Quantum Random Number Generator

Introduction & Circuit Design

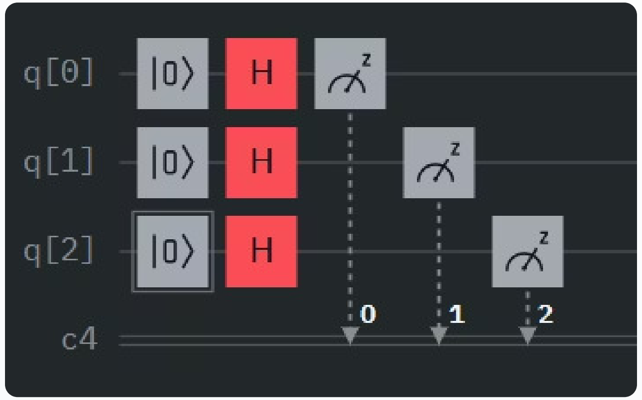
Quantum Random Number Generators (QRNGs) use **quantum superposition and measurement** to produce true randomness.

Introduction:

- A qubit is the fundamental unit of quantum information.
- Unlike a classical bit, it can exist in a superposition of 0 and 1 simultaneously.
- Measuring a qubit collapses it to either 0 or 1 with probabilities determined by its quantum state.

Circuit design:

- Three qubits initialized in $|0\rangle$ state.
- Apply **Hadamard gate** to each qubit → equal superposition of $|0\rangle$ and $|1\rangle$.
- Measure all qubits → produce random classical bitstrings.



Ensures **50% probability for 0 or 1** for each qubit, producing uniformly random outputs.

Calibration and Error Mitigation

Challenge:

- Quantum hardware and simulators introduce **systematic readout errors** and minor bias, affecting randomness quality.

Calibration Phase:

- Separate **calibration circuits** were constructed for all possible basis states (2^{n_q}).
- Measurements from these circuits form the **response matrix** M, which quantifies how actual measurements deviate from ideal outcomes.

Error Mitigation Process:

- The inverse of the calibration matrix M^{-1} is applied to the raw probability vector p_{raw}: $p_{mitigated} = M^{-1} \cdot \vec{p}_{raw}$
- This correction minimizes measurement bias and restores uniformity in probability distribution.
- Negative probabilities (due to inversion noise) are clipped to zero and renormalized.

Advantage of this method

- Produces a **bias-free**, physically consistent probability distribution.
- Prepares data for reliable statistical validation in the next analysis stage.
- Integrated **error mitigation** ensures minimal bias in output.

Analytical Framework

- Conducted up to **2048 measurement shots** per run to gather sufficient data for statistical analysis.
- Computed the **mitigated probability distribution** across all 2^{n_q} quantum states.

Statistical Tests Implemented:

- **Chi-Square Uniformity Test:** $\chi 2 = \sum_i \frac{(O_i - E_i)^2}{E_i}$
  - $p\text{-value} > 0.05$ → no significant deviation from uniform distribution.
- **Shannon Entropy Calculation:** $H = -\sum_i p_i \log_2 p_i$
  - Observed entropy $H \approx 2.99$H bits for 3 qubits (max = 3 bits) → near-perfect randomness.

Dynamic Configuration:

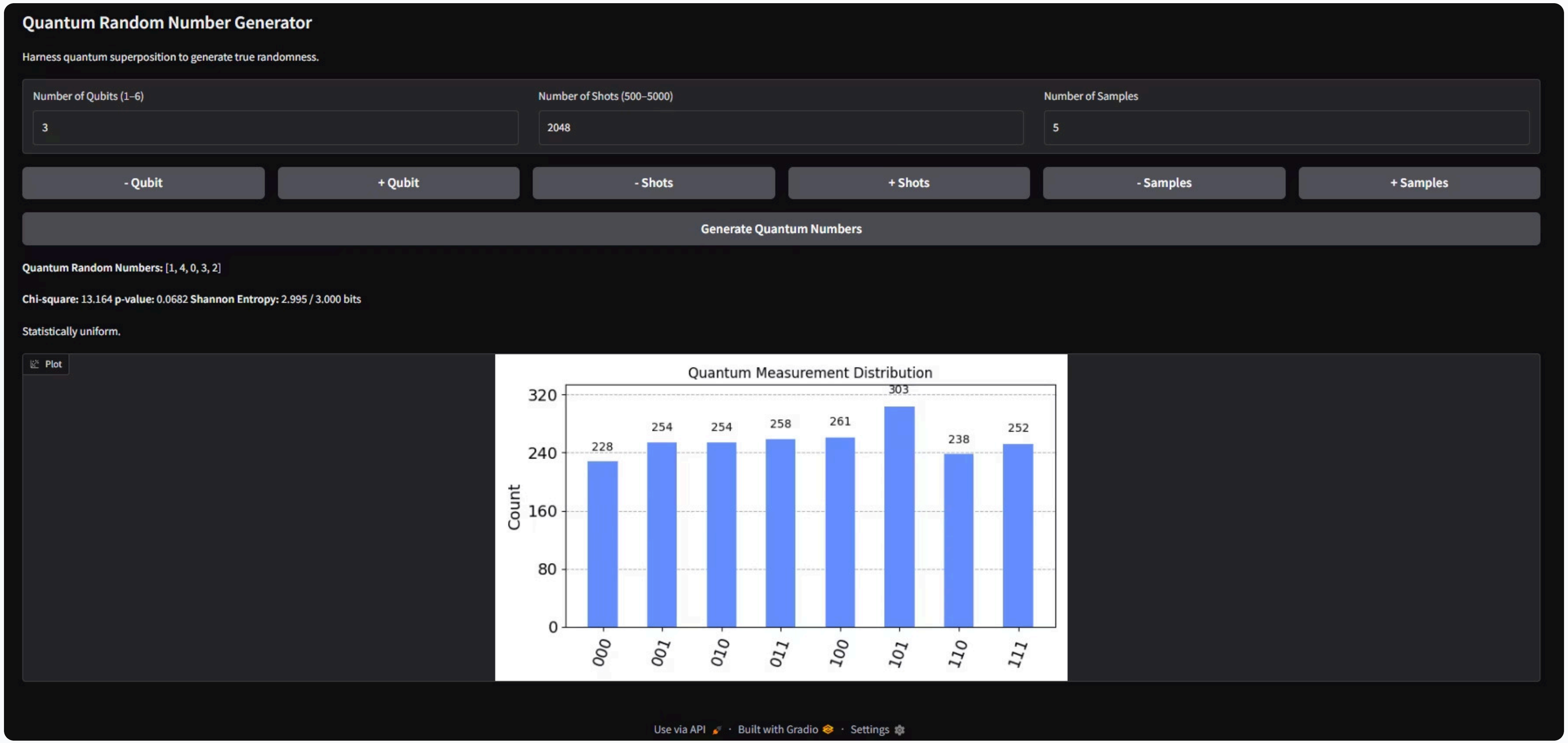
- **Qubits (1–6):** adjusts random bit precision.
- **Shots (500–5000):** controls statistical reliability.
- **Samples (1–20):** determines number of random outputs generated.

Conclusion

- Fully interactive QRNG with tunable parameters and built-in error mitigation.
- Achieves high entropy and unbiased randomness suitable for **secure, reproducible, and verifiable** quantum random number generation.

Live Demo Interface

> Hosted on **Hugging Face Spaces** for live access: https://huggingface.co/spaces/lvsl/qrng-demoh



Github link: https://github.com/Lalitha124/qrng-demo

Made with GAMMA

Thank You

Lalitha Lakkaraju

Roll No: M25IQT007

MTech Quantum Technologies 1st Year