

Classically Verifiable Quantum advantage from a computational bell test

BY -

Apurva Dhingra (Phd AI and ML @ IIT Bombay, India)

Barnokhon Tashpulatova(BTech CS @ Uni of Washington)

Kush Dhuvad(MSc Physics @ IIT Jodhpur)

Submission Date : 9 August, 2024

Demo Date : 15 August, 2024

Efficiently Verifiable Quantum Computational Advantage

01	**Current Limitations in Quantum Advantage**	• Require exponential classical compute to verify
02	**Proposed Interactive Protocol**	New protocol based on : • Trapdoor (secret data with classical verifier) • Claw-free computationally difficult to find a pair (x_0, x_1) such that $f(x_0) = f(x_1)$
03	**Connection to Bell's inequality**	• Novel connection to Bell's inequality • Helps improve quantum circuit complexity
04	**Trapdoor Claw-free construction**	• Rabin's function : $f(x) = x^2 \bmod N$.

Implementation

- Implement the algorithm for a toy example.
- **Done Successfully**

Generalization

- Generalize or enlarge the problem.
- Resources estimation
- **Done Successfully**

General in terms of N from $f(x) = x^2 \bmod N$.

Optimization

- Optimize for the most adequate hardware
- **Optimized circuit depth for best hardware.**

Protocol

Prover (quantum)

Verifier (classical)

Round 1

2. Generate state $\Sigma_x |x\rangle_x |f_i(x)\rangle_y$

3. Measure y register, yielding bitstring y
   State is now $(|x_0\rangle + |x_1\rangle)_x |y\rangle_y$;
   y register can be discarded

f_i ←

1. Sample $(f_i, t) \leftarrow \text{Gen}(1^n)$

y →

4. Using trapdoor t compute x_0 and x_1

Choice ←

5. Randomly choose to request a preimage or continue

If preimage requested:

6a. Projectively measure x register, yielding x — x →

7a. If $x \in \{x_0, x_1\}$ return Accept

Otherwise, continue:

Round 2

7b. Add one ancilla b; use CNOTs to compute $|r \cdot x_0\rangle_b |x_0\rangle_x + |r \cdot x_1\rangle_b |x_1\rangle_x$ where $r \cdot x$ is bitwise inner product

8b. Measure x register in Hadamard basis, yielding a string d. Discard x, state is now $|\psi\rangle_b \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$

r ←

6b. Choose random bitstring r

d →

9b. Using r, x_0, x_1, d, determine $|\psi\rangle_b$

Round 3

11b. Measure ancilla b in the rotated basis

$\left\{\begin{matrix}\cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle \\ \cos\left(\frac{\theta}{2}\right)|1\rangle - \sin\left(\frac{\theta}{2}\right)|0\rangle\end{matrix}\right\}$, yielding a bit b

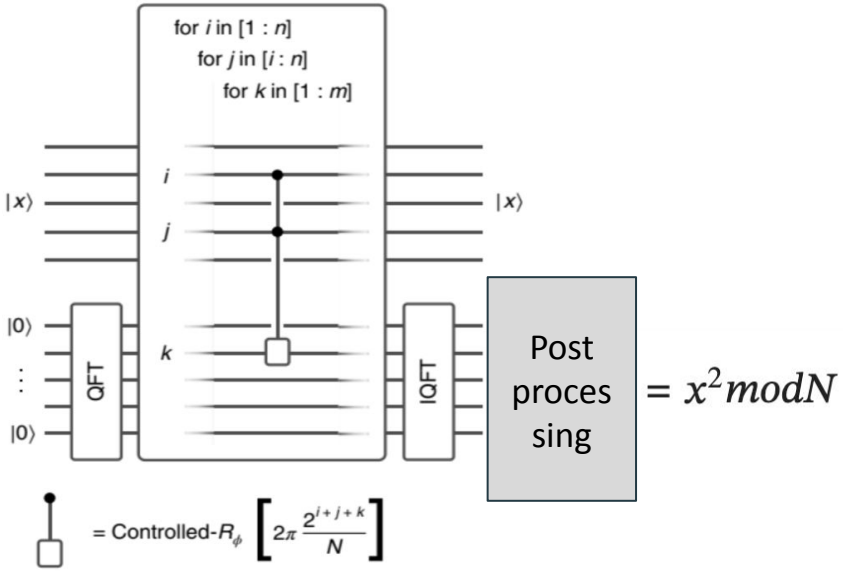
θ ←

10b. Choose random $\theta \in \left\{\frac{\pi}{4}, -\frac{\pi}{4}\right\}$

b →

11b. If b was likely given $|\psi\rangle_b$ return Accept

Implementation Phase circuits for $x^2 \bmod N$ (Quantum Phase estimation QPE)

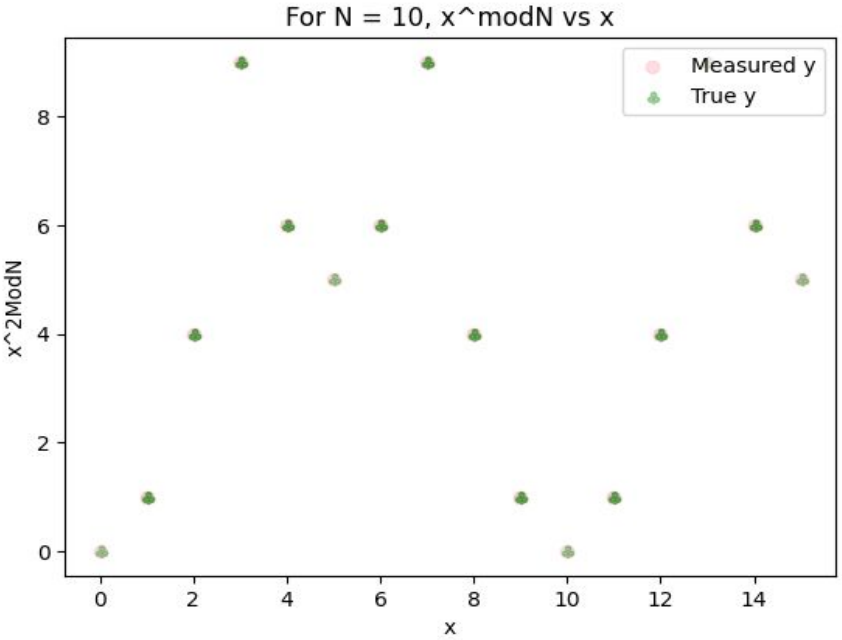


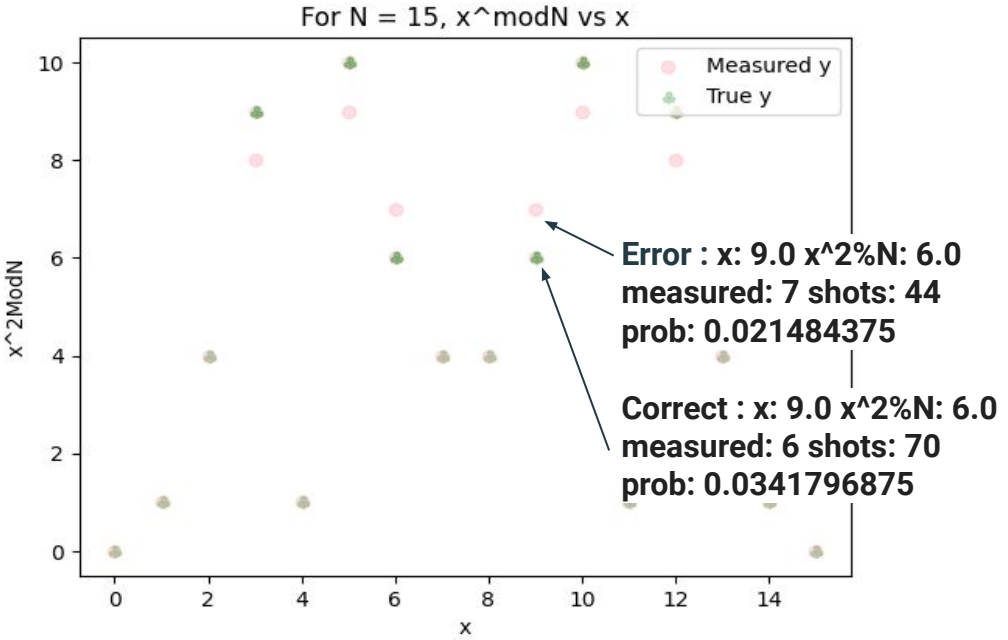
$= x^2 mod N$

1. Implemented the protocol (Round 1,2,3) for $f = x^2 \bmod N$.
2. Using post-processing, we managed to get this working for general N (other than $!= 2^n$).

Metric of success - for some N without any errors.

Results and analysis - Round 1





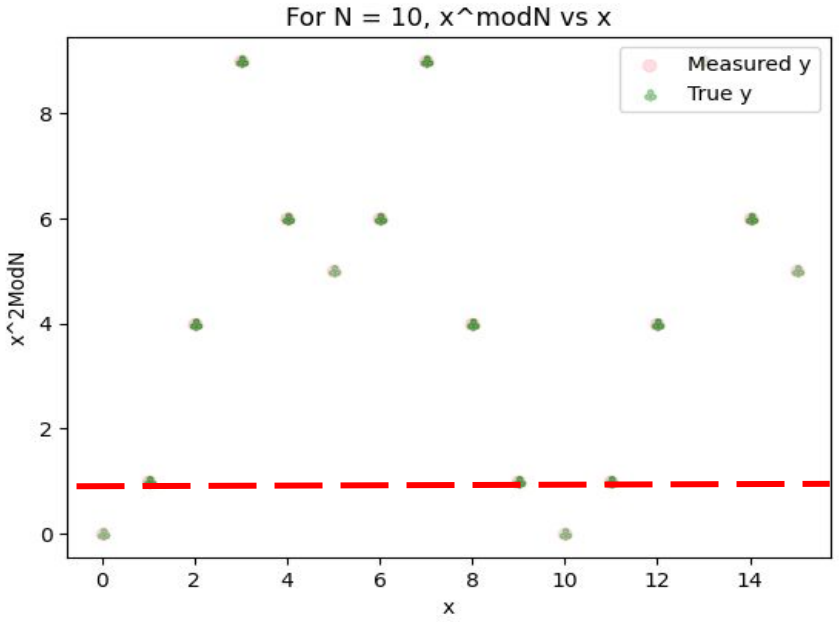
For N =10, the y = x^2 mod N values match the true values as shown.

For N =15, y = x^2 mod N

(Here 5 of the measured values differ from the true)

Note : y = x^2 mod N

Results - Round 2 & 3



For N =10, the y = x^2 mod N values match the true values as shown.

Round 2

- Entangled with r : $|r.x_0\rangle_b|x_0\rangle + |r.x_1\rangle_b|x_1\rangle$
- Measures the x register in the Hadamard basis and outcome is bitstring d, the new state is

Round 3 $(-1)^{d.x_0}|r.x_0\rangle + (-1)^{d.x_1}|r.x_1\rangle$

- Ancilla measured in rotated basis

The probability that the verifier will accept the single-qubit measurement result = pCHSH.

Theorem 1 : For a perfect quantum prover,

$$\hat{p}_{\mathrm{CHSH}} = \cos^2(\pi/8) \approx 0.85.$$

Gates and devices - Our Implementation (N=10) Resource Estimatlon

DEVICES	PROVIDERS	DEPTH	MULTI QUBIT GATE COUNT	TOTAL GATE COUNT
ionq.qpu.aria-2	Azure Quantum	268	243	561
ionq.qpu.aria-1	Azure Quantum	268	243	561
rigetti.qpu.ankaa-2	Azure Quantum	268	243	561
quantinuum.qpu.h1-1	Azure Quantum	268	243	561
ionq.qpu	Azure Quantum	268	243	561
fez	IBM Quantum	2056	546	4317
torino	IBM Quantum	2085	531	4212
strasbourg	IBM Quantum	3997	552	8815
brussels	IBM Quantum	4141	552	9231
kyiv	IBM Quantum	4164	552	9391
nazca	IBM Quantum	4190	552	9519
kyoto	IBM Quantum	4240	552	9391
kawasaki	IBM Quantum	4250	552	9215
rensselaer	IBM Quantum	4252	552	9663
quebec	IBM Quantum	4281	552	9599

Note : We didn’t implement any code for optimizing qubit number or number of gates.

Optimizing for specific hardware

Optimizing - Depth of the quantum circuit

Hardware - Azure ion hardware

Results Before optimizing :

DEVICES	PROVIDERS	DEPTH	MULTI QUBIT GATE COUNT	TOTAL GATE COUNT
ionq.qpu.aria-2	Azure Quantum	268	243	561
ionq.qpu.aria-1	Azure Quantum	268	243	561
rigetti.qpu.ankaa-2	Azure Quantum	268	243	561
quantinuum.qpu.h1-1	Azure Quantum	268	243	561
ionq.qpu	Azure Quantum	268	243	561

Results after optimizing for depth:

Width = 9, Depth = 255 , Gate Counts={'U': 245, 'CX': 243}

Future steps

1. For better Estimation from QPE :

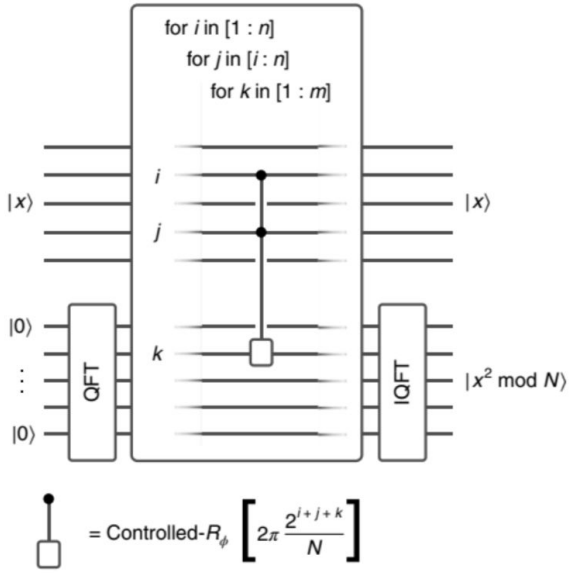
- Note when QFT is taken it is with respect to 2^$y.size$, where $y.size$ is the number of qubits in $|y\rangle$ register.

- For better Estimation from QPE, we propose using QFT_N (QFT with respect to N != 2^n.)

$$\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_n \omega_N^{nk}, \quad k = 0, 1, 2, \ldots, N-1,$$

$$\mathrm{QFT} : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{xk} |k\rangle.$$

2. Implement code for optimizing qubit number and number of gates. Compare if our proposed QFT_N will work better than existing QFT.



Benchmarking and Progress Tracking in Quantum Computing

Measure and Benchmark:
Quantify quantum advantage to track progress, compare to classical computing, and evaluate quantum processors.

Practical Impact:
Identify suitable problems, optimize resource allocation, and drive commercialization.

Theoretical Insights:
Enhance understanding of quantum mechanics, improve algorithm development.

Standardization and Comparison:
Create metrics, compare platforms, and guide future research.

References

1. Kahanamoku-Meyer, G. D., Choi, S., Vazirani, U. V., & Yao, N. Y. (2022). Classically verifiable quantum advantage from a computational Bell test. *Nature Physics*, *18*(8), 918-924. (Link).

2. Code Implementation of the paper - (Link)

3. Classiq Documentation

THANK YOU