Advancements in Applications of Quantum Entanglement

Yue Yu*
Teensen Genesis School, Nanchang, Jiangxi 330000, China.
*Corresponding author e-mail: yy6688@txyzedu.com

Abstract. Quantum entanglement, an unknown “spooky action” that confused scientists like Einstein, has become one of the research hotspots in quantum mechanics. Based on the technique, applications distributed among diverse fields have appeared, e.g., cryptography, computer science, distant communication, etc, which has attracted interest from researchers in varied fields. This article reviews the basics of manifestations of quantum entanglement, namely quantum key distribution, quantum computation, and quantum teleportation. An overview of milestones is presented, e.g., Bennett-Brassard 1984 protocol, entanglement-based quantum computers, Shor’s and Grover’s algorithm as well as the process of transporting quantum states at an unprecedented speed. Moreover, the implementations of quantum entanglement are demonstrated, evolving these technologies to higher levels. Finally, a brief conclusion and expectations for future developments on entanglement are given.

1. Introduction
During the time when quantum mechanics was developing into the correct description of the world, the intriguing phenomenon of quantum entanglement was discovered. At first Einstein, Podolsky, and Rosen wrote a joint paper in 1935 about this newest finding. They produced a thought experiment in an attempt to show that the quantum theory is yet complete, named the Einstein-Podolsky-Rosen (EPR) paradox [1]. Schrodinger wrote another paper shortly after, in which he discussed the concept of quantum entanglement and stressed the importance of it [2], but like Einstein he found it difficult to understand why entanglement seemed to violate the theory of relativity. It’s Bell who found a loophole in EPR’s argument in 1964 [3]. He formalized their idea in terms of the local hidden variable model (LHVM), and stated that LHVM has to follow the assumptions of realism, locality, and free will. Then he showed that quantum entanglement obviously violates these assumptions, which means that it does not follow classical formalisms, but only follows quantum mechanics. Then quantum entanglement was established to be one of the foundations for applications of quantum mechanics. The important applications of entanglement in technology weren’t proposed until the 1990s. After the discovery of quantum cryptography, quantum computation, quantum teleportation and other fields, a new field with quantum entanglement as the main concept was formed, namely quantum information.

In 1984, Bennett and Brassard found that they could utilize the special quantum features of particles to perform secure communication, and then developed the famous Bennett-Brassard 1984 protocol [4], which could distribute quantum keys in a way that users are able to detect eavesdropping. Later in 1991, Ekert proposed the use of quantum entanglement in BB84, which significantly enhanced its security [5]. The real problem has always been the implementation of quantum key distribution (QKD), as until now researchers are trying to find an effective way to put QKD into action. Another great finding, quantum computation, started as an idea in Richard P. Feynman’s paper [6] from 1982. He proposed that by using quantum mechanics in computers, calculations could be more efficient than on classical computers.
Besides, Deutsch gave a detailed model of quantum computation for the first time [7, 8]. The utilization of quantum entanglement in these devices was realized in later years [9]. One of the most fascinating manifestations of quantum feature of non-locality is quantum teleportation. First proposed by Bennett in 1993 [10], experimental adaptations continue to develop over the years. Notably in 2017, a group of Chinese scientists attempted a teleportation at distance of 1,400 km from a ground station to a satellite named Micius. Later in the same year, a successful BB84 communication was established between ground stations in China and Austria over the satellite Micius [11, 12].

This review summarizes the main applications of quantum entanglement, offering a more intuitive way to exploit entanglement in various ways. Firstly, the basics of quantum key distribution and the advancements with entanglement are introduced. Subsequently, the hot topics of quantum computation are discussed, and the architecture of the computer and quantum algorithms are explained in detail. Finally, a full teleportation of quantum states, including concerns and future developments, will be explained.

2. Application of quantum entanglement

Quantum entanglement is already a well-known and widely used theorem in quantum mechanics. It is applied to many different fields extended out of quantum mechanics. Figure 1 (collected from Ref. [13]) summarizes fundamental insights and technological applications for different numbers of involved particles and different local dimensionalities.

![Figure 1. Applications of quantum mechanics, with different system sizes. N is the number of involved particles, and d is the local dimension [13].](image)

2.1. Quantum key distribution

QKD is used to apply the laws of the quantum world to information security. Non-cloning theorem in quantum mechanics declares that a perfect copy of an unknown quantum state cannot be cloned [14, 15]. If Alice distributes a quantum key, another person cannot have a perfect copy of this key anymore, therefore not able to take away information. Meanwhile, by looking at the key, disturbance is introduced to the quantum state, and Alice and Bob could notice and use another quantum key instead. Another major advantage of QKD is that there will be no record for eavesdropper to have after a QKD session is over, since the communication is through quantum states. Eavesdropping has to be done during the session, otherwise the communication will be secure forever. This is significantly better than classical key distribution [4, 16, 17].

2.1.1. Bennett-Brassard 1984 protocol. The Bennett-Brassard 1984 protocol (BB84) is one of the most famous quantum key distribution schemes [1]. There was no quantum entanglement, only the direct use
of quantum communication. BB84 uses measurement in two different orthogonal bases. It utilizes photon polarization, one of which is rectilinear with vertical polarization at 0° and horizontal polarization at 90°, and the other is diagonal with vertical polarization at 45° and horizontal at 135°. Then values of 0 and 1 can be assigned to these two different polarizations [4, 17].

2.1.2. Advancement with quantum entanglement. Artur Ekert proposed a variant of QKD using quantum entanglement later in 1991 [5]. Two entangled particles will be sent to both Alice and Bob, and they can measure values similar to BB84. If an eavesdropper tries to measure the particles’ information, the entanglement state between two particles will collapse. If the eavesdropper gets the values that Alice and Bob obtained in their measurement, it means that the quantum states have collapsed and therefore will not violate Bell's inequality. If the Bell inequalities are violated and the quantum states are not altered before Alice and Bob measure the particles, they will know that no eavesdropping has happened [18, 19].

2.2. Quantum computation
Quantum Computation is the application of quantum mechanics, especially quantum entanglement, in computation devices. There are two main research directions around quantum computation, the development in quantum algorithm and the innovation in physical quantum volume.

2.2.1. Entanglement in quantum architecture. In quantum computers, there are two paths to increase the processing speed, one is to increase the amount of qubit. The other is to create larger entangled state, which is the application of entanglement theory. A quantum computer can process much faster than a classical one mainly because of the superposition of qubits. In classical computers, bits can only be assigned to values of 0 or 1, and calculations can be done with a large number of bits. In quantum computers, however, qubits are in quantum states that have probabilities to carry values of 0 and 1 at the same time. Calculations can be done simultaneously as a result and the processing speed can become significantly higher than classical computers.

The addition of knowledge of quantum entanglement can increase the processing speed even more. When two or more particles are in a quantum state, and each particle’s state cannot be separated, there is an entanglement in between. A change in the state of one particle will result in a change in the state of another, no matter how far apart the particles are. Utilizing this fact, quantum computers can use entangled qubits, and multiple calculations can be done on different qubits at the same time. In the past few years, IBM has introduced quantum computers with 20-qubits, 27-qubits, and 63-qubits respectively. In all three cases, entanglement is detected for all neighbouring pairs of qubits, indicating entanglement across the devices. As the ability to entangle qubits is steadily improving, more complex quantum algorithms can be implemented [20].

2.2.2. Quantum algorithm. Quantum algorithms are used to solve problems on quantum computers instead of classical computers. They are written in ways that can only be implemented physically on computers with qubits.

2.2.2.1. Hidden subgroup problem. Shor’s algorithm used for integer factorization is one of the first applications of quantum computers. In the factorization problem, we need to find prime numbers p and q, given an integer N = p x q. Classically, the best way to calculate this runs in time exp(O(log N)1/3(log log N)2/3)) [21, 22]. Shor’s algorithm solves this problem significantly faster, in time O(log N3) [23, 24]. This is due to the fact that Shor’s algorithm reduces the task to a specific mathematical problem called hidden subgroup problem (HSP) [25, 26]. There are other applications of this method, summarized in Table 1 (collected from Ref. [23]).
Table 1. This table lists the problems and matching Cryptosystems that could be expressed as HSP and potentially solved by a quantum algorithm [23, 27-30]

| Problem                | Cryptosystem                  |
|------------------------|-------------------------------|
| Factorization          | RSA                           |
| Discrete log           | Diffie-Hellman, DSA, …         |
| Elliptic curve discrete log | ECDH, ECDSA, …              |
| Principal ideal        | Buchmann-Williams             |
| Shortest lattice vector | NTRU, Ajtai-Dwork, …          |
| Graph isomorphism      | –                             |

2.2.2.2. *Unconstructed search problem*. Unconstructed search problem is one of the most basic problems in computer science. It basically asks when given the ability to evaluate a function $f:\{0, 1\}^n \rightarrow \{0, 1\}$, find $x$ such that $f(x) = 1$, if such an $x$ exists; otherwise, output ‘not found’ [23]. Any classical algorithms have to solve this problem at most with evaluations $N = 2^n$, but Grover wrote a quantum algorithm that can solve this problem with $O = \sqrt{N}$ evaluations at most [31]. It fails with a small but fixed probability, the algorithm is bounded error. This algorithm doesn’t use whatever is inside $f$, instead it takes in $f$ as a whole similar to the use of a black box.

Take an example of circuit satisfiability problem (Circuit SAT), as shown in Figure 2 (collected from Ref. [23]). The problem has AND, OR, and NOT gates which take in $n$ bits and output 1 bit. The task is to find if there exist and input such that the output is 1. Best of classical algorithms run in time $2^n$ in the worst case, but when Grover’s algorithm is used, the runtime is improved to $O(2^{n/2}\text{poly}(n))$. An efficient algorithm for Circuit SAT can be used to solve a huge amount of problems related to electronic circuits [23, 32].

![Figure 2](image-url)  
**Figure 2.** An example of circuit satisfiability problem. The answer should be yes here as an input exist such that the output would be 1 [23].

2.3. *Quantum teleportation*

In the famous quantum teleportation, quantum states can be teleported through space without ever existing in between two places. That is, energy-matter must already exists at the destination, and must be entangled with the transceiver.

There are basically three steps in this process. First, consider a setup in Figure 3(collected from Ref. [33]), where a photon on Alice’s side is in an entangled state with the energy-matter at Bob’s location. Photon pairs are usually used, sent in optic fibres, sometimes ions are used instead [34, 35]. Then, Alice performs Bell-state measurement (BSM) between the entangled photon she has and the photon with quantum information they want to teleport [36, 37]. BSM tells nothing about the quantum state of the teleported photon, but something about the relationship between the two photons on Alice’s side. Usually only part of BSM is realized [38, 39]. The third and final step is for Alice to send the results she gets to Bob through the classical channel, and Bob performs a result-dependent unitary rotation on his photon. That is when the full quantum state of the teleported photon is transferred to Bob’s photon.
However, it is important to note that this process is not faster than the speed of light, since communication through the classical channel is slower than the speed of light.

The main issue with quantum teleportation is BSM. BSM is proved to have no greater efficiency than 50% with linear optics [40], and the length of the optic fibres need to meet an unrealistic standard, within the coherence length of the photons [41, 42]. Therefore, new improvements should be done in these areas to increase the efficiency of quantum teleportation and thus the efficiency of quantum communication.

![Figure 3. A classical setup for quantum teleportation, with Alice as the sender and Bob as the receiver [33].](image)

3. Conclusion
In summary, a review on the main applications of quantum entanglement is presented including the field of quantum cryptography, computation, and transportation. Protocols of quantum key distribution are inspected including the renowned BB84. Besides, the utilization of quantum entanglement are introduced in quantum computers to produce faster processing speed. Subsequently, famous quantum algorithms have been discussed, which could solve problems at a rate that classical algorithm cannot achieve. Lastly, combining the relevant knowledge of quantum entanglement, the almost-instantaneous quantum states teleportation is reviewed. These applications offer guidelines for the development of quantum physics in the future. In the coming decade, successful experiments on these applications worldwide will face great challenges. If these challenges can be met, then the use of quantum entanglement for faster, safer, and more effective communications will bring a giant leap to the world technology.

References
[1] Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete?. Physical review, 47(10), 777.
[2] Schrödinger, E. (1935, October). Discussion of probability relations between separated systems. In Mathematical Proceedings of the Cambridge Philosophical Society (Vol. 31, No. 4, pp. 555-563). Cambridge University Press.
[3] Bell, J. S. (1964). On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3), 195.

[4] Bennett, C. H., & Brassard, G. (1984, December). Quantum cryptography: Public key distribution and con tos5. In *Proceedings of the International Conference on Computers, Systems and Signal Processing* (pp. 175-179).

[5] Ekert, A. K. (1991). Quantum cryptography based on Bell’s theorem. *Physical review letters*, 67(6), 661.

[6] Feynman, R. P. (1982). Simulating physics with computers. *Int. J. Theor. Phys.*, 21(6/7).

[7] Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818), 97-117.

[8] Deutsch, D. E. (1989). Quantum computational networks. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 425(1868), 73-90.

[9] Jozsa, R., & Linden, N. (2003). On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 459(2036), 2011-2032.

[10] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., & Wootters, W. K. (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical review letters*, 70(13), 1895.

[11] Yin, J., Cao, Y., Li, Y. H., Liao, S. K., Zhang, L., Ren, J. G., ... & Pan, J. W. (2017). Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343), 1140-1144.

[12] Liao, S. K., Cai, W. Q., Handsteiner, J., Liu, B., Yin, J., Zhang, L., ... & Pan, J. W. (2018). Satellite-relayed intercontinental quantum network. *Physical review letters*, 120(3), 030501.

[13] Erhard, M., Krenn, M., & Zeilinger, A. (2020). Advances in high-dimensional quantum entanglement. *Nature Reviews Physics*, 2(7), 365-381.

[14] Dieks, D. G. B. J. (1982). Communication by EPR devices. *Physics Letters A*, 92(6), 271-272.

[15] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886), 802-803.

[16] Xu, F., Ma, X., Zhang, Q., Lo, H. K., & Pan, J. W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2), 025002.

[17] Information from http://www2.optics.rochester.edu/workgroups/lukishova/QuantumOpticsLab/2010/OPT253_reports/Justin_Essay.pdf

[18] Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15), 880.

[19] Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K. (2009). Quantum entanglement. *Reviews of modern physics*, 81(2), 865.

[20] Mooney, G. J., Hill, C. D., & Hollenberg, L. C. (2019). Entanglement in a 20-qubit superconducting quantum computer. *Scientific reports*, 9(1), 1-8.

[21] Buhler, J. P., Lenstra, H. W., & Pomerance, C. (1993). Factoring integers with the number field sieve. In *The development of the number field sieve* (pp. 50-94). Springer, Berlin, Heidelberg.

[22] Pomerance, C. (1996). A tale of two sieves. In *Notices Amer. Math. Soc*.

[23] Montanaro, A. (2016). Quantum algorithms: an overview. *npj Quantum Information*, 2(1), 1-8.

[24] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2), 303-332.

[25] Boneh, D., & Lipton, R. J. (1995, August). Quantum cryptanalysis of hidden linear functions. In *Annual International Cryptology Conference* (pp. 424-437). Springer, Berlin, Heidelberg.

[26] Brassard, G., & Høyer, P. (1997). Proceedings of Fifth Israeli Symposium on Theory of Computing and Systems.

[27] Proos, J., & Zalka, C. (2003). Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Information & Computation*, 3(4), 317-344.

[28] Hallgren, S. (2007). Polynomial-time quantum algorithms for Pell's equation and the principal
ideal problem. *Journal of the ACM (JACM)*, 54(1), 1-19.

[29] Kuperberg, G. (2005). A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1), 170-188.

[30] Regev, O. (2004). *A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space* (No. quant-ph/0406151).

[31] Grover, L. K. (1997). Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 79(2), 325.

[32] Prasad, M. R., Biere, A., & Gupta, A. (2005). A survey of recent advances in SAT-based formal verification. *International Journal on Software Tools for Technology Transfer*, 7(2), 156-173.

[33] Gisin, N., & Thew, R. (2007). Quantum communication. *Nature photonics*, 1(3), 165-171.

[34] Barrett, M. D., Chiaverini, J., Schaetz, T., Britton, J., Itano, W. M., Jost, J. D., ... & Wineland, D. J. (2004). Deterministic quantum teleportation of atomic qubits. *Nature*, 429(6993), 737-739.

[35] Riebe, M., Häffner, H., Roos, C. F., Hänsel, W., Benhelm, J., Lancaster, G. P. T., ... & Blatt, R. (2004). Deterministic quantum teleportation with atoms. *Nature*, 429(6993), 734-737.

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

[37] Weinfurter, H. (1994). Experimental Bell-state analysis. *EPL (Europhysics Letters)*, 25(8), 559.

[38] Boschi, D., Branca, S., De Martini, F., Hardy, L., & Popescu, S. (1998). Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 80(6), 1121.

[39] Kim, Y. H., Kulik, S. P., & Shih, Y. (2001). Quantum teleportation of a polarization state with a complete Bell state measurement. *Physical Review Letters*, 86(7), 1370.

[40] Lütkenhaus, N., Calsamiglia, J., & Suominen, K. A. (1999). Bell measurements for teleportation. *Physical Review A*, 59(5), 3295.

[41] Thew, R. T., Tanzilli, S., Krainer, L., Zeller, S. C., Rochas, A., Rech, I., ... & Gisin, N. (2006). Low jitter up-conversion detectors for telecom wavelength GHz QKD. *New Journal of Physics*, 8(3), 32.

[42] Diamanti, E., Takesue, H., Langrock, C., Fejer, M. M., & Yamamoto, Y. (2006). 100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors. *Optics express*, 14(26), 13073-13082.