Notes on Interrogating Random Quantum Circuits

National Institute of Standards and Technology
U.S. Department of Commerce

Luís T. A. N. Brandão · René Peralta

Cryptographic Technology Group, Computer Security Division, National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

An App of Quantum Computing

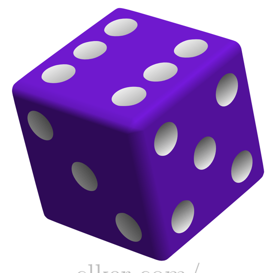
- National Quantum Initiative Act calls for quantum computing apps
- Google reported an experiment achieving quantum supremacy
- Aaronson proposed an application for **certifiable randomness**

Certifiable Randomness

Our RNG outputted: 3 5 2 3 1 6 ...

Can we be sure this is really random?

With **certifiable randomness**, we can verify randomness!!

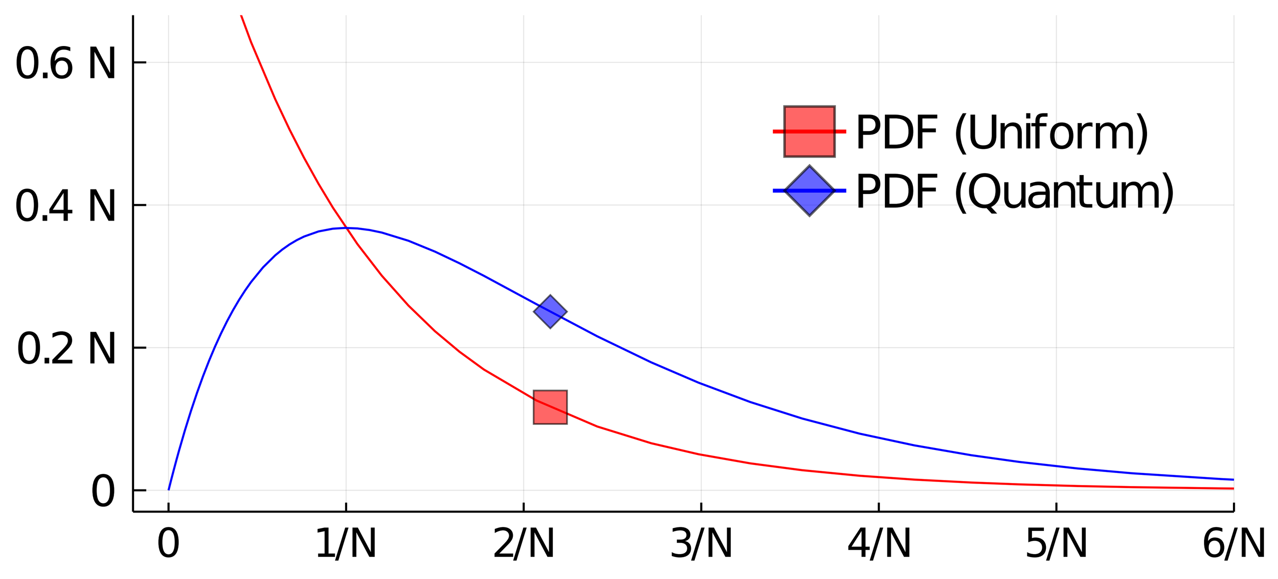


clker.com/ clipart-two-purple-dice.html

How: prove something must have been **quantumly** computed, using a **probabilistic** process, i.e., cannot have been computed deterministically.

Distribution of QC-values

- We consider quantum circuits with 53 qubits (as showcased by Google).
- For any fixed input, their output (53-bit strings) is probabilistic.
- QC-value: probability that a string s is output by a **q**uantum **c**ircuit.



The uniform (X_U) and quantum (X_Q) distributions have different statistics: $E[X_U] = 1/N$ vs. $E[X_Q] = 2/N$ and $V[X_U] = 1/N^2$ vs. $V[X_Q] = 2/N^2$.

Legend: E (expected value); V (variance)

An analysis suited for NIST/ITL

- Perform a statistical analysis, to determine randomness and safety bounds
- Propose an adversarial model for conservative estimation of parameters
- Abstract from the computational assumptions, using a black-box model

Metrology | **Cryptography** | **Quantum Computing**

Technical challenges/achievements:

- Derive the misleading power of adversarial sampling
- Obtain formulas to measure randomness (based on information entropy)
- Honest evaluations have low fidelity (e.g., 0.002 probability of correctness)

The Adversary $\mathcal{A}$

Confusion matrix		Classification: Positive	Classification: Negative
Actual condition	Positive (Honest operator)	**T**rue **P**ositive ratio (TP)	**F**alse **N**egative ratio (FN)
	Negative (Malicious operator)	**F**alse **P**ositive ratio (FP)	**T**rue **N**egative ratio (TN)

accuracy = (TP + TN)/All; precision = TP / (TP + FP); recall = TP / (TP + FN); ...

- **$\mathcal{A}$'s goal:** Produce a sample that minimizes the expected entropy, but conditioned to be accepted by the client with probability $\geq$ FP.
- **$\mathcal{A}$'s capability:** Can evaluate the quantum circuit more times than needed; can choose which strings to include (including pseudo-random).

clker.com/clipart-10778.html

Results in black-box model: $\mathcal{A}$ can only evaluate the circuit as a black-box.

How Many Strings to Sample?

What sample size $\boldsymbol{m}$ (how many strings) are needed to safely distinguish honest quantum sampling (with some expected entropy H), from a malicious sampling with fewer quantum strings (possibly all pseudo-random)?

$$m = 2 \cdot \left(\frac{\mathrm{erf}^{-1}(1-2\cdot\epsilon)}{\phi_1-\phi_2}\right)^2 \cdot \left(\sqrt{1+\phi_1\cdot(2-\phi_1)}+\sqrt{1+\phi_2}\right)^2$$

(ϵ = FN = FP; ϕ_1 is the honest fidelity; $\phi_2 = q/m$ is the adversarial pseudo-fidelity; q is the # of quantumly obtained strings included in the sample.)

Results for $n = 53$ qubits and honest fidelity $\phi_1 = 0.002$

ϵ	m for $\phi_2 = 0$	m for $\frac{\phi_2}{\phi_1} = 1/100$	m for $\frac{\phi_2}{\phi_1} = 1/4$	m for $\frac{\phi_2}{\phi_1} = 1/2$
2^{-40}	4.98E+7	5.08E+7	8.85E+7	1.99E+8
10^{-3}	9.57E+6	9.76E+6	1.70E+7	3.83E+7
10^{-1}	1.65E+6	1.68E+6	2.93E+6	6.59E+6

For fidelity 0.002, **about 50 million strings** are needed to reduce the classification bias to less than 2^{-40}.
About 2 million strings are needed if the fidelity is 0.01.

A more sophisticated analysis can correlate the amount of certifiable entropy (H) with the adversarial sampling budget β and other parameters. (See paper)

Poster prepared for the ITL Virtual Science Day 2020 (October 29). Poster based on paper with the same title (2020-May-29): DOI: 10.13140/RG.2.2.24562.94400. The first author is a Foreign Guest Researcher at NIST (Contractor via Strativia).