Quantum Computing Challenges and Impact on Cyber Security

Hassan Jalil Hadi[1], Yue Cao[1(✉)], Mohammed Ali Alshara[2], Naveed Ahmad[2], Muhammad Saqib Riaz[2], and Jun Li[3]

[1] School of Cyber Science and Engineering, Wuhan University, Wuhan, China
Yue.cao@whu.edu.cn

[2] College of Computer and Information Science, Prince Sultan University, Riyadh, Saudi Arabia
{malshara,nahmed,yjaved}@psu.edu.sa

[3] Datang Internet Technology (Wuhan) Co., Ltd and Hubei Engineering Research Center of Industrial Internet Integration Technology, Wuhan, China
jun_li@bjdv.com

Abstract. Quantum computers pose a significant danger to cyber security. If major fault-tolerant, quantum computers are built, the most extensively used cryptography techniques would fail. The present level of analysis, in terms of quantum technologies and applications, is still in its infancy. The researchers have a hazy view of how to prepare for future quantum computing breakthroughs, particularly in cyber security. The powerful quantum computers capable of breaching current cryptography protections are yet a decade or more away. History has demonstrated that transitioning to quantum-resistant techniques for classical cryptography will most likely take a quantifiable amount of time. In this paper, a comparative analysis of modern cryptographic algorithms concerning quantum computing is performed and its impact on cyber security has been reviewed.

Keywords: Quantum Computing · Quantum Cryptography · Cyber Security · AES · Quantum Key Distribution (QKD)

1 Introduction

Quantum computing (QC) is grounded in quantum mechanics. Quantum mechanics is the theory that regulates how nature operates at the atomic level. This technology can calculate in all four states at the same time, and this scales exponentially. Traditional computers will not be sped up by quantum computing (QC). Instead, it will give an exponential advantage for some sorts of operations, such as factoring very large numbers, with substantial implications for cyber security. Quantum computing (QC) has the potential to revolutionize cyber security in several ways. Cryptography depends heavily on the generation of random quantum numbers. The random generator techniques used by conventional random number generators are frequently manipulated since they are not

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2024
Published by Springer Nature Switzerland AG 2024. All Rights Reserved
S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 571, pp. 333–343, 2024.
https://doi.org/10.1007/978-3-031-56583-0_22

truly random. High-tech companies are creating quantum random number generators (QRNG), which employ quantum optics to produce true unpredictability [1]. The foundation of QuantumSecure Communications (QKD) is the sharing of cryptographic keys between two or more entities, enabling them to secretly exchange information. This secure communication method makes use of quantum physics for entirely private exchanges of keys and can even detect the existence of an eavesdropper.

The potential of quantum computing to decrypt public-key encryption, notably the RSA algorithm, is its most contentious use in cyber security. The RSA encryption algorithm is the core of the almost $4 trillion e-commerce industry [2]. Conventional computers would take billions of years to crack the RSA encryption algorithm on the other hand QC with around 4,000 error-free qubits potentially overcome RSA in seconds. Yet, this would take around 1 million noisy qubits being used today. Today's highly sensitive economic and national security information could be at high risk once a sufficiently strong QC becomes accessible. The threat of quantum computers to public-key cryptography has prompted the creation of quantum-resistant algorithms. Machine learning (ML) has similarly altered information security, enabling the discovery and avoidance of new threats. The cost of training deep ML models rises dramatically as the amount of data and complexity grows. Quantum machine learning (QML) is a novel arena that claims to improve ML algorithms tenfold faster, extra energy efficient, and more time efficient. Consequently, very effective procedures for recognizing and combating novel assault strategies might develop.

Cryptology is a phenomenon that means to deceive a message. The basic purpose of cryptology is to achieve the security principles i.e., confidentiality, integrity, and availability. Quantum computers can affect the existing techniques in both ways i.e., negatively, and positively. The negative side is that existing techniques could be broken up by quantum computers [4]. Scientists and researchers should be aware of these challenges and proper planning is required to overcome these challenges with timelines when quantum computers will become a reality [5]. Cryptographic techniques based on quantum computing will be more secure than existing cryptographic techniques. Symmetric cryptography is using a single key to encrypt and decrypt the message. Keeping that key secure is a great challenge, especially over public networks [3]. AES and DES is an important symmetric technique. Asymmetric cryptography has the advantage over symmetric cryptography in that it uses two keys instead of one. Encryption is done with one key, the public key, while decryption is done with the other key, the private key [5,7]. RCA and ECC are the two important asymmetric techniques. Quantum computing (QC) has the prospective to overhaul cyber security, but there are momentous difficulties to overwhelm and fundamental inventions to achieve.

A survey conducted in 2022 revealed that nearly half (47%) of the participants worldwide expressed significant worry about security risks associated with quantum computing. Out of all the countries, Australians were the most apprehensive, with 58% expressing concern. Quantum computing, based on the principles of quantum mechanics, has the potential to perform virtual experiments

and solve intricate problems that are currently beyond the capabilities of conventional computers. However, cybersecurity experts are alarmed that this technology could potentially breach most modern cryptographic systems, making it a major security threat as shown in Fig. 1.

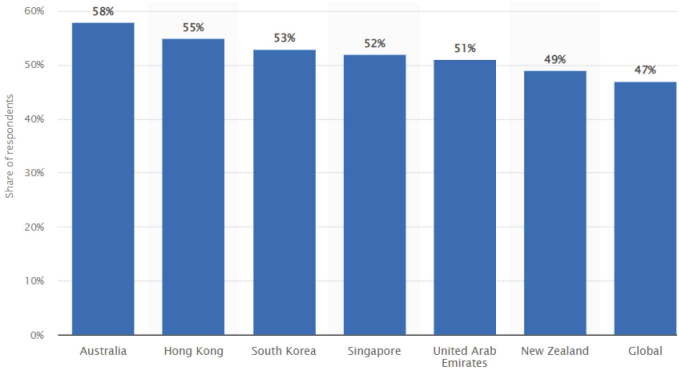

Fig. 1. Concerns about security threats of quantum computing worldwide in 2022

2 Motivation

Massive quantum computers will significantly upsurge computing volume, opening new possibilities for cyber defense. Defense in the nuclear age will have the aptitude to recognize and avert quantum-era threats before they cause any harm [4,6]. Though, QC might be a double-edged sword, meanwhile it may depict new vulnerabilities, such as the capability to rapidly respond to complex arithmetic problems, which are the groundwork of numerous types of encryptions. Industries and organizations may begin preparing now, while post-quantum cryptography ethics are still being determined. That's our motivation to endorse the capabilities and threats of quantum computing toward cyber security.

3 Research Contribution

- Quantum Computing is a new technology and research area that can become a danger to existing cybersecurity algorithms.
- According to the existing research materials, we have identified the challenges and dangers that could be faced by existing cryptographic algorithms.
- The possible solutions to safeguard the classical crypto algorithms have also been taken into consideration and analyzed.

4 Literature Review

Quantum cryptography is the very latest area with plenty of possibilities for advancement. There is a lot of work to be done, and so many issues remain unresolved. The Post Quantum cryptographic solutions are complex due to the unpredictable nature of their deployment on conventional hardware. The classical secret sharing suggested in classical cryptography employed traditional computational power to facilitate secret key sharing. With the introduction of quantum systems, computational power may be overturned. To understand the post-quantum cryptographic situation, it is required to go through the conventional or classic cryptographic structure and its applications in Quantum cryptography. Quantum cryptography provides new ways to communicate securely. Unlike traditional classical cryptography, which uses a variety of mathematical strategies to prevent eavesdroppers from decrypting encrypted data, quantum cryptography is concerned with the physics of information. The transmission and storage of data is always accomplished by physical methods, such as photons in optical fibers or electrons in electric current. Eavesdropping may be thought of as taking measurements on a physical item, in this instance the information carrier. The principles of physics dictate what the eavesdropper can measure and how he can measure it. We can develop and construct a communication system that can always detect eavesdropping using quantum processes. This is because investigations on the quantum transporter of information perturb it, leaving traces behind. From classical to quantum ciphers, here's a quick rundown of the hunt for unbreakable ciphers.

First, Richard Feynman gives the idea of quantum computing in 1982 which works on the principles of quantum mechanics. However, the first two-bit quantum computer was physically developed in 1998 [1]. These computers are very fast and have great computational capability as compared to traditional computers being used today. Quantum computers are a danger to current cryptosystems public key cryptosystems and private key cryptosystems used for data security [5]. Hash-based encryption is also in threat [4].

4.1 Public Key/Asymmetric Cryptography Affected

All of the current public key cryptography methods are based on the factorization of two big prime integers (RSA) and the computation of discrete (DSA and ECC) logarithms [3]. Asymmetric encryption now in use is at risk because of Shor's technique, which is based on huge prime integer factorization. Shor's algorithm's operation will be illustrated with the aid of an example. Let's say we're trying to determine the prime factors that make up the number 15.

This will need to be calculated using a 4-qubit register. Consider the 4-qubit register as a conventional computer's 4-bit register. Since 15 is represented by the binary number 1111, it is simple to determine the prime factors of 15 using a 4-qubit register. operations for every value (0–15) stored in the register can be performed which is the needed step required to perform on a quantum computer. The steps of the algorithm are described below (Table 1):-

Table 1. Qubit registers with remainders

Ref No	Type	Technique	Advantages	Limitation
[1–4]	Public key	RSA	– Dual Keys are involved. – Large Key length up to 2048 bits	– Slow Processing. – Shores algorithm can break it.
[1–3]	Public key	ECC	– Fast generation of keys. – Less computing power is required.	– Smaller Keys are needed. – Smaller quantum computers could break it.
[1–3]	Symmetric Key	AES	– Uses various length keys w.r.t application requirements. – Become more secure if the key length is twice. – Only method of attack is brute force	– Too simple algebraic structure. – Every block is encrypted similarly. – Grover's algorithm is dangerous.
[3]	Hash Function	SHA Family	– Secure from quantum computers	– Grover's algorithm is danger.
[1–4]	Public key	Shore's Algorithm	– It can break public key algorithms. – It is fast as compared to Grover's algorithm. – Polynomial time factorization	– It can factor short prime number only. – Thousands of qubits are required to break long keys.
[1, 2, 4]	Symmetric	Grover's Algorithm	– It can break symmetric cryptography. – Perfectly carry out algorithm scanning	– Its speed is slow

- Quantum Let $n = 15$, is the number whose factorization is required.
- $x = a$ random number will be selected such that $1 < x < n - 1$.
- x power is raised to every value available in the register and divided by n. The remainder of this operation will be stored in the second 4-qubit register which is the superposition results. Let's select $x = 2$ which is greater than 1 and smaller than 14.
- Received remainders as given in Fig. 1. If the x power is increased to every value in a 4-qubit register, which is a maximum value of 15, and then divided by 15. In the sequence of four numbers, we see that we receive remainders (1, 2, 4, and 8). We may deduce from these results that f = 4 is the sequence for $x = 2$ and $n = 15$. With the above equation, the value of f may be utilized to compute a potential factor. Factors to consider:

$$P = xf/2 - 1 \tag{1}$$

- If a result that isn't a prime number is produced, the process is repeated with alternative f values [3] (Fig. 2).

Register 1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Register 2	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8

Fig. 2. 4 Qubit registers with remainders

4.2 Symmetric Cryptography Affected

Symmetric cryptography is based on one key called a private key which is used to encrypt the data and its inverse is used to decrypt the data [3]. Grover's created an algorithm that is used by quantum computers to break symmetric cryptography. It works on square root speed-up instead of the classical brute force algorithm. For example, for a $n - bit$ cipher quantum computer will take $2n/2$ time. It searches unsorted databases. This algorithm can search N entries in unsorted database in $\sqrt{N}$searches. 56-bit DES can be decrypted in only 185 searches [3]. Its limitation is that it is slower than Shor's algorithm.

4.3 Hash-Based Cryptography/Key-Less Cryptography Affected

Hash-based cryptography is also facing the same danger from quantum computers as asymmetric and symmetric cryptography [3,4]. They contain fixed length cipher which is easily breakable by Grover's algorithm. Additionally, it is also tested that Grover's algorithm can be used in combination with the birthday paradox to break hash cryptography [3] (Table 2).

Table 2. Qubit registers with remainders

Ref No	Type	Technique	Advantages	Limitation
[10]	Quantum Communication	Implementation of multipolarities quantum communication network (QCN) By employing the cluster sate-based concept	– Used in distributed quantum computing. – Design for next generation of cyber security system (NGCCS)	– The PQC based on unproven assumptions. – Might be broken In future by developing more sophisticated quantum algorithm.
[11]	QKD for Security protocol	QPC protocol based on multi-particle enabled states (Bell State & 5- qubit state)	– Use of multi-particle entangled states design QPC protocols	– Security Analysis concern: It shows the attacks from outside eavesdroppers, and the attacks from participant and TP are all invalid to under testing protocol.
[12]	QKD for Security protocol	QKD protocol (BB84) deployment with practical implantation on IBM QX	– Using the BB84 protocol the existence of a third-party eavesdropper can be detected. – Observed that with a greater number of qubits that are sniffed by eavesdroppers, the detection will be higher	– Dedicated exercise on BB84 protocol only.
[13]	QKD for Security protocol	Use of protocol dependent on inherent secure nature of quantum cryptography	– Secure against internal and external eavesdropping, masquerading, and brute-force attacks	– Proposed Protocol is vulnerable to super Dense coding of quantum states
[14]	Quantum Security Scheme	A quantum security scheme (QSC)	– Simple Random (No Computation cost). – Intruder-Eve can be detected even on qubit	– Only for RSA based security protocols

4.4 Challenges to Quantum Computers

Several challenges are preventing quantum computers to become a reality [2]. These are probabilistic which means that quantum computers can generate thousands of other solutions besides the correct one. Qubits are not error-free, they can be affected by noise, heat, stray magnetic coupling. Qubits can be affected with bit-flips and phase errors. Coherence is another issue faced by qubits which means that qubits cannot maintain their state for a longer period [2,3].

4.5 Alternate Methods for Secure Communication

Different alternate methods are proposed for secure communication which is based on mathematical problems under the umbrella of post-quantum cryptography which are lattice-based cryptography, code-based cryptography, hash-based signatures, and Multivariate-based cryptography. Quantum cryptography is another proposed method which is based on quantum computing principles i.e., quantum key distribution (QKD) [5].

5 Discussion and Evaluation

RSA is the most important and widely used public key technique which exploits the difficulty of factorizing the product of two large prime numbers [8] Shore's algorithm is a real threat to RSA-2048 because it can factor prime numbers in polynomial time rather than exponential times [1]. It is tested in 2001 and successfully factored the prime number 15 using 7 qubits [2]. A Quantum computer with thousands of qubits is required to factorize the RSA-2048. It is the limitation of Shore's algorithm. It is not a permanent solution to increase the key size for securing the algorithms. There is a chance that RSA-2048 has the 1/7 probability to break by 2026 and $\frac{1}{2}$until 2031. ECC is another public key algorithm that is using the elliptic curve technique to encrypt the data. It has shorter keys to encrypt data which is the disadvantage of this algorithm [1,2]. A modified form of Shore's algorithm can break ECC easily [3,4].

Symmetric cryptography is based on one key called a private key which is used to encrypt the data and its inverse are used to decrypt the data [9]. It is more secure than public cryptography because no public key is involved in it. It can be broken by brute force attack which is not easy to break even by quantum computers because quantum computers must check each key combination to match. For a 128-bit cipher, it would take 6 months to check each possibility [10]. If the key size of symmetric algorithms is increased twice then they will provide the same level of security as quantum computers [11,12]. Hash functions also suffer the same threat from quantum computers as asymmetric and symmetric cryptography. To secure hash functions against Grover's algorithm, a hash function must provide 3-bit output for a b-bit security level. If the output size of the hash function is doubled then it will become quantum resistant. SHA-2 and SHA-3 with longer key outputs are safe against quantum computers [14].

6 Impact on Cyber Security

The technique of managing the risk associated with cyber security has become more reliable thanks to theories about quantum computing. Current risk management techniques rely on traditional probability methodologies since current cyber security risk management models are built around the behavior of cyber security [15]. Instead of employing human intellect, which is inadequate, these techniques combine Hilbert space with quantum cognition. From the perspective of cyber security, a risk is defined as the likelihood that threats to or assaults on cyber security assets may result in negative outcomes [16]. Although the foundations of classical probability theories serve as the basis for quantum cognitions, they can be substituted by the axioms of Hilbert space. It might create brand-new, highly efficient mental models by utilizing quantum cognition.

The technique of managing the risk associated with cyber security has become more reliable due to theories about quantum computing. Current risk management techniques rely on traditional probability methodologies since current cyber security risk management models are built around the behavior of cyber security. Instead of employing human intellect, which is inadequate, these techniques combine Hilbert space with quantum cognition. From the perspective of cyber security, a risk is defined as the likelihood that threats to or assaults on cyber security assets may result in negative outcomes. Although the foundations of traditional probability theories serve as the basis for quantum cognitions, they can be substituted by axioms of Hilbert space. It may create brand-new, highly efficient mental models by using quantum cognition. To better decision-making, it will aid in the understanding of the object, the detection of enemies, and the capabilities. Quantum cognition aids in the capacity to recognize superpositions of likely states that are hard to identify using conventional probability theories. In certain circumstances, the probability assets can depend on a single state instead of putting in just one perspective of a problem [17].

As a result of all these factors, quantum computing poses a major threat to our planet. And every nation competing for the top spot is paying close attention to this issue. The main issue with quantum computing is its capability to break practically every type of encryption now in use. Additionally, because of the state details, unauthorized parties may import information. The confidential data of other countries would be in jeopardy if state-sponsored hackers, who are being used in many battles, got their hands on quantum computers. Because, according to experts, the strength of quantum computers may easily break current encryption techniques like RSA, AES, DSA, and ECDSA [18]. Additionally, it will lead to a rise in uncertainty among nations, and they will all begin to doubt one another. This will provide the framework for spatial interactions that will be discouraging. After then, a conflict may even break out. If an unauthorized party manages to get their hands on a machine like this, not only state data but also the data of everyone else is at risk.

Another danger is that even if it is not spoken on the ground, combining a quantum computer with artificial intelligence would be disastrous. While an AI system might suggest a course of action, it is unable to analyze vast amounts

of data and select the best option, as quantum computers can [19]. Therefore, the biggest threat to machines and artificial intelligence would be eliminated if those two fields ever united. Unfortunately, the largest threat to robots and the environment is people, therefore with power as previously described, quantum technology and AI might eliminate the whole human species without even removing the possibility to comprehend problems .

7 Conclusion and Future Direction

Quantum computing (QC) has the prospective to overhaul cyber security, but there are momentous difficulties to overwhelmed and fundamental inventions to achieve. Cryptographic techniques based on quantum computing will be more secure than existing cryptographic techniques. Several alternative approaches (under the umbrella of post-quantum cryptography) for secure communication-based on mathematical issues are presented. In the future, Mistrustful Quantum Cryptography (MQC), Position-based quantum cryptography and Device-independent quantum cryptography roles in quantum communication network would be analyzed.

Acknowledgement. The authors would like to thanks Prince Sultan University for the support by paying the registration fees of this article. This work is supported in part by the Wuhan AI Innovation Program (Grant No. 2023010402040020) and the Hubei Province Key Research and Development Program (Grant No. 2021AAA007).

References

1. Vaishnavi, A., Pillai, S.: Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. J. Phys: Conf. Ser. **1964**, 042002 (2021). https://doi.org/10.1088/1742-6596/1964/4/042002
2. Kirsch, Z.J., Ming, C.: Quantum computing: the risk to existing encryption methods (2015)
3. Mavroeidis, V., et al.: The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200 (2018)
4. Arslan, B., et al.: A study on the use of quantum computers, risk assessment, and security problems. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE (2018)
5. Mosca, M.: Cybersecurity in an era with quantum computers: will we be ready? IEEE Secur. Priv. **16**(5), 38–41 (2018)
6. Wallden, P., Kashefi, E.: Cyber security in the quantum era. Commun. ACM **62**(4), 120–120 (2019)
7. Nafis, N.M.: Quantum computing era in perspective of cyber security. No. 4012. EasyChair (2020). Wang, Lidong, and Cheryl Ann
8. Alexander. Cyber security during the COVID-19 pandemic. AIMS Electron. Electr. Eng. **5**(2), 146–157 (2021)
9. Kania, E.B., Costello, J.K.: Quantum technologies, US-China strategic competition, and future dynamics of cyber stability. In: 2017 International Conference on Cyber Conflict (CyCon US). IEEE (2017)

10. Riedel, M.F., Binosi, D., Thew, R., Calarco, T.: The European quantum technologies flagship program. Quantum Sci. Technol. **2**(3), 030501 (2017)
11. Djordjevic, I.B.: Cluster states-based quantum networks. In: IEEE Photonics Conference (IPC), vol. 2020, pp. 1–2 (2020). https://doi.org/10.1109/IPC47351.2020.9252479
12. Ji, Z., Zhang, H., Wang, H.: Quantum private comparison protocols with several multi-particle entangled states. IEEE Access **7**, 44613–44621 (2019). https://doi.org/10.1109/ACCESS.2019.2906687
13. AL-Mubayedh, D., AL-Khalis, M., AL-Azman, G., AL-Abdali, M., Al Fosail, M., Nagy, N.: Quantum cryptography on IBM QX. In: 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1–6 (2019). https://doi.org/10.1109/CAIS.2019.8769567
14. Ul Ain, N.: A novel approach for secure multi-party secret sharing scheme via quantum cryptography. In: 2017 International Conference on Communication, Computing and Digital Systems (C-CODE), pp. 112–116 (2017). https://doi.org/10.1109/C-CODE.2017.7918912
15. Ford, P.: The quantum cybersecurity threat may arrive sooner than you think. Computer **56**(2), 134–136 (2023). https://doi.org/10.1109/MC.2022.3227657
16. Lakshmi, D., Nagpal, N., Chandrasekaran, S.: A quantum-based approach for offensive security against cyber attacks in electrical infrastructure. Appl. Soft Comput. **136**, 110071 (2023)
17. Dwivedi, A., Saini, G.K., Musa, U.I., Kunal.: Cybersecurity and prevention in the quantum era. In: 2023 2nd International Conference for Innovation in Technology (INOCON), pp. 1–6. Bangalore (2023). https://doi.org/10.1109/INOCON57975.2023.10101186.
18. Csenkey, K., Bindel, N.: Post-quantum cryptographic assemblages and the governance of the quantum threat. J. Cybersecur. **9**(1), tyad001 (2023)
19. Fernández Pérez, I., Prieta, F.D.L., Rodríguez-González, S., Corchado, J.M., Prieto, J.: Quantum AI: achievements and challenges in the interplay of quantum computing and artificial intelligence. In: Julián, V., Carneiro, J., Alonso, R.S., Chamoso, P., Novais, P. (eds.) ISAml 2022. LNNS, vol. 603, pp. 155–166. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-22356-3_15