Sri Lanka Institute of Information Technology

2024

Introduction to Cyber Security

Assignment

Year 2, Semester 1

The Growth of Quantum Cryptography in Data Security.

IT23400368

MMM ARKAM

Y2.S1.WD.CS.01.01

MALABE CAMPUS

Table of Contents:

1. Abstract.

This report reviews the developments that have occurred in the field of quantum cryptography for possible applications in protecting communication from the threat of the present world.

The paper begins by introducing the basic concept of QKD and how it uses quantum mechanics to generate secure keys, which notify users of any attempt at eavesdropping. The report will cover major developments starting from the introduction of the BB84 protocol back in 1984 to the very first implementation of QKD systems in real-world applications, namely Micius satellite and secure banking systems.

Major results are that quantum cryptography, opposite to the traditional approaches, offers better security. With the development of quantum computing, it has become even more developed.

This report attempts to project quantum cryptography as the future of cybersecurity by giving an understanding of its applications and research in course. Quantum cryptography can be an important step towards the pursuit of a safe way of digital communication-a way to address all vulnerabilities related to classical methods of cryptography.

2. Introduction.

Quantum cryptography is an up-and-coming field in the world of cybersecurity, introducing new ways of securing communications using some principles of quantum mechanics. This report discusses the evolution and current applications, while also looking at future developments in quantum cryptography with the objective of explaining the topic in detail and presenting the latest information in a clear and well-researched manner.

Quantum cryptography basically serves to ensure that the cryptographic key is exchanged in a secure way through QKD. On the other hand, while classical cryptography relies on complex mathematical algorithms, quantum cryptography relies on the quantum particles, such as photons, for generating the encryption keys. The key benefit is that any attempt to tap into or measure these particles would alter their state, thereby serving as an alert to the sender and receiver of the presence of an interceptor.

The report now proceeds with the discussion on some salient features in the development of the same, starting with probably one of the first founding models for QKD-the BB84 protocol that was introduced in 1984. The report further discusses real-life applications, such as the Micius satellite experiment and the implementation of QKD in banking and telecommunications, currently studied by governments and financial institutions desiring to secure sensitive communications and transactions.

This report mainly tries to provide insight into how quantum cryptography addresses the loopholes of traditional methods of cryptography as the quantum computing aspect gets more advanced. By embedding the latest research and development within the frame, this report tends to develop a lucid understanding of how quantum cryptography evolves the syntax of secure communication and might shape the future of cybersecurity.

Objectives of the report.

- Understanding the basics of quantum cryptography.

- Explain how quantum cryptography works and identify the unique properties of that makes communication secure.

- Analyzing the evolution of quantum cryptography.

- Analyzing the development of the topic from its theoretical foundation to current practical.

- Exploring the current and emerging applications.

- Explore the latest real-world implementation in this topic.

- Identifying the future development in this area.

identify the future potential of QC. And how could it solve the future data security.

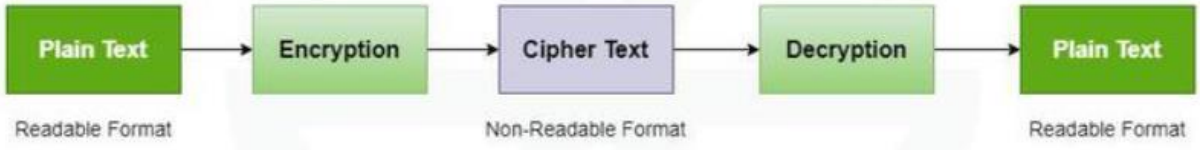
3. Evolution of Quantum Cryptography.

3.1 Introduction to Cryptography.

- Cryptography refers to the techniques for protecting information so that it is accessible only to the people who are authorized.

  Encryption- process of changing plain text into unreadable format (cipher text).
  Decryption – process of changing the unreadable format (cipher text) into readable format (plain text).

- Cryptography involves the processes for encryption, whereby data, through an algorithm and a key, is changed into an unreadable code format.
- It refers to the original information as "plaintext" and the already converted information in unreadable code format as "ciphertext." Subsequently, only the owner of the correct decryption key can transform this ciphertext back into readable information**.**
- People and organizations nowadays are using cryptography in their daily life to protect their privacy and keep their conversation and data confidential. Cryptography guarantees confidentiality because it encrypts the message sent.
- A good example of this is WhatsApp, a messaging tool that encrypts conversations between individuals so they cannot be hacked or intercepted..



3.1.1 Objectives of Cryptography.

- **Confidentiality:** only the intended recipient can access the information.
- **Integrity:** protect data from being modified.
- **Authentication:** verify the sender's identity.
- **Non- repudiation**: to ensure that sender and receiver cannot deny sending and receiving.

3.1.2 Ancient cryptography

Between 100-44 BC, to share secret messages within the Roman army, Julius Caesar is credited for using what has come to be called the Caesar Cipher, a substitution cipher wherein each letter of the plaintext is replaced by a different letter determined by moving a set number of letters either forward or backward within the Latin alphabet.

3.1.3 Weaknesses in classical cryptography

- It is vulnerable to some methods like brute-force attacks frequently analysis.
- Distributing the key is very challenging. It can lead to interception or misuse of key.
- It is hard to detect If an eavesdropper intercepts the connection and listens to the communication.

To overcome these types of weaknesses some scientists developed quantum cryptography.

3.2 Origin of Quantum Cryptography

- Quantum cryptography was born to reduce the limitations in classical cryptography for secure communication. In the 1970s, investigations began into how quantum mechanics could be used in data security, based on properties peculiar to quantum particles.

- In 1984 when Charles Bennett and Gilles Brassard produced what is considered the first practical application of quantum cryptography, known as the **BB84 protocol**. By exploiting the quantum behavior of photons, more colloquially known as particles of light, they were able to devise a method that would create encryption keys.

Photons: A photon is a basic particle with both wave-like and particle-like properties and present in electromagnetic radiation.

- There are 2 important elements of quantum mechanics on which quantum cryptography depends:

  1. Heisenberg Uncertainty Principle:

  The Heisenberg Uncertainty Principle simply states that one cannot know the definite position and speed of a particle in the same instant. In other words, the better the accuracy with which one knows either of the two, the lesser will be the accuracy with which one can know the other.

  2. Photon Polarization Principle:

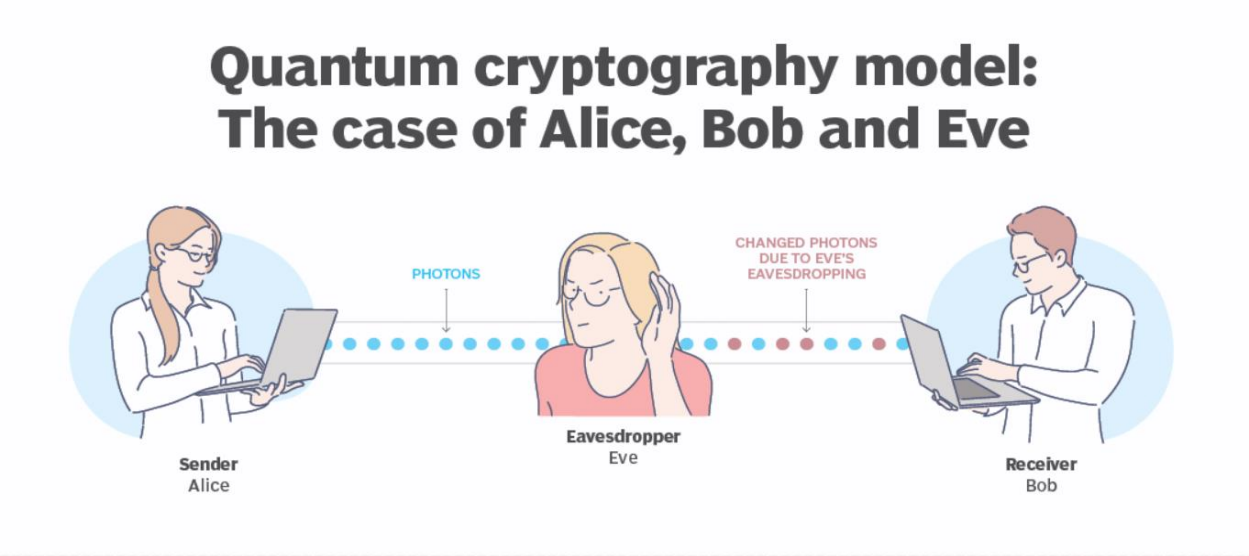
  It is a principle which states that the eavesdropper cannot copy unique quantum bits due to the no cloning principle, being an unknown quantum state. Any attempt to measure properties will disturb the other information.

3.3 The Birth of Quantum Key Distribution

Quantum Key Distribution was developed to further enhance security in communication with the use of some quantum properties. In 1984, Charles Bennett and Gilles Brassard presented so-called BB84 protocol, which was the **first practical QKD protocol** using photons, or particles of light, as a means of generating encryption keys.

But what makes QKD so special is that just by intercepting the key, the quantum state of the photon's changes, and this makes eavesdropping detectable. Should an attacker try to listen in, the sender and receiver will immediately know because the intercepted key becomes useless. This idea, derived from quantum mechanics, was revolutionary because for the first time it provided an entirely new level of security than classically achievable.

QKD was, therefore, the advent of a new age to come in secure communication and it promised more about what the future held in store in quantum cryptography and its realistic applications.



3.3.1 How does it work?

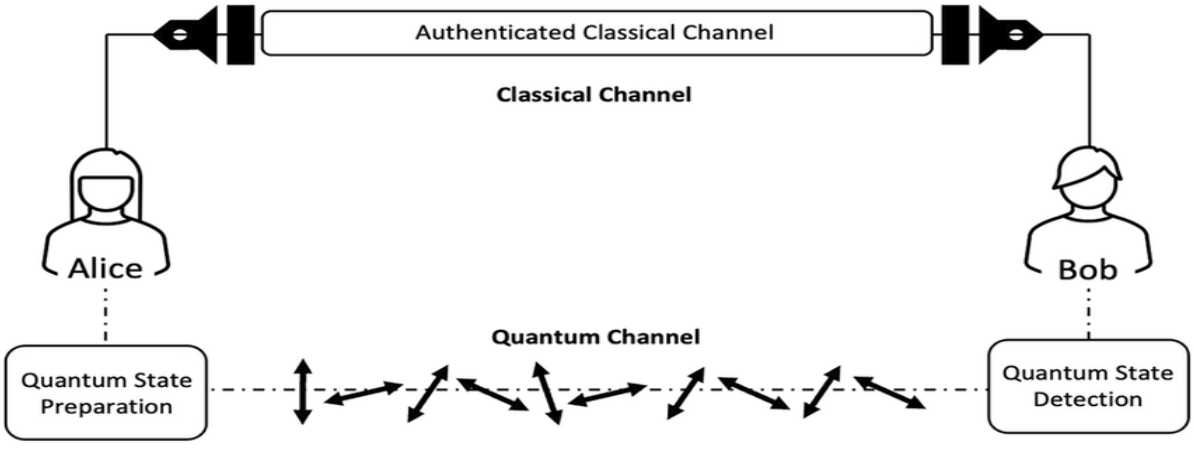
Key Generation: A sender named "Alice" prepares and transmits a series of light particles called photons to another person referred to as "Bob." Each photon is intended to be received in a certain polarization state (horizontal, vertical, or diagonal) which encodes binary values of either 0 or 1.

Random Measurements: Bob has selected a specific measurement technique to employ for each of the arriving photons in a random manner. The basis in this case may or may not be similar to that applied by Alice in encoding the photon. Consequently, if Bob uses the same basis as that of Alice, he is likely to obtain the same value. Otherwise, it will be a random value which he returns.

Key Matching: When the last of the photons has been received by Bob, Alice and Bob then proceed to discuss the constants of the measurements in a public manner (via the internet). They do not disclose the actual figures, only the ones encoded with a respective bases. Only those that satisfactorily match their bases results are retained. This becomes their key.

Eavesdropper Detection: Should an intruder (Eve) attempt to come between the photons, then thanks to the measurement of photons, the state is altered, creating some faults. When Alice and Bob observe such discrepancies, they understand someone is spying and therefore gets rid of the key.

Secure Communication: After this key agreement is achieved, Alice and Bob can employ the key for any purpose, including the secure encryption or decryption of messages exchanged between them.



Transmitting station bit	0	1	1	0	1	0	0	1
Transmitting station basis	+	+	X	+	X	X	X	+
Polarization	↑	→	↖	↑	↖	↗	↗	→
Receiving station basis	+	X	X	X	+	X	+	+
Receiving measurement	↑	↗	↖	↗	→	↗	→	→
Open channel discussion								
Shared key	0		1			0		1

3.4 The BB84 protocol: The first quantum cryptography protocol.

The first practical realization of QKD was the BB84 protocol. In 1984, Charles Bennett and Gilles Brassard proposed a breakthrough for cryptography by using quantum physics to exchange securely an encryption key. This protocol uses polarization of photons, or light particles, to encode information like 0s and 1s. The novelty of BB84 consists in the fact that this protocol guarantees security by making any eventual eavesdropping detectable.

If an eavesdropper, Eve, tries to intercept the photons in the BB84 protocol, measurement will change their state and thus introduce errors in the key. This is owed to the Heisenberg Uncertainty Principle: a measurement of certain quantum properties disturbs other properties. Consequently, Alice and Bob also recognize this interference and discard this key.

Important as it was, the real milestone of the BB84 protocol was in showing just how quantum properties could be leveraged to achieve a level of security inaccessible to classical cryptography. The protocol opened the gates to further research and development of quantum cryptography, and it is still being extensively considered today.

3.5 Early experiments in QC.

1. In 1991

In the early days of quantum cryptography, researcher were mainly focused to prove that the idea of secure quantum communication can work practically. In 1991, one of the first successful experiments was performed by a team of scientists headed by Artur Ekert. This experiment was based on the principles of quantum entanglement, meaning pairs of particles that have an interconnectedness in their state whereby one instantly influences the state of the other, even over considerable separations. The experiment was advanced work by Ekert, where he showed how entangled particles could be used in secure key exchange because it would make it difficult for anyone to spy.

2. In 1992

Another key early experiment was attempted by Bennett, Brassard, and Claude Crépeau in 1992. They implemented an extremely basic QKD system using the BB84 protocol. This experiment thus showed that quantum cryptography could be employed over short distances with extremely simple laboratory equipment. At this time, however, it had limitations to high error rates and short distances of transmission.

3. in 1997

Till 1997, quantum cryptography experiments progressed, and secure key distribution over longer distances was possible. One of the milestone experiments, performed by researchers at the University of Geneva, sent quantum keys through 23 kilometers of optical fiber. More importantly, it was proof that QKD could be applied in real networks.

These experiments served as the foundation for continued research and refinement that are creating today's more robust, commercially available QKD systems.

3.6 Real World Implementations and Applications

Quantum cryptography has come a long way from theory into the very real world. Perhaps one of the greatest advances in actual use is quantum key distribution, QKD, to distribute secret keys between pairs of entities securely. Nowadays, several organizations are researching QKD, especially those dealing with sensitive information in finance and governments.

Scenario 1 (Micius satellite):

In 2017, Chinese scientists launched the Micius satellite, which could achieve QKD up to 4,600 kilometers. The satellite successfully transmitted quantum keys from space to ground stations, thereby demarcating that long-distance key distribution is secure. This experiment showed the use of satellites in building a global quantum network, a concept that could underpin greater security in international communications.

Scenario 2 (Secure Banking):

Another very important application of quantum cryptography is in secure banking. Several banks and other financial institutions are at the moment carrying out tests on QKD systems that will offer security for transactions and protect customers' information. These systems help prevent hackers from stealing sensitive information during online transactions.

Scenario 3 (Telecommunication networks):

In addition, quantum cryptography integrates into telecommunications networks. Companies are developing quantum communication systems that can prevent the illegal access of data while it travels over fiber optic cables. Technology will provide immediate detection of tampering, even in the case of an attempt at interception, by the sending and receiving parties.

Scenario 4 (Cloud computing):

Further research is also in progress to extend the use of quantum cryptography to cloud computing. As more and more companies begin to move towards using cloud storage, the security of data from unauthorized access will be of utmost importance. Quantum encryption would thus provide an extra layer of security in cloud storage. *Although quantum cryptography is still at the beginning of practical development, its possible future applications in banking, telecommunications, and cloud computing provide hope for a safer future on digital platforms*.

3.7 How Quantum Cryptography Differs from Classical Cryptography

Security Basis:
The basis for the security of classical cryptography lies in a problem that is mathematical, whereas for quantum cryptography, it lies in the laws of physics. Thus, inherent in quantum cryptography are its impenetrable securities, as no number of computing powers can break the rules of quantum mechanics.

Eavesdropping Detection:
In the case of a classical system, one could secretly listen to the communication without being detected, while in quantum cryptography any attempt to eavesdrop will instantly change the state of photons to indicate that someone tries to spy on them.

Key Exchange:
Classically, cryptography has a big problem in key exchange. When the key is intercepted, the entire system is compromised. Quantum cryptography, however, does the key exchange securely through QKD, and any interference is noticed immediately.

Vulnerability to Quantum Computers:
The classical encryption techniques are highly susceptible to being broken easily by quantum computers, hence posing a threat for the future. In contrast, since quantum cryptography is based on quantum mechanics, it will be immune to such attacks.

Still today, there is a greater use of classical cryptography because it is more practical and easier to set up. However, with the development of quantum computers in the future, the weaknesses of classical cryptography will be more pronounced. Thus, researchers and companies continuously invest in quantum cryptography for protection against an unseen foe.

3.8 Growth and Interest in Quantum Research

The research in this field has grown greatly in the last decades. From a very obscure scientific field, it turned into one of the biggest areas of interest, especially since technology advances and better data security is needed. Quantum mechanics is the science behind how atoms, photons, and similar particles act on a very small scale, opening many possibilities toward new technologies. Arguably, quantum computing and quantum cryptography are some of the exciting developments arising from research into the quantum, whose power might totally alter how we approach computing and secure communication.

Early Interest in Quantum Research began early in the 20th century, with scientists like **Albert Einstein** and **Niels Bohr** making groundbreaking discoveries in quantum mechanics. These furthered the understanding that particles could exist in a complete, random fashion, and this completely revolutionized scientific perspective on how the world works at its very core. This type of physics initially inspired curiosity about other ways quantum mechanics could be applied to technology and advanced development. For years, though, much of the work in this area remained highly theoretical and did not encompass many realistic applications.

Quantum Computing Rise In recent decades, particularly within computing, quantum research has gained immense popularity. Classically, it is becoming inefficient for classical computers to solve some complex problems where data continuously piles up in the world. This is because they use bits that process information as 0s and 1s. Quantum computers, on the one hand, represent qubits for 0 and 1 all at once. Indeed, the ability to do so enables quantum computers to solve some types of problems a great deal faster than their classical counterparts.

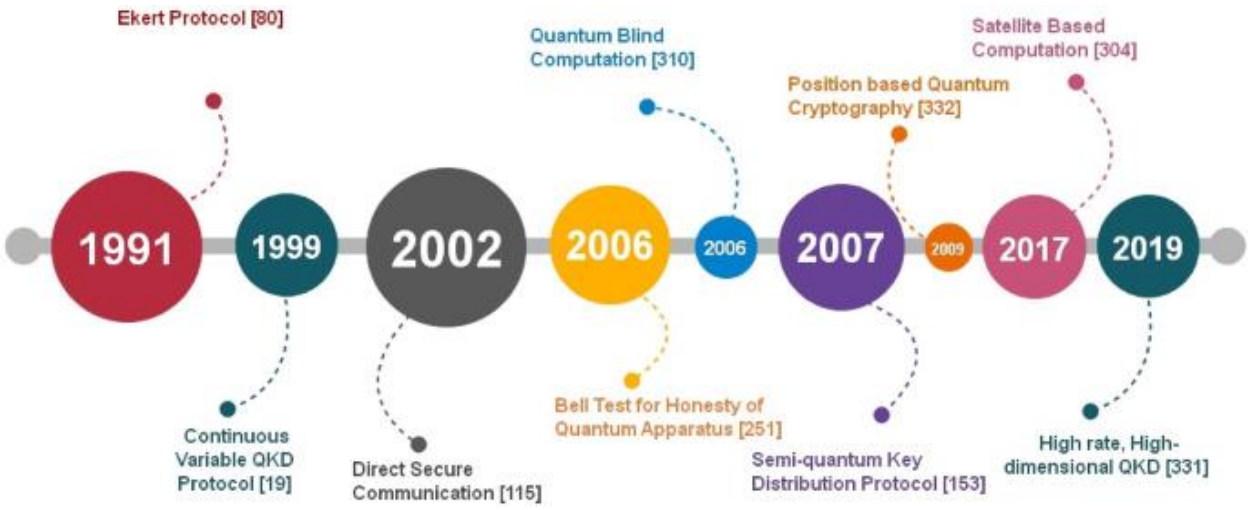
Governments, research institutions, and technology companies have all begun making significant investments in quantum computing studies. Companies such as IBM, Google, and Microsoft are building quantum computers; universities and government organizations are studying the search for new ways to improve quantum technology. This development has brought tremendous growth in funding and resources toward quantum research and, more importantly, more collaboration by scientists, engineers, and companies around the world.

Another field of growing interest is quantum cryptography. The latter relies on the principles of quantum mechanics to secure data. In traditional cryptography, information is encrypted using mathematical algorithms, which can be further deciphered by hackers. On the other hand, quantum cryptography depends on the principles of quantum particles; therefore, it is practically impossible for a hacker to intercept or alter information without being detected. With this, quantum cryptography has indeed become an interesting field for those who are concerned with data security, especially since more personal and sensitive information is stored digitally.

The first practical applications of quantum cryptography are Quantum Key Distribution, enabling both parties to share a secret encryption key over a quantum network. QKD attracts growing interest due to its higher level of security compared with classical encryption methods, which become more and more insecure with the development of powerful computers.

Growing Interest and Investment Interest in quantum research will only continue to increase, especially at this time when new challenges offered by data security and computing power as well as the limitations set by technology are offering. Various countries draw up national quantum strategies to support the related research and development programs. The European Union has kicked off, for example, the Quantum Flagship program-a 10-year program of research and development for a strategic development in quantum technologies.

From a small theoretical discipline, quantum grew to become one of the most promising areas of modern science and technology. Possible applications in quantum computing and cryptography have already drawn the attention of governments, companies, and scientists all over the world. While we are delving deeper into the might of quantum mechanics, so bright is the future that awaits us-a future of technological breakthroughs along with data security.



3.9 Challenges Faced in Quantum Cryptography.

1. **Complex technology:**

Quantum cryptography is based on very developed technology and is still in the development phase. Preparation and maintenance of equipment used in it, like quantum computers and photon detectors, is very difficult. This infuses a challenge in implementing wide scope usage of quantum cryptography systems or everyday applications.

2. **High cost:**

The development and maintenance costs of quantum cryptography systems are very expensive. The reason is that these systems involve special hardware and complex technology; therefore, their implementation is not in the normal budget of an enterprise or government. Therefore, quantum cryptography is not as widely accessible compared to traditional cryptography systems.

3. **Limited communication range:**

It works via fiber-optic cables, normally for a few hundred kilometers. For long distances, quantum repeaters are required to assist in the communication process; hence, this technology remains in the development phase. This technology can't be utilized for effective global communications if it is not advanced.

4. **Sensitive to the environment:**

Quantum particles, like those of photons, are very sensitive to environmental conditions: variation in temperature, vibration, and even minor agitations can easily affect their behavior. These sensitivities make quantum communication considerably less reliable in an uncontrolled environment because they may result in errors or losses of data.

5. **Key sharing issues:**

Quantum cryptography involves the sharing of keys in secrecy between two parties. The large-scale management and distribution of these keys are laborious and prone to loopholes. Much acquisition is put into secure key management systems to prevent interception or misuse of these keys.

6. **Difficult to fix with current systems:**

Most of the current information communication systems are based on classical cryptography. The integration of quantum cryptography into the current infrastructures is hard since the usage requires heavy changes in networks, hardware, and software. Changing these would be time-consuming and costly.

7. **Incomplete quantum hardware:**

Quantum cryptographic Hardware: quantum computers and detectors are still in their infancy. The systems need to be more practical, scalable, and efficient to see broader use. Until then, quantum cryptography will remain bottlenecked by the limitations in hardware.

8. Quantum hacking threats:

Although quantum cryptography is very secure, it is not totally immune from hacking. Other potential threats include quantum hacking methods such as intercept-resent attack and side-channel attack. Defense against these threats shall require further research and technological advances.

9. No common standards:

The development of universal standards for quantum cryptography does not exist yet, and thus it is hard for organizations to universally adopt and entrust the technology. Standardization of protocols, hardware, and security will be needed before quantum cryptography can become universally accepted.

10. Hard to understand for most people:

The complexity in physics on which quantum cryptography is based may be difficult to understand for the general public and most of the industries. There is a great need for the education of people to understand its benefits and its limitations. However, by nature, it is a specialized field, and that makes educating the public about the use of this technology a bit uphill.

3.10 Recent Developments and Innovations.

- **Scientists build mass-producible miniature quantum memory elements.**

A miniature quantum memory element allows for the temporary storage of quantum information and is therefore an essential element for quantum networks, including secure communication. Researchers at the University of Basel, together with colleagues from Switzerland, Germany, and Finland, have developed a new method to mass-produce these miniature quantum memory elements by using small glass cells filled with rubidium atoms. They succeeded in storing quantum information in the form of photons for short periods by heating the cells and applying strong magnetic fields; the period of time was roughly 100 nanoseconds. Using this breakthrough, that could mean thousands of these quantum memory elements can be fabricated onto a single wafer-a promising prelude to scalable quantum communication and computing systems.

That is important, because it brings quantum technologies one step closer to real applications: from information transmission in highly secure ways to connecting quantum computers and, finally, enhancing the efficiency of quantum networks. Researchers continue to optimize this technology, with one of the points of focus being an increase in the time photons can be stored while preserving their quantum states.

- **Single photons from a silicon chip.**

The development of single photons from a silicon chip is significant to take these quantum technologies to more accessible and scalable levels. During this process, scientists have developed a means through which individual photons can be generated on a silicon chip. Single photons, the tiny units of light, stand at the core in quantum communications because they enable the transference of information securely over long distances by means of QKD.

It works by creating and manipulating the single photons on a silicon photonic chip that is integrated into the quantum networks. That is important because silicon is already an established material in the semiconductor industry, which means the

costs are low, and it can be mass-produced. The capability for single-photon generation from silicon chips will most likely enable quantum cryptography systems' integration with the existing infrastructure at a lower cost and more efficiently.

4. Future Developments in Quantum Cryptography.

4.1 Improving quantum key distribution.

One of the main trends in future development concerning quantum cryptography is improving quantum key distribution. QKD will allow both parties to create a key in such a way that the detection of any attempt at eavesdropping will be realizable. QKD is currently a very promising technology, though there are some ways to enhance its effectiveness.

First, there are studies to extend the distance QKD can work today, the main limitation of QKD is the loss of quantum signals while the latter pass-through fiber optic cables. By using repeaters and satellite communication, scientists try to extend the range of QKD to make this technology more applicable in real-life conditions.

A second effort is in the direction of a more efficient and faster QKD. This means the elaboration of new protocols that will have faster key creation without compromising its security features. Better efficiency will make QKD more applicable in everyday uses, such as banking or even secure messaging.

Finally, there is incorporation with the existing QKD with communication systems. The effort that researchers are putting mostly is to come up with hybrid systems that can put together both classical and quantum methods of communication in a single system to ensure ease of adoption for QKD by businesses and governments.

In general, increased quantum key distribution will mark a great milestone toward secure communication in our digital world.

4.2 Creating secure quantum networks.

Another key future development in quantum cryptography is in the establishment of secure quantum networks. These networks are planned to securely connect several users by sharing encryption keys according to the rules of quantum mechanics.

The aim is to implement a reliable system of communication, which is totally safe from eavesdroppers. Previous studies have shown that QKD can successfully provide secure keys. However, building up a network represents a host of other challenges, such as integrity and security of the whole channel of communication.

Scientists are investigating the integration of QKD into existing network infrastructures, and this will go a long way to hybrid networks that combine both classical and quantum systems. In this respect, integration is a must as consideration to proposals of quantum networks for them to become practical and accessible for everyday applications.

For example, the University of Science and Technology of China has shown a satellite-based quantum network which could send secure keys over longer distances. This experiment shows the role that quantum technology could play in supporting future global communication networks.

Another ingredient in the recipe of secure quantum networks is multi-user protocols. Current research aims at further refining these protocols to be scalable while ensuring high standards of security. In any case, secure quantum networks will seriously improve communication security and offer strong solutions for keeping sensitive information secure.

4.3 Expanding quantum cryptography to everyday use.

The development of the application areas of quantum cryptography toward everyday use will be one of the most important to make secure communication available to all, including devices like smartphones, computers, and even over the internet. Making quantum cryptography user-friendly significantly increases the level of protection for personal data and communications, as evidenced by research.

First, there is a need to develop more simplified QKD systems that can easily be incorporated into already existing technologies. For example, devices are being

developed capable of generating and sharing quantum keys securely without any requirement for special knowledge of users about how to do this. Although previous studies had shown the potential of QKD in real life, scaling this technology to everyday use would be one sure way of widespread adoption.

With the prospect of scientists continuing to improve these quantum technologies, this promises a future where each and every one of us might have the chance to benefit from secure communications, rendering privacy possible in a digitally encroaching world.

4.4 Making quantum devices cheaper and more accessible.

One of the most pointed targets in the future of quantum cryptography is the wider affordability and accessibility of quantum devices. At present, quantum technologies are really expensive and complicated.

Therefore, they can be afforded and used only by big organizations and research institutions. However, the latest research efforts have aimed at simplifying QKD systems and reducing the cost of producing quantum chips and components.

Currently, researchers are working on methods of mass production of quantum devices, such as silicon-based quantum chips, which have less expensive production costs. Previous studies already demonstrated that the incorporation of quantum devices into current technology could be less costly and, consequently, more feasible for widespread application in banking and telecommunications.

With further development, one would hope to see quantum cryptography get cheaper and hence see its deployment in the everyday world to more enterprise or personal usage.

5. Conclusion

The main developments, challenges, and future prospects have been discussed in regard to quantum cryptography in this report. Major findings include that QKD offers unique benefits in promising a secure way of communicating using the principles of quantum mechanics. Quantum cryptography has moved from theory into application, including experimental applications such as satellite-based QKD, and quantum-secured communications within industries such as banking and telecommunications. Another factor necessitating such innovation is the limitations in classical cryptographic systems existing today.

Further development in improving QKD technology, building secure quantum networks, and reducing quantum devices to more cost-effective and broadly usable levels will further push the boundaries of cybersecurity. These will make international communication even more secure and the data of organizations and individuals safer.

Quantum cryptography certainly holds bright prospects for meeting the emerging threats and vulnerabilities in this dynamic landscape. While technology will become more mature and more scalable, its place in guarding sensitive data against the attacks that may be mounted in the future will be even more crucial. These can hardly be more significant issues about personal privacy and world security, so quantum cryptography can potentially be a game-changer within a few years.

6. References

1. A. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, pp. 661-663, 1991.

2. C. H. Bennett, G. Brassard, and C. Crépeau, “Practical Quantum Cryptography: Implementation of BB84,” 1992.

3. University of Geneva, “Quantum Cryptography over 23 km,” *Physical Review A*, 1997.
4. S.-K. Liao, et al., “Satellite-to-Ground Quantum Key Distribution,” *Physical Review Letters*, vol. 118, no. 14, pp. 140501, 2017. DOI: 10.1103/PhysRevLett.118.140501.

5. L. Zhang and Q. Zeng, “Quantum Key Distribution: A Review,” *IEEE Access*, vol. 6, pp. 6769-6781, 2018. DOI: 10.1109/ACCESS.2018.2792651.

6. J.-W. Pan, C. Simon, M. P. DeMicheli, and H. Zbinden, “Experimental Quantum Key Distribution: A Review,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 23, no. 4, pp. 1-10, 2017. DOI: 10.1109/JSTQE.2017.2670678.

7. T. Y. Chen, et al., “Practical Quantum Key Distribution with Quantum Repeaters,” *Nature Communications*, vol. 8, no. 1, pp. 1115, 2017. DOI: 10.1038/s41467-017-01225-4.
8. P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, “New High-Intensity Source of Polarized Photons,” *Physical Review Letters*, vol. 75, no. 24, pp. 4337-4341, 1995. DOI: 10.1103/PhysRevLett.75.4337.

9. C. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984, pp. 175-179.

10. H.-K. Lo, M. Curty, and K. Tamaki, “Secure Quantum Key Distribution,” *Nature Photonics*, vol. 8, no. 8, pp. 595-604, Aug. 2014. DOI: 10.1038/nphoton.2014.149.

11. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145-195, Mar. 2002. DOI: 10.1103/RevModPhys.74.145.

12. J. W. Silverstone, et al., “On-chip quantum interference between silicon photon-pair sources,” *Nature Photonics*, 2015.

13. L. D. Santis, et al., “A solid-state single-photon source with high-fidelity entanglement generation,” *Nature*, 2017.

14. “University of Basel develops mass-producible miniature quantum memory element.” [Online]. Available: https://quantumzeitgeist.com/university-of-basel-develops-mass-producible-miniature-quantum-memory-element/.

15. “Recent Advances in Quantum Key Distribution: A Review.” [Online]. Available: https://link.springer.com/article/10.1007/s11831-021-09561-2..

16. Tech-Champion, "Unlocking the Potential of Quantum Cryptography: A Comprehensive Guide," *Tech-Champion*, Sep. 2023. [Online]. Available: https://tech-champion.com/cybersecurity/unlocking-the-potential-of-quantum-cryptography-a-comprehensive-guide/.