Wavefunction Warriors - Quantum Hash Writeup

By: Nicholas Gould, Krish Majethia, Nandan Patel, Sanskriti, Sabri

Our circuit for Quantum Hashing involved Quantum Walking and Random Unitaries to meet the following criteria: Output Determinism, Entropy Preservation, Computational Difficulty, Preimage & Collision Resistance, Feasibility, Speed, and Purely Quantum Hashing.

In our first set of random unitaries, we take 2 bits from the input message and encode them onto the message register. Then, we map the state of the message register to a unitary that gets applied to the coin register.

Depending on the state of the message and coin qubits, we perform a quantum walk. For the quantum states where the coin qubit is a |1>, we increment the position register of the quantum walk. Conversely, for states where the coin is |0>, we decrement the position register. The reason for the quantum walk is to randomize the output while still retaining output determinism.

Before the final measurement, we create a random unitary generated by Qiskit that is based on the input message. The purpose of the random unitary is to reduce collisions along with the quantum walk.

With this implementation of quantum hashing, we demonstrated that efficient quantum hashing works on up to 256-bit inputs while using less than 20 qubits.