Quantum Key Distribution

Natalie Tirabassi, James Wolf, Nolan Brant, Troy Hueni

Cleveland State University

ABSTRACT

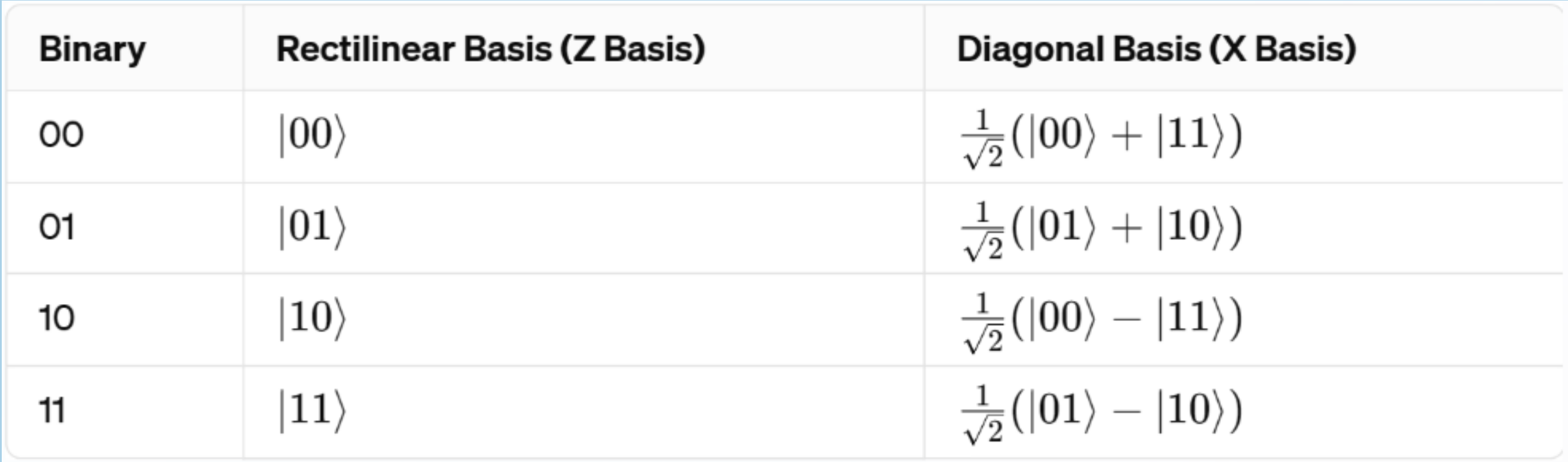
In today's world, information can be shared faster than ever. With technology becoming more advanced, sensitive information needs to be secure and just as fast. Quantum computing could be the answer to efficient and safe communication. Quantum Key Distribution is a cutting-edge cryptographic protocol that uses quantum mechanics to secure communication channels. By utilizing the quantum properties of entanglement and superposition, this technology enables the creation of unbreakable encryption keys, providing a secure means of exchanging information. Our project focuses on investigating different QKD protocols, including BB84, E91, and B92 to illuminate their operational mechanisms and significance. This research should help to foster a more secure foundation for the future of secure communications in the quantum era.

INTRODUCTION

Quantum Key Distribution is a secure communication method which uses photons to encode a message. These photons are transmitted through fiber optic cables between the communicating parties. The individual photons have random quantum states, and when received, the photons are sent through a beam splitter and take one of two paths into a photon collector. Then the receiver responds to the sender with data of the sequence, which is then compared with the data from the emitter, which sent each photon. Once this process is completed, binary code can be pulled from the data and the information can be decoded.

METHODS

In quantum key distribution, a two-level system is used to encode information based on photon polarization. The rectilinear basis represents binary 0 with photons at 0 degrees (|H⟩) and binary 1 with photons at 90 degrees (|V⟩). The diagonal basis encodes binary 0 with 45-degree photons in a diagonal orientation (|D⟩) and binary 1 with 45-degree photons in the opposite diagonal (|A⟩). These polarization bases form the fundamental framework for quantum communication protocols, allowing secure transmission of information through quantum channels.

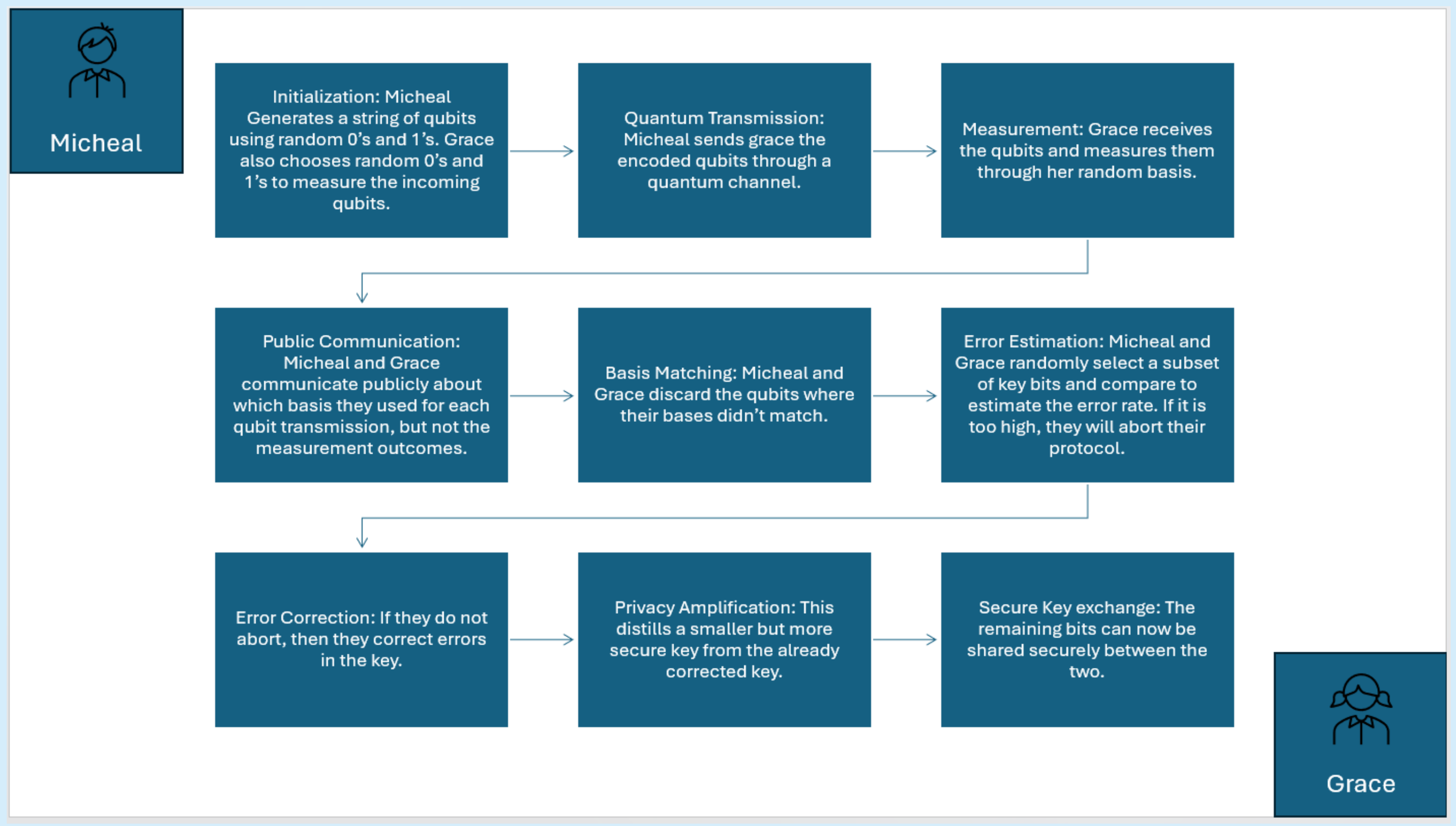


Binary	Rectilinear Basis (Z Basis)	Diagonal Basis (X Basis)
00	$\|00\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
01	$\|01\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$
10	$\|10\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
11	$\|11\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$

Figure 1. QKD Language Chart

RESULTS

The BB84 protocol enables secure information transmission between Michael and Grace while detecting eavesdropping by Eve. Michael sends photons encoded with a private key, protected by the no-cloning theorem against undetectable interception. They communicate over a Quantum Channel, with Michael sending random bits and bases to Grace. Grace measures photon polarizations based on randomly chosen bases, decoding Michael's bits. After sharing bases information publicly and removing mismatched bits, they obtain an identical shifted key. Comparing parts of this key helps detect Eve; any discrepancies prompt a key reset via another Quantum Channel.



Initialization: Micheal Generates a string of qubits using random 0's and 1's. Grace also chooses random 0's and 1's to measure the incoming qubits.

Quantum Transmission: Micheal sends grace the encoded qubits through a quantum channel.

Measurement: Grace receives the qubits and measures them through her random basis.

Public Communication: Micheal and Grace communicate publicly about which basis they used for each qubit transmission, but not the measurement outcomes.

Basis Matching: Micheal and Grace discard the qubits where their bases didn't match.

Error Estimation: Micheal and Grace randomly select a subset of key bits and compare to estimate the error rate. If it is too high, they will abort their protocol.

Error Correction: If they do not abort, then they correct errors in the key.

Privacy Amplification: This distills a smaller but more secure key from the already corrected key.

Secure Key exchange: The remaining bits can now be shared securely between the two.

Figure 2. Basic QKD Communication Example

The Eckert 91 protocol, or E91, uses a single source of photons which generates quantum entangled pairs of photons. One photon from each pair will be sent to the two communicating parties. Once all the photons have been received, the photons will be measured, and the message can be deciphered.

The B92 protocol is a simplified version of BB84 in which a binary system is used. With B92, the bits decide which bases the sender must use. The receiver will still select random bases to uncover the bits they have been sent.

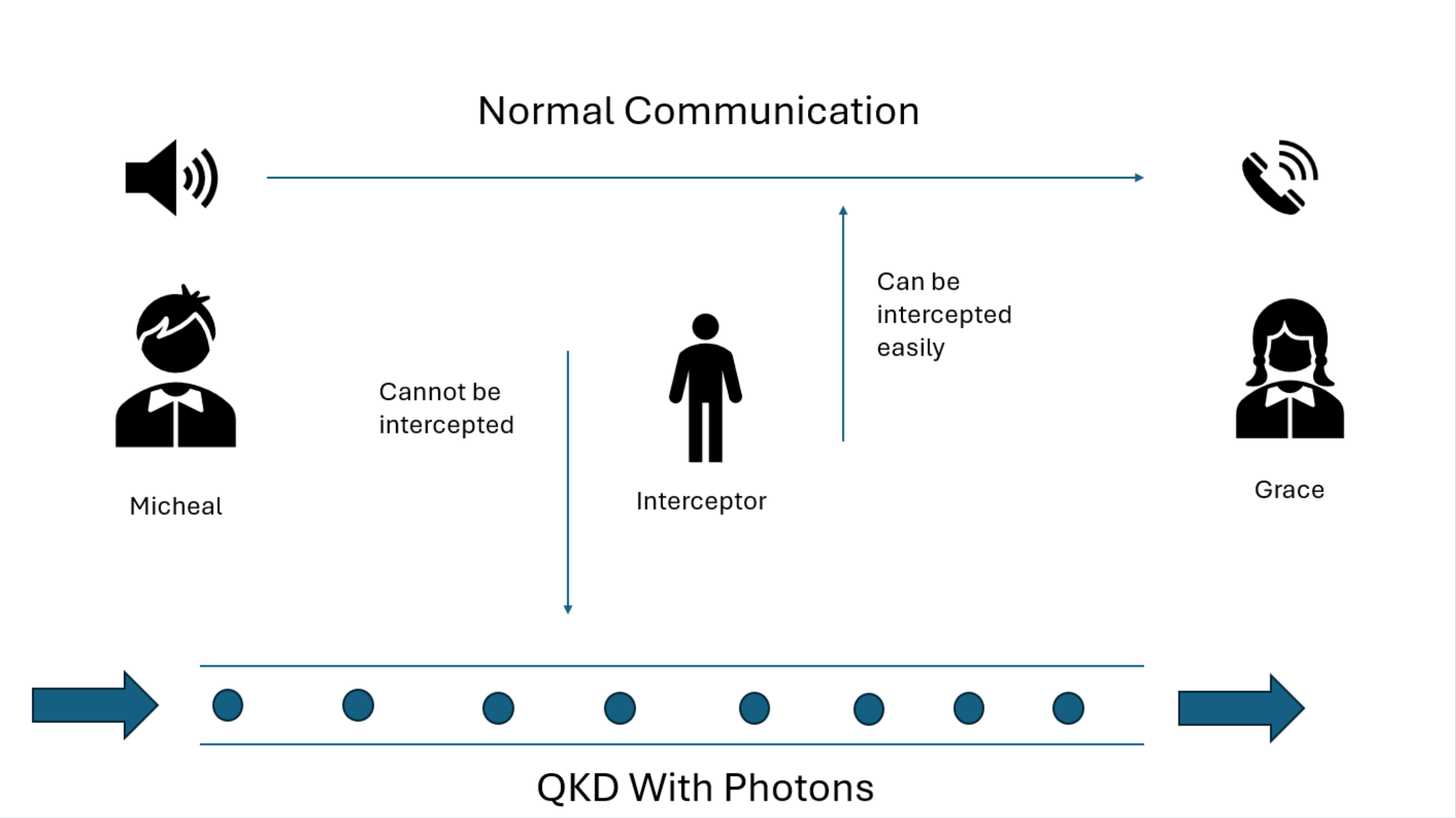


Figure 3. QKD Comparison to Normal Communication

DISCUSSION/CONCLUSION

The security and effectiveness of quantum computing heavily implies that its presence will only increase in the coming years. High-tech encrypted messaging and the ability to detect unwanted eavesdroppers ensures users that their data and messages are completely secure. This has been one of the main concerns of wireless data transmission since its origins in the 20th century. Different QKD protocols allow information to be transferred various ways for a range of purposes. Although this technology is extremely promising, wide-scale use will not be implemented until its basic limitations are overcome. These limitations include the inability to authenticate QKD transmission sources, the possibility of a denial-of-service attack, and many more. However, successful attempts of quantum communication, performed by universities and institutions in the 2000's, give hope for a future where we will be able to communicate without any fear of interception from a third party. It can also improve our government's national security, deterring cyberattacks from domestic and international threats.

References

Anilkumar, Chunduru, et al. "A Secure Method of Communication through Bb84 Protocol in Quantum Key Distribution." *Scalable Computing: Practice & Experience*, vol. 25, no. 1, Jan. 2024, pp. 25–33.

Stipčević, Mario. "Enhancing the Security of the BB84 Quantum Key Distribution Protocol against Detector-Blinding Attacks via the Use of an Active Quantum Entropy Source in the Receiving Station." *Entropy*, vol. 25, no. 11, Nov. 2023, p. 1518.

Acknowledgments

We would like to thank the Choose Ohio First Program and Cleveland State University, as well as Case Western Reserve University, for the opportunity to speak about our research.