Notes on Interrogating Random Quantum Circuits

Luís T. A. N. Brandão* · René Peralta

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

A Metrological Perspective

Context:

- National Quantum Initiative Act calls for apps of quantum computing [NQIA]
- Google reported an experiment achieving quantum supremacy [Goo19]
- Aaronson proposed an application related to certifiable randomness [Aar19]

Goals:

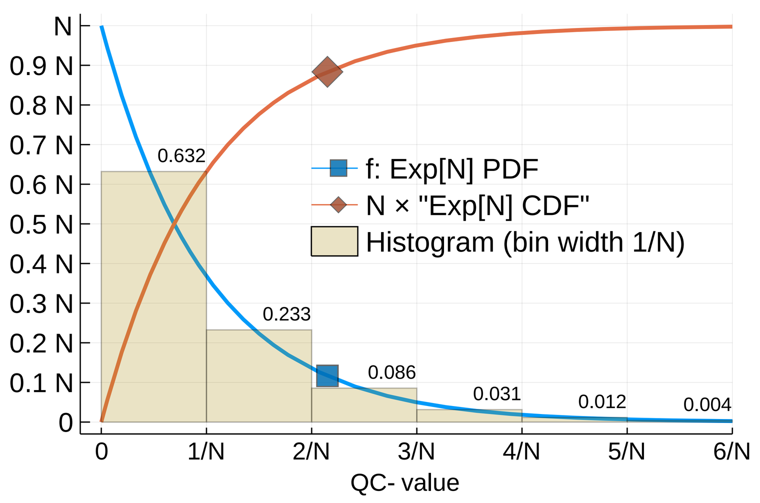
- Perform a statistical analysis, to determine preliminary lower/upper bounds
- Propose an adversarial model for conservative estimation of parameters
- Abstract from the computational assumptions, using a black-box model

Technical challenges/achievements:

- Develop rationale to support a quantified measure of entropy
- Explore the role of adversarial over-sampling and string collisions
- Derive and conjecture new formulas of interest

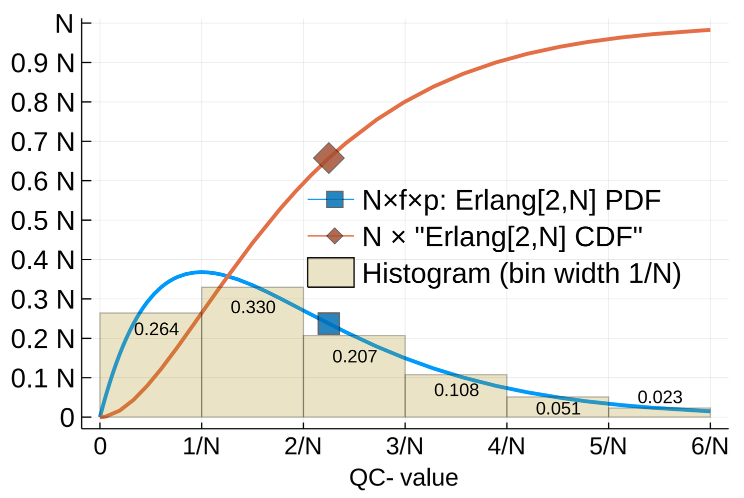
Distribution of QC-values

- The output of a **r**andom **q**uantum **c**ircuit (RQC) $\mathcal{C}$ is probabilistic.
- We look at RQCs whose output space is the set S_n of bit-strings with $n = 53$ bits.
- The distribution of strings sampled from a RQC **might look uniform, but it is not.**
- Each string s has a probability value (QC-value) $\{\text{Prob}(s \leftarrow \mathcal{C}) : s \in S_n\}$ of being output.
- How does the distribution of QC-values relate to the string-sampling distribution?



Upon **uniform** string sampling

$\text{Exp}[X_U] = 1/N \quad \text{Var}[X_U] = 1/N^2$



Upon **quantum** string sampling

$\text{Exp}[X_U] = 2/N \quad \text{Var}[X_U] = 2/N^2$

- A classical computer cannot efficiently find which strings are more likely than others.
- A quantum computer can efficiently sample from the true distribution*.
- A super-computer can later (effortfully) confirm that "some" quantum sampling occurred.

* with an associated *fidelity* (probability of correct evaluation).

Toward Certifiable Randomness

- The output of a quantum evaluation of a RQC contains inherent fresh randomness.
- But a classical computer with enough computation time can simulate a RQC sampling.

Two practical questions:

1. Under a claim that a sequence of bit-strings has been sampled by quantum evaluation of a given RQC, how much **entropy** can be safely assumed to be contained in it?
2. Given a goal of entropy, how many strings should be sampled to enable a verification with high assurance?

Information Entropy

- Information entropy (there are several flavors) is a quantitative measure of randomness.
- E.g., Shannon entropy is the expected negative binary logarithm, $-\log_2$, of probabilities.
- For $n = 53$ qubits, a quantumly sampled string has expected entropy $h \approx 52.39$ bits.

$$h = \sum_{i=1}^{N} p_i \cdot \log_2(p_i) \approx \log_2(N) + (\gamma - 1)/\log(2) \approx n - 0.60995,$$

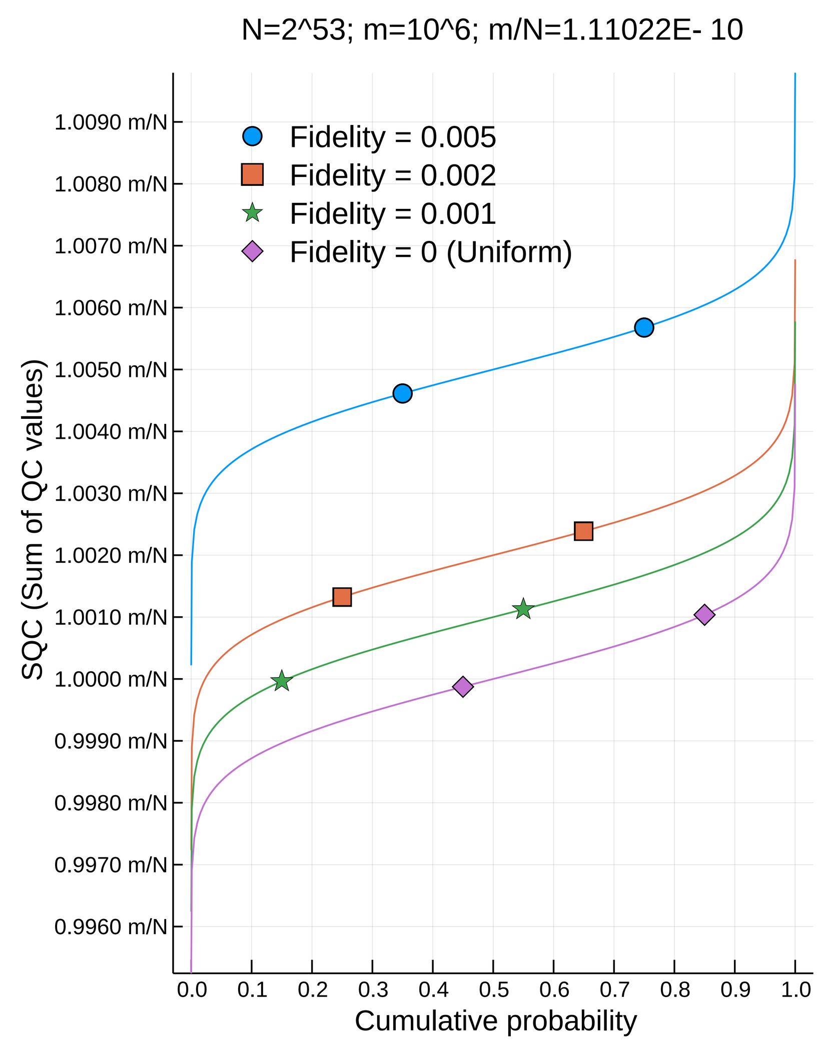
$(\gamma \approx 0.57722$ is the Euler-Mascheroni constant$)$

- On the other hand, a pseudo-randomly computed string has entropy 0.

Fidelity

Fidelity: probability ϕ that a quantum evaluation is correct. For an honest sample with m strings, the expected number of strings obtained from correct quantum evaluation is $m \cdot \phi$.

- An estimate of the fidelity gives us an idea of the number (q) of quantumly obtained strings that are in a sample with m strings.
- The fidelity of a sample is directly estimated by the sum of QC-values (SQC): $\hat{F} = \text{SQC}/m - 1$.
- Thus, the client accepts only when the SQC is "large enough" (meaning likelihood of large enough q).
- In the right-side graphic, each curve (for each ϕ) is an Inverse-CDF of the SQC. Can two fidelities be confused: ϕ_1 (honest) and ϕ_2 (malicious)?
- For $m = 10^6$, if the threshold is set to accept 80% of the $\phi_1 = 0.002$ cases, then that test would incorrectly accept 12% of the cases with $\phi_2 = 0$.
- In practice we want to distinguish between two positive fidelities.



Inverse CDFs of SQC with $m = 10^6$

Confusion matrix		Classification: Positive	Classification: Negative
Actual condition	Positive (Honest operator)	**True Positive** ratio (TP)	**False Negative** ratio (FN)
	Negative (Malicious operator)	**False Positive** ratio (FP)	**True Negative** ratio (TN)

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

The Adversary $\mathcal{A}$

- **Adversarial goal:** Produce a sample that minimizes the expected entropy, but conditioned to be accepted by the client with probability $\geq$ FP.
- **Adversarial capability:**
  - Can over-sample the RQC (obtain more strings than needed) with fidelity 1
  - Can choose which strings to include (including pseudo-random ones)
  - Black-box approach (does not take advantage of the circuit specification $\mathcal{C}$)
- **Over-sampling allows reducing entropy from quantumly obtained strings:**
  - Rejection sampling: bias the set of selectable strings
  - Observe collisions (repeated strings are likely to have a higher QC-value)

How Many Strings to Sample?

Problem: What sample size $\boldsymbol{m}$ should a client ask for, from the quantum computer server?

Depends on the goal $(H, \epsilon_1, \epsilon_2)$ of the client and other experimental parameters (ϕ_1, β):

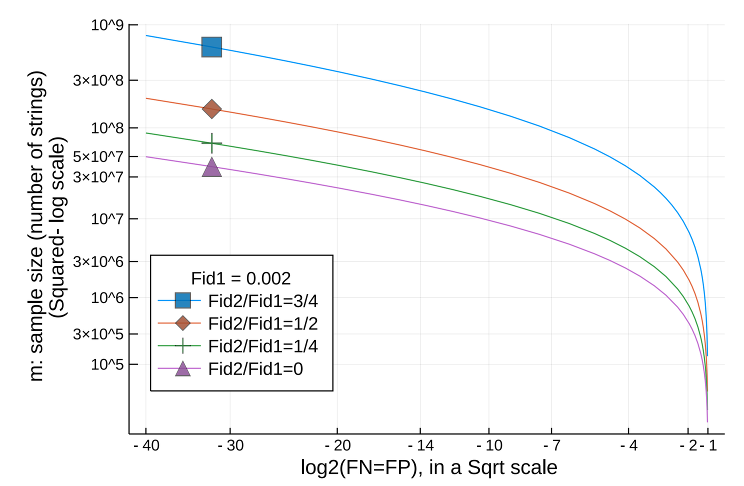
- H: amount of certifiable entropy ($\leftarrow$ min number q of strings to obtain quantumly).
- (ϵ_1, ϵ_2): rates (FN, FP), e.g., at most $\epsilon = 2^{-40}$ for crypto applications
- ϕ_1: honest fidelity, e.g., 0.002 (achievable) or 0.01 (foreseen), for $n = 53$ qubits.
- β: adversarial sampling budget $(\beta > m)$ with fidelity 1

The client then determines the sample size m. Below, $\phi_2 = q/m$, where q is the number of quantumly obtained strings that the adversary includes in the sample.

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

ϕ_1	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 $\frac{\phi_2}{\phi_1} = 1/2$
0.002	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
0.01	2^{-40}	2.01E+6	2.05E+6	3.57E+6	8.05E+6
	10^{-3}	3.86E+5	3.94E+5	6.88E+5	1.55E+6
	10^{-1}	6.63E+4	6.77E+4	1.18E+5	2.66E+5

Number of strings for SQC distinguishability



Sample size vs. FN=FP, with $\phi_1 = 0.002$

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.

Entropy estimation (first approximation): $H \approx q \cdot (h_\beta - \log_2(M/q) + \log_2(q!))$

For a better approximation, the reduction term $\log(M/q)$ is updated as a sum of terms per string (as if $q = 1$ done q times). The value q is the minimum allowing the adversary $(\mathcal{A})$ to satisfy the FP condition. If the pre-sampling budget $\beta = b \cdot N$ is large enough $(> \sqrt{N})$ to enable string collisions, then $\mathcal{A}$ organizes the strings per observed multiplicity c. Each bin c has an expected number M_c of strings and an expected average QC-value A_c.

$$M_c \approx N \cdot \frac{b^c}{(1+b)^{1+c}}$$

$$A_c \approx \frac{1}{N} \cdot \frac{1+c}{1+b}$$

β	c	M_c	$N \cdot A_c$	q_c	h_c	H_c
2^{32}	1	$2^{31.9999999}$	1.999999	1024.0	≈ 52.39	$\approx 2.088E+4$
	2	$2^{10.999999}$	2.999999	512.0	≈ 51.34	$\approx 2.075E+4$

Example where choosing strings with collisions reduces the final entropy

Some References

- [Aar19] S. Aaronson. *Certified Randomness from Quantum Supremacy.* Unpublished manuscript. 2019. [See also: *Aspects of Certified Randomness from Quantum Supremacy.* Slide-deck, May 2019. https://www.scottaaronson.com/talks/certrand2.ppt]
- [BP20] L. Brandão and R. Peralta. *Notes on interrogating random quantum circuits.* National Institute of Standards and Technology. 2020. doi:10.13140/RG.2.2.24562.9440. Preprint: `https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=929546`
- [Goo19] F. Arute et al. *Quantum supremacy using a programmable superconducting processor.* In: Nature 574.7779 (Oct. 2019), pp. 505–510. doi:10.1038/s41586-019-1666-5. arXiv:1910.11333
- [NQIA] U.S.Congress. *National Quantum Initiative Act — Public Law No. 368.* 115th Congress (2017-2018) of the United States. 2018. https://www.congress.gov/bill/115th-congress/house-bill/6227/text

Date: August 3, 2020. All content in this poster is based on the following two documents:

Slide presentation (2019-Dec-13): *Some Notes on Interrogating Random Quantum Circuits*
`https://csrc.nist.gov/Presentations/2019/interrogating-random-quantum-circuits`

Paper (2020-May-29) [BP20]

* The first author is a Foreign Guest Researcher at NIST (Contractor from Strativia since February 2020).