Lecture 2: Quantum Randomness

QURIOS
THE QUANTUM TECHNOLOGIES ACADEMY

Classical vs. Quantum Randomness

Randomness in classical systems often arises from complexity, chaos, or a lack of complete knowledge about a system. For example, rolling a die or flipping a coin appears random due to the difficulty in precisely measuring and predicting all contributing factors (e.g., force, angle, and air resistance). However, classical processes are ultimately deterministic if all variables are known and thus not truly random. That also holds for random number generators based on classical algorithms.

In contrast, quantum randomness is inherent and fundamental to quantum mechanics. It is not due to a lack of knowledge but is a direct consequence of quantum principles such as:

- **Measurement**: The act of measurement forces the quantum state into one of the possible outcomes, which is entirely random within the probabilities defined by the quantum state.
- **Superposition**: A quantum particle exists in multiple states simultaneously, and its state is determined only upon measurement.
- **Entanglement**: Measurements on entangled particles produce outcomes that are individually random but exhibit correlations when compared.

This fundamental randomness is the cornerstone of quantum technologies like Quantum Random Number Generators (QRNGs).

Heisenberg Uncertainty Principle

The **Heisenberg Uncertainty Principle** states that it is fundamentally impossible to precisely obtain exact values for certain **complementary observables**. Such complementary observables for example are **position and momentum**, but also the **polarisation of a photon** with relation to different bases. So for example it is impossible to know the polarisation of a photon with respect to the **horizontal-vertical (H-V) basis** AND with respect to the **diagonal-antidiagonal (D-A) basis** at the same time. This inherent uncertainty leads to **true randomness** in quantum measurements:

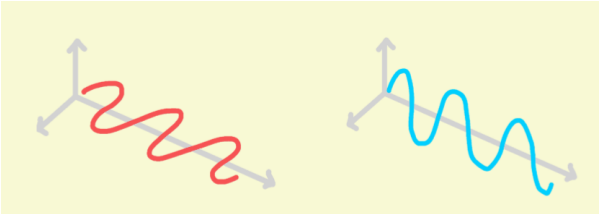
$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

where Δx is the uncertainty in position, Δp is the uncertainty in momentum, and $\hbar$ is the reduced Planck constant.

Quantum Sources of Randomness

Quantum processes provide true randomness due to the inherent unpredictability of quantum mechanics. Examples include:

- **Photon Polarization**: When a photon passes through a polarizing filter, its measured polarization is random if the photon's state is in superposition.



Polarization of light

- **Quantum Superposition**: A particle in a superposition collapses to one of its possible states randomly when measured.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

A superposition in the $\{|0\rangle, |1\rangle\}$- basis.

Randomness Testing

To evaluate randomness in generated sequences, statistical tests are applied:

- **NIST Statistical Test Suite**: A comprehensive set of tests to evaluate the quality of random number generators.
- **Diehard Tests**: A collection of statistical tests designed to assess randomness.

These tests validate that sequences exhibit no discernible patterns but cannot guarantee true randomness, which is a property of the generating process itself.

Quantum Randomness

Quantum randomness arises from the fundamental principles of quantum mechanics, which ensure that certain processes are inherently unpredictable. Unlike classical systems, where outcomes are deterministic and can be calculated if initial conditions are known, quantum systems can exist in superpositions, meaning they do not have predetermined states before measurement.

Mathematical Representation:

- **State of Randomness (R) and Adversary (E):**

$$\rho_{RE} = \pi_R \otimes \rho_E$$

  - This describes the state of randomness R and an adversary E trying to predict R.

- **Maximally Mixed State on R:**

$$\pi_R = \frac{1}{2^l} \sum_{r \in \{0,1\}^l} |r\rangle\langle r|$$

  - The randomness R is uniformly distributed over all possible outcomes, making it maximally random.

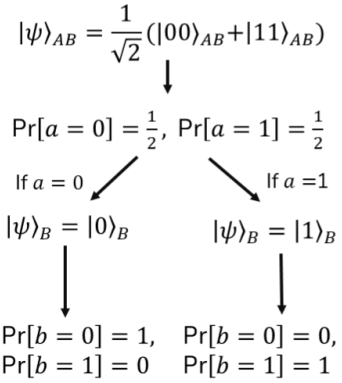
- **Adversary's Independence:**

  - The state ρ_E of the adversary is completely independent of π_R, as indicated by the tensor product $\pi_R \otimes \rho_E$.
  - This ensures that the adversary cannot gain any knowledge about R.

Shared Randomness from Entanglement

Quantum entanglement creates correlations between particles that can be leveraged to generate shared randomness:

- **Entangled Photons**: Measurements of entangled photon pairs produce correlated outcomes that are individually random but exhibit strong dependencies.

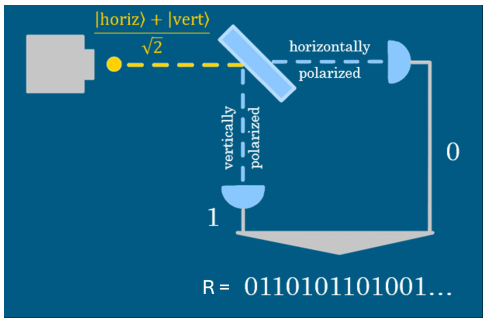


- **Applications in Cryptography**: Shared randomness from entanglement underpins secure quantum communication protocols.

Quantum Random Number Generation

Quantum Random Number Generators (QRNGs) exploit quantum processes to generate true randomness:

- **Single Photon Source**: Photons are emitted individually and passed through a polarization filter.
- **Random Bit Generation**: The photon's polarization measurement (e.g., horizontal or vertical) is recorded as a binary bit (0 or 1).



QRNG schematics

QRNGs are crucial for cryptography, where unpredictability is essential for secure key generation.
Limitation: An realistic QRNG always deviates from an ideal device.