Data Security with Quantum Cryptography

Michael Chillemi

Data security is becoming more relevant currently. As technology advances our security must as well. Over the years quantum computing has become an extraordinary topic. Currently most computers or devices we utilize currently run off binary. Quantum computing uses “quantum bits” which can be represented as a one, zero, or both at the same time. This means that a quantum computer can perform computations exponentially faster and more efficiently. As an example, let’s say a supercomputer would be able to solve a specific problem in 10,000 years. Researchers have theorized that a quantum computer can take the same exact problem and solve it in minutes. The idea of a computer being able to accomplish this task in not only incredible but, regarding security this can be immensely terrifying.

Having a system that will be able to produce these types of results is a major threat to data security. What does this mean for our future? It means that quantum computing will be able to easily crack some of the more advance security measures faster. That includes most encryption systems that are used today. This paper will explore the many ways quantum computing can change the world we live in today and how it can be used to greatly improve our security.

Daniel Bernstein, and Tanja Lange, (2017). Post-quantum cryptography. *Nature (London)*,549(7671), 188-194. https://dio.org/10.1038/nature23461

This article goes into detail about how necessary it is for safe online communication. So many of the devices we utilize today relies so much on communication devices like cars, cell phones, and medical devices that implanted in people’s bodies. But once quantum computing becomes more relevant all of the current cryptography and security systems, we rely on now will no longer be effective.

In the article goes more in depth on the many possibilities after quantum computing becomes more relevant. In this future of possibilities, you can also accept the scary fact that an attacker or a hacker can get their hands on a quantum computer. Someone with malicious intent getting their hands on a tool that is as powerful as a quantum computer is very freighting. The article dives into the many different security measures we can upgrade using quantum cryptography. In recent years many researchers have figured out different ways to start implementing and testing these new quantum cryptography systems.

Although we have made so many advancements in quantum cryptography, we still have a long way to go. One big issue that plays a big part in the development of these new systems is time and money. These systems and research are not cheap by any means necessary. But these are the many steps necessary to take in order to be able to implement these improved ways of security. A lot of the times its better to figure what doesn’t work or what can be broken before it can be used against the system on a later date. Once researchers get more testing done and have more knowledge on these systems it won’t be long until they are established in the world, we live in. But an important lesson to take from this article is what risks or future problems this can lead to if it is not tested or researched properly.

Anne Broadbent, and Christian Schaffner, (2016). Quantum cryptography beyond quantum key distribution. *Designs, Codes, and Cryptography*, *78*(1), 351–382. <https://doi.org/10.1007/s10623-015-0157-4>

This article dives into the topic of quantum key distribution which is one of the most well-known topics in quantum cryptography. But this article also discusses other applications for quantum cryptography such as quantum money, randomness generation and many more applications. First the article dives into the discussing about one of the most popular topics in quantum cryptography which is quantum key distribution. What makes quantum key distribution so interesting is how these keys are processed. In quantum key distribution the data for the keys is processed by particles. How a particle is set to a value depends on a couple attributes. One is the state of the particle whether it is positively or negatively charged will dictate the value of that particle. Another factor that plays into how a value is dictated is what direction the particle is rotating.

Later in the article it discusses other subtopics in quantum cryptography. One of the topics is the security side of quantum cryptography and how secure it really is. Which in theory it will be the most secure way of encrypting and decrypting data. A term the article uses to define how secure it is everlasting security. What is great about how secure it is that these computers can easily detect if someone is eavesdropping which will change the value of the keys. But if no eavesdropping is detected and is too difficult for most people to accomplish then the idea of key recycling can come into play. Another great feature that the article touches base on is quantum uncloneability. In general quantum information cannot be cloned or duplicated. This can be very useful since in the real world today copying information can be rather easy to achieve.

The more I dive into these articles about quantum cryptography the more I understand how big of an advancement this would be in our society. These theories open a whole new idea of the most optimal way to secure our information. Not only will to be very easy to send secure messages from one party to another but, we can easily detect if an attacker is trying to eavesdrop or steal information. One last feature that stuck out to me was the uncloneability of quantum information. This feature will make key distribution and sending messages a lot easier to maintain. Especially the possibility of reusing keys which will make our lives a lot easier when sending information from one party to another. The only downside in all of this how long it will take to achieve and fully implementing these in the world we live in today. While we are a long way to go to achieving this goal, we are taking the proper steps to ensure our future will benefit greatly from these advancements.

Diogo Lima, and Gustavo Rigolin, (2020). Asymptotic security analysis of teleportation-based quantum cryptography. *Quantum Information Processing*, *19*(7). <https://doi.org/10.1007/s11128-020-02701-w>

This article investigates asymptotic security analysis of teleportation based on quantum cryptography. In the article it tests the teleportation-based quantum cryptography protocol against all types of attacks whether its individual or collective attacks. At the start of the article the researchers refer to previous protocols and evaluate the security behind those protocols. It discusses the positives and negatives these protocols presented and compared them to how quantum cryptography will fix these issues. After discussing the previous protocols, the article dives into how asymptotic security analysis of teleportation can be modified to possibly produce a less error rate involving quantum cryptography.

The researchers then investigate different modifications to the protocol to determine greater secret key rates against multiple types of attacks. In the article it dives deep in the actual mathematics and quantum physics of all the protocols. The article provides this information for the reader to not only explain the differences but give you a full visual of the main differences. The modifications done to the protocol prove to have a more secure transmission of keys with a slight greater quantum bit error rate. In the conclusion of the article, it presents many proofs of the GR10 protocol which is the asymptotic security analysis of teleportation protocol. After testing many individual and coherent attacks and comparing the error rates have shown that this protocol has an immense amount of security.

Data security is one of our main and growing priorities currently. Every day as we speak security is being updated and more of a high demand in today’s job market. Testing new ways to improve our security is a necessity for combating present and future attacks. This article proves modifications to the GR10 protocol involving quantum cryptography can make a huge stride forward in future security. Doing these many tests will only help us in the future to provide us with the proper information we need in order to properly implement these systems in order to provide greater security.

Neha Sharma, and Ramkumar Ramachandran, (2021). The emerging trends of quantum computing towards data security and key management. *Archives of Computational Methods in Engineering*, *28*(7), 5021–5034. https://doi.org/10.1007/s11831-021-09578-7

In this article it discusses numerous ways how data security will be affected by quantum computing. One aspect the article focused on was network security and how quantum cryptography will play a major role in the future. Quantum cryptography is composed of many applications such as quantum key distribution, quantum bit commitment, and quantum coin tossing. Quantum cryptography was first introduced in the seventies by Stephen Wiesner and was later worked on by Bennett. Some of the fundamentals that involves quantum cryptography is based off physics. Some examples are photons, qubits, entanglement, and superposition.

Quantum cryptography will be one of the most promising communication systems we will end up developing. This is based off conscience of quantum mechanics with the use of particles to be able to deliver information. Even though RSA encryption is a very strong algorithm that we currently run lots of encryption on. Quantum cryptography will be able to crack RSA encryption. Quantum key distribution is the use of sending particles out to send keys and messages safely to both parties. A tool that QKD uses is a distributer which can dictate whether any information is altered when a outside part is trying to eavesdrop on the message. These keys are generated randomly and sent over a network. To send messages to the other party they use fiberoptic quantum links which is being used as a photon stream.

The impact these topics can have on the world today would be major advancements. Not only their will be a more secure way for messages to be sent and received but many protocols are in place and being developed to combat anyone who tries to intervene. With the ability of our current security being at risk to quantum computers it is great to see that there are tons of research being developed on how to use it for positive improvements in the world.

Kexin Wang, Xinke Tang, Adrian Wonfor, Robert Collins, Gerald Buller, Richard Penty, Ian White, and Xu Wang (2021). 40Gbits−1 Data transmission in an installed optical link encrypted using physical layer security seeded by quantum key distribution. *Journal of Lightwave Technology*, *39*(19), 6130–6141. https://doi.org/10.1109/JLT.2021.3095539

This article discusses the how important telecommunications have become over the years. It also talks about the many threats that quantum computing will bring to public key encryption algorithms. Also, it discusses the many new advancements we have approached with the introduction of quantum cryptography. Working with telecommunication systems it has been a real challenge over the past couple of years to ensure a secure way to utilize optical communication systems. In today’s world open-source interconnection networks models use digital encryption methods like RSA, and AES. This is issue for the sole fact that these optical digital systems can be easily measured and perfectly copied by a third party.

A method that is being developed and constantly tested is quantum key distribution. This is proven to be a very reliable way to be able to generate and transmit security keys. The article goes into much greater detail on their process and tests they made when transmitting a 40 Gb “scheme” over 32 miles with bit-by-bit time dominion spectral phase encoding technique. Using a laser source to transmit the data and after further investigation and experimenting they concluded the security of the transmission and were able to authenticate that only the authorized user could receive the message.

Even though this study and experiment was conducted over a distance we wouldn’t think is as large as we would want it. Researchers are continuing to work on improving the distance of this transmission so that it can be reachable at great distances. The researchers also suggested that stretching it over larger distances and increasing the encoding and scrambling rate can improve the security even more. These advancements in quantum cryptography will be very useful for the future. Not only will it be more secure for private personal to send and receive messages to each other on earth. But we can take this technology and utilize it off our planet into space. This would not only be a faster way to communicate with our fellow researcher in space. It will ensure a more secure connection to make sure no outsiders try to sabotage or steal private information.