Random Number Generation: Quantum vs Classical

Anil Kumar Gundu
National University of Singapore

September 26, 2025

1 Quantum Random Number Generation (QRNG) using Hadamard Gate :

The procedure can be described step by step as follows:

1. Start with a qubit in the state $|0\rangle$.
2. Apply the Hadamard gate. This creates a superposition of $|0\rangle$ and $|1\rangle$ with equal probability 50% :
$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
3. Measure the qubit: When measured, the qubit will collapse to a single state, for example :
   - Collapse to $|0\rangle$ with probability $\frac{1}{2}$
   - Collapse to $|1\rangle$ with probability $\frac{1}{2}$

   Each measurement is truly random and independent.
4. Repeat the procedure to generate multiple random bits.

- **Advantages:**
  - True randomness guaranteed by quantum mechanics
  - No patterns or correlations between bits
  - Can generate unbiased sequences (ideal qubit)
- **Disadvantages:**
  - Requires quantum hardware or simulator
  - Slower than classical generation on typical CPUs

2 Classical Pseudo-Random Number Generation (PRNG) using LFSR :

1. Initialize a register of n bits with a seed.
2. Update the register at each step using a linear feedback function, e.g..
3. Shift the register and output one bit
4. Repeat to generate the desired number of bits.

- **Advantages:**
  - Very fast and easy to implement

  - Reproducible sequences if seed is known
  - Works entirely on classical computers

- **Disadvantages:**
  - Not truly random; deterministic sequence
  - Periodic: sequence eventually repeats
  - Predictable if the seed or algorithm is known
  - Slight bias possible if taps are not chosen carefully