Application of Quantum Cryptography for Business Data Security

Howard Morgenthaler
Computer Science Undergraduate
Texas A&M University
howiemorgenthaler@tamu.edu

***Abstract*—As quantum computing evolves over time, the use of quantum computers becomes more realistic. Quantum computing is computing based on quantum theory. Specifically, they use the fact that a photon stays in a superposition of eithr up or down. This allows the bits that are used in quantum computing to be able to represent multiple states at one time. Compare this to classical computing where bits are either 1 or 0, and this can lead to destroying current crypto-systems. This will shown by analyzing Shor's algorithms. However, making cybersecurity based on quantum computing allows us to go past the inhibitions of classical systems. Analyzing quantum key distribution and the BB84 protocol will prove it is impossible to break through cybersecurity using quantum computers. Thus, we must focus heavily on how to apply and integrate these techniques to real world practices. This is a major issue we will run into when we start producing more quantum computers/systems.**

***Index Terms*—quantum computing, cryptography, encryption, quantum key distribution, data security**

I. Introduction

Quantum computing has been progressing heavily in research in just a few decades. A large benefit to quantum computing is that it is able to have multiple states off of one bit. It takes advantage of the base idea of quantum theory: photons are in a superposition of up or down until observed. Thus, a single bit can be represented as a 1 and a 0 due to it being in either state until it is measured, representing multiple data. The amount of bits that can be represented is, then, exponential. This main idea is what makes it faster and more efficient than classical computing. Due to the speed at which it can solve complex problems, its advantage to classical computing, there are many benefits to be found with it.

However, in the realm of cyber security, this can lead to problems. It has be found that "hard to solve" problems, which form the basis of classical cryptography, can be solved very quickly with quantum computing. These systems that use symmetric and asymmetric encryption algorithms have been solvable with quantum algorithms. To put it into perspective, these algorithms are so fast and accurate that they could crack an encryption algorithm used today faster than it takes to encrypt the data [6]. Plus, there are many others doing research into this area to find faster algorithms that can solve larger bit encryption keys. This is a great threat to security for everyone. Not only could it damage those who have a digital service hold their personal information, but it could be used to take very confidential information, like trade secrets or classified documents. Also, losing data integrity could have very serious consequences. For example, if someone were to crack a secure data storage of a medical institution then it could lead to loss of lives [5].

Now, the evolution of classical computers to quantum computers is not just a threat to current security. On the other hand, it could be a savior to all security. It has been found that, through quantum computing, we can make perfect security for a channel. Using the ideas of quantum theory, the superposition of photons, we are, also, able to know when there is an eavesdropper on the channel. This is due to the state of a photon/particle collapsing once observed. We use quantum key distribution, or QKD, to make a secure quantum key between two nodes. The first protocol on which many encryption algorithms are based off of is BB84. We will go into detail on this protocol in a later section.

It's important to not just know how these ideas work, but how they can be taken advantage of. We must figure out how to integrate these quantum cryptography techniques into today's data transmission systems and storage. Transmitting data over these networks, securely, should be efficient, as well. These will be the two goals of this paper. I want to reiterate the word integrate. Creating systems to utilize quantum cryptography can not be used right away, throwing away the current system at once. This would lead to both confusion and inconvenience. Thus, the uses described in this paper will be focused on using quantum keys in today's current systems rather than assuming a perfect quantum computer world.

II. Related Work

As this is becoming a very important field, and quicker, there has been much research in this area. Research has been conducted over quantum computing with regards to cybersecurity for decades now. Thus, resulting in much information to learn and gain inspiration from. D. Tosh, O. Galindo, V. Kreinovich and O. Kosheleva [4] explains how it is hard to implement due to the complexity of it. This complexity makes it much slower since it takes much more time to send qubits. They suggest two possible ways to fix this issue: compression and only sending relevant bits. This will decrease the amount of bits being sent at a time, thus reducing much needed time. However, they also bring up the method of teleportation which allows for quantum computers to send to

other quantum computers quickly since it doesn't use quantum channels, but rather signals. Petros Wallden and Elham Kashefi [3] found that the use of quantum computers in cybersecurity are becoming a real thing and will most likely be used in the next decade. This leads to a major issue in that hackers could reach this technology before those with very important information do. Plus, these two groups will have them well before civilians do.

Current crypto systems use quantum symmetric and asymmetric algorithms to protect data being sent from one source to another. However, works have been produced showing the ability of quantum computing to break current cybersecurity techniques. RSA, the main encryption algorithm used today, could, possibly, even be broken faster than the key can be made [6]. Shor founded the basis for attacking the discrete logarithm problem and factoring large numbers. This can be very dreadful to see for people today, especially businesses, government, and medical agencies who carry information that is very important.

On the other hand, there are advantages that come with quantum computing in the realm of cybersecurity, as well. Techniques have been found that make keys unbreakable, even by quantum algorithms. They are based on QKD, or quantum key distribution. The main protocol is BB84, which can even tell you when a person is eavesdropping. V. B. [1] analyzes the likelihood of picking up on an eavesdropper on the channel. For a very short key, there is a 50% chance that you will be able to pick up on an eavesdropper. However, as the amount of bits, i.e. the key, increases the chance of finding the eavesdropper exponentially. Now, considering a channel with noise, as noise increases the probability of picking up on an eavesdropper still is exponential, but the rate of change decreases. This is due to the chance that errors in the key exchange have a higher chance of being affected by noise.

Variations have been produced from the BB84 protocol to try to make it more secure [5]. V, A., V, K. created a protocol based on BB84 where they added the use of a Xor bitwise operator. Alice performs the operator on the bits matching with Bob and the remaining not match bits to generate the key. They put a big emphasis on how it is important to keep data secure from quantum hackers in the medical field. Severe consequences, like loss of life, could incur if medical data is breached and changed as these numbers are needed to know the correct dosage to give a patient. Doctors, also, need to know what exactly the patient is ailing from to give them correct treatment. This shows how important it is for these quantum cryptography solutions to be put into place as soon as possible.

Businesses, government, and agencies will be the ones most benefiting from these breakthroughs, we should learn how it can be applied to these benefactors. It is discussed [2] how QKD technology can be integrated in power businesses. They present a solution, integrating it into the current system, where they use QKD technology to generate a key which is connected to all other QKD devices through a quantum network, i.e photo-switch and fiber cable. This key is then used by the encryption and authentication device to allow use of the data.

Another issue is that we are moving more towards a wireless society, WiFi and cellular, so we need to learn how to implement these secure wireless paths, too.[7]. This, also, requires us to learn how to send data from a quantum computer to another quicker. The main way QKD was used in this paper was that a quantum key is generated by the master server and is sent to a requester through the backend, after the requester was authenticated. Then this key is used over the channel to encrypt all data sent over the channel.

Mehic M, Fazio P, Voznak M, and Chromy E [8] discusses how QKD would be implemented on a network. As basic systems goes, it attempts to find the shortest link between nodes, but for security, the packets must be encrypted. It uses common reactive and proactive protocols to do so. Now, they mention how there needs to be sufficient material to encrypt the data over the quantum channel. Thus, they decided to use a flag for each link saying whether it has enough material or not. If not, it won't send the data down the link since it won't be able to be encrypt it. It makes sure that key material is constantly being dropped into the link so it can used to send encrypted data if it runs out of material at some point.

III. Problem Statement

As quantum computing progresses, we will gain more in total security, but lose confidence in current security. There is going to be a major shift from what we currently have for cybersecurity due to the threat of others using more sophisticated hacking systems with quantum algorithms. To be able to make sure that transition goes smoothly, we need to know how to implement these protocols into our already made systems. It will not be as simple as just making it and then using it. We have to integrate into what we already have and make sure that it is both efficient and cheap enough to do so. There has already been much research in creating the most efficient protocols, both for tearing down current crypto systems and creating better forms of security. However, these quantum computers are already starting to be made, so it is time to start discussing the most effective use for applications.

IV. The Threat to Current Cybersecurity

Current cryptography relies heavily on mathematical concepts. It takes advantage of the fact of complex math problems that can take a very long time to solve. [9] According to classical computation, this remains true given a very large key. However, when it comes to the advancement of computation with regards to quantum computing, these mathematical problems seem trivial.

Peter Shor was the first to show this fact. The two main mathematical problems that classical cryptography relies on is prime factorization and the discrete logarithm. In fact, RSA, a major encryption algorithm used today, utilizes the toughness of factorization to encrypt much of the data in the world. Shor developed quantum algorithms to be able to crack both of these problems. This is terrifying since, even though it was not shown to be able to solve these problems in linear time,

it is possible to take them down in polynomial time [6]. Not only that, but there has been much research in creating faster algorithms to break much larger keys.

V. Quantum Security: QKD and BB84

Here we will be discussing what quantum key distribution is and how it works. Then, we will go over the first QKD protocol: BB84, and finally discuss the limitations of QKD in the real world.

Quantum key distribution (QKD) is the secure communication of a key between two parties. Specifically, it is sharing a key generated by the laws of quantum physics over a quantum channel (fiber optic cables) and sending it through a public channel. The quantum channel sends random bits from one party to another where if there is any eavesdropping on the channel then it can be detected. This is due to quantum bits being in a state of entanglement and, once observed, they fall into a single state. This disruption can be detected with a high probability [10]. Now, once the parties have decided there is no foul play on the channel, they use their shared bits to create a key that is sent through the classical channel which will be used to secure data transmission.

To illustrate this process, we will discuss BB84 which was developed by Charles Bennett and Gilles Brassard. Alice creates a bit string of arbitrary length and chooses a random sequence of bases which are either vertical/horizontal or diagonal. The bits are 1 if it is vertical or measured at 45 degrees in diagonal and 0 if measured as horizontal or -45 degrees. Then she encodes these bits use the bases, sending the bits as photons which are in a state of superposition. Once Bob receives these bits from the quantum channel, he measures them in the bases of his choosing using a photon detector and gets a string of bits that are the same length as Alice's.

Afterwards, they communicate over the classical channel about which bits were measured by the same basis. They choose a certain amount of those bits to test if they are the same for both of them. It is considered safe to use the photons sent across the channel if they have the same n bits of the subset they chose, where n is agreed upon based on many factors such as noise/error and length of of the bit string. However, if the amount of matching bits is less than n then they assume there has been eavesdropping and the process restarts. This insures the integrity of the key being used for communication. Lastly, through the manipulation of the other bits, Alice is able to make a secret key for her and Bob.

Researchers have taken this protocol, as well as other ways of using QKD to increase security and complexity of the keys created by QKD. This includes using bitwise operations on the remaining bits in BB84 [5]. There is another form of QKD being researched into which is called continuous variable QKD. As photons are light, CVQKD uses quadratures of the light sent by the laser [11]. This gives a continuous projection of the phase and amplitude of the field. I mention this as it is a potential alternative to protocols like BB84.

As the real world isn't perfect, there are many issues that QKD can run into when implementing it. To get an accurate idea of how these protocols can be used, we have to understand the limitations. Firstly, photons can only be sent down a fiber optic channel and fiber channels can only send a photon so far. Thus, we need to create an environment that is able to send a photon over large distances as a key may need to be used for two greatly separated nodes. Countries have already started researching into this issue. There has been findings on sending photons over thousands of kilometers, even doing earth to space transmission [12].

Another issue is the speed at which we can send quantum information as it is much slower than classical information transmission. Two methods that have been researched are compression and only sending relevant bits [4]. The idea behind compression is using less bits to represent information. Meanwhile, only sending relevant bits saves time by not wasting transmission. We can do this through quantum algorithms that can show what bits are relevant.

Noise/error, an issue that I mentioned previously, that comes with sending photons down a fiber channel and receiving photons through a detector. The issue this causes for QKD is that it gives room for eavesdroppers to take advantage of. Thus, as noise increases the possibility of detecting an eavesdropper decreases [1]. Furthermore, creating a quantum key and using a quantum channel needs to be very precise to ensure shared key information. This makes the error tolerance needed for a genuine key very small. There are already error correcting codes being theorized right now to help reduce the amount of error.

The final issue we're going to mention is that QKD, although it could provide a secure channel, does not necessarily prove that the source of the quantum channel is secure. It could be anyone sending quantum bits to a receiver and then generating a quantum key for the channel. The receiver must be able to authenticate the sender to know that the transmission is coming from a trusted and genuine source.

VI. Quantum Networks

Quantum networks are a system that is completely made up of quantum links. In other words, it allows for the use of quantum cryptography in every node of communication in a network of computers. Theoretically, to create an internet that uses only quantum devices an optimal quantum network will need to be made that deals with all limitations, but this is a slight tangent. On a smaller scale, this is what will allow businesses to utilize the full potential of secure communication with all of their data transmission. Thus, we will discuss what is already theorized to get a good understanding of what will be used to implement quantum cryptography into businesses.

The main theories, today, are to use nodes in a network to keep information secure under quantum keys over large distance transmission. This makes up for photons not being able to travel over a certain distance. Instead of trying to increase the distance a photon can travel, we simply remake a quantum key at each node to send the information to it's destination. Quantum repeaters are considered the ultimate way to make a complete quantum communication. Creating

such devices would result in quantum key information being sent over arbitrarily large distances [14]. The main idea is to take an entangled state and constantly apply entanglement switching and entanglement purification to it. In other words, it is the constant manipulation of particles during a transmission. The process separates the quantum channel into segments where each segment is given an entangled (EPR) pair. These pairs are stored into the quantum memories of each node in every segment, respectively where each entanglement goes through an entangled purification. Then, each segment's nodes have are entangled together and entanglement switching is performed to allow Alice, the sender, to be continuously entangled with every node. This will keep going down the chain until, eventually, Alice is entangled with Bob and they can communicate on the channel [13]. Plus, this process is much less susceptible to errors.

However, we do run into an issue with this solution in that it is practically impossible to implement as of right now. Thus, we have to look into other solutions for the problem of making a quantum network. A solution that I wish I could take credit, but found something similar during my research, is the use of classical channels to transfer data that is secured by a quantum key between nodes [9]. By doing this, we are able to communicate through long distances with the help of nodes in the network. Each node has a quantum link attached to it with surrounding nodes and constantly encrypts and decrypts the data in order to send the data over a large network with a quantum key. The transmission rate is faster due to it being over a quantum channel, but the constant encryption and decryption could counteract that increase. It makes it more realistic technology-wise, but not as secure as a quantum repeater due to keys needing to be held in classical memory. This, on the other hand, gives a good starting point to start integrating quantum cryptography into the world of business.

VII. The Hardware Application

To define this network with regards to businesses we will correlate each node to a trusted device on the business network. Since the devices that communicate with each other already have classical channels in place for data communication we can leave these in place. However, each node would need a QKD device for each node it already communicates with. This will create a quantum channel between each node necessary for communication, creating the quantum network. This allows the integration of quantum technology to be simple, by only adding. To maximize communication, and minimize time and money each node and link/edge can have a level of priority attached to it. Then, the quantum links using fiber cable and devices can start being created according to priority. By doing this assessment, it could create a more optimized network than the current one already in place.

Whenever data is trying to be sent through a network, we propose two ways to send it. The first is using a reactive protocol that has a RREP and RREQ so that every node the route reply passes through starts a QKD with previous node in the RREP so that way the key is ready to be used or can be used quicker during the transmission of data. The other is using a proactive protocol that starts a QKD with the next node once it receives the data. Another way for the proactive protocol to work to have it be faster during the transmission is for nodes to constantly be generating keys with each other and storing them into memory, but this is very expensive and reduces the integrity and confidentiality of the quantum keys if stored in classical memory.

These quantum keys can be doubled with classical keys during the channel to ensure a double protection during the transmission. The information will be encrypted with a quantum key using the QKD device, go through and encrypted classical channel, be decrypted using the classical key and then the quantum key on the other end. This process is repeated for each node the data traverses through. Authenticating the source can be done through the classical channel using current methods to know that the data received came from a trusted source. Finally, we can use error correcting code during the quantum channel to reduce errors. This will help keep errors during quantum communication below the fault tolerance.

VIII. The Network Application

Unfortunately, I did not have time to generate a simulation for these processes, but we will use the research produced in [8] which tests different network protocols, AODV, OLSR, OSPF, and DSDV on a quantum network. To explain the network layer of quantum cryptography we must first discuss key material for quantum keys. Each time a quantum key is generated it uses a certain amount of key material to create it based on the amount of data being sent. This is due to a quantum key needing to be the same amount as the length of the data [8]. Key material can be generated overtime at a certain rate, but a key may need to be generated when a channel does not have enough key material. In this case, it might be better to take a slightly longer route that already has key material generated. Thus, we will have the amount of key material in a channel as a value that can be accessed while finding the route to send the data down.

Of course, anytime you transmit data you would like it to go down the shortest path which is what these network protocols do and why they are being assessed. We will take into consideration for the reactive route AODV. When a RREQ is sent throughout the network from the source that wants to send to a destination, we will add the amount of data that it wants to send as a flag or in the header during the RREQ. Everything about AODV will work as usual except that a node will not forward the RREQ until its key material is greater than or equal to the amount of data trying to be sent. Once the RREQ has reached the destination and the route reply is initiated, then during the RREP a quantum key will be generated using QKD for each neighboring node the RREP passes through. That way once the data is being transmitted through the route the quantum keys needed will be as close to generating as possible and will be able to automatically send the data.

For the proactive solution we will be using DSDV since it

was shown to be the most effective protocol [8]. DSDV will continuously have each node update its routing table to know which next-hop node it needs to take to get to a different node the quickest way possible. A threshold is set for the required key material and if a channel is below that amount then the routing table will update and each node will find a different node as the next hop to that destination until that channel generates enough key material to be above said threshold. Then, once a node wants to send data to a destination, it will follow through the route created by DSDV. At each node transfer, it will create a quantum key from QKD and then send the encrypted data through the classical channel until it reaches the destination.

Again, I have not been able to test these method so I am not sure which one is more efficient, but according to [8] AODV is not very efficient and DSDV is. However, they did not present the use of AODV the way this paper has so the optimization that was presented could make up for the difference. Thus, this is something that needs to be further looked into and tested.

REFERENCES

[1] , V. Bindhu, "Cyber Security Analysis for Quantum Computing. Journal of IoT in Social, Mobile, Analytics, and Cloud", p.133-142, 2022 doi:10.36548/jismac.2022.2.006.

[2] Bingzhen Zhao, Xiaoming Zha, , Zhiyu Chen, Rui Shi, Dong Wang, Tianliang Peng, Longchuan Yan, Performance analysis of quantum key distribution technology for power business Appl Sci,20, 2020.

[3] Petros Wallden and Elham Kashefi. 2019. Cyber security in the quantum era. Commun. ACM 62, 4 (April 2019), 120. https://doi.org/10.1145/3241037

[4] Deepak Tosh, Oscar Galindo, Vladik Kreinovich and Olga Kosheleva, "Towards Security of Cyber- Physical Systems using Quantum Computing Algorithms," 2020 IEEE 15th International Conference of System of Systems Engineering (SoSE), 2020, pp. 313-320, doi: 10.1109/SoSE50414.2020.9130525.

[5] Anusuya Devi V and Kalaivani V, Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. Pers Ubiquit Comput (2021). https://doi.org/10.1007/s00779-021-01546-z

[6] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", 1996. https://doi.org/10.48550/arXiv.quant-ph/950802

[7] Sai Suguna Y, Kavya Reddy B, Keerthi Durga V, Roshini A (2018) Secure quantum key distribution encryption method for efficient data communication in wireless body area sensor net-works. Int J Eng Technol:331–335

[8] Mehic Miralem, Fazio Peppino, Voznak Miroslav, Chromy Erik (2016) Toward designing a quantum key distribution network simulation model. Inf Commun Technol Serv 14:4

[9] DIANATI, Mehrdad and Romain ALLEAUME. Architecture of the Secoqc Quantum Key Distribution network. In: First International Conference on Quantum, Nano, and Micro Technologies. Gosier: IEEE, 2007, pp. 13–19. ISBN 0-7695-2759-0. DOI: 10.1109/ICQNM.2007.3

[10] Charles H. Bennett, Gilles Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science, Volume 560, Part 1, 2014, Pages 7-11, ISSN 0304-3975, https://doi.org/10.1016/j.tcs.2014.05.025. (https://www.sciencedirect.com/science/article/pii/S0304397514004241)

[11] Zheshen Zhang and Paul L. Voss, "Security of a discretely signaled continuous variable quantum key distribution protocol for high rate systems," Opt. Express 17, 12090-12108 (2009)

[12] Chen Yu-Ao., Zhang Qiang, Chen Teng-Yun. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589, 214–219 (2021). https://doi.org/10.1038/s41586-020-03093-8

[13] Briegel, H.-J. and Dur, W. and Cirac, J. I. and Zoller, P., "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication", Phys. Rev. Lett., 81,26,5932–5935,1998,Dec,doi: 10.1103/PhysRevLett.81.5932, https://link.aps.org/doi/10.1103/PhysRevLett.81.5932

[14] Qiao Ruihong and Meng Ying 2019 J. Phys.: Conf. Ser. 1237 052032 DOI 10.1088/1742-6596/1237/5/052032