Simulating Quantum Key Distribution in Three Polarization Bases

Panebianco, Katherine (School: North Carolina School of Science and Mathematics)

With the rise in quantum computing’s potential to break current encryption schemes, new methods of data encryption are needed to keep messages secure. Quantum Key Distribution (QKD) presents a solution that ensures perfectly secure encryption by utilizing the superposition and measurement of quantum states in various polarization bases. Our research simulated an established method of QKD in two polarization bases (BB84 Protocol) and a proposed new method in three polarization bases (3 Basis Protocol). Data collection focused on the key rate (number of particles sent to obtain a key of a certain length) in a non-eavesdropper setting and error rate (percentage of the key that contains errors) in an eavesdropper setting. We hypothesized that the 3 Basis Protocol would have a key rate of 0.33, lower than the BB84 Protocol’s 0.5 key rate, but that the BB84 Protocol would have a lower error rate (of 0.25), making it harder to catch an eavesdropper. Five hundred simulations were run of each protocol, confirming the 3 Basis Protocol’s hypothesized lower key rate of 0.33, but revealing both protocols to have an error rate of 0.25. These results suggest that there is no efficiency advantage in adding a third basis to QKD procedures. Further experimentation with the number of bases in QKD protocols has proved that the 0.25 error rate is constant for any number of bases, supporting the conclusion that the two basis BB84 Protocol remains the most efficient.