

# Quantum Randomness: More Than Just Random Numbers

## Introduction

Classical randomness is typically derived from deterministic processes disguised with complexity or chaos (e.g., pseudo-random number generators, PRNGs). Quantum randomness, on the other hand, is intrinsic. When a quantum system is measured, it truly "chooses" an outcome among possibilities—unpredictably and irreducibly.

## The Quantum Origin of Randomness

Quantum mechanics is inherently probabilistic. The Born rule states that the probability of a measurement outcome is given by the square modulus of the state's amplitude.

For a qubit in state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , measuring in the computational basis gives:

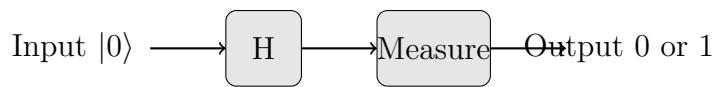
$$P(0) = |\alpha|^2, \quad P(1) = |\beta|^2$$

For example, preparing a qubit in the state  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  and measuring in the Z-basis yields truly random outcomes: 0 or 1 with equal probability.

## Quantum Random Number Generators (QRNGs)

QRNGs exploit this phenomenon to generate truly unpredictable numbers. Typical architecture:

- Prepare a qubit in a superposition (e.g., with Hadamard gate).
- Measure the qubit.
- Interpret the outcome as a random bit.



# Applications of Quantum Randomness

- **Cryptography:** Secure key generation.
- **Monte Carlo methods:** Random sampling in simulations.
- **Quantum Games:** Unbiased decision-making in quantum protocols.

## Insights and Learnings

- True randomness is not computationally generated, but physically intrinsic.
- Classical PRNGs can be predicted with enough state knowledge. Quantum RNGs cannot.
- Measuring a qubit collapses its state, producing inherently random results.
- Certification and entropy estimation of QRNGs are active research areas.

## MCQs

**Q1.** What is the source of quantum randomness?

- A. Chaotic classical dynamics
- B. Measurement-induced collapse
- C. Hidden variables
- D. Deterministic unitary evolution

**Answer: B**

*Explanation:* Quantum randomness arises from the measurement process which collapses a superposition into one outcome probabilistically.

**Q2.** In a QRNG, which state would yield truly random output when measured in the computational basis?

- A.  $|0\rangle$
- B.  $|1\rangle$
- C.  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- D.  $|+\rangle$  measured in X-basis

**Answer: C**

*Explanation:* This is a Hadamard-applied qubit, giving 0 or 1 with equal probability in Z-basis.

**Q3.** Which of the following statements is TRUE?

- A. Classical PRNGs are more secure than QRNGs.
- B. QRNGs require a large classical seed.
- C. QRNGs can generate unpredictably random numbers.

D. QRNGs require machine learning models.

**Answer: C**

**Q4.** Which quantum gate is typically used to prepare a qubit for randomness?

- A. X
- B. Z
- C. H
- D. T

**Answer: C**

*Explanation:* The Hadamard gate creates equal superposition, crucial for unbiased random bit generation.

## Further Reading

- Quantum Certified Randomness
- Qiskit QRNG Tutorial
- QRNG Review - Ma et al.