HIGH SCHOOL EDITION
Journal of Student Research
Volume 14 Issue 1 (2025)

Understanding Quantum Key Distribution: The Role of Entanglement in Keeping Information Safe

Lara Kawle[1], Monica Sava[#], Kay Diaz[#] and Jothsna Kethar[#]

[1]Woodbridge Academy Magnet School, USA
[#]Advisor

ABSTRACT

In the growing digital age, where information flows seamlessly across the globe, data security has emerged as a critical concern for individuals, businesses, and governments alike. As modern society faces these challenges, the dynamic mechanisms of quantum mechanics offer transformative potential—not only in breaking complex computational barriers but also in enhancing the technological landscape with unprecedented solutions for secure communication and groundbreaking discoveries. As a subset of quantum computing, quantum entanglement is a complex phenomenon that utilizes entangled qubits to offer unique advantages, such as error resiliency and faster computational abilities. With the help of entanglement and qubits, two entangled, indistinguishable particles can be linked even at large distances. Not only does quantum entanglement provide profound opportunities for the future in dynamic computational powers, but it also provides promising results for its implication in Quantum Key Distribution (QKD). With the help of quantum entanglement, eavesdropping over network channels will disrupt a qubit's entangled state and thus alert of possible unauthorized access as part of QKD. This paper will discuss the relationship of quantum entanglement to QKD, QKD protocols currently using quantum entanglement, the advantages and disadvantages of entanglement-based QKD, and the current research directions for entanglement-based QKD protocols.

Understanding Quantum Entanglement

Quantum entanglement is a phenomenon in quantum mechanics where two or more particles become interconnected in such a way that the state of one particle is instantly correlated with the state of another, regardless of the distance separating them. To simplify the concept of quantum entanglement, the comparison between its fundamental unit, an entangled particle, and a regular particle can provide insight on the technological benefits that quantum entanglement provides. A particle is known as the smallest unit of matter in space, which can either be polarized upwards or downwards. However, an entangled particle is mainly different from that of a regular particle due to its ability to be assigned polarized upwards, polarized downwards, or in a superposition of both of these states.

Superposition refers to the idea that two particles can be considered one state until it is measured. This thought was depicted in a famous experiment conducted by physicist Erwin Schrödinger, the Schrödinger's cat experiment. To conduct this experiment, a cat, an internal monitor, and a flash of poison were placed in a sealed box. After a certain period of time, if the radioactive atoms in the poison were to decay, a mechanism would trigger the release of the poison and notify the experimenters via the internal monitor of a possible radioactivity presence. Without opening the box, it can be considered that the cat is in a superposition of both dead and alive, as the cat cannot be assigned a label without opening the box and validating that state.

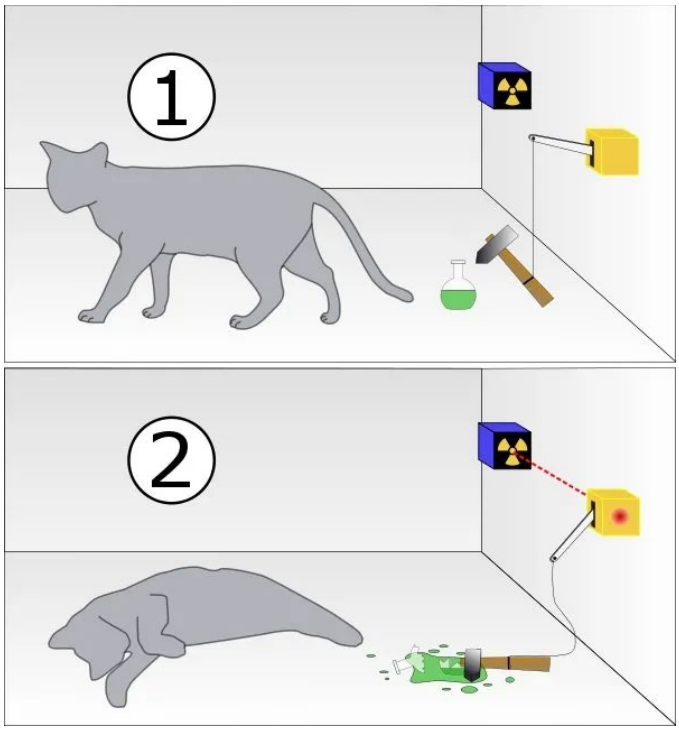

Figure 1. This is a model of the two possible outcomes from Schrödinger's experiment. The figure is from (Moloo, 2021).

To connect back to quantum entanglement, a particle can have an upward and downward polarized state simultaneously, while also representing combinations in every possible configuration. These various states ultimately provide the wave function of these particles. In quantum entanglement, two particles are considered entangled when the particles' values are codependent on each other. Because there are only two states a particle can be polarized in (upward or downward), if one particle's polarized state is determined, one can determine the other particle's polarized state in the other direction, even at larger distances. This concept can go against many scientific theorems valued today, such as the movement of light and the theory of relativity, thus giving it is name of "spooky action at a distance," as coined by Einstein (Wong, 2019).

Understanding Quantum Cryptography

Quantum cryptography utilizes basic quantum physics concepts, such as quantum entanglement and qubits, to establish security and proper control over data. Similar to the idea of how particles can be represented in multiple polarization states, a qubit can exhibit a state of superposition of a value of '0' and '1' as bits. Unlike a normal bit that can only be assigned one state, whether it be a '0' or '1', a qubit can simultaneously be in both states, which provides a unique feature for quantum cryptography to store information in those states. Because of the wide range of possibilities quantum states could have, it makes it rather challenging for a hacker to read the information without altering a qubit's original state. To keep this communication of qubits secure, quantum entanglement is implemented into quantum cryptography to encourage safe cryptographic messages over long distances (Shinde et al., 2024). These cryptographic keys are almost certain to be secure due to their ensured probability of leading to purely random keys and can be communicated over distances up to 10 km (Jennewein et al., 2008). Thus, with the implementation of qubits and quantum entanglement into quantum cryptography, the field could become a whole new ground for secure communications over long distances.

Eavesdropping and Security

A major fault in cryptography and online security is the possibility of eavesdropping, or when an interception is made to determine information about a specific dataset. Typically, this is done through a two-stage process. First, an interceptor produces copies of pieces of information without altering the original state of the set and then reads the resulting values from the copies for encoding. Because the interceptor does not change anything about the original dataset, the receiver of the information will not be able to differentiate between whether the information had been intercepted or not. Without leveraging the principles of quantum physics, eavesdropping attacks can be mitigated using various methods.

For one, the usage of encryption, whether it be symmetric or asymmetric key encryption, can be utilized for working towards secure communication by using a key to transmit information across two parties. Encryption can be modeled with the famous example of two hypothetical parties, ‘Alice’ and ‘Bob', trying to send a message across a secure communication channel.

In symmetric key encryption, a shared key between the two parties are used for the two functions of encrypting and decrypting a specific set of information. The main issue with using symmetric key encryption is the possibility of an interceptor gaining access to that key. With that, there is no measure to prevent the interceptor from decrypting a message, as the key withholds the function to both encrypt and decrypt.

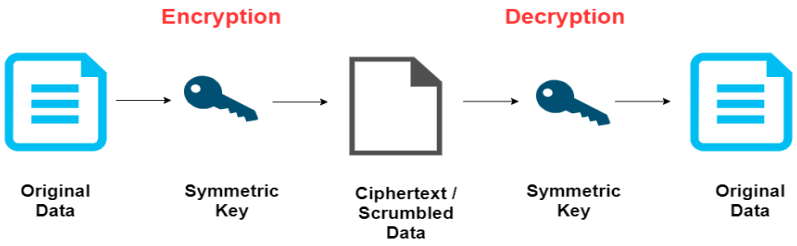

Figure 2. This is a model depicting the process of encryption and decryption in symmetric key encryption. The figure is from (Bhanuka, 2020).

However, in asymmetric key encryption, the two parties are not utilizing a shared key. Instead, the key is broken into two keys: a public key and a private key. In this case, the public key is responsible for encrypting a message. If a hacker were to get access to the public key, it would make no difference. This is because the public key can be shared with anyone and is computationally infeasible to derive a private key from its associated public key. The private key’s main role is to decrypt the message and is a secret key that only the recipient is able to withhold. Because the private key is held confidential, it is almost impossible for a hacker to reveal the hidden information, as they would only be able to see an encrypted message. Overall, because of the two-step process that is undergone in asymmetric encryption, asymmetric encryption is considered to be more secure to be used in communication channels as compared to symmetric encryption (Al-Shabi, 2018).

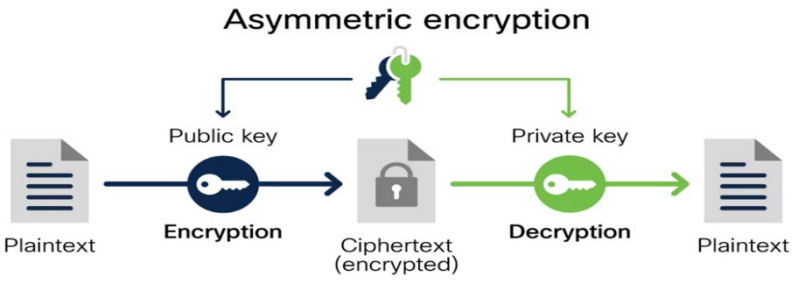

Figure 3. This is a model depicting the process of encryption and decryption in asymmetric key encryption. The figure is from (Abu Shaqra, 2024).

Quantum Key Distribution (QKD)

Although similar in its usage of shared keys to decrypt and encrypt messages, quantum key distribution (QKD) applies the principles of quantum mechanics to make it nearly impossible for hackers to gain access to private information without alarming the intended parties. This is because it utilizes a fundamental aspect of quantum physics: the process of measuring a quantum system can disrupt the quantum relationship that has already been made. This characteristic, combined with the no-cloning theorem—which states that it is impossible to create exact copies of an unknown quantum state—makes it impossible for attackers to duplicate quantum data as they would with traditional networks.

The process behind how QKD operates is done with the usage of photon movement across cables. A stream of these photons, or a qubit, moves towards the receiving end until they are met with a beam splitter. This beam splitter forces the photon to only take one direction, thus preventing photons moving in different directions to pass through. When the receiver receives the photons that were able to pass through the beam splitter, they can compare their results to that of the sender to determine which photons were sent for the right beam collector. When the photons that were sent for a different beam splitter are removed from the sequence, what is left is a specific sequence that can alternatively work as a key to encrypt data. Thus, not only do the two individuals are able to pass information with a key that is only known to them, it also prevents unwanted recipients from eavesdropping without notifying the original recipients of a hacker (Gillis, 2022).

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 4. This is a model depicting the process of producing a shared key with QKD. The figure is from (Haitjema).

The E-91 Protocol Using Quantum Entanglement

Entanglement-based QKD protocols allow for two objects to form a combined quantum state, in which the act of measuring one entangled particle will inevitably affect the state of its other entangled partner. If the situation were to come that an eavesdropper tries to intercept and measure a particle in an entangled pair, the disruption will be evident

when the recipient of the series of photons measure their particles. Thus, this change in measurement will notify the two communicators of a possible interceptor. There are several protocols already in place that use quantum entanglement within QKD protocols. One famous example of an encryption-based QKD protocol is the E-91 protocol. The process of communicating using entangled states with a classical information channel is the basis of the E-91 protocol. The protocol can be modeled once again with the fictional characters 'Alice' and 'Bob'. The source center prepares an entangled state and sends one particle to Alice and the other to Bob. Alice measures her particle using a randomly chosen direction, while Bob measures his particle using a direction randomly chosen from a different set of degrees. After recording their results, they use a classical communication channel to share the measurement bases they used.

Based on this exchange, Alice and Bob organize their results into two groups: decoy qubits, where they used different measurement bases, and raw key qubits, where their bases match. The decoy qubits are analyzed to detect potential eavesdropping by checking correlations between their measurements. If discrepancies are found, indicating an eavesdropper's interference, they discard the quantum channel and restart the process. If no issues are detected, the raw key qubits are converted into a shared key. In this protocol, the primary function of quantum entanglement is to generate pairs of entangled particles, enabling them to establish correlations with each other. The entangled and related nature of the particles allows Alice and Bob to draw conclusions from them. If an eavesdropper would try to measure the particles, it could disrupt the natural entangled state that was already set between the two and notify the two communicators of an eavesdropper (Roorkee, 2021).

Advantages and Limitations of Entanglement-Based QKD

Entanglement-based QKD provides several benefits due to its foundation of quantum mechanics. Firstly, its incorporation of protocols such as BB84 and E91, which have been statistically proven to be secure when confronted with an attack, further verifies its accuracy and efficiency against eavesdropping attacks. In addition, the system can be incorporated in various different quantum environments and real-world applications. Moreover, its capability to function effectively over vast distances offers promising potential for applications across a wide range of disciplines on a global scale.

However, even though entanglement-based QKD is a very appealing alternative to other cryptography methods, it does come with its own limitations—in particular, its practicality and scalability. A mistake in its alignment and timing of the process can lead to errors in producing the quantum key or even reduce its security against eavesdroppers. Furthermore, it is liable to attacks such as Trojan horse attacks, a type of malware that downloads as disguised as a regular program, or photon-number-splitting attacks, which can disrupt the ultimate creation of the shared key. Lastly, even though its benefits may surpass its disadvantages, the main problem with implementing entanglement-based QKD systems is its cost. The installation and maintenance of the system require a large degree of specialty and resources, which can present a significant challenge in rural and lower-income countries.

Current Research and Future Directions

Currently, several researchers are exploring the different options for entanglement-based QKD that can effectively surpass the stated limitations and provide a larger range of advantages for computer security. One study conducted by the Faculty of Physics, Astronomy, and Informations from Nicolaus Copernicus University compared the performance of various discrete variable and continuous variable QKD protocols based on different setups in noise and transmittance in the quantum channels (Lasota et al., 2024). Not only that, research was conducted from a team from Cornell University to develop a telecom band entanglement source for WKD. According to their results, they were able to conduct long-distance QKD over 500 kilometers, representing a future in global quantum communicator networks (Li et al., 2024). Lastly, one team was able to use an efficient resonator to create a quantum communication system capable of distributing secure quantum keys across 12 km of fiber while maintaining low error rates and high efficiency

(Steiner et al., 2023). The research that is currently being done provides the real possibility of the usage of entanglement-based QKD protocols in real-world applications with increased accuracy and security for those who use it. Overall, these advancements highlight the ongoing progress in entanglement-based QKD, paving the way for more secure global networks.

Conclusion

In the increasingly digital world, ensuring proper security and safety online has become a significant issue for this generation. Without digital protocols that ensure the security of online databases, important systems are vulnerable to malicious attacks from eavesdroppers and hackers. With this, quantum entanglement provides promising advantages for QKD to ensure that any attempt at eavesdropping disrupts the quantum state, making breaches detectable and enhancing trustworthiness in communication systems. With further research, entanglement-based QKD systems have the potential to reach countries on a global scale and pave the way for widespread adoption of entanglement-based cryptographic systems. Not only that, the implementation of artificial intelligence could lead to encouraging findings of innovative solutions in improving quantum computers and internal systems. Integrating these configurations across the globe ensures a world where internet safety and regulation is valued, while promoting the incorporation of quantum mechanics for future endeavors.

Acknowledgments

I would like to thank my advisors Dr. Monica Sava, Prof. Kay Diaz, Ms. Jothsna Kethar, and the Gifted Gabber team, who supported and worked with me to make this research a success. In addition, I would like to thank my family for the unconditional love and moral support they provided that encouraged me to finish the study.

References

(2022). Distance Based Security using Quantum Entanglement:a survey. doi: 10.1109/icccnt54827.2022.9984468

A Guide To Quantum Key Distribution And Its Security Benefits. (2024, September 10). Quantum Zeitgeist. https://quantumzeitgeist.com/a-guide-to-quantum-key-distribution-and-its-security-benefits/

Abu-Shaqra, B. (2024, February 21). *Using Asymmetric Keys*. Www.linkedin.com. https://www.linkedin.com/pulse/using-asymmetric-keys-baha-abu-shaqra-phd-dti-uottawa--khtjf

Al-Shabi, M. A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(3), p8779. https://doi.org/10.29322/ijsrp.9.03.2019.p8779

Bhanuka, R. (2021, July 31). *Symmetric-Key Cryptography (Private Key Encryption)*. Medium. https://medium.com/@rajithabhanuka/symmetric-key-cryptography-private-key-encryption-3edbaed70e4a

Brahim, Ouchao. (2023). Quantum Cryptography Simulation of Entanglement and Quantum Teleportation. doi: 10.3390/cmsf2023006008

C., Dumps. (2022). Pre-established entanglement distribution algorithm in quantum networks. IEEE\/OSA Journal of Optical Communications and Networking, 14(12):1020-1020. doi: 10.1364/jocn.465432

Ekert, A. K., Huttner, B., Palma, G. M., & Peres, A. (1994). Eavesdropping on quantum-cryptographical systems. *Physical Review A*, *50*(2), 1047–1056. https://doi.org/10.1103/physreva.50.1047

F.J., Duarte. (2024). Quantum entanglement physics and Bell's theorem. doi: 10.1364/opticaopen.25954564

Gillis, A. (2022, November). *What is Quantum Key Distribution (QKD) and How Does it Work?* SearchSecurity. https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD

Haitjema, M. (2007, December 2). *Quantum Key Distribution - QKD*. Wustl.edu. https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., & Zeilinger, A. (2000). Quantum Cryptography with Entangled Photons. *Physical Review Letters*, *84*(20), 4729–4732. https://doi.org/10.1103/physrevlett.84.4729

Mariani, L., Salatino, L., Attanasio, C., Pagano, S., & Citro, R. (2024). Simulation of an entanglement-based quantum key distribution protocol. *The European Physical Journal Plus*, *139*(7). https://doi.org/10.1140/epjp/s13360-024-05337-2

Md., Ferdous, Ahammed., Mohammad, Ismat, Kadir. (2024). Entanglement and teleportation in quantum key distribution for secure wireless systems. IET quantum communication, doi: 10.1049/qtc2.12092

Mikołaj, Lasota., Olena, Kovalenko., Vladyslav, C., Usenko. (2022). Robustness of entanglement-based discrete- and continuous-variable quantum key distribution against channel noise. doi: 10.48550/arxiv.2308.07007

Moloo, N. (2021, February 28). *Understanding Quantum Superposition Through the Schrödinger's Cat Thought Experiment*. Medium. https://studentsxstudents.com/understanding-quantum-superposition-through-the-schr%C3%B6dingers-cat-thought-experiment-d0cea6e13063

Roorkee, Q. C. G., IIT. (2021, September 6). *Fundamentals of Quantum Key Distribution — BB84, B92 & E91 protocols*. Medium. https://medium.com/@qcgiitr/fundamentals-of-quantum-key-distribution-bb84-b92-e91-protocols-e1373b683ead

Shinde, S., Walke, M., Thole, R., Mishra, R., Kalamkar, M., & Garade, B. (2024). Quantum Cryptography: Mathematical Foundations and Practical Applications for Secure Communication Protocols. *Communications on Applied Nonlinear Analysis*, *31*(3s).

Till, Dolejsky., Erik, Fitzke., Lucas, Bialowons., Maximilian, Tippmann., Oleg, Nikiforov., Thomas, Walther. (2023). Flexible reconfigurable entanglement-based quantum key distribution network. European Physical Journal-special Topics, doi: 10.1140/epjs/s11734-023-00980-9

Trevor, J., Steiner., Maximilian, Shen., Joshua, E., Castro., John, E., Bowers., Galan, Moody. (2023). Continuous entanglement distribution from an AlGaAs-on-insulator microcomb for quantum communications. Optica quantum, 1(2):55-55. doi: 10.1364/opticaq.510032

Wong, B. (2019). ON QUANTUM ENTANGLEMENT. *Internal Journal of Automatic Control System*, *5*(2), 1–7. https://www.researchgate.net/publication/339426925_ON_QUANTUM_ENTANGLEMENT

Wu-Zhen, Li., Chun, Zhou., Yang, Wang., Li, Chen., Renhui, Chen., Zhao-Qi-Zhi, Han., M., Gao., Xiao-Hua, Wang., Di-Yuan, Zheng., Mengyu, Xie., Yin-Hai, Li., Zhi-Yuan, Zhou., Wan-Su, Bao., Bao-Sen, Shi. (2024). Quantum key distribution based on mid-infrared and telecom band two-color entanglement source. doi: 10.48550/arxiv.2408.07552

Zheshen, Zhang., Chenglong, You., Omar, S., Magaña-Loaiza., Robert, Fickler., Roberto, de, J., León-Montiel., Juan, P., Torres., Travis, S., Humble., Shuai, Liu., Xin, Yi., Quntao, Zhuang. (2024). Entanglement-based quantum information technology: a tutorial. Advances in Optics and Photonics, 16(1):60-60. doi: 10.1364/aop.497143