Hybrid Quantum Random Number Generator (QRNG)

—

combination of electronic shot noise + multi-layer quantum randomness in a simple, fully simulated Qiskit environment.

Content

- Goal: Generate high-quality random numbers using quantum mechanics.
- Key Idea: Combine electronic shot noise with quantum superposition and optional entanglement (CNOT gates).
- Motivation: True randomness is crucial for cryptography, simulations, and quantum computing applications.

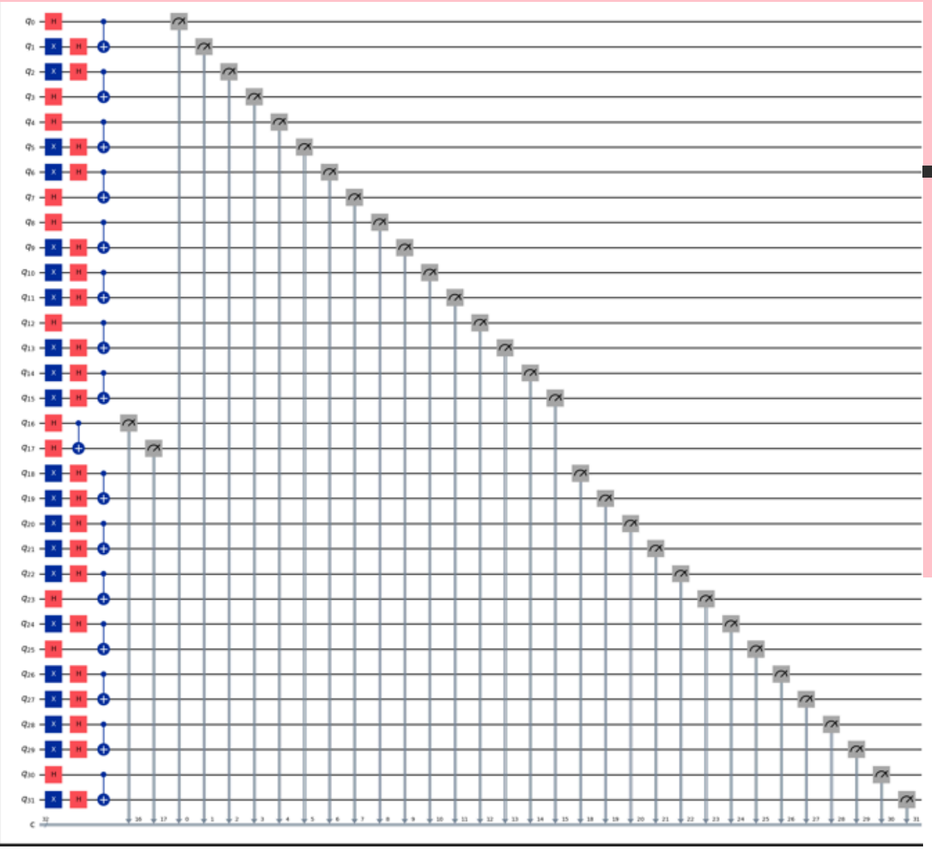
Electronic Shot Noise

- Definition: Electronic shot noise is the fluctuation in electric current due to the discrete nature of charge carriers (usually electrons) in a conductor.
- Physical Origin: It arises fundamentally from the quantum nature of charge and is especially relevant at low currents or in photonic/electronic systems.
- Significance: This intrinsic unpredictability is harnessed for random number generation since it presents true quantum randomness as opposed to algorithmic pseudorandomness

Python Simulation of Shot Noise

- Simulation Steps:
- Uses numpy.random.choice to generate binary random bits simulating the detection of single electrons/photons in a time interval.
- These bits initialize the state of qubits in the quantum circuit, serving as classical random input.
- Role in QRNG: The shot noise simulates a classical entropy pool for the hybrid scheme, ensuring entropy injection is not solely algorithmic.

Core Quantum Circuit Design

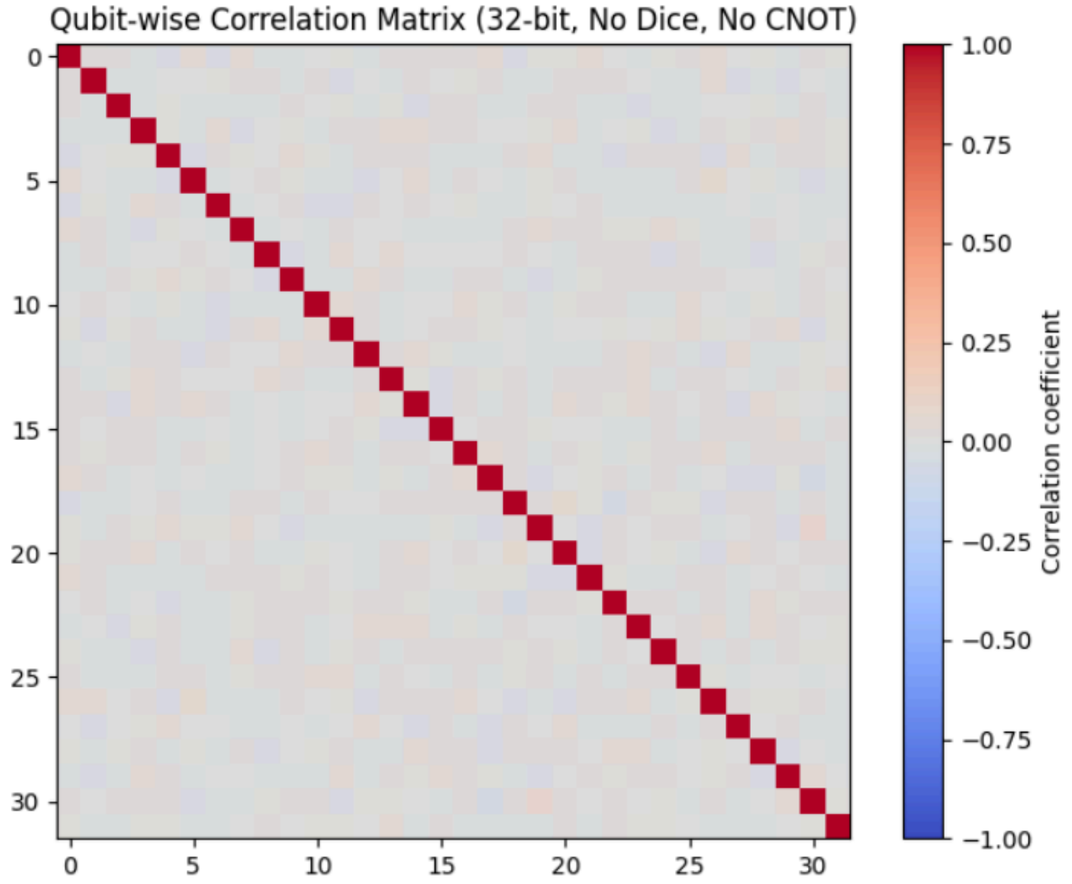


- Design:
- Qubits: 32 qubits
- Initialization: Set to shot noise bits using X gates
- Superposition: Hadamard gate applied to all qubits
- CNOT (optional): Adds entanglement for increased randomness
- Dice logic (optional):
- Randomly pairs qubits for CNOT
- Random measurement order

No Dice No C-Not

2000 shots

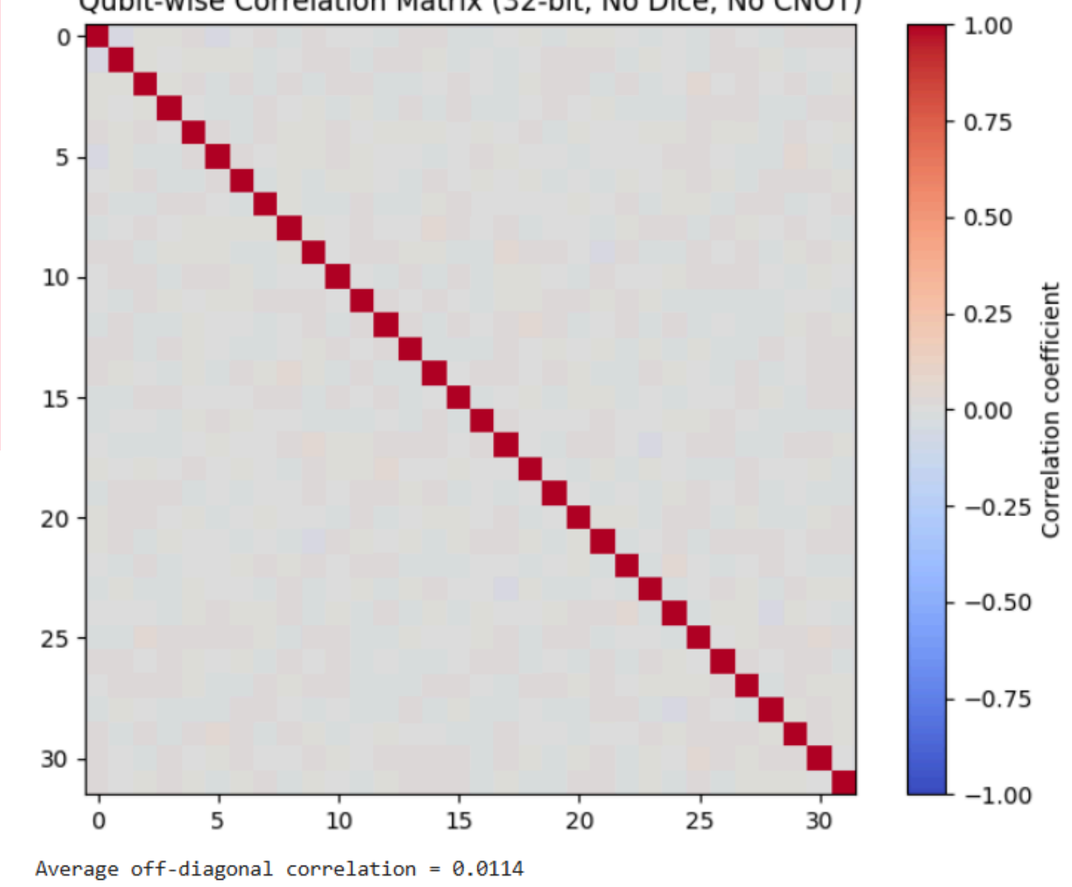
```
Example random number generated: 1766896316
Shannon entropy: 10.9658 bits (max = 32)
Min-entropy: 10.9658 bits
```




```
Average off-diagonal correlation = 0.0171
```

5000shots

```
Example random number generated: 2779394142
Shannon entropy: 12.2877 bits (max = 32)
Min-entropy: 12.2877 bits
```

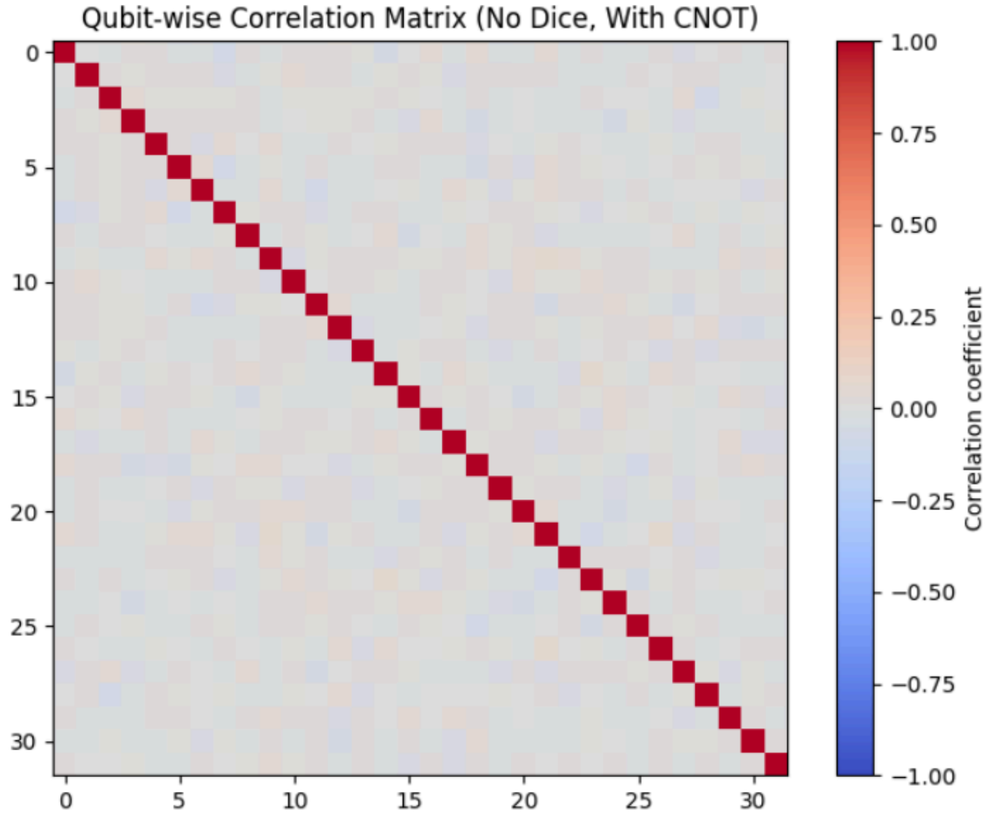



```
Average off-diagonal correlation = 0.0114
```

No Dice with C-Not

2000 shots

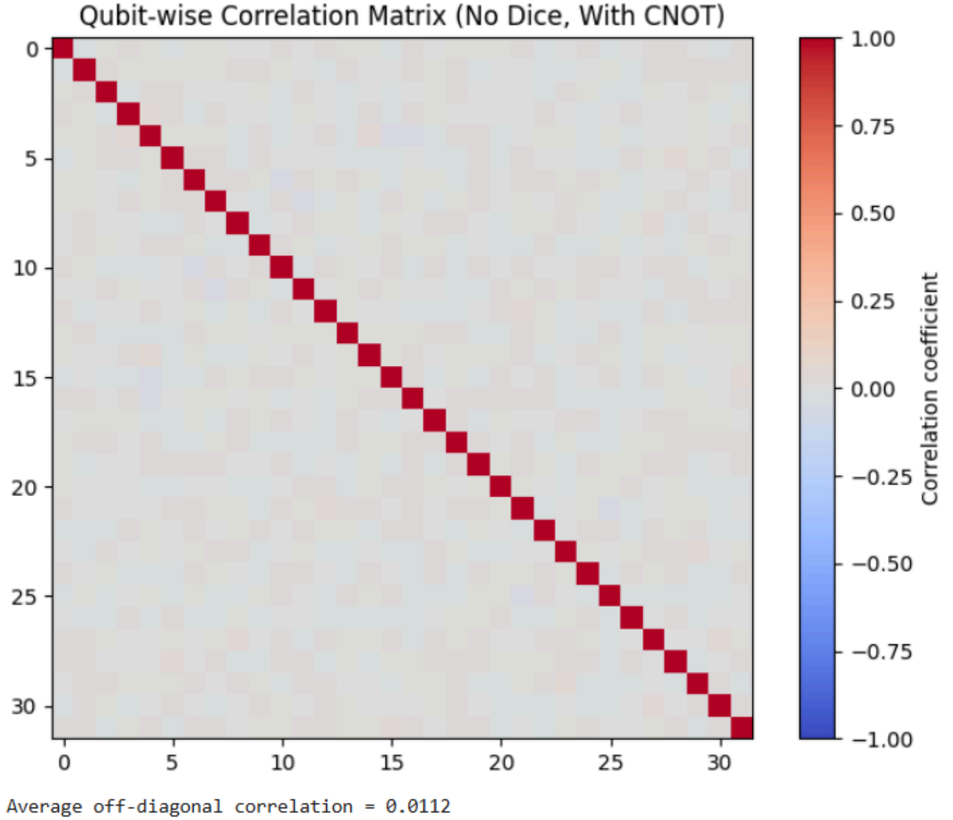
Example random number generated: 598628882
Shannon entropy: 10.9658 bits (max = 32)
Min-entropy: 10.9658 bits



Average off-diagonal correlation = 0.0188

5000 shots

Example random number generated: 2274344145
Shannon entropy: 12.2873 bits (max = 32)
Min-entropy: 11.2877 bits

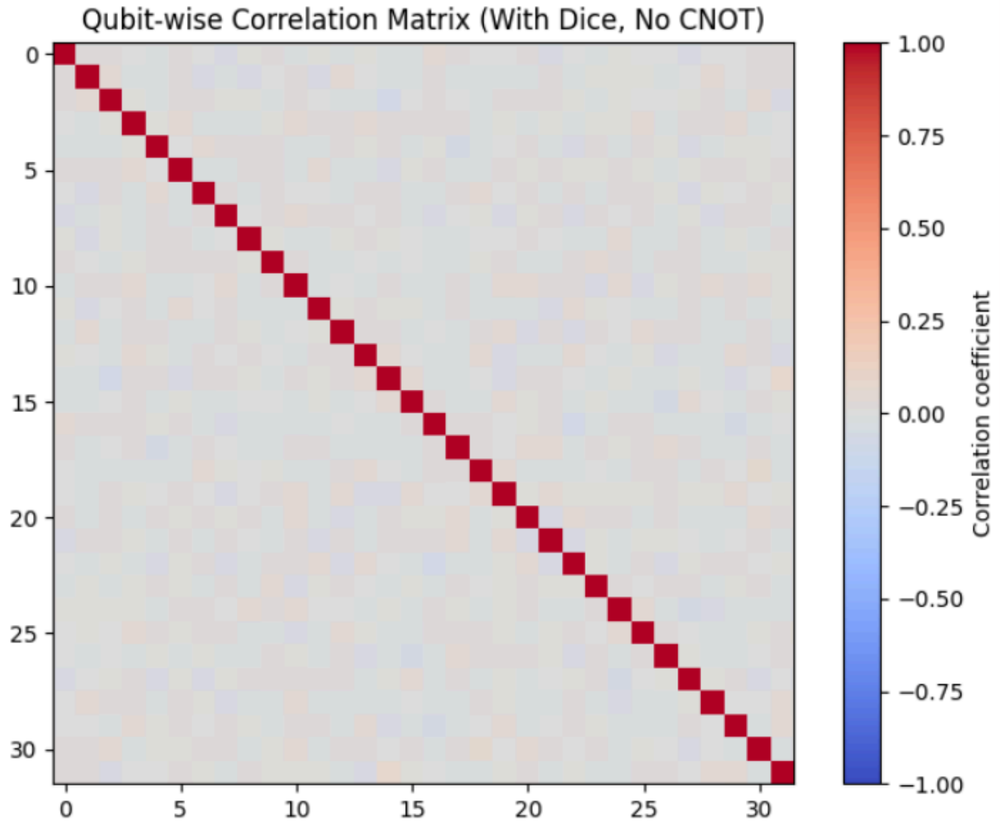


Average off-diagonal correlation = 0.0112

With Dice without C-Not

2000 shots

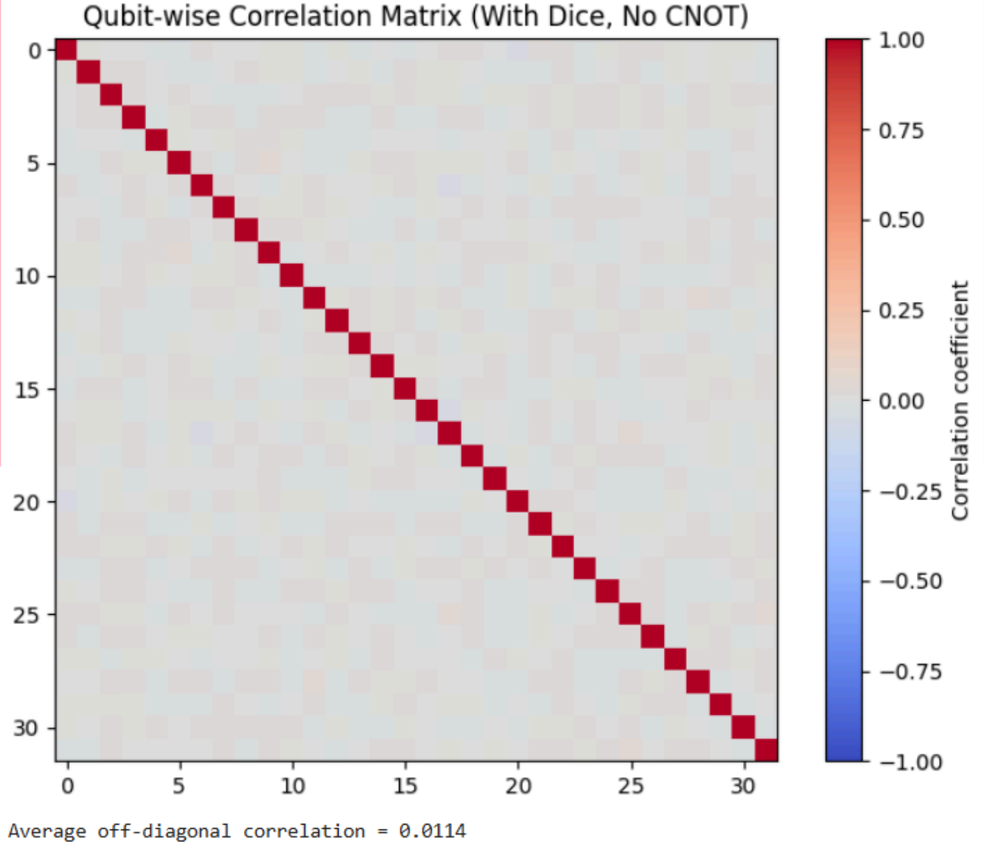
```
Example random number generated: 873074882
Shannon entropy: 10.9658 bits (max = 32)
Min-entropy: 10.9658 bits
```




```
Average off-diagonal correlation = 0.0180
```

5000 shots

```
Example random number generated: 3050892603
Shannon entropy: 12.2877 bits (max = 32)
Min-entropy: 12.2877 bits
```

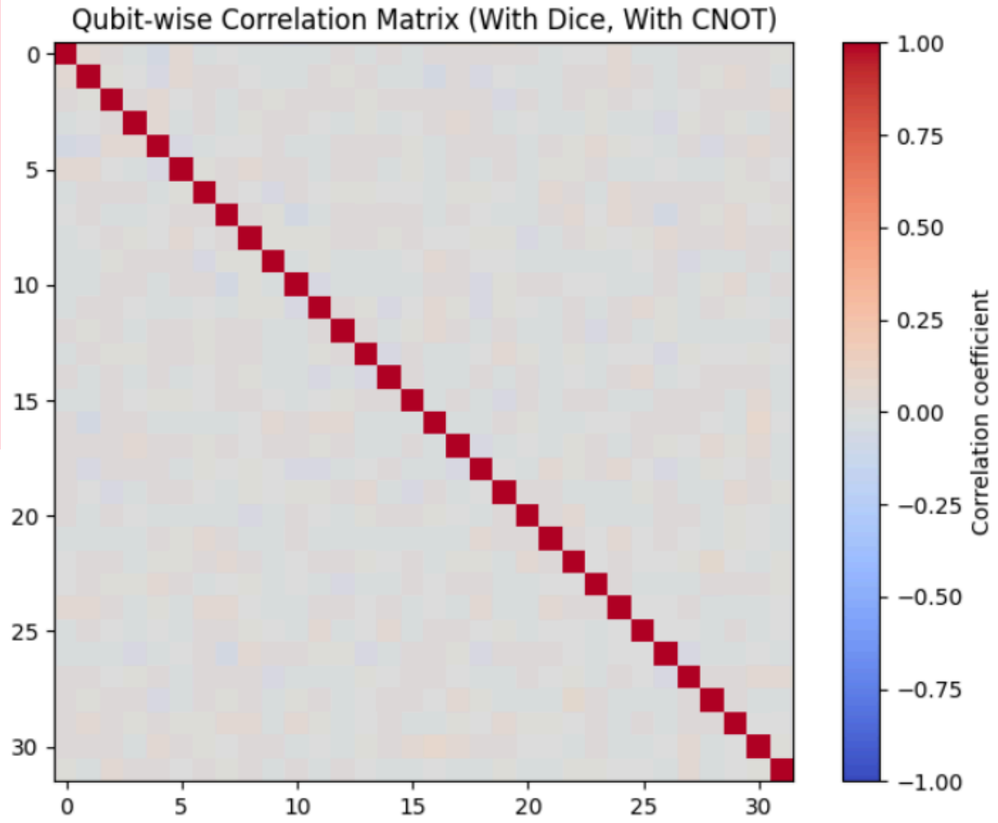



```
Average off-diagonal correlation = 0.0114
```

With Dice withC-Not

2000 shots

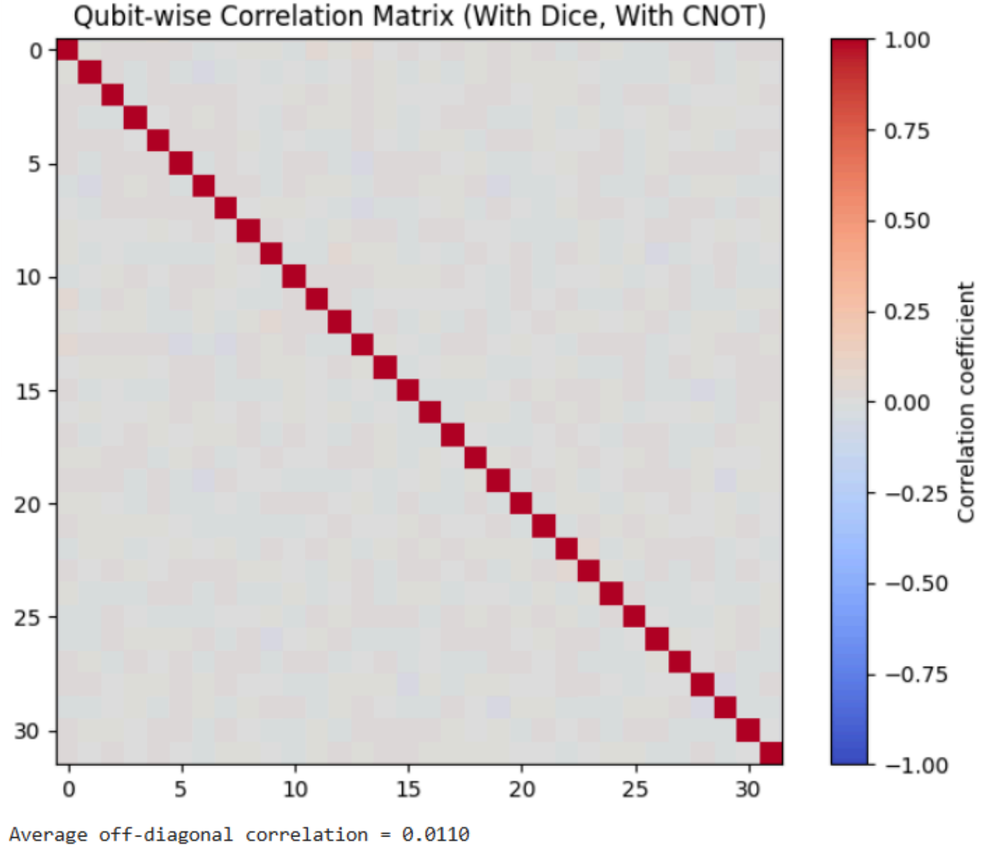
Example random number generated: 595616887
Shannon entropy: 10.9658 bits (max = 32)
Min-entropy: 10.9658 bits



Average off-diagonal correlation = 0.0166

5000 shots

Example random number generated: 277934150
Shannon entropy: 12.2877 bits (max = 32)
Min-entropy: 12.2877 bits



Average off-diagonal correlation = 0.0110

Comparison of 8 Cases (Average Off-Diagonal Correlation)

Case	Dice	CNOT	Shots	Avg Off-Diagonal Correlation	Observation
1	No	No	2000	0.0171	Baseline, moderate correlation
2	No	No	5000	0.0114	More shots stabilize output, correlation decreases
3	No	Yes	2000	0.0188	CNOT reduces correlation slightly
4	No	Yes	5000	0.0112	More shots further reduce correlation
5	Yes	No	2000	0.018	Dice reduces bias in measurement order, correlation still moderate
6	Yes	No	5000	0.0114	More shots stabilize distribution
7	Yes	Yes	2000	0.0166	Dice + CNOT reduces bias, improves randomness
8	Yes	Yes	5000	0.011	**Lowest correlation, best performance**

Conclusion

- Best performing configuration: Dice + CNOT, 5000 shots(lowest average off-diagonal correlation = 0.0110).
- Key Points:
- Combines classical and quantum randomness
- Dice logic reduces correlation and bias
- 32-bit strings are sufficient for basic cryptography / simulations

Final Recommendation:

- For a 32-bit hybrid QRNG with shot-noise initialization:
- Use Dice + CNOT + 5000 shots for most uniform, low-correlation, high-entropy output.
- Other configurations still produce reasonable randomness but are slightly less optimal.

Why This Project is Unique & Innovative

1. Hybrid Randomness Approach

- Combines classical electronic shot-noise simulation with quantum superposition for randomness.
- Goes beyond standard quantum RNGs that only rely on qubits.

2. Multi-Layer Randomness Enhancement

- Introduced Dice logic to randomize measurement order.
- Applied CNOT gates to induce entanglement and reduce qubit correlations.
- Tested with multiple shots (2000 & 5000) to optimize randomness and stability.

Why This Project is Unique & Innovative

3. Comprehensive Simulation & Analysis

32-bit quantum circuit modeled fully in Qiskit.

Detailed analysis including:

Shannon entropy & Min-entropy

Qubit-wise correlation heatmaps

Comparison across 8 different configurations

Provides a thorough quantitative understanding of quantum-classical hybrid RNG performance.

4. Practical Relevance

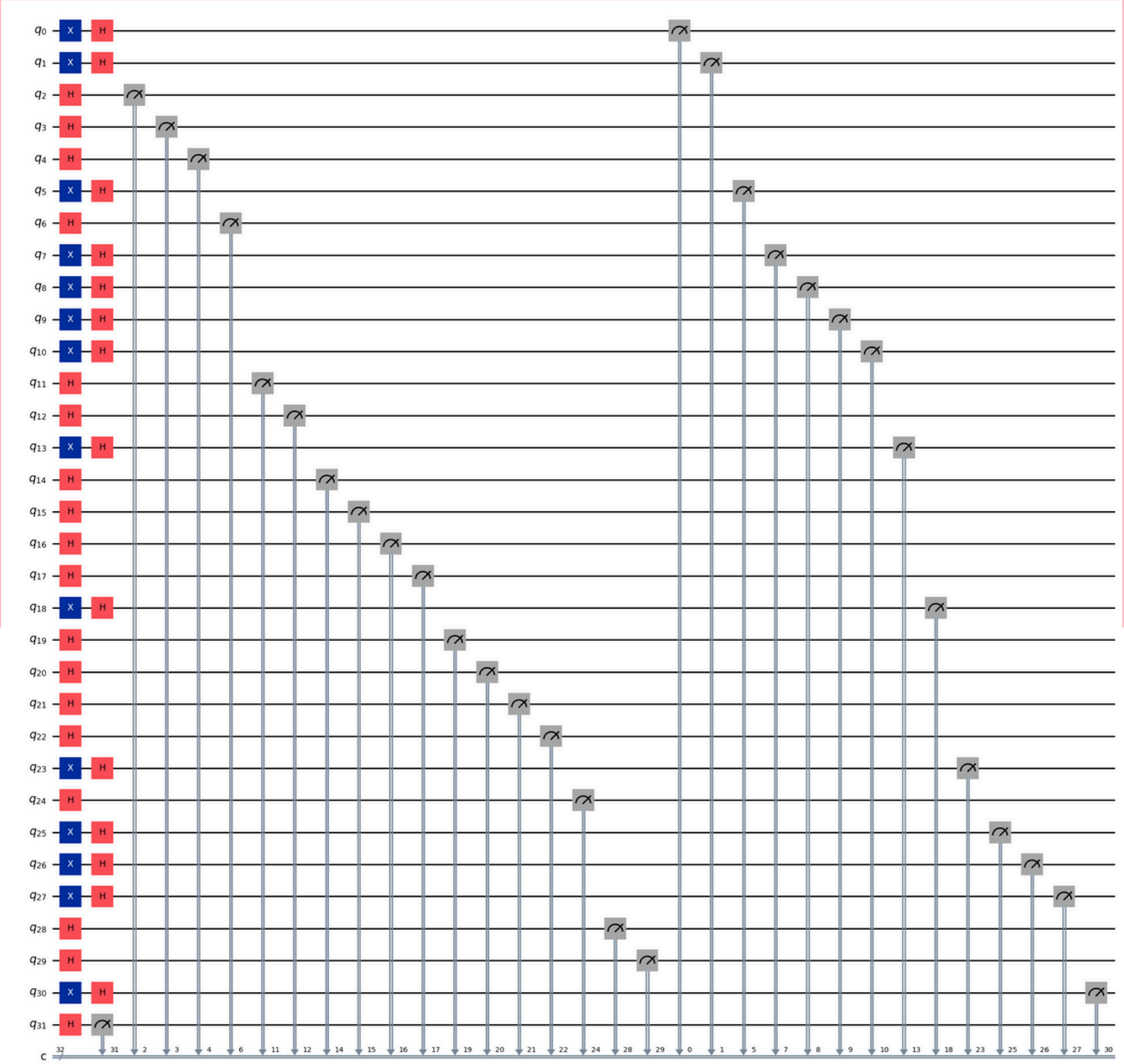
Results demonstrate a low-correlation, high-entropy random number generator, suitable for:

Cryptography

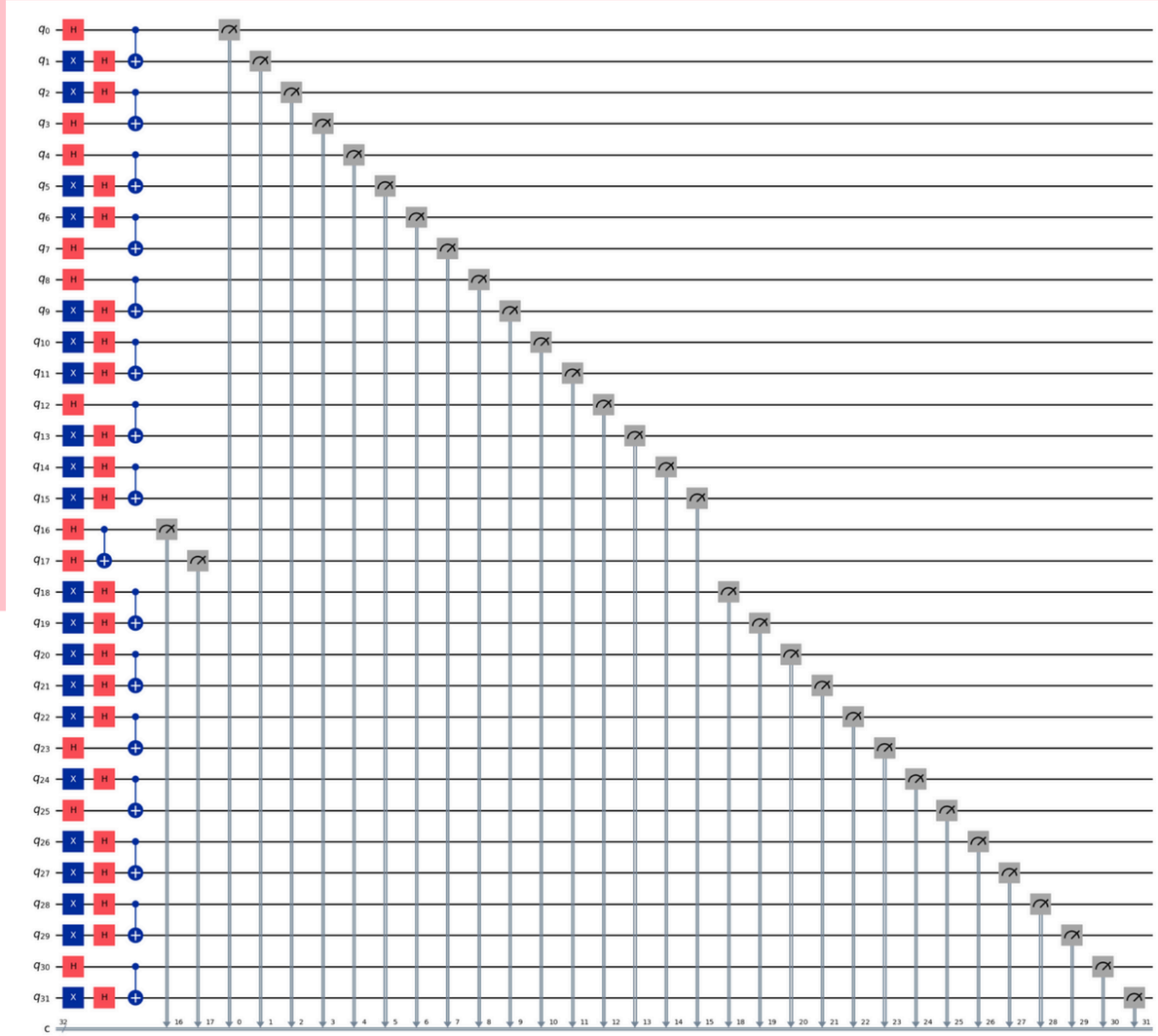
Simulations in quantum computing

Benchmarking quantum algorithms

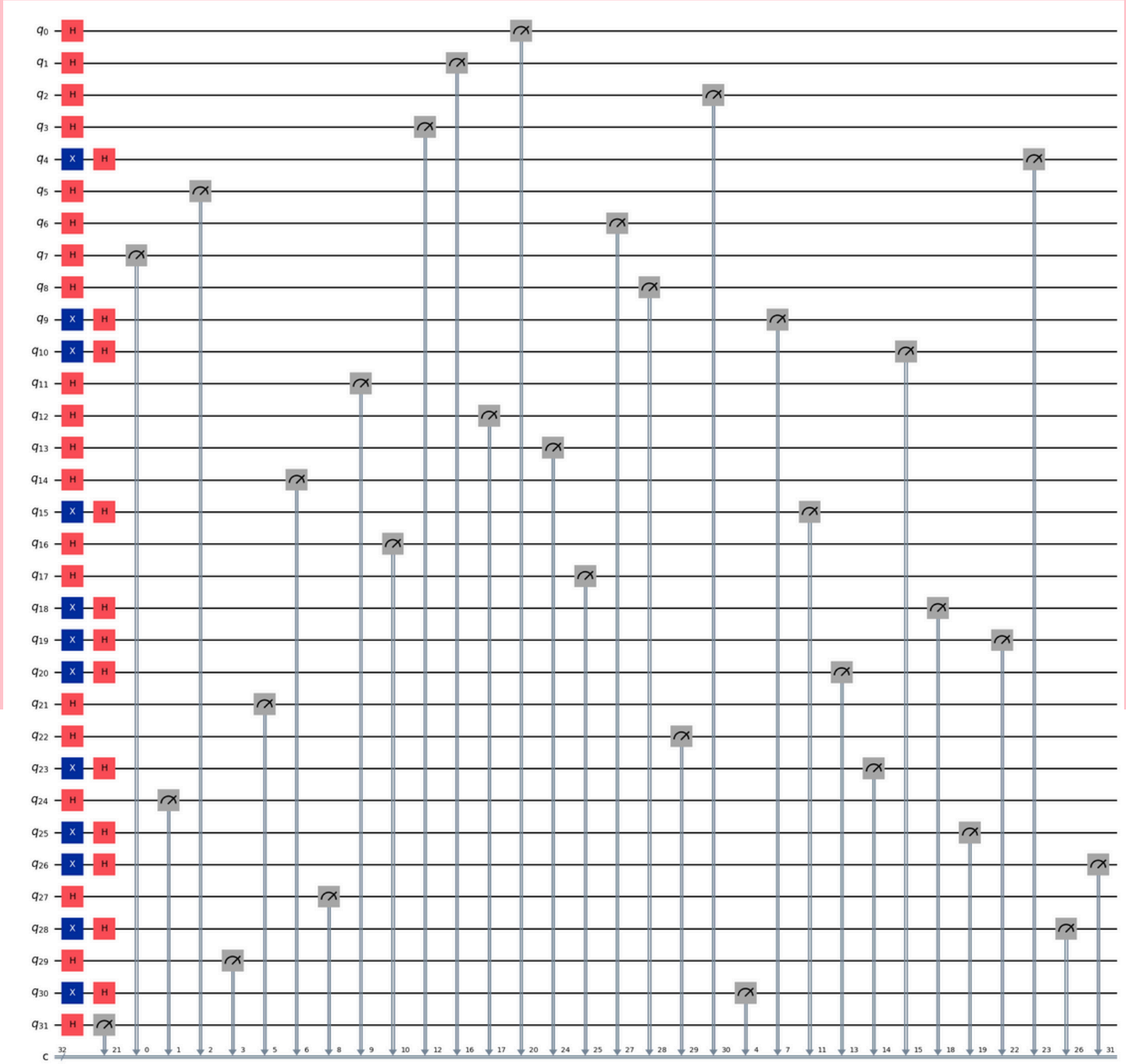
No Dice without C-Not



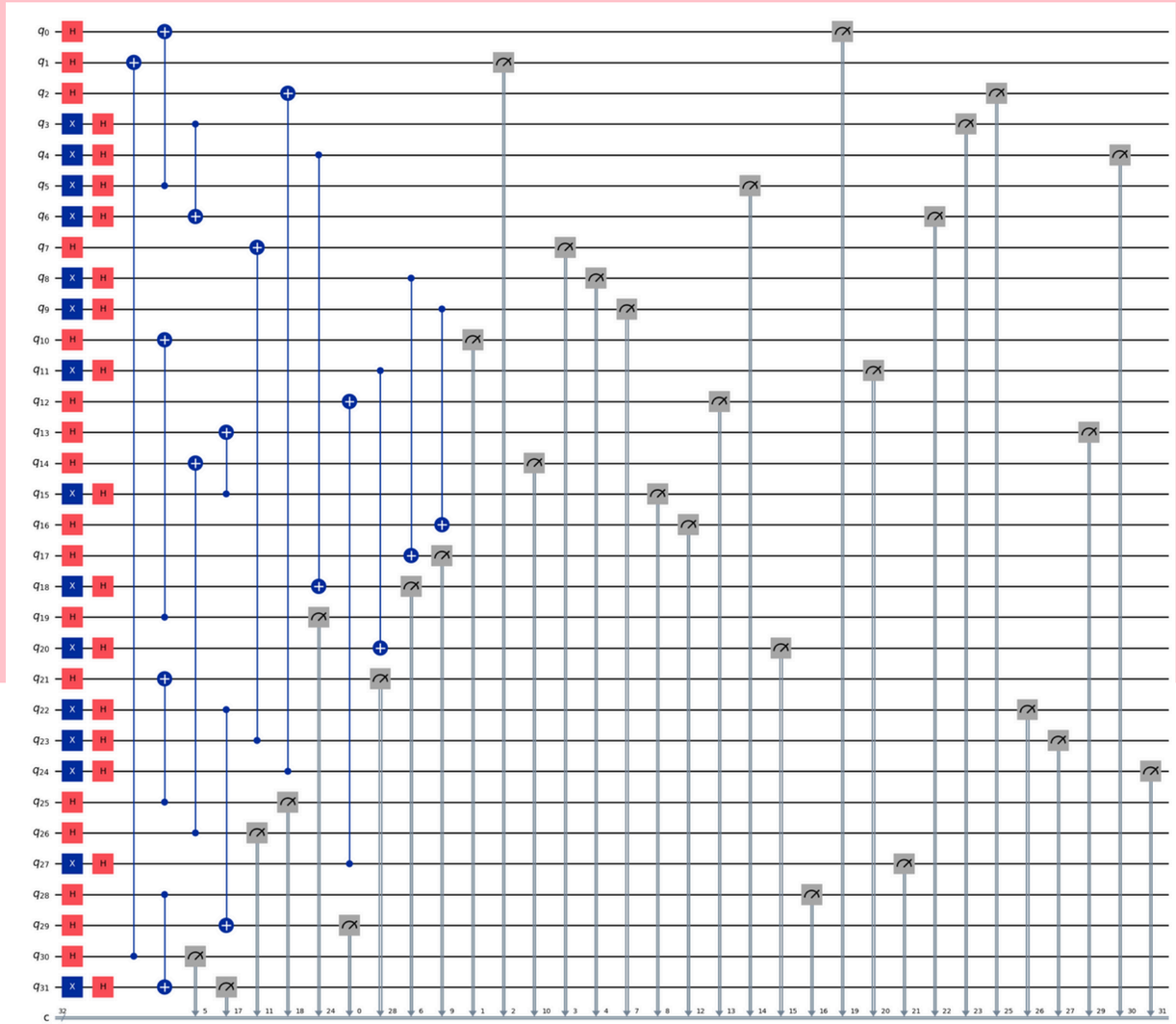
No Dice with C-Not



With Dice without C-Not



With Dice with C-Not



Thank You