International Journal of Advanced Research in Technology and Innovation
e-ISSN: 2682-8324 | Vol. 4, No. 1, 55-65, 2022
http://myjms.mohe.gov.my/index.php/ijarti

Quantum Computing and Its Application

Amirul Asyraf Zhahir[1], Siti Munirah Mohd[2*], Mohd Ilias M Shuhud[3], Bahari Idrus[4], Hishamuddin Zainuddin[5], Nurhidaya Mohamad Jan[6], Mohamed Ridza Wahiddin[7]

[1,3] Faculty of Science and Technology, Universiti Sains Islam Malaysia, Negeri Sembilan, Malaysia
[2,6] GENIUS Insan College, Universiti Sains Islam Malaysia, Negeri Sembilan, Malaysia
[4] Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia
[5] Department of Physics, Faculty of Science, Universiti Putra Malaysia, Selangor, Malaysia
[7] Cybersecurity & Systems Unit, Universiti Sains Islam Malaysia, Negeri Sembilan, Malaysia

*Corresponding Author: smunirahm@usim.edu.my

Accepted: 15 February 2022 | Published: 1 March 2022

DOI: https://doi.org/10.55057/ijarti.2022.4.1.7

Abstract: *Quantum computing is different from classical computing. It is based on quantum mechanics principles, utilizing the attributes such as entanglement and superposition. The significant difference between a quantum computer and a classical computer is the ability to process information astonishingly faster. This is possible due to the quantum entanglement concept. Interests in the quantum entanglement concept have been exponentially growing over the years. In the last decade, significant progress in implementations of quantum computation in quantum information has been achieved. This study selected secondary resource indexed literature from several databases with specific keywords in almost a century. In this paper, quantum computing and its application is presented along with the essence of quantum entanglement role in quantum computing. This study will provide a general understanding of quantum computing and its application and quantum entanglement.*

Keywords: quantum computing, quantum entanglement, quantum state

1. Introduction

In 1935, a thought experiment named Einstein-Podolsky-Rosen (EPR) Paradox was produced by Einstein, Podolsky and Rosen, discussing a new fascinating phenomenon (Einstein, Podolsky, & Rosen, 1935). Shortly after, Schrodinger wrote about the concept of quantum entanglement based on the EPR Paradox, and Schrodinger, too, did not understand how it violates the theory of relativity (Schrödinger, 1935). Later in 1964, according to Bell, the quantum entanglement violates the classical mechanics' attributes, realism, locality, completeness and only follows quantum mechanics (Bell, 1964). The concept of quantum entanglement was then established but was not widely recognized until discovering its applications and how important its role is.

Quantum entanglement is the core feature of quantum mechanics (Yu, 2021). It is deemed a strange physical wonder, which can be described as; when two or more objects are entangled, the state of one object can automatically provide the information of the state of another object, regardless of the distance between them. This essential resource has been applied in quantum information (Shi, Chen, & Hu, 2021). It became fundamental for quantum information processing and was used in various areas such as quantum computing, quantum teleportation,

and quantum cryptography. In addition, it is seen as a key ingredient for quantum computers to demonstrate computing capabilities over classical computers (Mooney, Hill, & Hollenberg, 2019). The interest in quantum entanglement has grown exponentially over the last decades, and significant progress has already been achieved in quantum computing (Wang, Li, Yin, & Zeng, 2018). Recently in 2021, a quantum-in computing chip named “Eagle”, packed in 127 quantum bits (qubits), has been revealed by IBM, establishing a recent significant achievement in quantum computing (Ball, 2021). According to IBM, it is a step towards their goal to create 433-qubits quantum processor in 2022, followed by 1121-qubits by 2023. Thus, genuinely understanding the quantum computing fundamentals and entanglement is vital in preparing for advancing technology in quantum computing in the future.

This review paper aims to provide a general understanding of quantum computing with its application and the essence of quantum entanglement. This paper is organized as follows. Section 2 describes the methodology used using several databases and specific keywords to select chosen literature for this study. In section 3, the quantum entanglement concept and general descriptions of the quantum states, both pure and mixed states. Section 4 discusses quantum computing technology and some of its applications. Finally, Section 5 is dedicated to the conclusion.

2. Methodology

This paper indexed the literature in Scopus, American Physical Society Site (APS), Cambridge Core, Nature, and other publications selected by specific keywords, namely quantum computing, quantum entanglement, and quantum state dated from 1935 to 2021. Twenty-seven (27) related literature was chosen for this study. This literature consists of the general information of quantum computing technology and the quantum entanglement concept. Document analysis was done and organized by using Microsoft Word 2021. As a result, this review observed and manifested information from the chosen literature. Figure 1 portrays the methodology.

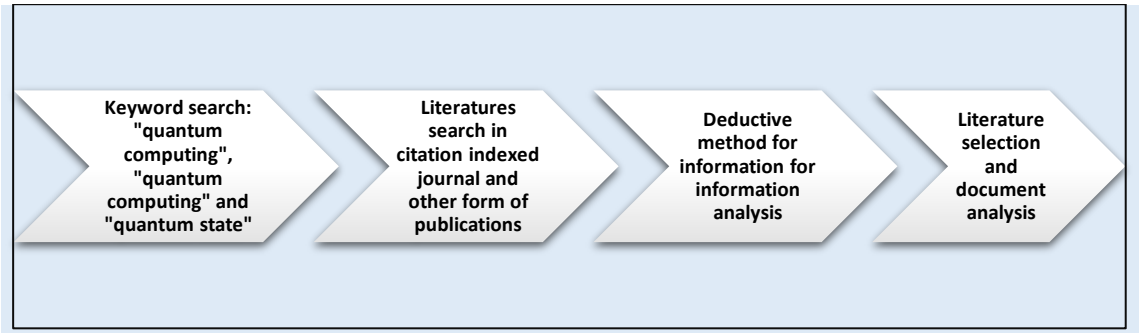

Figure 1: Research methodology

3. Quantum entanglement

Quantum entanglement is a phenomenon in which the quantum state of multiple subsystems cannot be described as separated independently of other subsystems even though the distance between the subsystems is far away from each other (Guo, 2019). Figure 2 depicts an entanglement between quantum systems.

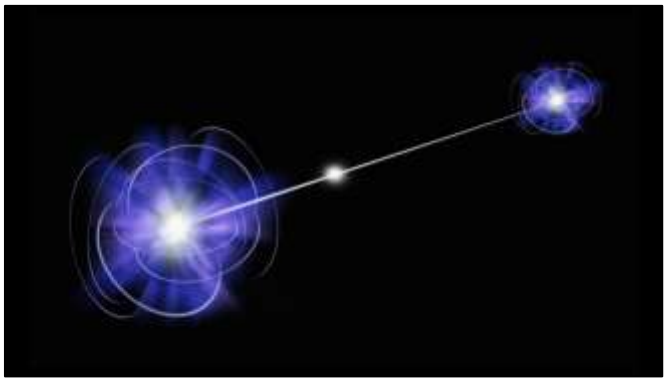

Figure 2: Quantum entanglement
Source: Castelvecchi, 2020

A simplified explanation will help better understand the concept of quantum entanglement. There were two coins, and one coin had "head" as a value and the other one "tail" as a value for both sides of the coins. A coin each were given to two people, Alice and Bob. Both people have been separated far away, Alice was on the earth, and Bob was on mars. They were told that the coin that they currently possessed must be either "head" or "tail" as a value. In this situation, their coins are correlated, entangled classically. Assume that both Alice and Bob arrived at their destination. Alice looked at her coin and found out that she had the "head". Once Alice knew the coin's value, she simultaneously knew Bob's coin value. This logical scenario defies classical mechanics and adheres to the quantum mechanics principle.

A quantum bit or qubit is the basic unit in carrying information in quantum information (Erhard, Krenn, & Zeilinger, 2020). An easier way to understand, a classical computer uses a bit to represent its information; it can only be 0 or 1. In contrast, a quantum computer uses a qubit or quantum bit to represent its information. A qubit vector state unit is denoted as $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Compared to a classical bit, a qubit holds both values 0 and 1 simultaneously; in accordance with quantum mechanics, it is known as superposition (Fedorov & Gelfand, 2021; Matthews, 2021). Superposition is defined as the ability of a quantum system to be in multiple states at once until it is measured or observed. Superposition can be presented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1)$$

It was entangled when a pair or more of quantum subsystems created a superposition state (Ferrie, 2019). Combining the principle of entanglement and superposition would significantly increment computing power.

3.1 Quantum state

A pure state is a quantum state that can be described by a wave function, and a mixed state is a quantum state that can be described by a density matrix (Guo, 2019). A pure state can be presented as:

$$|\Psi\rangle_{AB} = |\Psi\rangle_A \otimes |\Psi\rangle_B \quad (2)$$

A mixed state can be expressed as:

$$\rho=\sum_i P_i|\psi_i\rangle\langle\psi_i| \quad ,\sum_i P_i=1,\ P_i\geq 0 \tag{3}$$

Distinguishing a pure and a mixed state is possible by computing the trace, Tr of the density matrix of the given state as stated in equations (4) and (5):

It is a pure state if:

$$\rho^2=\rho,\ Tr\left(\rho^2\right)=1 \tag{4}$$

It is a mixed state if:

$$\rho^2=\rho,\ Tr\left(\rho^2\right)<1 \tag{5}$$

4. Quantum computing

4.1 Quantum computer vs classical computer

A quantum computer was proposed to simulate processes that a classical computer cannot achieve (Maslov, Kim, Bravyi, Yoder, & Sheldon, 2021; Song et al., 2019; Zhong et al., 2020). It offers an unrivalled approach to information processing (Tura, 2021). Quantum computers utilize the collective attributes of the quantum state, such as superposition, interference, and entanglement abiding by quantum mechanics principle, unlike its classical counterpart, abiding by classical physics principle.

Both classical computers and quantum computers can solve some similar computational problems. The main difference between a classical computer and a quantum computer is the time rate of solving some of the computational issues (Bravyi, Gosset, & König, 2018). Furthermore, the utilization of the quantum entanglement principle in quantum computers greatly intensifies the processing speed (Castelvecchi, 2017). According to Yu (2021), increasing the amount of qubit or creating a more significant entangled state can further enhance the processing speed of the quantum computer. There are various other distinctions between a classical and a quantum computer. Table 1 shows the differences between a quantum and a classical computer to put it into perspective.

Table 1: Differences of the quantum computer and classical computer

Quantum computer	Classical computer
Governed by quantum mechanics principles	Governed by classical physics principles
Quantum gate operations or energy state manipulation	Boolean logic operations
Gates are reversible	Gates run forward
Use qubit or quantum bit to represent information	Use bit to represent information
High rates of error	Low rates of error
Operate at extremely cold temperature	Operate at room temperature
Extremely sensitive to noise	Minimal inherent noise
Uncompromising restriction on copying and measuring signals	No restriction on copying and measuring signals

Quantum computers are advancing swiftly, gaining momentum over the years, threatening the existence of classical computers in approaching certain types of problems, especially those involving a daunting number of variables and outcomes. However, such progression elicits substantial opportunities across the discipline in the modern era.

4.2 Applications of quantum computing

4.2.1 Quantum computing in cloud

Cloud-based quantum computing services have been introduced and used in several backgrounds, namely teaching, research, and games. This provides a path to quantum computing, a quantum computing platform that anyone can access publicly in a cloud environment setting. It is accessible to users around the globe to execute real quantum processing tasks (Almudever, Lao, Wille, & Guerreschi, 2020). Table 2 depicts some of the existing cloud-based quantum computing platforms.

Table 2: Existing cloud-based quantum computing platforms

Developer	Quantum Cloud	Source	Description
Xanadu	Xanadu Quantum Cloud	www.xanadu.ai/cloud	A photonic quantum computing platform
Rigetti Computing	Forest	www.rigetti.com	A quantum programming toolkit
Microsoft	Microsoft Azure Quantum	www.azure.microsoft.com	A quantum system and toolkit for quantum computing
IBM	IBM Q Experience	www.quantum-computing.ibm.com	A quantum system, simulators, and programming tools
Google	Quantum Playground	www.quantumplayground.net	A quantum simulator and 3D quantum state visualization
Qutech	Quantum Inspire	www.quantum-inspire.com	A quantum computing platform provides a fully programmable 2-qubit electron spin quantum processor and a 5-qubit transmon processor
Amazon	Amazon Bracket	www.aws.amazon.com/braket	A quantum simulator that can be run on different quantum hardware technologies

4.2.2 Quantum computing in industries

Quantum computing will revolutionize numerous industries in the future. According to Dilmegani (2021), IBM predicted that quantum computing would evolve over three horizons in the industrial revolution. Horizon 1: Applications for the upcoming few years. Horizon 2: Stable quantum computers but not at the optimal level. Horizon 3: Beyond 15 years. Figure 3 illustrates some of the potential quantum computing applications in industries.

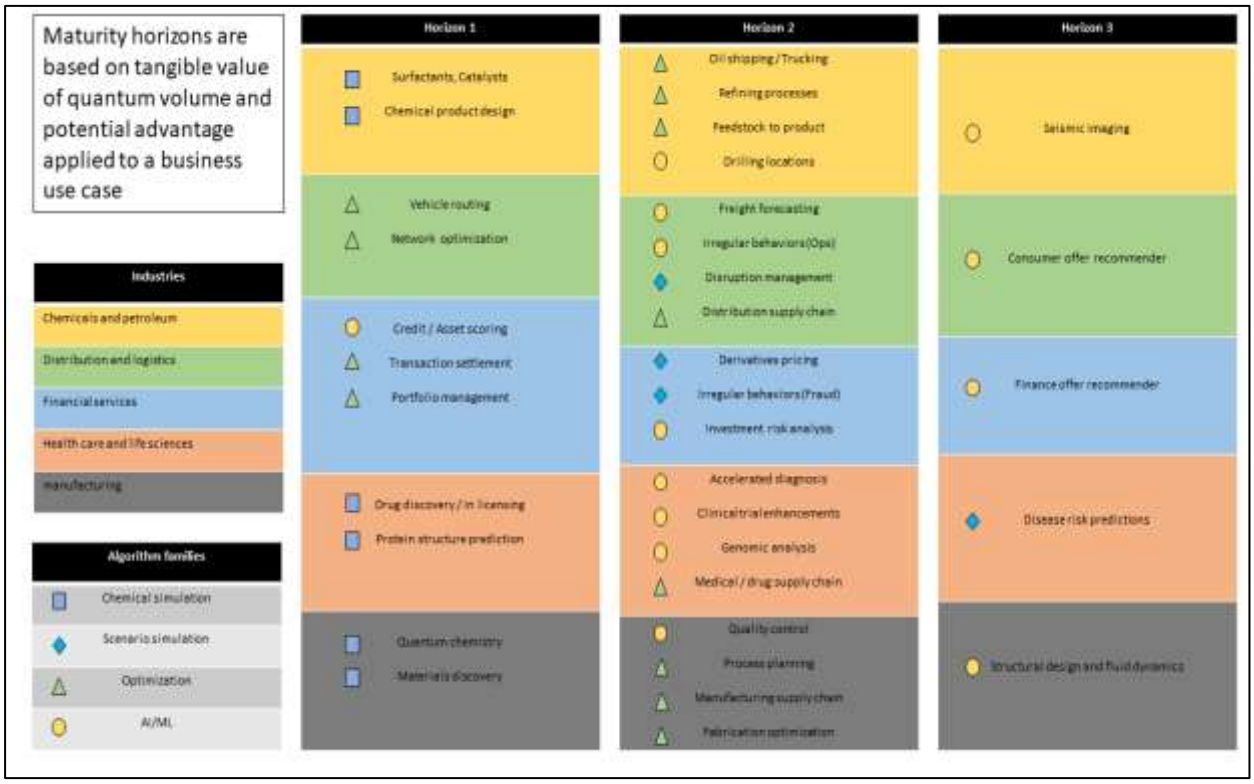

Figure 3: Potential quantum computing applications in industries. Adapted from "Top 20+ Quantum Computing Applications / Use Cases", Dilmegani, 2021. Retrieved from https://research.aimultiple.com/quantum-computing-applications/. Copyright 2019 by IBM Corporation.

Based on Figure 3, quantum computing technology can significantly impact various industries. For example, in health care and life sciences, an oncologist from the German cancer research center collaborates with a team of physicists and computer scientists, planning to utilize quantum computing to help cancer patients classify and select specific therapies from heterogeneous therapies data sets (Abbott, 2021). Another example in renewable energy, Giani (2021), expressed the need for quantum computing to solve crucial renewable energy problems.

4.2.3 Quantum computing in security

Data security is essential as it protects critical information, including files, databases, accounts, and networks. Effective data security is critical to public and private sector organizations in this modern digital technology era, as the consequences of data breaches can cause severe problems. The field of cybersecurity has become increasingly significant due to the reliance on computer systems and technology advancements. Cybersecurity has constantly been improving alongside its counterpart, cyber threats, over the years. Cybersecurity experts use cryptography to design algorithms and other measures to protect the data.

Cryptography is the practice of protecting information from unauthorized access, ensuring the integrity and authentication of the data (Bruss, Erdélyi, Meyer, Riege, & Rothe, 2007). An encryption technique is utilized to obtain secure transmission. An algorithm (known as a cypher) combines the message with additional information (known as a key) to produce a cryptogram. The method of encrypting and decrypting is called cryptosystem (or cypher system), while the information used is called a key. Figure 4 illustrates the basic cryptography scenario between Alice, Bob and Eve.

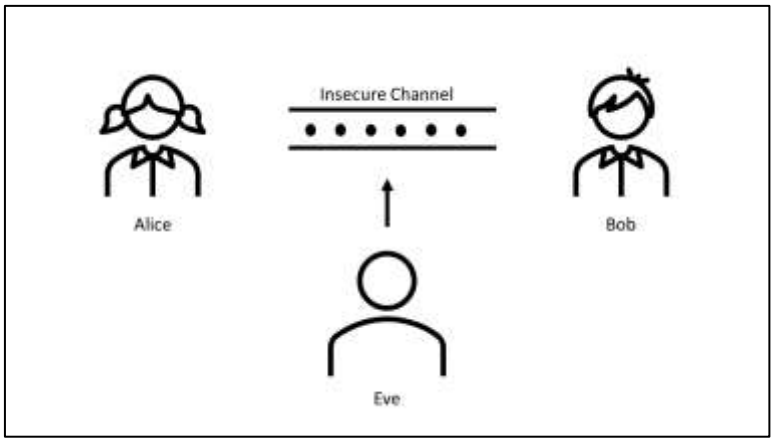

Figure 4: Basic scenario of cryptography
Source: Sehgal & Gupta, 2019

Based on Figure 4, Alice wishes to communicate with Bob using an insecure channel (such as the internet). Alice and Bob can use the cryptosystem and protect the information transferred even with the insecure channel by using an agreed-upon secret key. However, considering that the channel is insecure, Eve, an eavesdropper (unauthorized personnel), may still tap into the communication channel and intercept the information.

Classical cryptography is based on computational mathematics, and quantum cryptography is based on physics following the laws of quantum mechanics to secure private information transmission (Upadhyay, 2019). Table 3 depicts some of the differences between classical and quantum cryptography.

Table 3: Differences between classical and quantum cryptography

Classical cryptography	Quantum cryptography
Based on mathematical computation	Based on quantum mechanics
Widely used	Sophisticated
Digital signature is present	Digital signature is absent
Bit rate depends on computational power	Average bit rate is 1 Mbps
Bit storage 2^n n-bit strings	Bit storage one n-bit string
Communication range millions of miles	Communication range 40,000km
Deployed and tested	In initial stages, not fully tested
Communication medium independent	Communication medium dependent
Low cost	High cost

Based on Table 3, some of the differences between classical and quantum cryptography is illustrated. Classical cryptography utilizes two methods to secure data and prevent data breaches: secret key (asymmetric) cryptography and public key (symmetric). Whereas quantum cryptography utilizes quantum key distribution (QKD), a series of photons uses a qubit sequence to transmit the code from one end to another. By comparing the measurements of the properties of the photons, the two ends can determine the safe key to use to encrypt and decrypt the information sent over. Any disturbance to the qubit sequence will distort it and be detected by sender and receiver; thus, a new bit sequence is generated. Figure 5 illustrates the

scenario of quantum cryptography in BB84 protocol, one of the most common protocols in quantum key distribution.

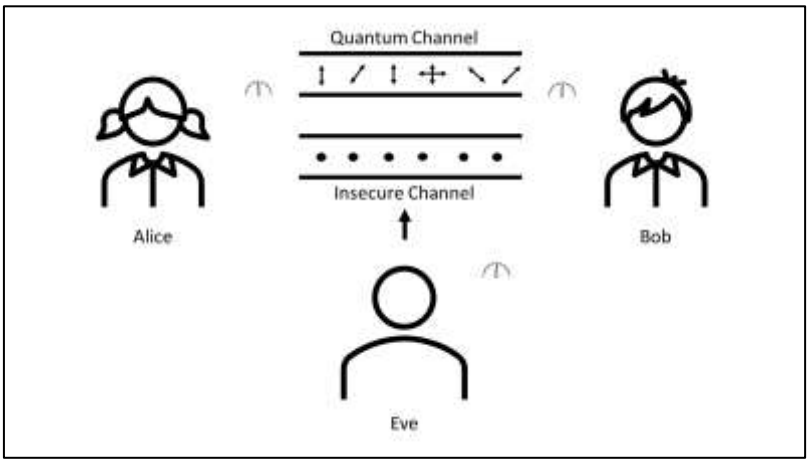

Figure 5: Basic scenario of quantum cryptography
Source: Kumar & Garhwal, 2021

Alice wishes to communicate with Bob over an insecure channel (such as the internet). Alice uses a series of photons with a random basis, rectilinear or diagonal basis assigned to each bit sequence, then transmitted to Bob through a quantum channel to encrypt and decrypt the information sent over the insecure channel. The photons polarization will then be measured by Bob using a random basis. Suppose Bob measured the same polarization as Alice, then Bob received the intended bits sent. If Bob chooses the wrong basis, then the bits he reads are random. Next, Bob will notify Alice of the basis he used, and Alice will report back if Bob had chosen the right basis. Finally, Alice and Bob will discard the bits measured with a different basis. Both Alice and Bob should now have an identical string of bits called sifted key. After consistency is ensured, both now have the shared secret key. Discarding noise and measurement error factors if the measured bits are different, it indicates the presence of an eavesdropper named Eve on the quantum channel, resulting in Alice sending a newly generated bit sequence. Eve would have no choice but to measure the photons transmitted before reaching Bob with a random basis to decode the photons. The no cloning theorem assures that Eve could not replicate the unknown state, thus distorting the photons sequence sent to Bob. Therefore, the photons received by Bob will be random and 25% incorrect compared to Alice, considering the error rate of 50% made by Eve. The chance for Eve to obtain the secret key is slim to none if a sufficiently long bits sequence is compared. Table 4 shows the example of bits, basis and polarisation between Alice and Bob without interference from Eve.

Table 4: Sifted key without eavesdropper's interference

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	X	X	+	X	+	+	X
Alice's polarization	↑	↗	↖	→	↗	↑	→	↖
Bob's basis	+	X	+	X	+	+	X	X
Bob's measurement	↑	↗	→	↗	→	↑	↗	↖
Bob's bit	0	1	0	1	0	0	1	1
Sifted key	0	1	-	-	-	0	-	1

Table 4 depicts the process of quantum cryptography between Alice and Bob without the interference of Eve. As mentioned, any disturbance to the transmission will distort the photons.

Table 5 shows the example of bits, basis and polarization between Alice, Bob with interference from Eve.

Table 5: Sifted key with eavesdropper's interference

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	X	X	+	X	+	+	X
Alice's polarization	↑	↗	↖	→	↗	↑	→	↖
Eve's basis	+	X	+	+	X	X	+	+
Eve's measurement	↑	↗	↑	→	↗	↖	→	↑
Eve's bit	0	1	0	0	1	0	0	0
Bob's basis	X	X	+	X	+	X	+	X
Bob's measurement	↗	↗	↑	↗	→	↖	→	↗
Bob's bit	1	1	0	1	0	0	0	1
Sifted key	-	1	0	-	-	0	0	-
Error generated	-	√	×	-	-	√	√	-

Table 5 depicts the process of quantum cryptography between Alice and Bob with the interference of an eavesdropper, Eve. An error was detected due to interference from the eavesdropper. A new series of photons are usually generated for the shared secret key to ensure total protection of the information transferred over the insecure channel. There are also other protocols under quantum key distribution. Figure 6 shows some other protocols under quantum key distribution.

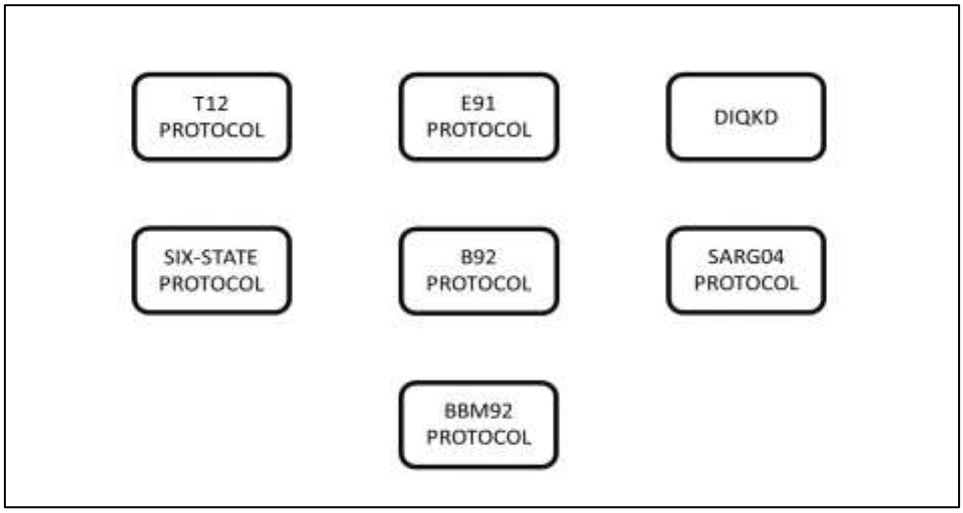

Figure 6: Quantum key distribution protocols
Source: Kumar & Garhwal, 2021

5. Conclusion

In conclusion, a review of quantum computing and its application and the essence of quantum entanglement in quantum computing was presented. The differences between quantum computers and classical computers were also discussed, focusing on the utilization of quantum entanglement in a quantum computer, an essential key in enhancing the quantum computers processing speed. Next, some existing quantum computing applications were also stated. Even though it is still in the early development phase for quantum computing to penetrate the market for commercial use, considering its limitations, quantum computing has a huge potential to change the technological world.

Acknowledgements
This paper is part of a research project supported by the Malaysian Ministry of Higher Education Fundamental Research Grant Nos. FRGS/1/2021/ICT04/USIM/02/1 (USIM/FRGS/KGI/KPT/50121).

References

Abbott, A. (2021). Quantum computers to explore precision oncology. *Nature Biotechnology, 39*(11), 1324-1325. doi:10.1038/s41587-021-01116-x

Almudever, C., Lao, L., Wille, R., & Guerreschi, G. G. (2020). *Realizing Quantum Algorithms on Real Quantum Computing Devices*.

Ball, P. (2021). First quantum computer to pack 100 qubits enters crowded race. *599*, 542.

Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika, 1*(3), 195-200. doi:10.1103/PhysicsPhysiqueFizika.1.195

Bravyi, S., Gosset, D., & König, R. (2018). Quantum advantage with shallow circuits. *Science, 362*(6412), 308-311. doi:doi:10.1126/science.aar3106

Bruss, D., Erdélyi, G., Meyer, T., Riege, T., & Rothe, J. (2007). Quantum cryptography: A survey. *ACM Computing Surveys, 39*, 6-es. doi:10.1145/1242471.1242474

Castelvecchi, D. (2017). Quantum computers ready to leap out of the lab in 2017. *Nature, 541*(7635), 9-10. doi:10.1038/541009a

Castelvecchi, D. (2020). How 'spooky' is quantum physics? The answer could be incalculable. *577*, 461-462. doi:10.1038/d41586-020-00120-6

Dilmegani, C. (2021). Top 20+ Quantum Computing Applications / Use Cases. Retrieved from https://research.aimultiple.com/quantum-computing-applications/

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review, 47*(10), 777-780. doi:10.1103/PhysRev.47.777

Erhard, M., Krenn, M., & Zeilinger, A. (2020). Advances in high-dimensional quantum entanglement. *Nature Reviews Physics, 2*(7), 365-381. doi:10.1038/s42254-020-0193-5

Fedorov, A. K., & Gelfand, M. S. (2021). Towards practical applications in quantum computational biology. *Nature Computational Science, 1*(2), 114-119. doi:10.1038/s43588-021-00024-z

Ferrie, C. (2019). Quantum computing for all? *Nature Electronics, 2*(3), 90-90. doi:10.1038/s41928-019-0223-4

Giani, A. (2021). Quantum computing opportunities in renewable energy. *Nature Computational Science, 1*(2), 90-91. doi:10.1038/s43588-021-00032-z

Guo, Y. (2019). Introduction to quantum entanglement. *AIP Conference Proceedings, 2066*(1), 020009. doi:10.1063/1.5089051

Kumar, A., & Garhwal, S. (2021). State-of-the-Art Survey of Quantum Cryptography. *Archives of Computational Methods in Engineering, 28*(5), 3831-3868. doi:10.1007/s11831-021-09561-2

Maslov, D., Kim, J.-S., Bravyi, S., Yoder, T. J., & Sheldon, S. (2021). Quantum advantage for computations with limited space. *Nature Physics, 17*(8), 894-897. doi:10.1038/s41567-021-01271-7

Matthews, D. (2021). How to get started in quantum computing. *591*, 166-167.

Mooney, G. J., Hill, C. D., & Hollenberg, L. C. L. (2019). Entanglement in a 20-Qubit Superconducting Quantum Computer. *Scientific Reports, 9*(1), 13465. doi:10.1038/s41598-019-49805-7

Schrödinger, E. (1935). Discussion of Probability Relations between Separated Systems. *Mathematical Proceedings of the Cambridge Philosophical Society, 31*(4), 555-563. doi:10.1017/S0305004100013554

Sehgal, S. K., & Gupta, R. (2019). A Comparative Study of Classical and Quantum Cryptography. *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, 869-873.

Shi, X., Chen, L., & Hu, M. (2021). Multilinear monogamy relations for multiqubit states. *Physical Review A, 104*(1), 012426. doi:10.1103/PhysRevA.104.012426

Song, C., Cui, J., Wang, H., Hao, J., Feng, H., & Li, Y. (2019). Quantum computation with universal error mitigation on a superconducting quantum processor. *Science Advances, 5*(9), eaaw5686. doi:doi:10.1126/sciadv.aaw5686

Tura, J. (2021). Boosting simulation of quantum computers. *Nature Computational Science, 1*(10), 638-639. doi:10.1038/s43588-021-00145-5

Upadhyay, L. (2019). *Quantum Cryptography: A Survey*, Cham.

Wang, Y., Li, Y., Yin, Z.-Q., & Zeng, B. (2018). 16-qubit IBM universal quantum computer can be fully entangled. *npj Quantum Information, 4*, 1-6.

Yu, Y. (2021). Advancements in Applications of Quantum Entanglement. *Journal of Physics: Conference Series, 2012*(1), 012113. doi:10.1088/1742-6596/2012/1/012113

Zhong, H.-S., Wang, H., Deng, Y.-H., Chen, M.-C., Peng, L.-C., Luo, Y.-H., . . . Pan, J.-W. (2020). Quantum computational advantage using photons. *Science, 370*(6523), 1460-1463. doi:doi:10.1126/science.abe8770