Cybersecurity and Cryptography: The New Era of Quantum Computing

.

ABSTRACT

Aim: This paper aimsto examine the concepts of cybersecurity and cryptography with the advent of the current quantum computing.

Significance of Study: The numerous advantages attached to the use of the hyper-connected paradigm have given an inestimable and unavoidable value to its use. However, there is a need to protect information dissemination between parties to avoid the occurrence of catastrophic events that may come when an unauthorized party accesses this information. Thus, the use of quantum computing to improve the previously used cryptography for cybersecurity is very essential.

Problem Statement: In the past, cryptography was the adopted method to secure information in the cyber world thereby, preventing attack and also disallowing intruders from having access to secret information. However, the advent of quantum computing to improve the efficiency of cryptography has made its application very challenging due to its complex nature.

Discussion: An introduction to cryptography, cyber security, and quantum computing was executed. The mechanisms of cryptography in cyber security together with its transition into quantum cryptography were discussed. Characteristics of quantum information and quantum communication systemsregarding typical examples were stated. Post-quantum cryptography as a means of handling the challenges accorded with the use of quantum cryptography was discussed. Finally, consideration was given to the development and applications of the SWOT framework for various kinds of crypto algorithms.

Conclusion: The use of quantum cryptography has found wide applications in cyber security. Also, post-quantum cryptography has been proven to be effective in handling issues arising from the use of quantum cryptography in securing information from being accessed by a third party.

Keywords: Cybersecurity, Cryptography, Quantum Computing, Algorithm, Cyberattack

1. INTRODUCTION

The advent of the internet some years back has contributed to increasing the performance of various industrial machinery connected to it. In the early $21th$ century, records have shown rapid growth of communication technologies resulting in the existence of societies that are hyper-connected in nature. This paradigm shift has made communications unlimited to phone (video) calls, texting, social media, or news media alone. Wide applications of communications are also found in industrial machine control, stock acquisitions, bank transfers, management of automated houses, unmanned aerial vehicle control, and lots more. [1]. This over-reliance on communications in executing crucial assignments with the

use of a hyper-connected paradigm necessitates the privacy and security of information being transmitted. An unsecured hyper-connected automated industry can be catastrophic if the cyber-world becomes loose and vulnerable to attack. Reports of various social and economic catastrophic events have been recorded such as cyberwar and cybercrime emanating from hacking activities of the unsecured cyber world. This was achieved via the manipulation of critical infrastructures causing social and economic losses after production interruption, reduction of devices lifetime, and getting access to sensitive information [2].

Despite all the aforementioned benefits of cyberspace, its uncontrolled and unregulated attributes have made it to be quite challenging making information security to become a subject of major discussion. Also, the information industry and technology are now experiencing exceptional development. Sources of cyberspace attacks are materializing in various forms such as malicious software invasions, hacker attacks, and computer viruses. Other major cyber security challenges include

(1) network threats such as wiretapping and eavesdropping,

(2) network infrastructure complexity,

(3) infringement of security parameters such as availability, authorization, privacy, integrity, non-repudiation, and audit,

(4) leaking sensitive data. a business can gobankrupt if sensitive and secretive information/data about financial transactions such as e-commerce, credit card processing, bank transactions, and stock dealings are compromised.

All these are posing a serious threat to cyberspace information security. Nonetheless, the advancement of science and technology also poses new challenges to cyberspace security. Thus, these records of cyber vulnerabilities have substantiated the need fora high-significance level of cryptography and cybersecurity in securing the paradigmatic society. The duo is also facing the challenges of neo-invention of quantum computing in improving their efficacy and method of operation [3].

Cybersecurity has to do with controlling any damage to electronic communication services and systems by protecting the information involved alongside maintaining its integrity, confidentiality, availability, non-repudiation, and authentication. According to CISCO, cybersecurity involves practicing multiple layers of protection across systems and networks to avoid any attacks on sensitive information or business operations.

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it.

Algorithms which make the information to be unintelligible to an unintended third party are possible thanks to cryptography. The art of using cryptography to secure data is called encryption.

This is done to prevent information misuse if an unauthorized person is opportune to have access to it. The opposite of the process is called decryption in which the cipher text is decoded into the original text such that the receiver can now read the message.

Thus, cryptography serves the purposes of data security maintenance and safeguarding the integrity, confidentiality, and authenticity of the information [4].

UNDER PEER REVIEW

1.1 QUANTUM COMPUTING

Advancements in computing capabilities have led to a gradual transition from classical computing to quantum computing. Quantum computing represents a significant transition from classical computing. Complex calculations can be handled at 100 million times faster speed by quantum computers than standard computers using the principle of the 'superposition' property of a qubit. The qubit has the unique capacity of identifying dual states (such as 0 or 1, true or false, black or white) and also compares and copes with values falling between these two states. Unlike classical computers, which process data in binary bits (0s and 1s), quantum computers utilize quantum bits or qubits. These qubits harness the principles of quantum mechanics, specifically superposition and entanglement [4]. This enables them to evaluate complex calculations at unattainable speeds by their classical counterparts. This extraordinary capability, however, comes with significant cybersecurity implications. The paradigm of how mathematical operations are performed can be transformed. This makes it easy to execute an infinite combination of calculations while considering all options at the same time. Figure 1 represents the Bloch sphere showing the geometrical representation of a qubit. Qubits can take a value for each point on the surface described by the two angles φ and θ. The pole points are $|0\rangle$ or $|1\rangle$ [5].

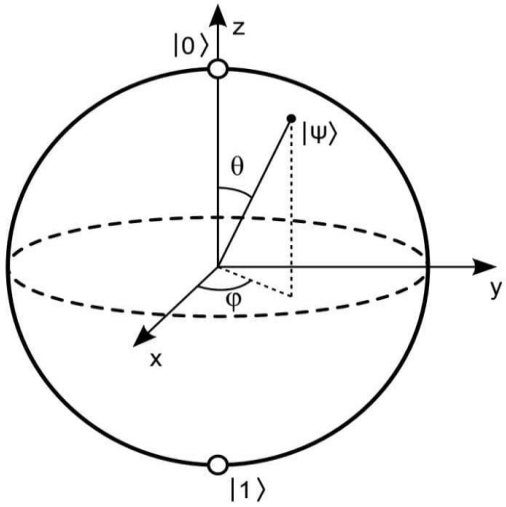

Figure 1: The Bloch sphere showing the geometrical representation of a qubit

Classical cryptographyrelies majorly on the computational difficulty of certain mathematical problems. The most pressing concern is the potential susceptibility of current encryption methods. Modern encryption, such as ECC and RSA, depends on the computational difficulty of problems like discrete logarithms and integer factorization. For example, a widely used cryptographic system called RSA encryption is based on the fact that factoring large numbers is computationally difficult for classical computers [2]. Modern cryptography differentiates the two forms of cryptosystems based on the way a message is encrypted: asymmetric and symmetric key schemes. Asymmetric key schemes or public key schemes comprise two different keys for each of the parties sharing secrets. To encrypt messages, a public key is used. To decrypt the received messages, the equivalent private key is used. In symmetric key schemes, the same key for decryption and encryption algorithms is used. RSA cryptosystem is one of the most used asymmetric key cryptosystem schemes.

However, quantum computers possess superior computational capabilities and advanced processing power which allow them to potentially break these cryptographic systems and solve these problems much faster than today's computers. Thus, rendering existing encryption methods outdated. A quantum computer running **Shor's** algorithm, for example, could factor large numbers perfectly, thereby breaking RSA encryption. This potential vulnerability has resulted in post-quantum cryptography. Figure 2 represents the Quantum Computer IBM Q [6].

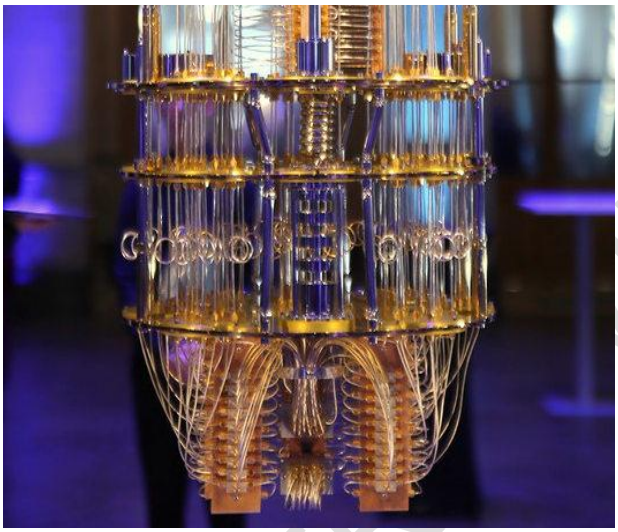

Figure 2: Quantum Computer IBM Q

The need to secure the information available in cyberspace led to the use of cybersecurity and cryptography. However, the advent of quantum computing has greatly interfered with the previous mode of operation of cybersecurity and cryptography thereby, making it quite challenging. Though different kinds of articles on research conducted in this area have been written, there are still limitations and bounds on the thorough review of the current mode of operation using quantum computing for the duo. This paper discusses the concepts of quantum computing as a tool for cybersecurity and cryptography.

2. CHARACTERISTICS OF QUANTUM INFORMATION

Characteristics of Quantum Information are mainly quantum no-cloning theory, quantum teleportation, the principle of uncertainty, and the hidden characteristics of quantum information. All these are adopted and utilized to resist cyberspace communication attacks which could either be active or passive in nature. Quantum no-cloning theory, which characterizes quantum information, comprises undeleting and un-cloned attributes of the unknown quantum state. Cloning is simply the creation/production of a completelyindistinguishable quantum state in another system entirely. Studies have shown that the duplication of quantum systems by machines is impossible [5]. The undeleting principle can assure that any damaging and deleting effect of the enemy on the quantum information will vacate a trace in secure communication. The deletion of an arbitrary quantum state copy is not permitted by the linearity of quantum theory as proposed in Nature. In quantum teleportation, the sender receives the classic information via the measurement of the original quantum state. This is disseminated by the sender through classical communication [7]. The remaining information that was not extracted by the sender

in the measurement is the quantum information. It is later transferred to the recipient via measurement. The uncertainty principle is called the Heisenberg's uncertainty principle. This was introduced by the German physicist Heisenberg in 1927. The ideology behind the uncertainty principle is that it is impossible to determine the position of the particle in the micro-environment, and its existence is usually with different probability in different places. Lastly, in the hidden attributes of quantum information, the quantum information possesses unique properties that classical information does not have. Specifically, the local measurement operation cannot receive the quantum code information in the entangled state, which can only be exposed by joint measurement [8].

UNDER PEER REVIEW

2.1 QUANTUM COMMUNICATION SYSTEM

Quantum communication can be categorized into quantum teleportation communication and quantum direct communication. In quantum teleportation communication, the qubits exist in both entangled and orthogonal superposition states, unlike classical communication. The quantum teleportation principle involves the establishment of a quantum channel via the maximum entangled state of two particles after which the quantum operation transmits the message. It should be noted that the difference between direct communication and teleportation is the communication channels selection. Figure 3 is the illustration of the quantum teleportation model depicting Alice transmitting one-bit quantum with Bob in another location [6]. Firstly, the EPR entanglement source generates an EPR pair. Secondly, Alice receives one of the particles, and the receiver Bob receives the other one via the quantum channel. Thirdly, Alice must measure the particles present in the EPR entangled pairs for ease of information transmission and the pending bits she holds. Then, Alice notifies Bob of the measurement results. Finally, based on the measurement results of Alice and the measurement of the EPR pair himself, Bob can then obtain information about the particles to be transmitted concerningAlice's measurement results and the EPR pair measurement [9].

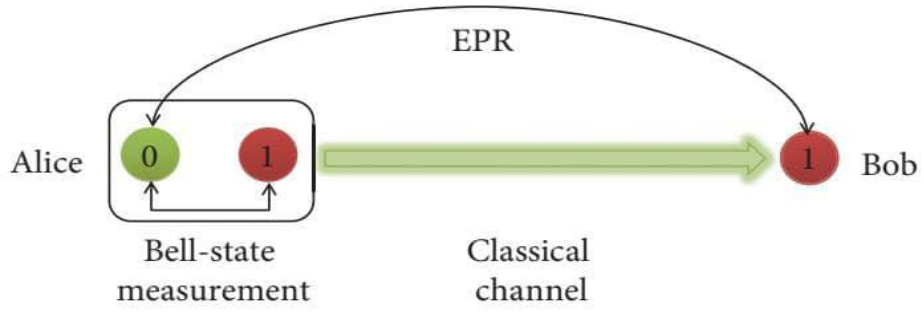

Figure 3: Illustration of the quantum teleportation model

The Quantum direct transmission model represents the easiest mode to accumulate quantum signals transmission in different locations. The quantum direct communication

model is shown in Figure 4 in which Alice intends to disseminate information to Bob via a quantum channel. In this model type, a series of photons must be first produced by Alice via the preparation device concerning the message she wants to disseminate to Bob. After the quantum source generation, information processing by quantum error correcting code (QECC) encoder and quantum source encoder is required. Then, direct transmission of the quantum information to the quantum channel (atmosphere or optical fiber) is executed. Here, the quantum channel is easily disrupted by the external noise. Therefore, QECC encoding is first executed by the receiver Bob to the received signal and then executes quantum source encoding. Finally, the initial quantum message is received by Bob [10].

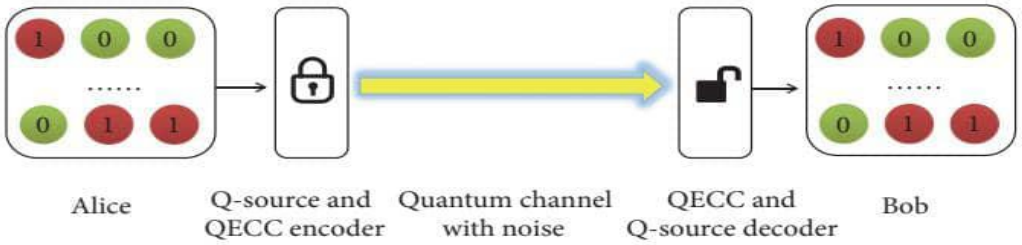

Figure 4: Quantum direct transmission model

2.2 QUANTUM CRYPTOGRAPHY

Quantum encryption is a cutting-edge methodology used in securing the transfer of information whose mechanism is based on the quantum mechanics principles. This method uses quantum bits, or "qubits", rather than traditional binary bits, for data encryption and decryption. Quantum encryption adopts another quantum concept called entanglement which is a process in which two particles, irrespective of distance, are connected so that the state of one immediately stimulates the other. This principle is adopted in Quantum Key Distribution (QKD), where the key for encrypted data decryption is shared via entangled particles. Any effort to interrupt the particles activates a change in their state, thus notifying the proposed recipients of a possible breach [11]. The benefits of quantum cryptography are numerous. Due to the interference invulnerability, quantum encryption is provided with an unprecedented level of security. The complexity of quantum cryptography makes traditional cryptographic systems insignificant because of the advancement of upcoming standards. Instant detection of breaches, man-in-a-middle attacks, and Eavesdropping are relatively impossible in a quantum encryption setup because of the current encryption methods. Concerning cybersecurity and encryption, eavesdropping is a cyberattack in which a malicious actor interrupts, listens, and invades encrypted communication without the approval of the communicating parties. The main objective is to steal sensitive information such as login credentials, personal details, or encryption keys. Interruption of a third party hinders the particle's status and signals the receiver and sender about the attempted attack because it's difficult to detect a quantum system without disturbing it [12].

2.3 LIMITATIONSAND CHALLENGES OF QUANTUM CRYPTOGRAPHY

Despite the distinct attributes of quantum cryptography in securing communication in this recent period of quantum computing, there are some limitations and challenges it possesses. The practical application of quantum key distribution systems is a main limitation of quantum cryptography. These systems frequently need specialized hardware due to their sensitivity to external disturbances such as temperature variations and noise which can cause errors. Another challenge is the limited range of quantum communication systems. Over distance, quantum information tends to lose its value as a result of factors such as transmission losses. This makes long-distance quantum communication to be challenging. However, researchers are enthusiastically working on the development of quantum repeaters and other methods to improve quantum communication efficiencies [7]. Nonetheless, quantum-resistant cryptographic solutions are still in the initial levels of development. While multiple post-quantum cryptographic algorithms have proved to be efficient, they need to be subjected to extensive standardization and testing before they can be broadly implemented. The transition to quantum-resistant cryptographic systems from traditional types also positions logistical limitations because of the requirements for broad changes in existing protocols and infrastructure. Another promising aspect of quantum cryptography is post-quantum cryptography (PQC) [13].

3.0 POST QUANTUM CRYPTOGRAPHY

PQC are cryptographic algorithms that are resistant to attacks from both quantum and classical computers. These algorithms are presently being actively investigated and developed to prepare for the quantum computing era and tackle the security vulnerabilities introduced by quantum computers.PQC algorithmsrefer to classical cryptographic `problems` that are not solvable via polynomial time through classical or quantum computers. The problem hardness is represented by the computational complexity of an algorithm having the ability to solve it. In this case, there is no provision of attached benefits by a quantum computer to solve the hard problem existing at the core of a PQC protocol. The emergence of PQC algorithms arose based on the assumption that a possible attacker will have a reliable and large enough quantum computer to break down classical algorithms [9]. Thus, new cryptography algorithms must be tough enough to withstand quantum and classical computers to be viable in this era of quantum computing. The division of the algorithms into seven different categories is a function of the hard problem nature whose security depends on Code-based, Hash-based, Lattice-based, Isogeny-based, Multivariate, Graph-based cryptography, and Multi-Party Computation (MPC). The various families/categories of PQC regarding the proposed schemes based on preference are shown in Figure 5. The application of various candidates of each family has started prevailing globally in China, the United States, the European Union, and so on with the PQC standardization processes [14].

UNDER PEER REVIEW

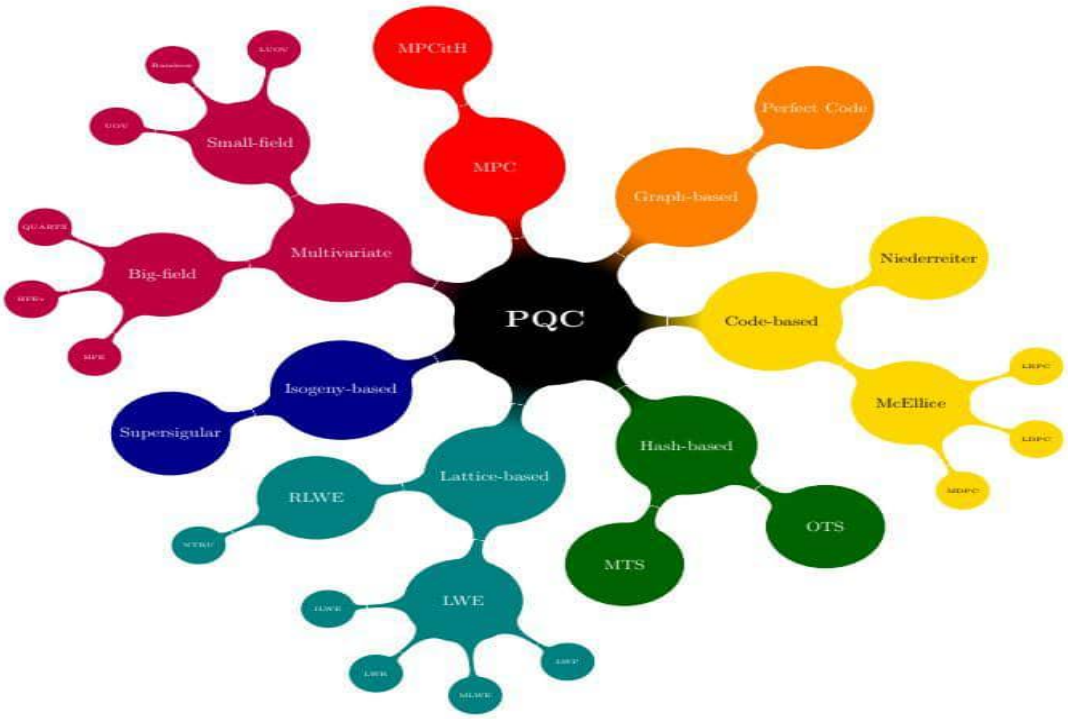

Figure 5: The various algorithm families/categories of PQC

UNDER PEER

3.1 Analyzing Classical Crypto Algorithm Vulnerabilities: A Quantum Computing SWOT Analysis

The various classical crypto algorithms include Rivest, Shamir, Adleman (RSA), Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), Diffie Hellman (DH) and Blowfish. RSA is a global standard algorithm thatappliesto common security infrastructure delivered by companies such as Nokia, Microsoft, and Cisco. It acts as a security strength for the aforementioned. AES is adopted for the provision of client/server encryption for web traffic in a related fashion. ECC is usually applicable in the field of the Internet of Things. Blowfish is another encryption algorithm thatpossesses a variable-length key that can be replaced with RSA. DH is peculiar for usage as an algorithm for secret key sharing among users [10]. The weaknesses and strengths of each of the algorithms are revealed in the process of applying them for quantum computing. Public Key algorithms are commonly applied for encryption purposes.

3.1.1 Rivest, Shamir, Adleman (RSA) Algorithm

RSA algorithms are purposely for the initiation of private key computation with a single public key using mathematical models without considering all the possible scenarios. The private key computation is via factoring in a number which is the product of two prime numbers. For instance, the multiplication of two prime numbers such as 7x3=21 can give a private key. The key length determines the algorithm's security [15]. RSA, for example, utilizes 2,048 bits which is equivalent to 617 decimal digits. This is indestructible by current computing capabilities, but quantum computers can break up into key pairs as long as the length of 4096-bit keys in just a few hours with the aid of Shor's algorithm. Figure 1 represents The SWOT analysis of RSA is presented in Figure 6 and this can be referred to as the Return of Copper Smith Attack (ROCA).

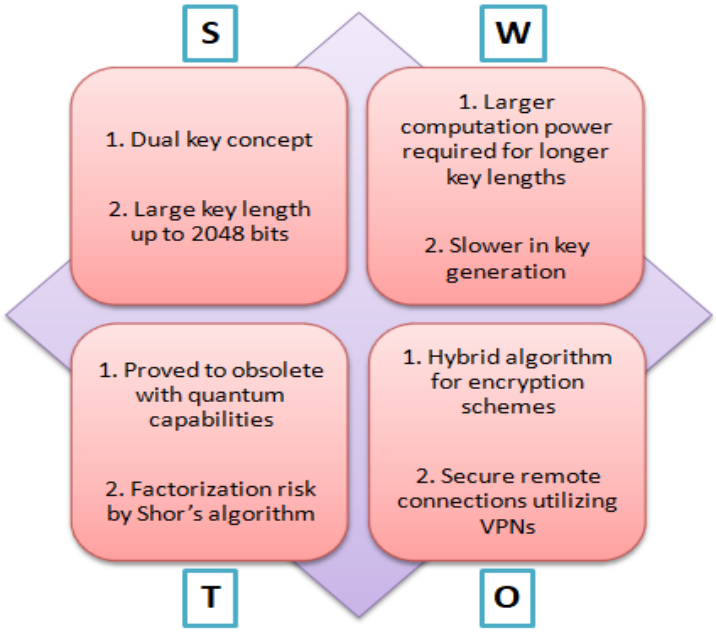

Figure 6: SWOT analysis of RSA

3.1.2 Elliptical curve cryptography (ECC) Algorithm

This cryptography algorithm type is adopted when the provision for security in innovative areas such as blockchain and the Internet of Things (IoT) is necessary. If an assumption of the asymmetric key of 80-bit size is made, then 1024 bits are needed by RSA while 60 bits are required for ECC. This makes elliptical curve keys to be lighter than longer keys. Shor's and Grover's Algorithm are a menace to ECC. Factoring is made easy by Shor's algorithm. This makes a private key discovery to be eventually certain by an intruder. Grover's algorithm enhances the ease of brute-forcing via the creation of uniform superposition over all the possible inputs, damagingly interfering with invalid states, and subsequently, finding inputs that satisfy the given function. Elliptical Curve Cryptography SWOT analysis is shown in Figure 7. A major limitation of ECC in quantum computing is its shorter key lengths. This makes it easier to crack than RSA for a quantum computer [16].

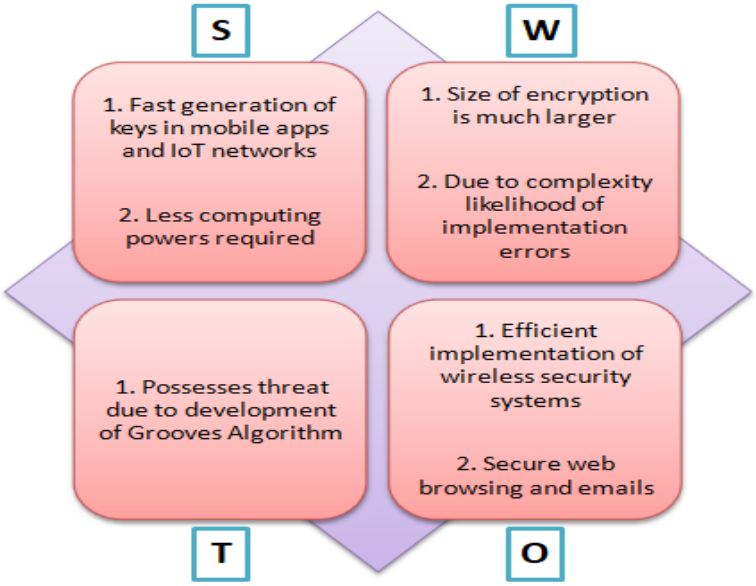

Figure 7: SWOT analysis of ECC

3.1.3 Advanced Encryption Standard (AES) Algorithm

This encryption algorithm type was first developed in 2001. AES comprises a block cipher that operates on symmetric key cryptography which provides integrity and confidentiality to the data. The key size commonly adopted in AES is 16 bytes or 128 bits. The operation was executed for 10 rounds. AES is a bit challenging to break using conventional computers as it requires 5x1021 years. However, the advent of post-quantum computing can make this be broken with the aid of Grover's Algorithm. AES SWOT analysis is presented in Figure 8. AES can be effective if the current key size is doubled [17].

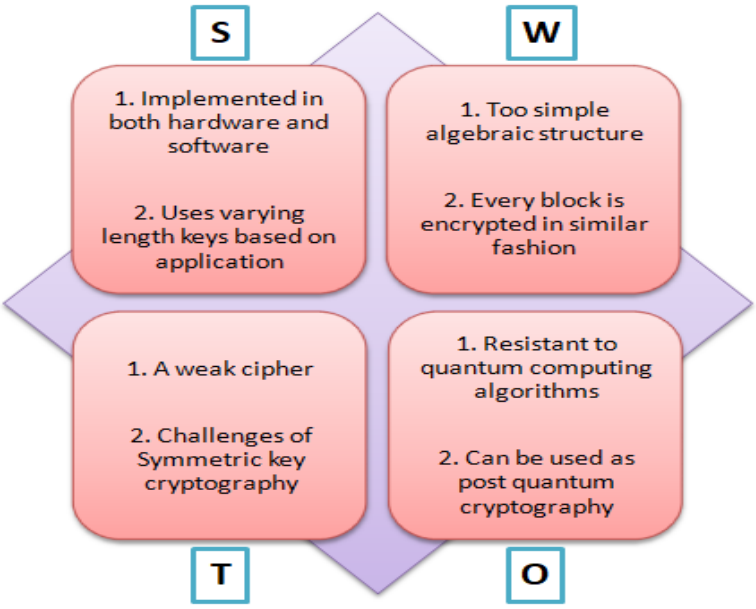

Figure 8: SWOT analysis of AES

3.1.4 Blowfish Algorithm

Blowfish Algorithm ranges between 32 and 448 bits, comprises of symmetric cryptographic block cipher, and was created in 1993 by Bruce Schneier. It possesses higher efficiency than the usually adopted algorithms (such as DES, AES, and RSA) and has lower power consumption and less time. It can generate longer keys such that each key also generates sub-keys. In return, each generated sub-key is fairly different from one another. In this manner, a much longer key is created which prevents any form of attack and increases the complexity. Atthe present moment, there is no evidence showing the Blowfish algorithm being hacked. The blowfish algorithm will only be broken by a factor of one or two despite quantum computing technology. The blowfish algorithm is reliable with the use of a longer key even with the advent of QC. A typical example is changing to a 256-bit key in quantum when compared to 128-bit in classical [18]. The Blowfish SWOT analysis is presented in Figure 9.

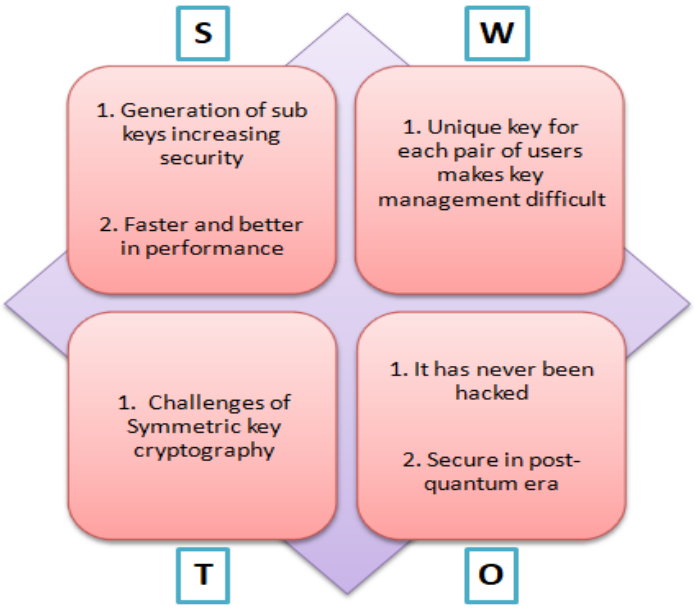

Figure 9: Blowfish SWOT analysis

UNDER PEER REVIEW

3.1.5 Diffie-Hellman Algorithm

The Diffie-Hellman Algorithm was first developed by Martin Hellman and Whitefield Diffie in 1976. Diffie-Hellman key exchange aimed to make provision for not only the key agreement but also exchange limitation that is impossible with the use of other encryption methods. The mechanism involves decision-making by two users upon a key pair. The public key is shared to communicate with each other over an insecure channel once the previous assignment is executed. No knowledge is required by the receiver or sender about the person on the other side of the network link [13]. The only limitation is the system's susceptibility to eavesdropping especially for man-in-middle attacks, and outsider and insider attacks. This was due to the inability to authenticate the users. Asidefrom this, this method can be rendered useless by Shor's algorithm via the cracking of its factorization in no time. Figure 10 presents the SWOT analysis of Diffie-Hellman [19].

UNDER PEER REVIEW

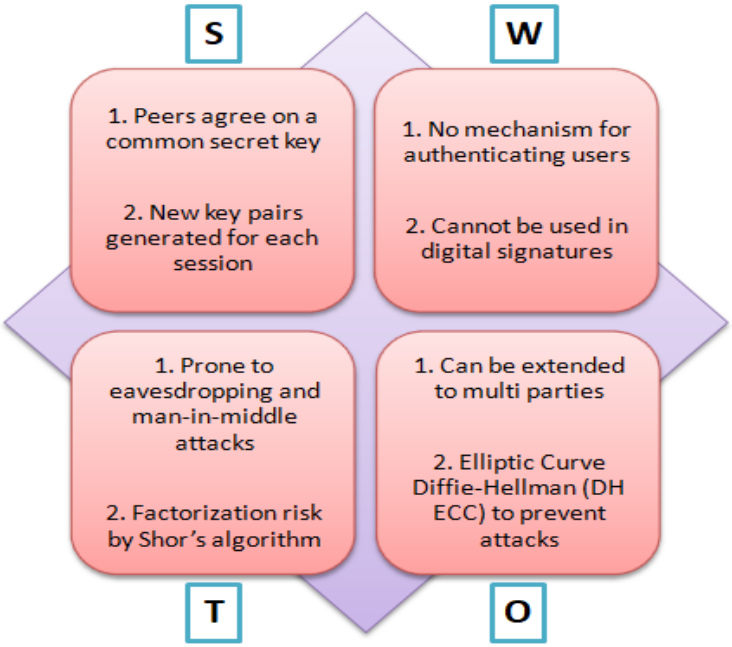

Figure 10: SWOT analysis of Diffie-Hellman

4.0 CONCLUSIONS

The use of a hyper-connected paradigm has become unavoidable because of the inestimable advantages attached to it. The use of quantum computing was recently adopted to improve the efficiency of cryptography previously used for cybersecurity. This paper discussed the concepts of cryptography, cyber security, and quantum computing. The mechanisms of cryptography in cyber security together with its transition into quantum cryptography were discussed. Characteristics of quantum information and quantum communication systems were stated. Post-quantum cryptography as a means of handling the challenges accorded with the use of quantum cryptography was discussed. Finally, consideration was given to the development and applications of the SWOT framework for various kinds of crypto algorithms. In conclusion, the use of quantum cryptography has found wide applications in cyber security. Also, post-quantum cryptography has been proven to be effective in handling issues arising from the use of quantum cryptography in securing information from being accessed by a third party.

UNDER PEER REVIEW

REFERENCES

[1] Shen J, Zhou T, Chen X, Li J, Susilo W. Anonymous and Traceable Group Data Sharing in Cloud Computing. IEEE Transactions on Information Forensics and Security. 2018; 13, 4, 912-925.

[2] Shen J, Shen J, Chen X, Huang X, Susilo W. An efficient public auditing protocol with novel dynamic structure for cloud data. IEEE Transactions on Information Forensics and Security. 2017; 12, 2402–2415.

[3] Gupta A, Kaur Walia N. Cryptography Algorithms: A Review. International Journal of Engineering Development and Research (IJEDR). 2014; 2, 2, 1667-1672.

[4] Mavroeidis V, Vishi K, Zych MD, Josang A. The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications (IJACSA). 2018; 9, 3, 34-46.

[5] Bartolucci S, Birchall P, Bomb´ın H, Cable H, Dawson C, Gimeno-Segovia M, Johnston E, Nickerson KKN, Pant M, Rudolph FPT, Sparrow C. Fusion-based quantum computation. Nature Communications. 2023; 14(1):912.

[6] Babbush R, McClean JR, Newman M, Gidney C, Boixo S, Neven H. Focus beyond quadratic speedups for error-corrected quantum advantage. PRX Quantum, 2021; 2(1), 27-39.

[7] Hoefler T, Haner T, Troyer M. Disentangling hype from practicality: On realistically achieving quantum advantage. Communications of the ACM. 2023; 66(5):82–87.

[8] Maslov D, Jin-Sung K, Bravyi S, Yoder TJ, Sheldon S. Quantum advantage for computations with limited space. Nature Physics. 2021; 17(8):894–897.

[9] Zlokapa A, Villalonga B, Boixo S, Lidar DA. Boundaries of quantum supremacy via random circuit sampling. npj Quantum Information. 2023; 9(1):36-49.

[10] Soni KK, Rasool A. Cryptographic attack possibilities over RSA algorithm through classical and quantum computation. International Conference on Smart Systems and Inventive Technology (ICSSIT). 2018; 11–15.

[11] Yasuda T, Dahan X, Huang YJ, Takagi T, Sakurai K. A multivariate quadratic challenge toward post-quantum generation cryptography. ACM Commun. Comput. Algebra. 2015; 49, 3, 105–107.

[12] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Commun. ACM. 1978; 21, 2, 120–126.

[13] Merkle R, Hellman M. Hiding information and signatures in trapdoor knapsacks. 1978; IEEE Transactions on Information Theory, 24, 5, 525–530.

[14] Wu Y, Bao WS, Cao S, Chen F, Chen MC, Chen X, Chung TW, Deng H, Du Y, Fan D, Gong M. Strong quantum computational advantage using a superconducting quantum processor. Phys. Rev. Lett. 2021; 127, 180501.

[15] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, Biswas R, Boixo S, Brandao FGSL, Buell DA. Quantum supremacy using a programmable superconducting processor. Nature. 2019; 574, 7779, 505–510.

[16] Ekert AK. Quantum cryptography based on bell's theorem. Phys. Rev. Lett. 1991; 67, 661–663.

UNDER PEER REVIEW

[17] Yadav SP, Singh R, Yadav V, Al-Turjman F, Kumar SA. Quantum-Safe Cryptography Algorithms and Approaches: Impacts of Quantum Computing on Cybersecurity. 2023; Walter de Gruyter GmbH & Co KG.
[18] Rangan KK, Abou Halloun J, Oyama H, Cherney S, Assoumani IA, Jairazbhoy N, Ng SK Quantum computing and resilient design perspectives for cybersecurity of feedback systems. IFAC-Papers OnLine. 2022; 55(7), 703-708.
[19] Said D. Quantum Computing and Machine Learning for Cybersecurity: Distributed Denial of Service (DDoS) Attack Detection on Smart Micro-Grid. Energies. 2023; 16(8), 3572.

UNDER PEER REVIEW