Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

Cyber Security Analysis for Quantum Computing

V. Bindhu

Professor and Head, Department of Electronics and Communication Engineering, PPG Institute of Technology, Coimbatore, India

E-mail: vbindhuppg@gmail.com

Abstract

The next phase of the quantum revolution is the Quantum computer Network, a network that connects distant quantum devices using quantum links in conjunction with conventional ones. Innovation that has made way for radically improved communications and computing skills. Regular computers use and analyse data in bits (0 or 1), whereas quantum computers use qubits, or quantum bits, which can simultaneously represent other states in addition to ones and zeros. This is how quantum computers vary from traditional computers. The majority of these methods for processing information on computers rely on symmetric or asymmetric cryptography algorithms. These encryption techniques can be vulnerable to attack. We analyse the quantum key distribution (QKD) technique with in a noise-free channel. In addition, we evaluate the QKD protocol with noisy channel to simulate real scenarios on the future Internet. Therefore, it would be essential to explore using quantum cryptography, which cannot be cracked by quantum computing, to secure the standard communications infrastructure used in cyber physical systems (CPS).

Keywords: Quantum computer, qubits, cryptography, cyber physical system

1. Introduction

The security of the internet will be seriously threatened by quantum computers. The most widely used cryptographic systems will fail when big fault-tolerant quantum mechanics are built. Engaging with this risk is therefore important and timely. Numerous sectors, including artificial intelligence, weather prediction, and medical research, hold significant potential for quantum computing. However, it also poses a serious risk to cyber security, suggesting a shift in how we protect our data. Even though most of the present kinds of encryption can be decrypted by quantum computers, we still need to foresee the threat and

DOI: https://doi.org/10.36548/jismac.2022.2.006
Received: 27.05.2022, received in revised form: 26.06.2022, accepted: 11.07.2022, published: 21.07.2022

develop quantum-proof solutions. Furthermore, quantum technology will enhance cyber security. In today's cutting-edge technology, quantum devices can be utilized to enhance security by performing activities that are otherwise impossible, including secret key expansion with complete security[1]. We need to find practical techniques to use quantum computers with the same security guarantees as those of secure (classical) computing because they will be a crucial component of our future network of communications and computations.

1.1 Quantum computing

A rapid developing new technology called quantum computing uses the principles of quantum mechanics to handle problems that are too complicated for conventional computers. Multiple variables that interact in intricate ways are considered complex problems. Because there are so many different electrons interact with one another, modelling the behaviour of individual molecules is a challenging task [2-4]. In order to solve these kinds of difficult problems, quantum algorithms create multivariate spaces where the relationships between the many data points begin to take shape.

1.2 Qubit

The qubit, the fundamental building block of quantum information, is the basis of quantum computation. Unlike a traditional computing bit, this one alternates between the states of 0 and 1 or a coherent superposition of the two values up until it has been measured and the value is determined. Due to this superposition, results can be obtained significantly more quickly than with a conventional system by rapid processing of large number of alternative outcomes using a small number of qubits[10-12]. The qubits are truly the core of the problem for quantum computing. There are more differences between a qubit and a classical bit than just the naming scheme.

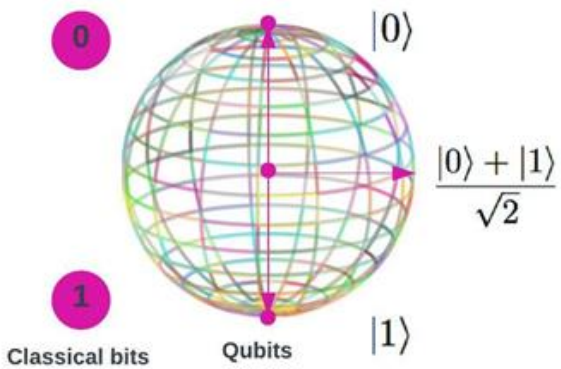

Figure 1. Qubit structure

1.3 Quantum cryptography

Applications for quantum computing can be found in two different branches of cryptography. It offers to completely transform the cracking of traditional asymmetric cyphers (at least the ones in use at the moment), while in it can offer a method in the field of encryption of symmetric conventional safe key exchange cyphers [13]. In order to protect and transfer data in a manner that cannot be intercepted, quantum cryptography employs the inherent features of quantum physics [16-18]. Data is encrypted and protected using cryptography so that only those with the proper secret key to decrypt it [14].

1.4 Quantum computing on cyber security

Cryptography will be one of the areas where quantum computing has the greatest immediate effects on cyber security. Public key encryption is currently used to encrypt nearly all critical communications and data transferred over internet or to the cloud [15]. It is currently far by most widely used type of internet encryption. Every internet browser being used today has the essential public - key encryption built in to protect traffic over the open internet [19]. Most businesses also employ public key encryption to protect their internal data, communications, and user access to linked devices [5].

2. Related Work

Advanced encryption standard picture files are encrypted and decrypted using a modified version of the AES technique plus quantum computing [6]. The shift became irregular when employing quantum random walk since it is standard during AES Shift Row operation due to the change technique. IBM Qiskit quantum simulators were used to simulate computing resources and speeds, while encryption performance was evaluated using number of pixel change rate and unified average change intensity (UACI).

Cyber security Impacts the security of computer systems from intrusions that might corrupt the data, software, or hardware [7]. By permitting illegal use, these assaults run the risk of exposing confidential information and causing harm or disruption. It seems inevitable that the portion of daily life and the economy that depends on computers will grow and eventually take over completely. Cybercrime and cyber warfare will be pervasive, making cyber security essential. The use of quantum encryption to secure the CPS's classical communications infrastructure, which cannot be cracked by quantum computers [8]. In this paper, we analyse why quantum computers can provide even more assistance, specifically

how they could be used to maximise system security in situations in which scalability should not be a problem and to make sure that we are not throwing away expressions on communicating and computational unnecessary information.

Cyberspace security has evolved into a core goal of homeland security for every country [9]. The majority of encryption techniques used today are based on vulnerable algorithms. One of the key justifications for which governments around the world invest in developing quantum computing technology. Quantum cryptography offers distinctive security that ensures secure communication by virtue of the resulting superposition behaviour's randomness using Quantum optics [20]. The benefits of using cryptographic techniques in space systems like satellites, which are a component of the telecoms sector, as well as how quantum can be used to improve the security of many sectors.

3. Proposed Work

A method for safe communication with a third party is cryptography. The goal of cryptography is to enable communication between sender and receiver and incomprehensible third parties. This provides message authentication to show that the data were not changed in transit. The secret key, which is a randomness number, is shared by either the sender or the receiver, which is a useful advantage for both. The distribution of the secret key is made possible by quantum communications. Quantum cryptography is used to carry out the key distribution process; no encrypted messages are sent-it states the quantum key distribution (QKD). Currently, the two main means of Internet telephony are cable and light.

3.1 Quantum Key distribution using BB84

Alice: Quantum sender

Bob: Quantum receiver

Step 1: Alice produces and transmits a random stream of photons to Bob through quantum channel.

Step 2: The four possible polarisation states for single-polarization photons encrypted with completely random binary bits are horizontal noted as H encoded 0, vertical V encoded as 1+, and diagonal + 45° encoded as 1 and - 45° encoded as 0 . Bob randomly selects the rectilinear (+) or diagonal () basis to measure each photon.

Step 3: Alice and Bob communicate and contrast the basis through public channel

Step 4: After this operation, only the appropriate basis will be left to be decoded to binary bits. Sifted keys indicate to the binary bits that are left remaining.

Step 5: Quantum channel for quantum signal transmission and public channel for traditional information exchange. In order to establish precise synchronisation of the quits between Alice and Bob, public channel can also be used as a clock channel that is synced with the quantum channel.

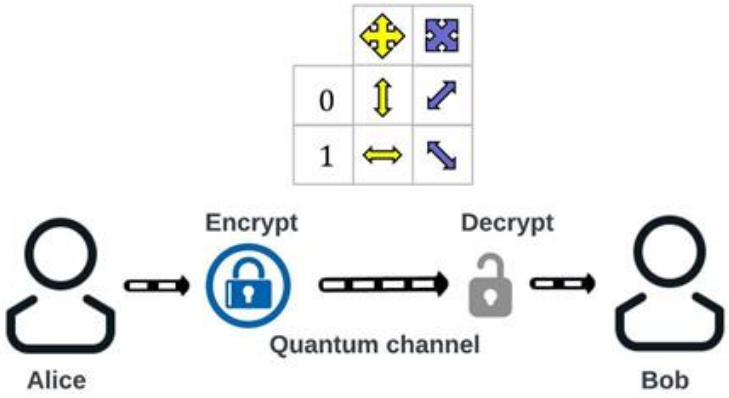

Figure 2. Quantum key distribution using quantum channel

The fundamental idea behind this type of communication is to create a quantum channel using the maximal entangled state of two photons .If Alice wishes to send Bob one bit, she can use two quantum bits (EPR)must be produced by an entangled EPR source. Inferred from the EPR through the quantum computer, one particle is transferred to Alice another to Bob's channel. The protons in an EPR entanglement pair are measured by Alice along using the pieces he is holding and sends Bob the measurement. At last, based on EPR measurement and Alice bit measurement, Bob receives the details regarding the transferred bits.

3.2 Sniffing Detection

They encrypt their data to guarantee confidentiality, but they are unable to stop an attacker from listening in on the channel. Furthermore, regardless of whether the eavesdropper is in cable communications or optical fibre communications, it cannot be identified due to the features of the equipment itself. A multimeter or oscilloscope can be used to monitor cable communications by the listener.

The eavesdropper in optical fibre communications can obtain information from a portion of the light signal. Due to external influences on the fibre loss, such as pressure and temperature, the eavesdropping-related loss cannot be felt.

For a little amount of quantum information, an observer of the quantum channel will, with a 50% chance, select the same measuring base as the sender. As a result, there is a 50% chance that an eavesdropper may be discovered while accessing a piece of quantum information. The chances of an eavesdropper being discovered are 1 (1/2) or the quantum data of–bit.

3.3 Proposed QKD with common Key Structure

- In the Quantum Key distribution system, both the transmitter and the receiver must use the same encryption/decryption key structure.
- The below figure 3 provides the new proposed source for the common key structure.
- If Alice wants to send Bob the message "HELLO BOB",using ASCII code.
- ASCII code uses 8 bits to encode each character.
- Now, Alice can employ a number of 0s and 1s to develop a common key that will be associated to the message itself.
- For e.g.: There are 33 number of 1 bits and 52 number of 0 bits in total number of 85 bits of a ASCII code. Along with all the actual message should be sent to Bob, Alice can also use the prefixed ASCII value of 33 (1's bits) and the suffix the ASCII code of 52 (0's bits).
- In doing so, Alice and Bob may secure the security of the hidden signal, which when decoded will reveal the actual bits in the message, in addition to sharing a straightforward constructed common key.
- The following method can also be used to produce the calculation for the likelihood of detecting of eavesdropping on the QKD protocol:

Probability of existence=Probability {(Base of Alice =Base of Bob) ∩ (Measurement of Alice ≠Measurement of Bob)

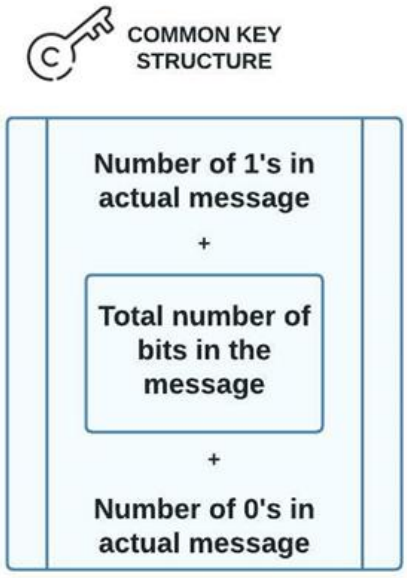

Figure 3. Common key structure for QKD

4. Results and Discussion

The likelihood of an eavesdropper being discovered in a noise-free channel is shown in Figure 4. The graph shows that when there are more than 30-40 transmissions, there is a high likelihood that someone is listening in.

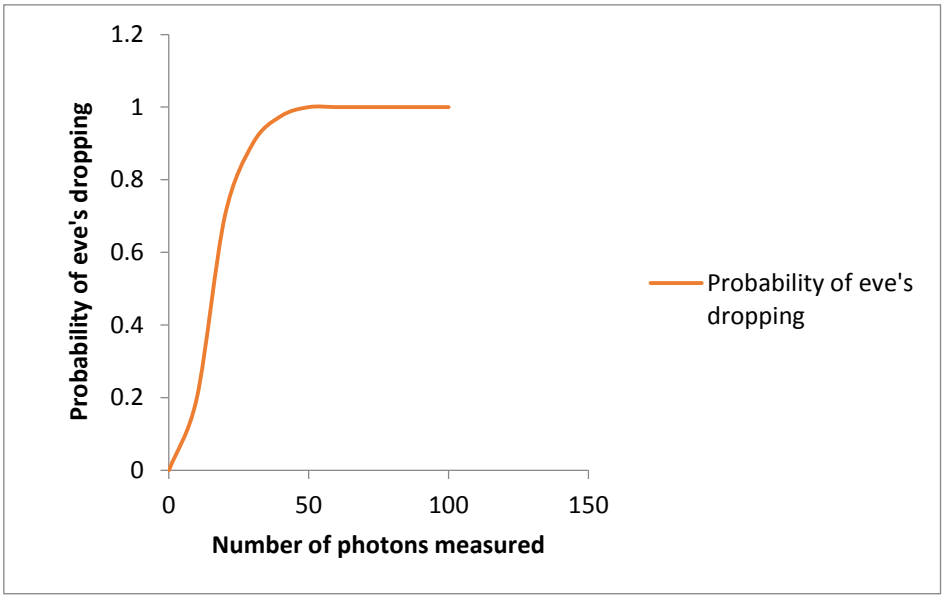

Figure 4. QKD performance on a noise free channel

The likelihood of an eavesdropper being discovered in a channel with 40% noise is shown in Figure 5. The graph demonstrates that when the transmitted photon count is close to 75, there is an almost 100% chance that the eavesdropper will be discovered.

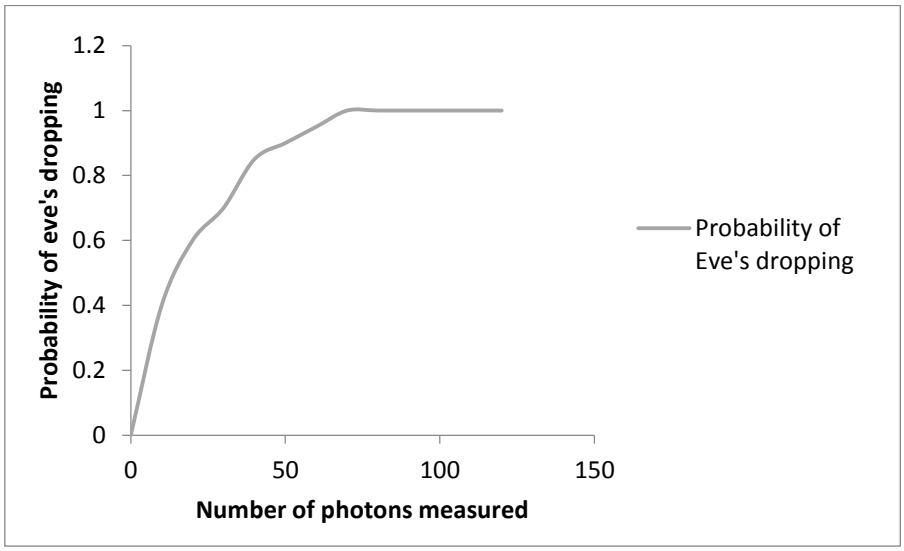

Figure 5. QKD performance with 40 % noise in the channel

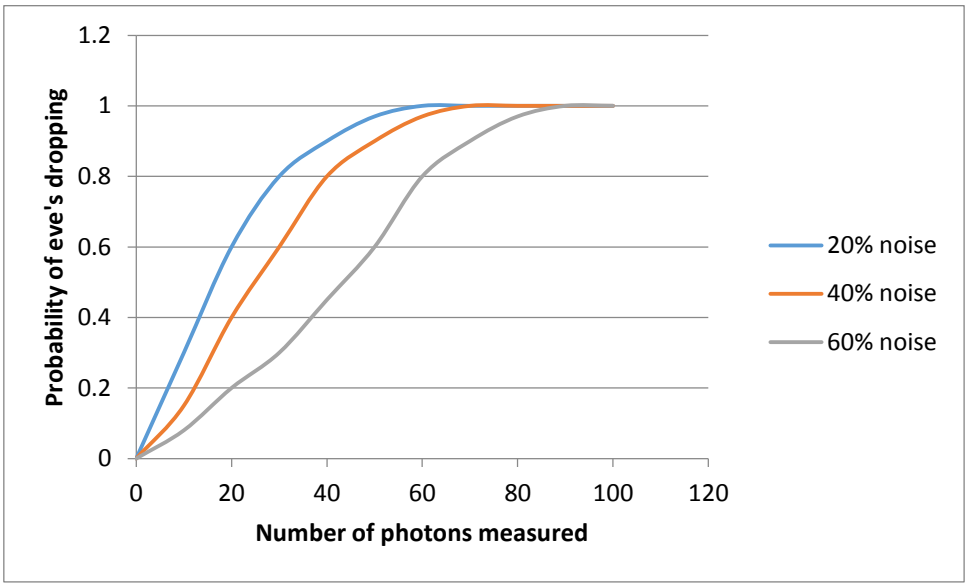

Figure 6. QKD performance with different noise ratio's in the channel

Figure 5 illustrates how the eavesdropper is identified depending on how likely it is that they are listening in on the channel with different probability of noise.

5. Conclusion

The fundamentals of quantum computing, its use in cyber security, and several related developing technologies have been examined. It is crucial that a workable quantum computer can still exist in the future. Its greatest advantages over traditional cryptography are its absolute security and snooping detection. These traits can address a crucial issue with cyberspace security for the coming Internet. The outcomes of our experimental research

demonstrate quantum cryptography's unwavering security and ability to detect snoopers, making it appropriate for use in future Internet communications

References

[1] https://www.ibm.com/topics/quantum-computing

[2] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 912–925, 2018.

[3] Li P., Li J., Huang Z., Gao C.Z., Chen W.B. and Chen K. Privacy-preserving outsourced classification in cloud computing, Cluster Computing, pp. 1-10, (2017)

[4] D. Chandra et al., "Quantum Topological Error Correction Codes: The Classical-to-Quantum Isomorphism Perspective," IEEE Access, vol. 6, Dec. 2018, pp. 13 729–57.

[5] https://businessinsights.bitdefender.com/how-quantum-computing-will-impact-cybersecurity

[6] Ko, Kyung-Kyu, and Eun-Sung Jung. 2021. "Development of Cybersecurity Technology and Algorithm Based on Quantum Computing" *Applied Sciences* 11, no. 19: 9085. https://doi.org/10.3390/app11199085

[7] Petros Wallden and Elham Kashefi. 2019. Cyber security in the quantum era. Commun. ACM 62, 4 (April 2019), 120. https://doi.org/10.1145/3241037

[8] D. Tosh, O. Galindo, V. Kreinovich and O. Kosheleva, "Towards Security of Cyber-Physical Systems using Quantum Computing Algorithms," *2020 IEEE 15th International Conference of System of Systems Engineering (SoSE)*, 2020, pp. 313-320, doi: 10.1109/SoSE50414.2020.9130525.

[9] Meraz, Rita and Vahala, Linda (2020) "Application of Quantum Cryptography to Cybersecurity and Critical Infrastructures in Space Communications," *OUR Journal: ODU Undergraduate Research Journal*: Vol. 7, Article 5.

[10] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A Vision for the Road Ahead," Science, vol. 362, no. 6412, Oct. 2018.

[11] V. Shankar, S. Chang, "Performance of Caffe on QCT Deep Learning Reference Architecture – A Preliminary Case Study", 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), p.35-39, 2017.

[12] S. Gupta, S. Mohanta, M. Chakraborty, S. Ghosh, "Quantum machine learning-using quantum computation in artificial intelligence and deep neural networks: Quantum

computation and machine learning in artificial intelligence", 8th Annual Automation and Electromechanical Engineering Conference (IEMECON), p.268-274, 2017.

[13] Huang, Z., Kim, J., Sadri, A., Dowey, S. & Dargusch, M. S. Industry 4.0: Development of a multi-agent system for dynamic value stream mapping in SMEs. J. Manuf. Syst. 52, 1–12. https://doi.org/10.1016/j.jmsy.2019.05.001 (2019).

[14] Illalba-Diez, J., Zheng, X., Schmidt, D. & Molina, M. Characterization of industry 4.0 lean management problem-solving behavioral patterns using EEG sensors and deep learning. Sensors.https://doi.org/10.3390/s19132841 (2019).

[15] J. Yin et al., "Satellite-Based Entanglement Distribution over 1200 Kilometers," Science, vol. 356, no. 6343, 2017, pp. 1140–44.

[16] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacy-preserving outsourced classifcation in cloud computing," Cluster Computing, pp. 1–10, 2017.

[17] Villalba-Diez, J. & Zheng, X. Quantum strategic organizational design: Alignment in industry 4.0 complex-networked cyberphysical lean management systems. Sensors.https://doi.org/10.3390/s20205856 (2020).

[18] Finn, K. R., Silk, M. J., Porter, M. A. & Pinter-Wollman, N. Te use of multilayer network analysis in animal behaviour. Anim. Behav. 149, 7–22. https://doi.org/10.1016/j.anbehav.2018.12.016 (2019).

[19] O. Cangea, C. Silvia Oprina, M. Dima, "Implementing quantum cryptography algorithms for data security", 2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), p.1-6, 2016.

[20] Y. Ismail, F. Petruccione, "The Race Towards Quantum Security", 2018 IST-Africa Week Conference (IST-Africa),p.1-7, 2018.

Author's biography

V. Bindhu received the B.E. degree in Electronics and Communication Engineering from Bharathiar University, Coimbatore, in 2002, M.E. degree in Applied Electronics from Anna University, Chennai, in 2007, and Ph.D. degree from Anna University, Chennai, in 2014. She has 10 years of teaching experience and 5 years of research experience. Currently, she is Professor at PPG Institute of Technology, Coimbatore. Her area of interest includes signal processing and VLSI design.