Applications of Quantum Randomness in Healthcare Informatics

Venkat, Anirudh (School: Huron High School)

The year 2022 saw the largest amount of healthcare data & device breaches in human history, with over 45 million individuals being affected. This trend is only growing. The backbone of current cryptographic systems is its ability to generate completely random keys. But in practice, this randomness is generated using pseudo-random number generators (PRNG), which is deterministic by design. Reputable PRNG's have been compromised by cybercriminals and state actors. Hardware based random number generators (using physical stimuli), though harder to hack, are slow, expensive and device dependent. In this work, I am proposing an alternative by constructing a True Random Number Generator (TRNG) using Quantum superposition. I developed a Quantum Random Number Generator (QRNG) on the Microsoft Azure cloud using the quantum computing language of Q#. The code was executed on an IonQ's trapped-ion real quantum computer with up to 11 qubits to generate Random number bits. Industry standard statistical tests (NIST 800-22) were executed to confirm the "true" randomness of the QRNG algorithm testing its a-periodicity, spectral ranking, non-predictability among others. Random numbers with bit stream lengths of 512 were generated using the QRNG algorithm and put through this series of test. The QRNG passed all the tests. The high P-value for entropy test showed that QRNGs are truly random and non-deterministic. Quantum random Number Generators (QRNG) can replace the current PRNG based cryptographic keys making our healthcare data and health related embedded devices secure.

Awards Won:
Central Intelligence Agency: First Award: $1000 award