Quantum random number generator

PNC - Qiskit fall fest 2025

Sneha Sharma

Classical random number generator

Classical Random Number Generators (RNGs) are fundamentally deterministic algorithms that only produce pseudo-random sequences . This reliance on software or predictable physical sources means their output is ultimately guessable, creating a critical vulnerability in cryptography and high-stakes simulations. To achieve genuine, uncompromised security and true unpredictability, we must shift to Quantum Random Number Generators (QRNGs), which harness the inherent, non-deterministic laws of quantum physics to produce truly random, reliable keys.

Quantum random number generator

QRNG create true, unpredictable randomness by observing quantum physics. Unlike classical, pseudo-random methods

- ➔ **emission of photon**
  light source emit a single photon.
- ➔ **Quantum indeterminacy**

  directed toward a 50/50 beam splitter.
- ➔ **True random output.**fundamentally impossible to predict the path, dictated by quantum uncertainty.

Quantum random number generator

A quantum random number generator works by measuring a fundamentally unpredictable quantum event—such as a single photon hitting a beam splitter and randomly taking one of two paths. Each measurement forces nature to “choose” an outcome that cannot be predicted, even with perfect information. These outcomes are then converted into bits, producing truly random numbers that are far more secure and reliable than those generated by classical methods.

Quantum n-number random generator using qiskit

```
def qrng_generate(N, bits_per_int):
    backend = Aer.get_backend('qasm_simulator')
    integers = []

    for _ in range(N):
        bitstring = ""
        for _ in range(bits_per_int):
            qc = QuantumCircuit(1, 1)
            qc.h(0)
            qc.measure(0, 0)

            result = backend.run(qc, shots=1).result().get_counts()
            bitstring += list(result.keys())[0]

        integers.append(int(bitstring, 2))

    return integers

print(qrng_generate(9, 4))
```