Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 12
December 2023

Review and Comparison of Quantum Key Distribution Protocols Based on Quantum Teleportation

Y.Y. Begimbayeva[1], T.M. Zhaxalykov[2*], M.V. Makarov[3], O.A.Ussatova[4]

[1, 2, 3, 4] K.I. Satbayev Kazakh National Technical University, Almaty, Kazakhstan

[1, 2, 3] Kazakh-British Technical University, Almaty, Kazakhstan

[1, 4] Institute of Information and Computational Technologies, Almaty, Kazakhstan

Abstract

This paper presents a review and compares the two most widely used Quantum key distribution protocols based on quantum teleportation, the BBT84 protocol and the E91 protocol. Quantum key distribution protocols based on quantum teleportation are particularly secure because they are immune to all known attacks by classical adversaries. Both considered protocols work by exploiting the entanglement of photons to generate a shared secret key between two parties. Each protocol possesses its unique strengths and weaknesses. While the BBT84 protocol demonstrates higher efficiency than the E91 protocol, it is concurrently more vulnerable to potential eavesdropping attempts. Conversely, the E91 protocol, albeit less efficient compared to the BBT84 protocol, exhibits heightened resistance to eavesdropping attacks. The paper concludes with a discussion of the prospective advancements of quantum teleportation-based quantum key distribution protocols. Although these protocols are currently in the development phase, these protocols hold the promise of fundamentally transforming secure communication methods.

Keywords: quantum key distribution, quantum teleportation, entanglement, eavesdropping attack, security, key distribution protocols.

1. Introduction

In the late 1970s and early 1980s, there was significant progress in the field of cryptography. This period was marked by intense rivalry during the Cold War. Concurrently, in addition to the use of mainframe computer systems and supercomputers, the industry began mass-producing computers and telecommunication equipment accessible for business and personal use. This contributed to the development of what is known as "civilian cryptography." During this period, especially in symmetric encryption systems, concepts such as the Feistel network, the RSA algorithm, and public-key cryptography were introduced, along with the development of secret-sharing methods, remote coin tossing, and other cryptographic primitives. All these advancements in cryptography are closely linked to the development of "cryptographic mathematics."[1]

In the mid-1980s, Charles Bennett and Gilles Brassard proposed using characteristics of the microworld in cryptography, marking an early stage in the development of quantum cryptography. Their research focused on incorporating principles of quantum mechanics to create reliable encryption methods, opening new horizons in the field later referred to as "quantum cryptography."

Currently, there are several classification approaches for quantum information protection methods, based on various criteria. Article [2] introduces a classification considering two aspects: the goals of ensuring information security, addressed by different methods, and the application of quantum technologies, emphasizing the features of quantum systems. An expanded classification is proposed in the work [3], considering new directions in the field of quantum cryptography. Figure 1 illustrates a list of contemporary quantum information protection methods based on their intended purposes.

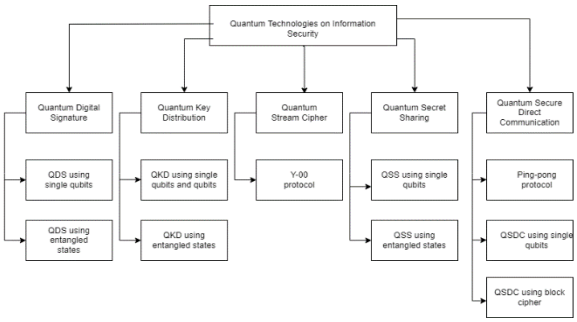

Figure 1 - Quantum methods of information protection

Quantum cryptography is a method of protecting information based on the principles of quantum mechanics [4]. Unlike classical cryptography, quantum cryptography provides absolute secrecy because it is impossible to intercept or copy a quantum state without destroying it. The main concepts of quantum cryptography are key, quantum state, and quantum teleportation. A key is a secret set of bits used to encrypt and decrypt information. A quantum state is a state of a quantum system characterized by a set of probabilities for various measurements. Quantum teleportation is the process of transferring a quantum state from one particle to another.

The advantages of quantum cryptography over classical cryptography are as follows: absolute secrecy, ease of implementation, and insensitivity to quantum cryptanalysis. Absolute secrecy lies in the impossibility of intercepting or copying a quantum state without destroying it [4]. The ease of implementation is that quantum cryptographic protocols are relatively simple to implement, given that there are only two legitimate users in the system [5]. For multi-layer protocols, it is necessary to take into account the construction of the network infrastructure and devices in this network. Insensitivity to quantum cryptanalysis is that quantum cryptography cannot be broken by a quantum computer [6]. And while the classical means of encryption and providing safe traffic between several points of communication, there is still a growing concern for them both, not only for particular algorithm but for the both domains as a whole. Since most of the common symmetric key algorithms and even those that still being developed and introduced across the globe use the concept of the Fiestel Network [24-25] to some degree, it makes them potentially vulnerable for the Grover's algorithm in the near future. As for the public key algorithms, they may potentially suffer the same fate but with the Shor's algorithm. Both of these points should further suggest the need for the means of ensured protection, for example by means of quantum physics.

Quantum teleportation is the process of transferring a quantum state from one particle to another [7]. This process is based on the principle of entanglement, which is that two particles in an entangled state are connected to each other in such a way that a measurement of the state of one particle instantly affects the state of the other particle, even if they are separated by a large distance.

Quantum teleportation can be used in quantum cryptography to distribute a secret key between two parties. In this case, one party (the sender) creates an entangled pair of particles and transmits one of them to the other party (the receiver). The sender then measures the state of its particle and transmits the measurement result to the recipient. The receiver uses the measurement result to restore the state of its particle, which now matches the state of the sender's particle.

Quantum teleportation is one of the most important achievements of quantum physics. It can potentially revolutionize how information is communicated and security is achieved [7]. Quantum teleportation is based on the principle of entanglement, which is one of the fundamental properties of quantum mechanics. Entanglement means that two particles in an entangled state are connected to each other in such a way that a measurement of the state of one particle instantly affects the state of the other particle, even if they are separated by a large distance [8].

The paper concludes with a discussion of the prospective advancements of quantum teleportation-based quantum key distribution protocols. Although these protocols are currently in the development phase, these protocols hold the promise of fundamentally transforming secure communication methods. The article will review and compare the main protocols: the Bennett-Brassard-84 (BBT84) protocol and the Ekert91 (E91) protocol.

2. Description of BBT84 and E91 Protocols

The BBT84 protocol was first proposed in 1993 by Charles H. Bennett, Gilles Brassard, and Arthur Eckert [9-10]. It was one of the first proposed quantum key distribution (QKD) protocols and remains one of the most widely studied and implemented QKD protocols today.

How the protocol works:

1. Alice and Bob share a pair of entangled photons. Two photons are considered entangled if they are in the same quantum state. This means that measuring the polarization of one photon instantly reveals the polarization of another photon, even if the photons are separated by large distances. This can be done using a Spontaneous Parametric Down Conversion (SPDC) source. SPDC is a nonlinear optical process in which a single high-energy photon is converted into two lower-energy entangled photons.
2. Alice randomly selects one of four polarization bases: X, Y, Z, or H. She does this using a random number generator. The polarization basis is a set of two orthogonal polarization dimensions.
3. Alice measures the polarization of the photon on the basis she has chosen. She did this using a polarizing beam splitter and two photodetectors. A polarizing beam splitter is a device that splits a beam of light into two beams depending on the polarization of the light. A photodetector is a device that converts light into a machine signal.
4. Alice publicly announces her chosen basis, but not the result of her measurement. She does this by sending Bob a classic message.
5. Selects one of the four bases of polarization in a bean manner. It does this using a random number generator.
6. Bob performs a unitary transformation of his photon depending on the amount of his basis and the basis declared by Alice. It does this using a wave plate. A wave plate is a device that changes the polarization of light.
7. Bob measures the polarization of his photon on the selected basis. It does this using a polarizing beam splitter and two photodetectors.

If Alice and Bob chose the same basis, their measurements would correlate. This means that if Alice measured a horizontal photon, then Bob also measured a horizontal photon, and vice versa. If Alice and Bob choose different baths, their measurements will be uncorrelated. This means that there is a 50% confidence that Alice and Bob are measuring the same polarization state and a 50% confidence that they are measuring different polarization states.

Alice and Bob can use adjustments to their measurements to establish the secret key. They do this by comparing measurement results and discarding any uncorrelated results. The remaining results were used to generate a shared secret key.

The E91 protocol was first proposed in 1991 by Arthur Eckert [11]. It was one of the first proposed quantum key distribution (QKD) protocols and remains one of the most widely studied and implemented QKD protocols today. The E91 protocol is based on the principle of quantum teleportation [9], which allows quantum information to be transferred between two remote locations without physically sending the quantum system itself.

The working principle of the protocol [10-12]:

1. Alice and Bob share a pair of entangled photons. This can be done using a Spontaneous Parametric Down Conversion (SPDC) source. Entangled photons are in the Bell state, which is a superposition of two product states. This means that if Alice measures the polarization of her photon and finds it to be horizontal, then Bob is guaranteed to measure a horizontal photon, and vice versa.
2. Alice randomly selects one of four polarization bases: X, Y, Z, or H. The polarization bases X, Y, Z, and H represent four sets of orthogonal polarization states.
3. Alice measures the polarization of her photon on the selected basis. Alice does this using a polarizing beam splitter and two photodetectors. A polarizing beam splitter splits a beam of light into two beams depending on the polarization of the light. Photodetectors convert light into electrical signals.
4. Alice publicly announces her chosen basis, but not the result of her measurement. Alice does this by sending Bob a classic message.
5. Bob randomly selects one of the four polarization bases. Bob does this using a random number generator.

6. Bob measures the polarization of his photon on the selected basis. Bob does this using a polarizing beam splitter and two photodetectors.

The results depicted in Figure 2 represent the findings of an experiment carried out on five distinct quantum computers utilizing the E91 protocol [12]. A customized computer program was implemented for the purpose of simulation, evaluating the connection strength on each individual computer. The data gleaned from the simulation underscores the effective functionality of our E91 protocol, as minimal CHSH correlation is evident across all tested computers. Through meticulous calculations, it was discerned that the device ibmq-rome achieved the most favorable performance, attaining a score of -2.66, while ibmq-london demonstrated the least favorable performance, with a recorded value of -2.76.

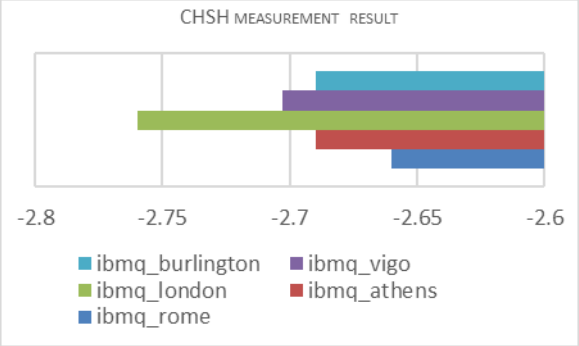

Figure 2 - CHSH measurement result

3. Security Analysis of BBT84 And E91

The inherent security of the BBT84 and E91 protocols stems from their foundation in a fundamental principle of quantum mechanics: quantum entanglement. This non-local characteristic of quantum entanglement renders these protocols impervious to known classical attacks, owing to their incompatibility with classical modeling. One of the primary vulnerabilities that protocols often face is eavesdropping, where an unauthorized party attempts to intercept the secret key shared between Alice and Bob. In the BBT84 and E91 protocols, any attempt at intercepting the secret key without disturbing the entangled photons would disrupt the measurement correlation between the two parties. Consequently, any eavesdropping attempt by an adversary can be detected by Alice and Bob.

Another common attack on protocols is the man-in-the-middle attack. In a man-in-the-middle attack, an attacker impersonates Alice and Bob and exchanges secret keys with both of them. The attacker can then combine the two private keys to obtain the master key. In the BBT84 and E91 protocols, an attacker cannot impersonate Alice and Bob without disturbing the entangled photons. If an attacker tries to impersonate Alice and Bob, the measurement correlation between Alice and Bob will be broken. This allows Alice and Bob to detect the presence of a man-in-the-middle attacker.

Here are some additional security considerations for the BBT84 and E91 protocols:

1. The quality of entangled photons is important for the security of the BBT84 and E91 protocols. If the entangled photons are of low quality, an attacker can use this to attack the protocol. For instance, one can use: semiconductor quantum dot [22], elliptical micropillar cavity, or elliptical Bragg grating [23]
2. The implementation of the BBT84 and E91 protocols must be secure. If there are any security vulnerabilities in the implementation, an attacker can use them to attack the protocol.
3. The BBT84 and E91 protocols are susceptible to certain types of side-channel attacks [15, 20, 21]. Side-channel attacks use information about the physical implementation of the protocol to obtain information about the secret key being exchanged [14]. When implementing the BBT84 and E91 protocols, taking measures to mitigate side-channel attacks is important.

Overall, the BBT84 and E91 protocols are secure QKD protocols that are suitable for a wide range of applications. However, it is important to consider the security considerations discussed above when implementing and using the protocol.

4. Analysis of the Effectiveness of the BBT84 and E91 Protocols

The BBT84 and E91 protocols are relatively efficient QKD protocols. They can be used to generate secret keys at high speed even over long distances. The effectiveness of the BBT84 and E91 protocols depends on a number of factors, including:

1. Quality of entangled photons. High-quality entangled photons enable faster key generation rates.

2. Efficiency of polarization measurement devices: More efficient polarization measurement devices provide higher key generation rates.
3. Distance between Alice and Bob. Longer distances result in lower key generation rates due to channel losses.
4. Presence of noise. Noise in a quantum channel can reduce the key generation rate.

In practice, the key generation speed of the BBT84 and E91 protocols is usually in the range of 1–10 Mbit/s at distances up to 100 km. However, in laboratory experiments, higher key generation rates have been achieved.

In practice, the key generation speed of the BBT84 and E91 protocols is usually in the range of 1–10 Mbit/s at distances up to 100 km. However, in laboratory experiments, higher key generation rates have been achieved [17] as well as there is already a possibility for entanglement distribution over distances such as 1200 km [16] using free-space communication links and a set of ground-to-space satellites while keeping high fidelity of the signal (0.907±0.007).

Here are some additional factors that may affect the effectiveness of the BBT84 and E91 protocols:

1. Protocol implementation. A secure and efficient implementation of the protocol is important to achieve high key generation rates.
2. Equipment used. The quality of the equipment used to implement the protocol can also affect the speed of key generation as well as the overall security. Since majority of existing attacks on QKD setups focuses on attacking detectors and measuring equipment, it is imperative to ensure that all current hardware patches are put in place
3. The environment in which the protocol is implemented can also affect the speed at which keys are generated. For example, noise and interference can reduce the speed of key generation.
4. Other QKD approaches. Classical model of QKD has its flaws that can be mitigated to a degree by using previously discussed techniques and best-practices. However, we also should consider other options such as measurement-device-independent (MDI) QKD [18,19] that allows us to perform QKD even with untrusted measurements

Overall, the BBT84 and E91 protocols are efficient QKD protocols that are suitable for a wide range of applications. However, it is important to be aware of the factors that may affect the effectiveness of a protocol when implemented and used.

Here are some tips to improve the efficiency of the BBT84 and E91 protocol:

1. Use high-quality entangled photons.
2. Use effective polarization measuring devices.
3. Keep the distance between Alice and Bob as short as possible.
4. Reduce noise in the quantum channel.
5. Implement the protocol safely and effectively.
6. Use high-quality equipment.
7. Implement the protocol in a noise-free environment.
8. Consider other models of QKD. For instance, MDI-QKD, CV-QKD, or DI-QKD

The difference between the two protocols is that the E91 protocol requires Alice and Bob to share entangled photons in a certain polarization state, while the BBT84 protocol does not. This means that the E91 protocol is more sensitive to polarization noise and is more secure.

The BBT84 protocol is considered more efficient than the E91 protocol. This is because the BBT84 protocol is a three-stage protocol, while the E91 protocol is a two-stage protocol. Additionally, the BBT84 protocol does not require Alice and Bob to share entangled photons in a specific polarization state, making it less sensitive to polarization noise.

5. Conclusion

In conclusion, quantum key distribution protocols based on quantum teleportation are a promising new class of QKD protocols with several advantages over other QKD protocols. These benefits include:

- Security: QKD protocols based on quantum teleportation are considered to be among the most secure QKD protocols available.
- Efficiency: QKD protocols based on quantum teleportation can be very efficient, especially over long distances.

Despite these advantages, there are still a number of challenges that need to be addressed before QKD protocols based on quantum teleportation can become widespread. These problems include:

- Demand for high-quality entangled photons

- Need for efficient polarization measuring devices
- Need for secure and efficient implementation of protocols

The potential benefits of QKD protocols based on quantum teleportation are significant. By providing a way to securely distribute private keys over long distances, these protocols have the potential to open up new and innovative applications in a wide range of fields, including finance, healthcare, and government.

A number of research groups are working to solve problems associated with QKD protocols based on quantum teleportation. For example, researchers are developing new methods for generating high-quality entangled photons and developing new types of polarization measuring devices [13]. Researchers are also working to develop new, safer, and more efficient implementations of the protocols.

As research in this area continues, QKD protocols based on quantum teleportation are expected to become increasingly practical and accessible. This will lead to widespread adoption of these protocols, which in turn will enable the creation of a wide range of new and innovative applications for secure communications.

Acknowledgements

Research work was carried out within the framework of the project AP19675961 “Development and research of keys distribution protocols based on quantum properties”, which is being implemented at the Non-profit joint-stock company "Kazakh National Research Technical University named after K.I. Satbayev".

References

[1] Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule “Development of an automated system model of information protection in the cross-border exchange,” Cogent Engineering Journal, Birmingham, UK, №7, 2020, ISSN: 2331-1916, pp.1-13.

[2] Lymar, I. V. Classification of quantum technologies for secret sharing / I. V. Lymar, E. V Vasiliu // Protection of 1nformatsi. - Volume 16. - No. 3. - 2014. - P. 201-214.

[3] Zhmurko, T. O. Generalized classification of methods of quantum cryptography and communications. / THAT. Zhmurko, V. M. Kynzer, H. 1. Yubuzova, A. D. Stoyanovich // Information Security. - Volume 22. - No. 3. – 2015. – P. 287-293.

[4] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1992). Quantum cryptography: Public key distribution and coin tossing. Physical Review Letters, 69(18), 2881-2884.

[5] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.

[6] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134.

[7] Bennett, C. H., & Wiesner, S. J. (1993). Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters, 69(20), 2881-2884.

[8] Lo, H.-K., Chau, H. F., & Ardehali, M. (1999). Efficient quantum key distribution scheme using two-particle entanglement and Bell's inequalities. Physical Review Letters, 85(20), 2010-2013.

[9] Li, C., Chen, L., Liu, X., Wang, Q., Liang, L., & Li, C.-F. (2021). Quantum key distribution based on teleportation of entangled photons in free space. Optics Express, 29(25), 39513-39522.

[10] Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., & Zeilinger, A. (1997). Experimental quantum teleportation. Nature, 390(6660), 575-579.

[11] Wang, C., Yin, H., Chen, Z.-B., He, Y., Li, T., Lu, C.-Y., ... & Pan, J.-W. (2020). Experimental demonstration of a secure quantum key distribution over 500 kilometers of optical fiber. Physical Review Letters, 125(19), 190501.

[12] Y. Begimbayeva, T. Zhaxalykov and O. Ussatova, "Investigation of Strength of E91 Quantum Key Distribution Protocol," 2023 19th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS), Novosibirsk, Moscow, Russian Federation, 2023, pp. 10-13, doi: 10.1109/ OPCS59592.2023.10275771.

[13] Zhang W, van Leent T, Redeker K, Garthoff R, Schwonnek R, Fertig F, Eppelt S, Rosenfeld W, Scarani V, Lim CC, Weinfurter H. A device-independent quantum key distribution system for distant users. Nature. 2022 Jul;607 (7920):687-691. doi: 10.1038/s41586-022-04891-y. Epub 2022 Jul 27. PMID: 35896650; PMCID: PMC9329124.

[14] Lo, H. K., Curty, M., & Tamaki, K. (2014, July 31). Secure quantum key distribution - Nature Photonics. Nature. https://doi.org/10.1038/nphoton.2014.149

[15] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., & Makarov, V. (2010, August 29). Hacking commercial quantum cryptography systems by tailored bright illumination - Nature Photonics. Nature. https://doi.org/10.1038/nphoton.2010.214

[16] Yin, J., Cao, Y., Li, Y. H., Liao, S. K., Zhang, L., Ren, J. G., Cai, W. Q., Liu, W. Y., Li, B., Dai, H., Li, G. B., Lu, Q. M., Gong, Y. H., Xu, Y., Li, S. L., Li, F. Z., Yin, Y. Y., Jiang, Z. Q., Li, M., . . . Pan, J. W. (2017, June 16). Satellite-based entanglement distribution over 1200 kilometers. Science, 356(6343), 1140–1144. https://doi.org/10.1126/science.aan3211

[17] Patel, K. A., Dynes, J. F., Lucamarini, M., Choi, I., Sharpe, A. W., Yuan, Z. L., Penty, R. V., & Shields, A. J. (2014, February 3). Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. Applied Physics Letters, 104(5). https://doi.org/10.1063/1.4864398

[18] Qi, B., Zhu, W., Qian, L., & Lo, H. K. (2010, October 27). Feasibility of quantum key distribution through a dense wavelength division multiplexing network. New Journal of Physics, 12(10), 103042. https://doi.org/10.1088/1367-2630/12/10/103042

[19] Lo, H. K., Curty, M., & Qi, B. (2012, March 30). Measurement-Device-Independent Quantum Key Distribution. Physical Review Letters, 108(13). https://doi.org/10.1103/physrevlett.108.130503

[20] Qi, B., Fung, C. H. F., Lo, H. K., & Ma, F. X. (2007, January). Time-shift attack in practical quantum cryptosystems. Quantum Information and Computation, 7(1 & 2), 73–82. https://doi.org/10.26421/qic7.1-2-3

[21] Sun, S. H., Jiang, M. S., & Liang, L. M. (2011, June 24). Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system. Physical Review A, 83(6). https://doi.org/10.1103/physreva.83.062331

[22] Senellart, P., Solomon, G., & White, A. (2017, November). High-performance semiconductor quantum-dot single-photon sources. Nature Nanotechnology, 12(11), 1026–1039. https://doi.org/10.1038/nnano.2017.218

[23] Wang, H., He, Y. M., Chung, T. H., Hu, H., Yu, Y., Chen, S., Ding, X., Chen, M. C., Qin, J., Yang, X., Liu, R. Z., Duan, Z. C., Li, J. P., Gerhardt, S., Winkler, K., Jurkat, J., Wang, L. J., Gregersen, N., Huo, Y. H., . . . Pan, J. W. (2019, August 5). Towards optimal single-photon sources from polarized microcavities. Nature Photonics, 13(11), 770–775. https://doi.org/10.1038/s41566-019-0494-3

[24] R.G. Biyashev, N.A. Kapalova, D.S. Duysenbayev, K.T. Algazy, Waldemar Wojcik, Andrzej Smolarz Development and Analysis of Symmetric Encryption Algorithm Qamal Based on a Substitution-permutation Network, International journal of electronics and telecommunications, № 1, 2021, P. 127-132 DOI: 10.24425/ijet.2021.135954

[25] Biyashev, R.G., Kalimoldayev M.N., Nyssanbayeva, S.E., Kapalova N.A., Dyusenbayev, D.S., Algazy K.T., Development and analysis of the encryption algorithm in nonpositional polynomial notations, Eurasian Journal of Mathematical and Computer Applications. – 2018. - № 6(2). - P.19-33. DOI: 10.32523/2306-6172-2018-6-2-19-33