Cryptography

Negative certifiable randomness

With X

The uniform (probabilistic process, i.e., cannot have been computed deterministically.

Can we be sure this is really random?

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

• QC-value: probability that a string

• For any fixed input, their output (53-bit strings) is probabilistic.

We consider quantum circuits with 53 qubits (as showcased by Google).

• Aaronson proposed an application for certifiable randomness

An App of Quantum Computing

• National Quantum Initiative Act calls for quantum computing apps
• Google reported an experiment achieving quantum supremacy
• X

U

• Google reported an experiment achieving quantum supremacy
• National Quantum Initiative Act calls for quantum computing apps

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!!

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 quantum circuit.

The uniform (X) and quantum (XQ) distributions have different statistics:


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

The uniform (X) and quantum (XQ) distributions have different statistics:


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

How Many Strings to Sample?

What sample size 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)?

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

(\epsilon = FN = FP; \phi_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 \( \phi_1 = 0.002 \)

\[
\begin{array}{cccc}
\epsilon & m \text{ for } \phi_2 = 0 & m \text{ for } \phi_2 = 1/100 & m \text{ for } \phi_2 = 1/4 & m \text{ for } \phi_2 = 1/2 \\
2^{-40} & 4.98E+7 & 5.08E+7 & 8.85E+7 & 1.99E+8 \\
10^{-3} & 9.57E+6 & 9.76E+6 & 1.70E+7 & 3.83E+7 \\
10^{-1} & 1.65E+6 & 1.68E+6 & 2.93E+6 & 6.59E+6 \\
\end{array}
\]

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 \( \beta \) and other parameters. (See paper)

How Many Strings to Sample?

What sample size 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)?

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

(\epsilon = FN = FP; \phi_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 \( \phi_1 = 0.002 \)

\[
\begin{array}{cccc}
\epsilon & m \text{ for } \phi_2 = 0 & m \text{ for } \phi_2 = 1/100 & m \text{ for } \phi_2 = 1/4 & m \text{ for } \phi_2 = 1/2 \\
2^{-40} & 4.98E+7 & 5.08E+7 & 8.85E+7 & 1.99E+8 \\
10^{-3} & 9.57E+6 & 9.76E+6 & 1.70E+7 & 3.83E+7 \\
10^{-1} & 1.65E+6 & 1.68E+6 & 2.93E+6 & 6.59E+6 \\
\end{array}
\]

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 \( \beta \) and other parameters. (See paper)

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