Improving Upon Quantum Cryptography Protocols Using Entanglement and Quantum Signatures

Kulkarni, Rohan (School: Montgomery High School)
Sharma, Ansh (School: West Windor-Plainsboro High School South)

With the advent of quantum computation methods such as Shor's algorithm to factor large primes, classical encryption protocols are rendered ineffective, necessitating new quantum cryptographic methods. BB84 is a prominent quantum key distribution protocol that utilizes the quantum no-cloning theorem to allow Alice and Bob to communicate and detect any interception from an eavesdropper Eve. However, the algorithm has considerable limitations: only an average of 50% of the bit sequence is retained in the final shared key and there are no means of authenticating the message sender's identity. We reduce the inefficient retention rate by utilizing quantum entangled systems, allowing select qubits to be added to the final one-time codepad regardless of their basis compatibility. Implementation of the entanglement scheme demonstrates successful increases in retention, generating shared keys with a longer average length than those produced by the traditional BB84 protocol. In our case study with n=10 bits in the initial sequence and one entangled pair of qubits, the algorithm successfully increases the key length by one bit, an improvement from 50% to 60% average efficiency. Furthermore, we propose increasing the number of entanglement pairs to provide more substantial retention improvements for large values of n. For example, entangling 0.2n qubits corresponds to a 0.1n average retention benefit. We also devise a quantum signature to augment the protocol with a method of verifying the sender's authenticity without leaking information about the message itself. Our implementation of the signature protocol is provably secure, utilizing a public quantum signature rendered from the sender's basis choices and the quantum swap test to verify the identity of the message sender.

Awards Won:
King Abdulaziz &amp
his Companions Foundation for Giftedness and Creativity: On-line Mawhiba Universal Enrichment Program
King Abdulaziz &amp
his Companions Foundation for Giftedness and Creativity: Award of $500
Air Force Research Laboratory on behalf of the United States Air Force: First Award of $750 in each Regeneron ISEF Category