PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 15 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Quantum Cryptography: Securing the Future of Digital Communication Through Quantum Mechanics

Revolutionizing digital security through quantum mechanics and unbreakable encryption.

By **Mohtasham Tahir** | University of Agriculture Faisalabad | Published: August 2026
mohtashimtahir999@gmail.com | Position: Information technologist

Introduction

In today's world people need to be able to communicate securely. This is very important for governments, banks, hospitals and individuals. These codes are based on math problems that are hard to solve. We have something called quantum computers. These computers are very powerful. Can solve those math problems quickly. They can break code we use to keep our information safe. Also, a way called quantum cryptography to keep information safe. This makes it very hard for someone to intercept and read our messages.

One of the well-known ways to use quantum cryptography is something called Quantum Key Distribution. This lets two people create a code that only they can understand. We know this code is secure because it is based on science. This paper is going to look at quantum cryptography. We will explore how it works how we can use it in life and what we can expect from it in the future. Quantum cryptography is an interesting topic and we will learn more, about it, including its theoretical basis, practical implementation and future prospects.

> ***"Unlike classical encryption quantum cryptography is not based on assumptions. It is secured by fundamental laws of physics."***

Technology Overview

People came up with the E91 protocol, which uses something called quantum entanglement to make it even safer. Over time people have thought of new ways to do this like using decoy states or making it so that the devices used to measure the quantum states do not affect the security of quantum cryptography, which is also known as quantum key distribution or QKD. They have also come up with a way to do it with variables, which is another type of quantum cryptography.

People have also made a lot of progress in testing quantum cryptography. They have been able to use it to send messages over long distances like through optical fibers or even through space using satellites. Some of these tests have been able to send messages over one thousand kilometers, which's a long way. Now people are working on making cryptography work with the systems we already have for communicating. At the time people are working on something called post-quantum cryptography, which is, like a backup plan.

Qubits: The Building Blocks of Quantum Computing

A qubit, which is a bit is the smallest thing that can hold quantum information. It is different from the bits we use in computers, which can only be a 0 or a 1. Qubits can be both 0 and 1 at the time, which is cool. This special thing about qubits lets quantum computers look at a lot of possibilities at once. Here is what I mean:

1 qubit=2 states

2 qubits=4 different states

If you have n qubits they can be in 2 to the power of n states. We can make qubits using different things like Superconducting circuits, ions, Photons and electrons. But qubits are easy to mess up so we have to keep them very cold and quiet to make them work right. Quantum computers need conditions to work properly which is why qubits are so sensitive to what is, around them. Qubits and quantum computers are still interesting even if they can be hard to work with.

Quantum Entanglement

Quantum entanglement is interesting. It happens when two or more qubits get connected in such a way that what happens to one qubit instantly affects the other no matter how apart they are. Albert Einstein said this is like "spooky action at a distance". He thought it was weird.

Key Characteristics:

- Entangled qubits have connected states
- If you measure one qubit it instantly changes the other
- This helps make quantum computations better

Quantum entanglement is important, for quantum algorithms. This is because it lets many qubits work together as one system than each one working alone. Quantum entanglement makes this possible.

IBM Quantum Computing Systems

IBM is a company that's good at making quantum computers. They are making processors that use something called superconducting qubits. IBM Quantum is making computers that people can use over the internet, they are making processors with a lot of qubits like tens or even over 100 and they are trying to figure out how to fix mistakes in computers and make them bigger

IBM has shown that they can make a lot of qubits work together in their quantum processors. For example: A system with 27 qubits was able to get all the qubits working together and a processor with 65 qubits was able to do some complicated things with the qubits. IBM Quantum has come up with some ideas recently like dynamic circuits. These circuits make it easier to get qubits that're far apart to work together and do complicated math problems more quickly. IBM Quantum is still working on these things. They are getting better at making quantum computers all the time. IBM Quantum and their quantum computers are important, for the future of computing.

Theoretical Foundations

Quantum cryptography is based on an important idea from quantum mechanics. Quantum cryptography is based on key principles of quantum mechanics. There is superposition, which's when a quantum system can be in many states, at the same time. Quantum cryptography is based on the Heisenberg Uncertainty Principle, which says that when we measure a system, we change its state. These principles of quantum mechanics including superposition and entanglement and the Heisenberg Uncertainty Principle and the No-Cloning Theorem make sure that if someone tries to listen in on a communication channel, they will introduce disturbances that we can detect.

Methodology

This research uses a mixed-method approach that combines analysis, simulation and experimental review.

Theoretical Analysis

The study starts with a mathematical formulation of quantum cryptographic protocols, particularly BB84 and E91.

Simulation

We do simulations to see how QKD protocols work under conditions including: Channel noise, Photon loss, eavesdropping attacks, such as intercept-resend and photon-number splitting

Experimental Review

This includes fiber-optic QKD systems, satellite-based communication and integrated photonic devices.

Performance Metrics

We use metrics to measure performance, including Key generation rate, Quantum bit error rate, which is also called QBER, Security level and Transmission distance. We want to see how well quantum cryptographic protocols, like BB84 and E91 work, in these areas.

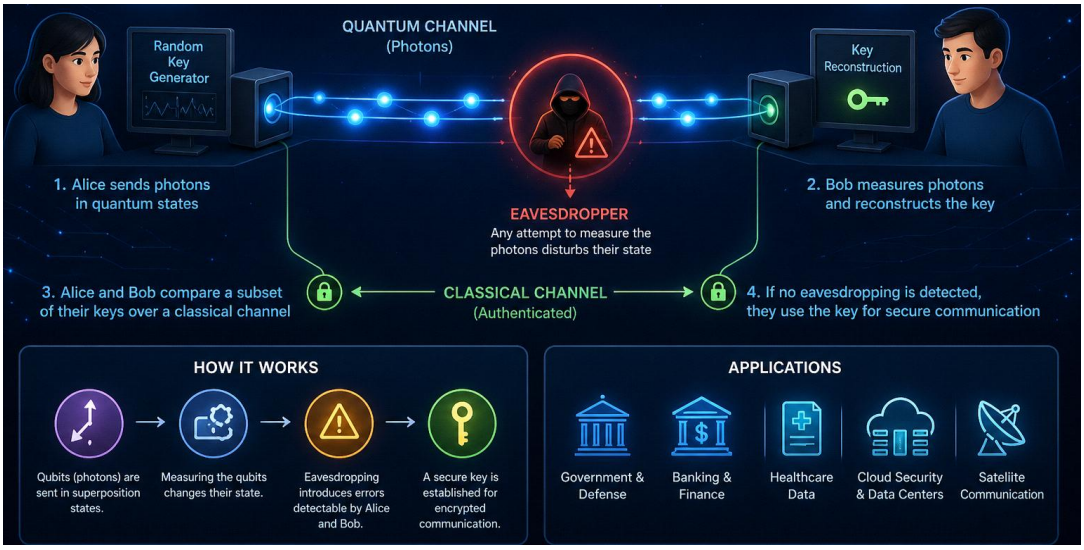

Figure 1: Overview of Quantum Cryptography principles and QKD *Credit: Research Gate*

Key Findings & Impact

Quantum Key Distribution Protocols

1. **BB84 Protocol**

The BB84 protocol uses particles that are polarized to send information. Alice sends these particles in different ways. She chooses how to send them by chance. Bob measures them in his way also chosen by chance. After sending they talk on a channel to see if they used the same way.

2. **E91 Protocol**

The E91 protocol uses pairs of particles that are connected. This connection makes it secure, based on a theorem, by Bell. If someone tries to listen they will be caught.

3. **Decoy-State Protocols**

These protocols make it more secure. They add information to detect when someone tries to steal by splitting light particles.

Applications

Quantum cryptography is really useful in areas like:

- Secure communication in government and military sectors
- Financial transactions and banking systems

- Keeping healthcare data safe
- Cloud security and data centres

Quantum cryptography helps keep things secure, in government and military sectors. It is also used for transactions and banking systems. Additionally quantum cryptography is used for security and data centres.

Challenges and Limitations

Quantum cryptography is really good at keeping things secure. It has some big problems. One of the problems with quantum cryptography is that it is very expensive to set up because it needs special equipment and infrastructure that costs a lot of money to build and take care of. Quantum cryptography also has a problem with how it can send information because it can only send it a short distance, which means it is not very useful for big networks. The system is also very sensitive to things like noise and changes in the environment, which can make it hard to send information accurately and reliably. Quantum cryptography systems are also hard to connect to the systems we already have which causes problems that need to be fixed before we can use cryptography on a big scale. Quantum cryptography has a lot of potential. These problems, with quantum cryptography need to be solved.

What's Next?

Quantum cryptography is something that people are going to keep studying in the future. They want to make it better so it can be used by people. One thing that would really help is if they could make repeaters. These repeaters can help send messages over long distances. They do this by keeping the quantum signals strong.

People are also trying to figure out how to use cryptography with other technologies like 5G. This will make it more useful, in the real world. Another thing that people are working on is making quantum devices smaller. They want to make them easier to use and more efficient. Quantum cryptography can also be used with types of security methods. This will make it even safer.

As people learn more about quantum computing and photonics quantum cryptography will get better. It will be used by more people, and it will be safer and more efficient. Quantum cryptography is going to be used in different industries, and it will be very important. Quantum cryptography will really change the way we send messages.

Conclusion

Quantum cryptography is a change; in the way we keep our messages safe. This means that it does not rely on computers to keep our messages safe. Quantum cryptography is very secure. There are still some problems to solve. People are working on it and making new discoveries. As quantum technology gets better quantum cryptography will become an important part of how we send messages in the future. It will be a key part of future communication systems.

About the Author

Mohtashim Tahir is a Data Automation Specialist and Full Stack Web Engineer based in Faisalabad, Pakistan, and is currently pursuing a bachelor's degree in information technology. His professional work focuses on the development of scalable, data-driven applications, while his research interests include data analytics, artificial intelligence, and innovative digital solutions for real-world challenges. They can be reached at mohtashimtahir999@gmail.com

Keywords: Quantum Cryptography; Quantum Key Distribution (QKD); Cybersecurity; Quantum Computing; Data Security; BB84 Protocol; E91 Protocol; Quantum Entanglement; Secure Communication; Encryption

References

1. Bennett, C. H. And Brassard, G. (1984). Quantum cryptography: key distribution and coin tossing. *Proceedings of IEEE International Conference.* https://www.scirp.org/reference/referencespapers?referenceid=3305086.
2. Bennett, C. H., Brassard, G. And Breidbart, S. (2014). *Quantum cryptography II: How to reuse a one-time pad safely even if P=NP*. Natural Computing. https://doi.org/10.1007/s11047-014-9453-6.
3. Ekert, A. K. (1991). *Quantum cryptography based on Bell's theorem*. Physical Review Letters. https://doi.org/10.1103/PhysRevLett.67.661.
4. Scarani, V., Bechmann-Pasquinucci, H. Cerf, N. J. And others. (2009). *The security of quantum key distribution.* Reviews of Modern Physics. https://doi.org/10.1103/RevModPhys.81.1301.
5. Gisin, N., Ribordy, G., Tittel, W. And Zbinden, H. (2002). *Quantum cryptography*. Reviews of Modern Physics https://doi.org/10.1103/RevModPhys.74.145.
6. Brassard, G. (1992). *Quantum cryptography: A information security perspective*. Scientific American.
7. Lo, H. K., Curty, M. And Tamaki, K. (2014). *Secure key distribution*. Nature Photonics. https://doi.org/10.1038/nphoton.2014.149.
8. Pirandola, S., Andersen, U. L., Banchi, L. And others. (2020). *Advances in cryptography. Advances in Optics and Photonics*. https://doi.org/10.1364/AOP.361502.
9. Shor, P. W. (1994). *Algorithms for computation: Discrete logarithms and factoring*. IEEE. https://doi.org/10.1109/SFCS.1994.365700.
10. Wiesner, S. (1983). *Conjugate coding*. ACM SIGACT News.
11. Deachapunya, S., Chiangga, S. And Weinfurter, H. (2018). *Experimental quantum cryptography based on BB84 protocol*. https://li01.tci-thaijo.org/index.php/cast/article/view/153119.
12. Branciard, C., Gisin, N., Kraus, B. And Scarani, V. (2005). *Security of cryptography protocols.* https://doi.org/10.1103/PhysRevA.72.032301.
13. Lydersen, L. And Skaar, J. (2008). *Security of key distribution with detector flaws*. https://arxiv.org/abs/0807.0767.
14. Marøy, Ø., Lydersen, L. And Skaar, J. (2009). *Quantum key distribution with imperfections*. https://arxiv.org/abs/0903.3525.
15. Curty, M., Ma, X., Lo, H. K. And Lütkenhaus, N. (2010). *Passive sources for QKD*. https://arxiv.org/abs/1009.3830.
16. Pereira, M., Currás-Lorenzo, G. And others. (2022). *Modified BB84 quantum key distribution protocol.* https://arxiv.org/abs/2210.11754.
17. Hughes, R. J., Morgan, G. L. And Peterson, C. G. (2000). *Quantum key distribution over fibers*. https://doi.org/10.1002/(SICI)1099-1131.
18. Elliott, C. (2002). *Building the quantum network*. New Journal of Physics. https://doi.org/10.1088/1367-2630/4/1/346.
19. Sasaki, M. And others. (2011). *Field test of key distribution network.* https://doi.org/10.1364/OE.19.010387.
20. Yin, J. And others. (2017). *Satellite-based entanglement distribution*. Science. https://doi.org/10.1126/science.aan3211.
21. Chen, Y. A. And others. (2021). *Integrated space-to-ground quantum communication network*. Nature. https://doi.org/10.1038/s41586-020-03093-8.
22. Pirandola, S. (2019). *End-to-end capacities of communication networks*. https://doi.org/10.1038/s41467-019-09873-9.
23. Bennett, C. H. And Brassard, G. (1985). *An update on cryptography*. Lecture Notes, in Computer Science. https://doi.org/10.1007/3-540-39568-7_39.
24. Brunner, N. And others. (2014). *Bell nonlocality*. Reviews of Modern Physics. https://doi.org/10.1103/RevModPhys.86.419.
25. Renner, R. (2008). *Security of key distribution*. International Journal of Quantum Information. https://doi.org/10.1142/S0219749908003256.