A Walk in Quantum Land

Vincent Cai, Daniel Jung, Jacob Paras,
Rohan Phanse, and Marcus Schubert

MRJDV

01

Quantum Circuit Design

Lively Quantum Random Walk

Liveliness

Parameter that controls step size of a random walk

Control

Classically parameterized by input, generates a quantum superposition step state over one or more qubits

Quantum Random Walk

Increment and decrement step functions controlled by ancilla qubits after coin function operation.

Quantum Random Walk & Step Function

Step Function

Circuit that maps every basis state to the next basis state or previous basis state (increment or decrement).

Coin Function

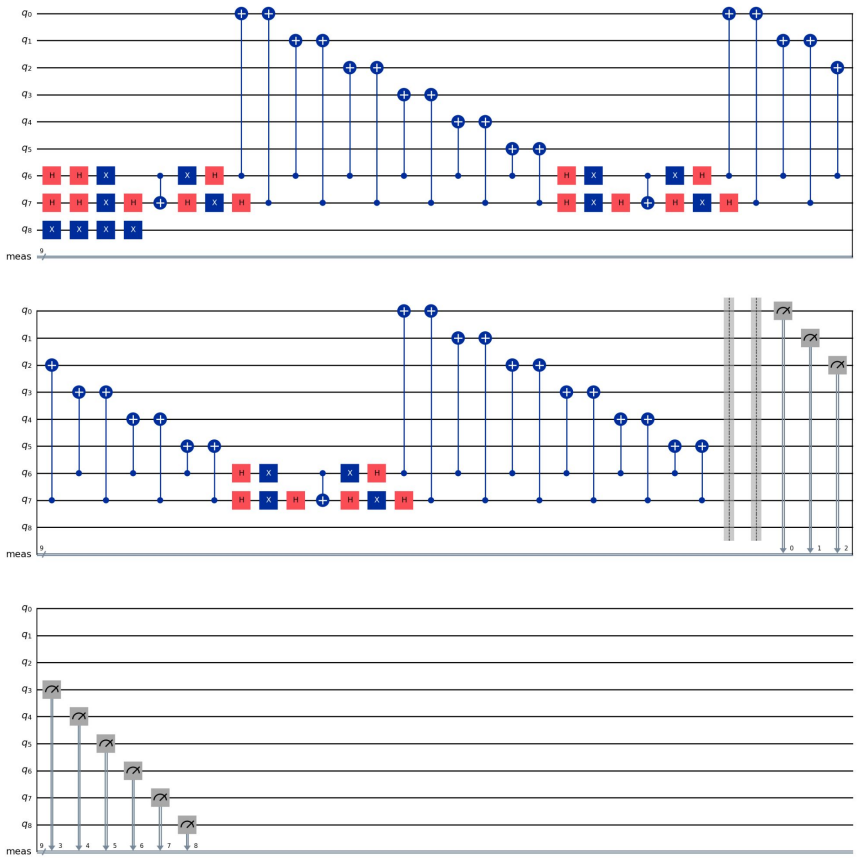
Generates a classically parameterized qutrit control register (superposition over three possible coin states)

Shift Function

Relies on the bit state to modify the coin and “shift” operators applied that bit.

The Circuit

Generated for bitstring message “101” with N=32 (2^5).

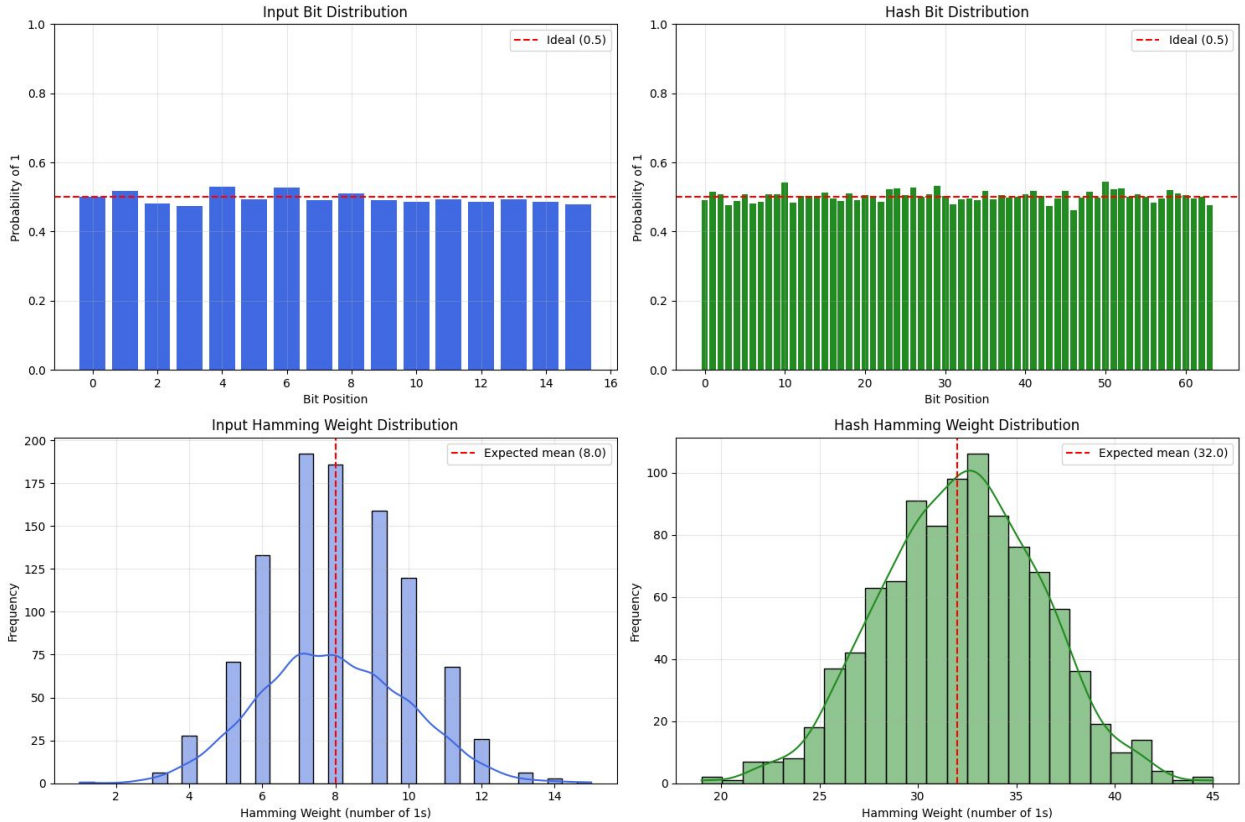


02

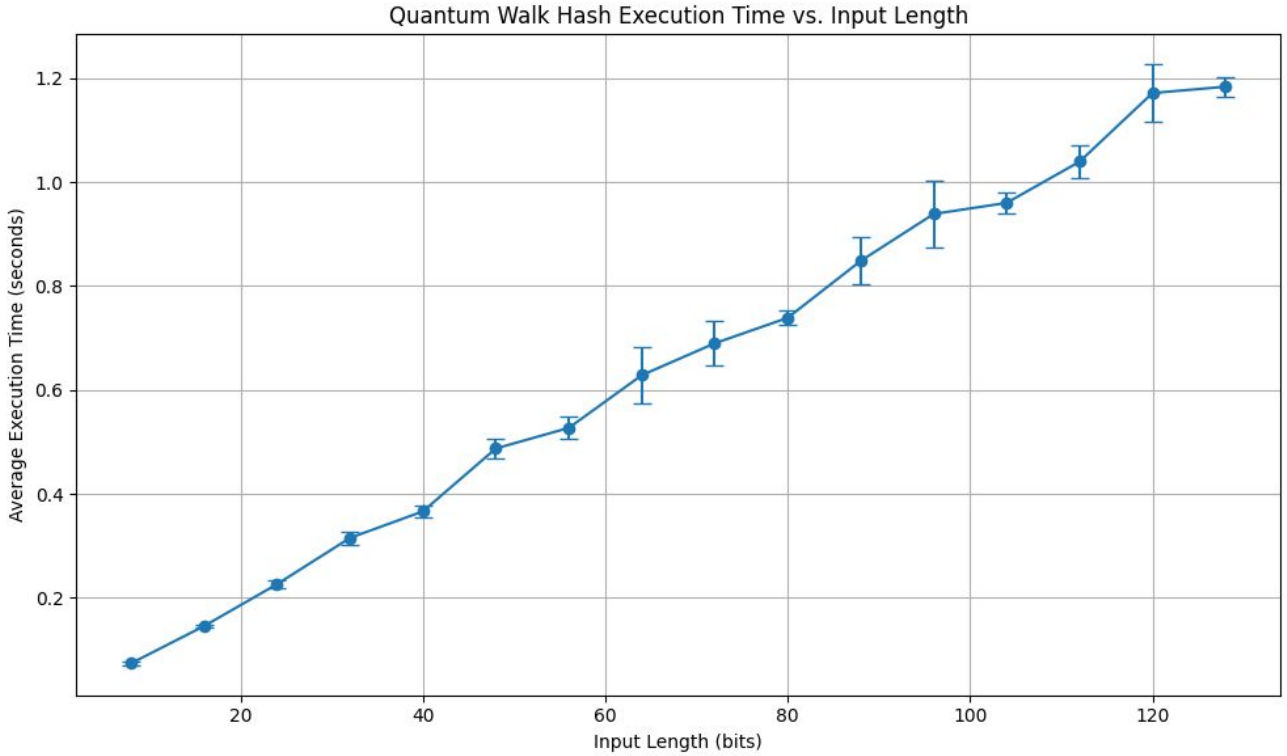
Testing the Hash

Preservation of Entropy

Comparison of the input and output distributions:

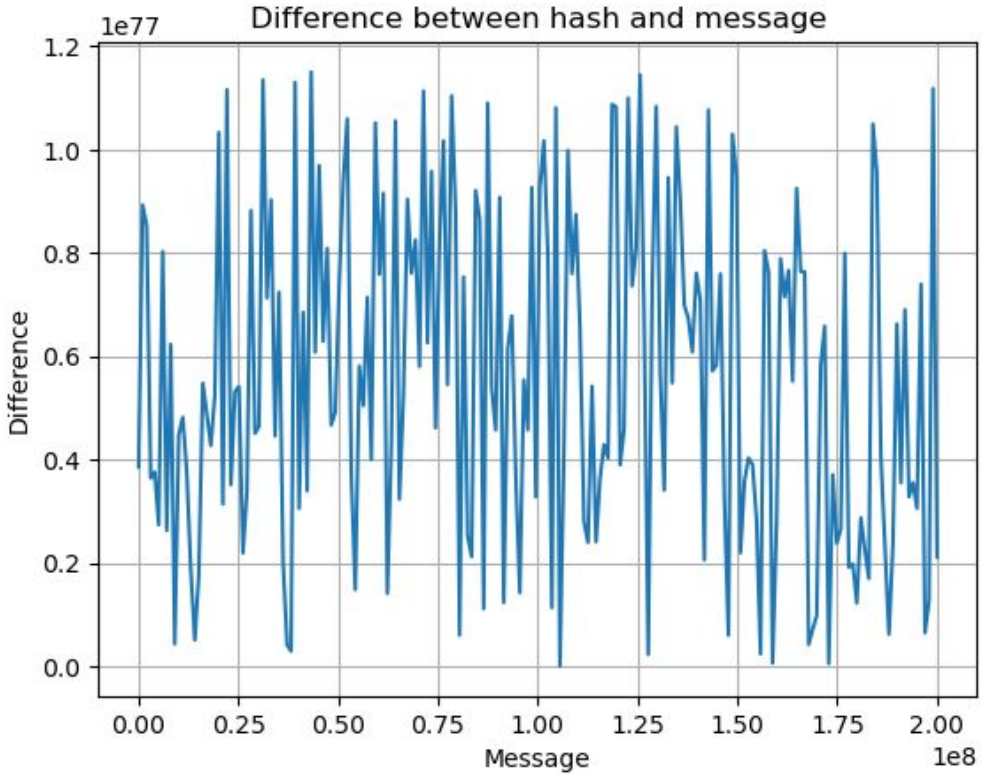


Computation Time



Preimage Resistance

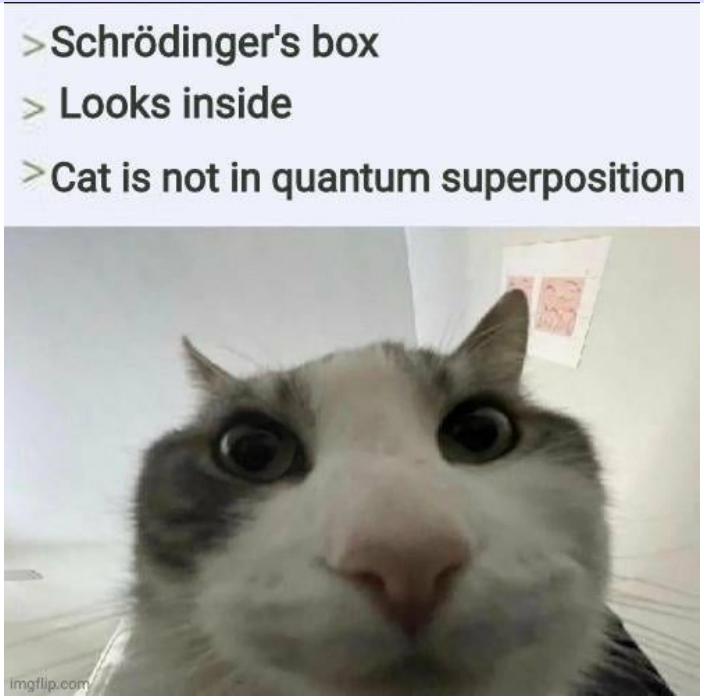
Measuring difference between the hashed output and the input message (bits converted to integers):



Other Evaluation Criteria

Output Determinism	• No stochastic parameters in circuit • embedding and postprocessing are deterministic processes • For various inputs: 1500 iterations, same input ⟶ same output
Computational Difficulty	• O(N) • Time complexity scales linearly with the number of input bits
Collision Resistance	• 2 million iterations with 0 collisions (GPU accelerated)
Computational Feasibility	• 5 (position) + 2 (coin operator) + 1 (message) = 8 cubits

Questions?


>Schrödinger's box
> Looks inside
>Cat is not in quantum superposition
imgflip.com

THANK YOU

MRJDV