ESC301
Literature Review

QiLin Xue
Spring 2023

1 Description of Paper Discovery

This year, I am planning to take a supervised reading course on quantum cryptography. I have communicated with the professor who agreed to teach me, and have recommended some papers we base the course off of. While many of these papers are very technical that may require months of work to write a proper literature review, I have chosen some less technical pieces to explore.

2 Introduction

Modern cryptography offers the ability to send messages securely and anonymously, but their working assumption relies on the fact that certain problems (such as factoring large numbers) are hard to solve. Because of this, we can never prove the security of our current systems, against both quantum or classical computers. As a result, interest in quantum cryptography has been growing in recent years, in part by the fact that quantum based protocols can be proven secure, using the fundamental laws of physics.

This literature review will focus around the goal of achieving this quantum internet, what steps we're taking to achieve it, and what are some current challenges? The first paper, *Quantum internet: A vision for the road ahead* published in *Science* is a review summary characterizing the five stages of a quantum internet and their potential applications[3].

The above article has a very optimistic outlook, and for good reason. In 2018, a team from China made great progress in realizing the first stage by implementing quantum key distribution (QKD) over 7600 km on Earth. Their work is described in *Satellite-Relayed Intercontinental Quantum Network,* published in *Physical Review Letters*[2].

Finally, we will discuss some of the security challengers that we must face, starting with one of the first "hacking strategies" known as Photon-number-splitting (PNS) attack. The paper *Limitations on Practical Quantum Cryptography* published in *Physical Review Letters* was one of the first to analyze this kind of attack back in 2000[1]. While more hacking strategies have been discovered since, we will discuss this as PNS attacks are still relevant today and is relatively accessible.

3 Review

3.1 Quantum Internet

The paper *Quantum internet: A vision for the road ahead* describes five stages to a quantum internet[3]:

1. Prepare and measure
2. Entanglement distribution
3. Quantum memory
4. Few-qubit fault-tolerant
5. Quantum computing

The first stage: "Prepare and measure" allows for basic quantum key distribution between two parties. As the stages become more and more advanced, we start being able to construct a quantum network that allows for the same security and anonymity that classical cryptography offers, but with the added benefit of being able to prove this security. What is interesting is that the holy grail of quantum computing that popular science authors write about is the last stage, and we're currently far from achieving that. However, this article demonstrates that we don't need to wait for that to create a useful network.

In fact, just having a single qubit at certain nodes of the network can already be very useful, and any noise caused by device imperfections could be fixed with classical error correcting codes.

3.2 Satellite-Relayed Intercontinental Quantum Network

The paper *Satellite-Relayed Intercontinental Quantum Network* describes the practical details of how QKD can be implemented using satellites at long distances of up to 7500 km[2]. Specifically, they used the Bennet-Brassard 1984 (BB84) protocol, which is one of the most popular and standard QKD protocols. It has the extra advantage that it is immune to photon-number-splitting attacks, which is particularly effective at attacking longer distance communications.

Fiber lasers emitted pulses with a wavelength of 850 nm at a repetition rate of 100 MHz. These pulses are encoded into random states as per the BB84 protocol, and sent to three ground stations. There were several effects that could cause information from being lost, such as

- Channel Loss
- Beam diffraction
- Atmospheric Turbulence
- Absorption

However, the authors noted that decoherence was not a problem, and can be safely ignored. Unlike traditional communications, the authors could not simply increase the signal power and were forced to put measures in place to reduce the background noise.

Accounting for the above effects, and the trajectory of the satellite, the satellite was able to transmit useful information for 300 seconds everyday, with a sifted key rate of $3-9$ kb/s depending on distance and weather conditions, and achieved an error rate of between $1.0\% - 2.4\%$, which were mainly a result of background noise and polarization errors.

These rates are optimal enough to faciliate an intercontinental video conference between the Chinese and Austria Academy of Sciences using the AES-128 standard, where the satellite QKD network was integrated with fiber-based quantum networks. A total of 2GB of data was transmitted in the 75-minute video conference.

3.3 Limitations on Practical Quantum Cryptography

While protocols such as BB84 theoretically protect against certain attacks such as the PNS attack, the paper *Limitations on Practical Quantum Cryptography* shows that in practice, these attacks can still be effective against realistic devices[1]. In ideal communication, where no information is being lost, the two particles communicating (known as Alice and Bob) can detect if an eavesdropper (known as Eve) is trying to intercept their communication in the BB84 protocol. The working principle, which relies on quantum entanglement and the fact that every detail of a quantum state cannot be exactly measured, allows Alice and Bob to detect if the qubits they are being sent have been tampered with.

However, under the presence of loss, it is difficult to determine if any lost or tampered information is due to natural background noise, or if it is due to Eve's attack. The authors derive a criterion that the error rate e of practical devices must satisfy in order to be secure against PNS attacks, given by

$$e < \frac{1}{4}(p_{\text{exp}} - p_{\text{multi}}) \tag{3.1}$$

where p_{exp} is known as the experimental detection probability: the probability that a qubit sent by the sender is detected by the receiver's detector. Similarly, p_{multi} is the multiphoton probability: the probability that a single photon source accidentally emits more than one photon. These numbers are difficult to quantify, so practical estimates are done by estimating the fidelity F, which is the overlap between two quantum states. It ranges from 0 (all the information is being leaked) to 1 (no information is being leaked). They derived

$$F > \frac{2\sqrt{d_B}}{\eta_B} \tag{3.2}$$

to be the criteria for the fidelity of the device to be secure against PNS attacks. Here, d_B is the dark count probability: the probability that the detector will detect a photon when no photon is present, and η_B is the detector efficiency: the probability that the detector will detect a photon when a photon is present. Back in 2000, realistic estimates on d_B, η_B and device parameters meant that the maximum distance QKD can be realized was around 24 km through optical fibers.

In general, the fidelity F falls off exponentially due to various noise, making it difficult to reliably send information over long distances. The use of quantum repeaters, which are analogs of classical repeaters, can be used to transmit qubits over longer distances while still maintaining security.

3.4 Next Steps

To realize guaranteed security through a quantum internet, we must be able to transmit qubits over long distances but also ensure they cannot be attacked, i.e. a full security proof is necessary. These two concepts will always be in a battle with one another, as longer distances will include more loss, which gives attackers more freedom to work with.

While Liao et. al were able to make great leaps by confirming the ability to do long distance QKD via satellites with low error rates on the order of 1%, which is a huge leap from the estimates provided in 2000, they did not comment on parameters such as the experimental detection probability or the multiphoton probability. These parameters are crucial to determining the security of the system, and it would be beneficial if we could have a more detailed analysis of the security of their satellite system for future work, though we acknowledge it was not the focus of their paper.

Nevertheless, security analyses are important if we are to realize a quantum internet. It may be promising to see if the satellite and ground stations can be repurposed to perform general quantum key distribution through different protocols, which have different advantages and weaknesses to different quantum hacking attacks. Furthermore, it would be very impactful if more research could be done in reducing background noise and sensor tracking, which are the main causes of error in the satellite system. Not only would it make future quantum internet systems more secure and faster, but it would also be useful in non-quantum applications of satellite systems.

3.5 Conclusion

In conclusion, this literature review focused on the goal of achieving a quantum internet, the steps being taken to achieve it, and the challenges we must overcome. The papers summarized the five stages of a quantum internet and their potential applications, described the practical details of implementing quantum key distribution using satellites over long distances, and finally discussed the photon-number-splitting attack, which is still relevant today.

The findings of this review demonstrate that while we are still far from achieving the holy grail of quantum computing, we are already able to securely transmit qubits over long distances for practical applications, such as video conferencing, though the security for these systems is still not proven.

However, there are still several challenges that need to be addressed, such as noise caused by device imperfections and background noise that affects the key rate and error rate. Further research is needed to develop methods that can mitigate these effects and improve the overall efficiency and security of quantum communication. Overall, the potential applications of a quantum internet are vast, and we are likely to see significant advancements in this field in the coming years.

4 References

References

[1] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330–1333, August 2000.

[2] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng-Zhi Peng, Jian-Yu Wang, Anton Zeilinger, and Jian-Wei Pan. Satellite-relayed intercontinental quantum network. *Physical Review Letters*, 120(3), January 2018.

[3] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412), October 2018.