Designing a Practical Quantum Network Using Standard Basis Rotation and Blockchain Verification

Meade, Evan (School: Keystone School)

The researcher has successfully designed a new quantum communication protocol which sends information directly on a quantum state. Due to the measurement principle and the no cloning theorem, communicating with quantum states has a unique capacity for protecting information and exposing eavesdroppers without requiring traditional encryption. A protocol such as the researcher's is increasingly valuable due to the rise of quantum computers, which threatens traditional encryption schemes. By employing a set of rotation operations selected from a closed, commutative group, two parties can perform a series of invertible transformations which ensure that the message state is immune to wiretapping, and reasonably immune to man-in-the-middle attacks. Additionally, a classical blockchain structure is used to help communicating parties verify each other's identities and expose attackers by constructing error rates. By analyzing contemporary research, the researcher has managed to select blockchain parameters which allow for the greatest resistance to attacks by quantum computers. The researcher verified his design through mathematical proofs, computer simulations, and experimental trials on an actual quantum computer. The proofs and simulations demonstrated that every case the protocol encounters leads to the correct measurement, thus establishing the theoretical validity of the design. The experimental data from the quantum computer returned above a 90% success rate over all trials, which is incredibly encouraging given current error rates in these machines. Given the promising results of the project, the protocol may soon be used to protect businesses, governments, and private citizens from certain types of monitoring, espionage, and cybercrime.

Awards Won:

Second Award of $2,000