As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(01): 141-146, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0801024
Available online at: http://www.ijmtst.com/vol8issue01.html

Review on Cryptography Using Quantum Computing

Ankita Pathare[1] | Dr. Bharti Deshmukh[2]

[1]Assistant Professor, Department of Computer Science, Prerna College of Commerce, Nagpur, MS, India.
[2]Assistant Professor, Department of Computer Application, Prerna College of Commerce, Nagpur, MS, India.

To Cite this Article
Ankita Pathare and Dr. Bharti Deshmukh. Review on Cryptography Using Quantum Computing. *International Journal for Modern Trends in Science and Technology* 2022, *8* pp. 141-146. https://doi.org/10.46501/IJMTST0801024

Article Info
Received: 02 December 2021; Accepted: 03 January 2022; Published: 08 January 2022.

ABSTRACT

Modern cryptographic algorithms are based on the basic process of calculating large integers to their primes, which is said to be "uncomfortable". But modern cryptography is susceptible to both technological advances in computing power and the development of mathematics to rapidly reverse large integer factorization. The solution, therefore, is to introduce quantum physics into the cryptography, leading to the evaluation of quantum cryptography. Quantum cryptography is one of the emerging topics in the field of computer industry. This article focuses on quantum cryptography and how this technology makes a valuable contribution to an intensive defence strategy of completely secure key distribution. The scope of this article covers the weaknesses of modern digital cryptographic systems, the basic concepts of quantum cryptography, the practical implementations of this technology, and its limitations. , and finally the future direction that quantum cryptography is headed. We describe the result of an apparatus and protocol designed to perform quantum key distribution, whereby two users do not share any secret information (no private or public keys are known). previously known) initially exchanges a random quantum transmission consisting of very weakly polarized light rays. In particular, readers can explore the following topics in depth: current cryptographic schemes (symmetric and asymmetric), the difference between quantum and classical computing, challenges of quantum computing, quantum algorithms (Shor and Grover), public key cryptographic schemes affected, symmetry affected schemes, impact on hash functions and post-quantum cryptography.

KEYWORDS:Quantum computers, post-quantum cryptography, Shor's algorithm, Grover's algorithm, asymmetric cryptography, symmetric cryptography.

1.INTRODUCTION

There is no doubt that advances in technology and especially electronic communication have become one of the main technological pillars of the modern era. The need for confidentiality, integrity, authentication, and non-repudiation in data transmission and storage makes cryptography one of the most important branches of information technology. Cryptography, derived from the Greek word hidden and written, is the process of securing data in transit or stored by third-party adversaries. There are two types of cryptographic systems; symmetrical and asymmetrical. The theory of quantum computation, first introduced as a concept in 1982 by Richard Feynman, has been the subject of extensive research and is arguably the destroyer of modern asymmetric cryptography. Currently. Furthermore, it is a fact that symmetric cryptography can also be affected by specific quantum algorithms; however, its security can be increased with the use of larger key spaces. In addition, algorithms that can break current asymmetric cryptographic schemes whose security is based on the difficulty of computing

large primes and the discrete logarithm problem have been introduced. It seems that even elliptic curve cryptography currently considered the most secure and efficient scheme is weak against quantum computers. Thus, the need for robust cryptographic algorithms for quantum computations arose. The remainder of the original article deals with symmetric cryptographic analysis, hash functions. In particular, emphasis is placed on algorithms that take advantage of the difficulty of computing large primes, as well as the discrete logarithm problem. We continue our introduction to quantum mechanics and the challenge of building a real quantum computer. we introduce two important quantum algorithms that can have a huge impact in asymmetric and less symmetric cryptography, the Shor algorithm and the Grover algorithm, respectively [1]. Finally, post-quantum cryptography is presented. In it, the focus is on the analysis of the distribution of quantum keys and some mathematical solutions such as network-based cryptography, multivariable-based cryptography, hash-based cryptography, and hash-based cryptography.

The Quantum cipher recently caused a stir when members of the European Union announced plans to invest $13 million in the research and development of a secure communication system based on this technology. The system, called SECOQC (Secure Communication Based on Quantum Cryptography), will serve as the strategic definition against the Echelon intelligence collection system used by the US, Australia, UK , Canada and New Zealand. In addition, a number of quantum information processing companies, including MagiQ Technologies and Quantum ID, are implementing quantum cryptographic solutions to meet the needs of businesses, governments and other organizations, where preventing unauthorized disclosure of information has become a key success factor in maintaining a competitive edge over competitors. While modern cryptographic systems are said to be very efficient, in other words, they are said to be "unattractive", so why should so much money be spent on developing a cryptographic system?

2.RELATED WORK

[3] discussed the timeline of quantum computing and also described quantum computing and quantum bits and different algorithms derived from computation. quantum.

[4] discussed various proposals for making qubits such as superconducting loop and Josephson junction, liquid state nuclear magnetic resonance (NMR) and so on.

[5] explains that we may never see quantum computers working again, because he says that several decades is the maximum lifespan of any science and technology bubble what great. Also, over time, the people who come up with this technology will become older and less enthusiastic, and the younger generation will look for something completely new and possibly successful.

[6] discussed the postulates of quantum mechanics, polarization, and entanglement, and explained how quantum computing can be used to communicate.

[7]suggested the potential of quantum computing in drug discovery.

[8] demonstrated that in location-based cryptography, the overall security of the system can be broken by an attacker, and they also propose and implement a complete listening condition. perfect for position-based quantum cryptography.

[9] discussed quantum displacement, its applications, future aspects of quantum displacement, and the pros and cons of quantum displacement

3.QUANTUM CRYPTOGRAPHY IN THEORY

Instead of relying on the intricacies of computing large numbers, quantum cryptography is based on the fundamental and invariant principles of quantum mechanics. According to the Heisenberg uncertainty principle, it is not possible to measure the quantum state of a system without affecting the system, so only the polarization of a photon or a particle of light 'at time' can be known. it is measured. This principle plays an essential role in preventing eavesdropping attempts in a cryptosystem based on quantum cryptography. Second, the principle of photon polarization describes how photons of light can be oriented or polarized in specific directions. In addition, a correctly polarized photon filter can only detect one polarized photon, otherwise the photon would be destroyed. as well as the Heisenberg uncertainty principle make quantum cryptography an interesting choice for ensuring data secrecy and defeating the undisciplined. Charles H.

Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984 as part of a study between physics and information. Bennet and Brassard show that an encryption key can be generated depending on how many photons reach the receiver and how they are received. [10]. Their belief corresponds to the fact that light can behave with properties of particles beyond light waves. These photons can be polarized in many different directions, and these orientations can be used to represent bits including bits and zeros. These bits can be used as a reliable method to form blocks of points and support systems like PKI by securely issuing keys. The representation of bits through polarized photons is the foundation of quantum cryptography, which serves as the fundamental principle for the distribution of quantum keys. So, while the strength of modern digital cryptography depends on the computational difficulty of computing large numbers, quantum cryptography is completely dependent on the laws of physics and not to the processing capabilities of current computer systems. yes, quantum cryptography provides an answer to the problem of uncertainty faced by current cryptography; It is no longer necessary to make assumptions about the computing power of malicious attackers or develop a theorem to quickly solve the problem of factorization of large integers.

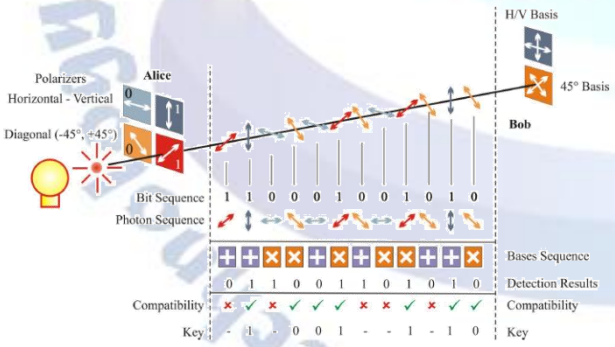

Figure 1- Key exchange in the BB84 protocol implemented with polarization of photons

4.PRESENT CRYPTOGRAPHY

A. Symmetric Cryptography

In symmetric cryptography, the sender and receiver use the same secret key and the same cryptographic algorithm to encrypt and decrypt data. For example, Alice can encrypt a clear text message using her shared secret key, and Bob can decrypt the message using the same cryptographic algorithm Alice used and the same encryption algorithm. a shared secret key. The key should be kept secret, which means that only Alice and Bob should know it; therefore, there is a need for an efficient means of exchanging secret keys over public networks. Asymmetric cryptography was introduced to solve the key distribution problem in symmetric cryptography. Popular symmetric algorithms include the Advanced Encryption Standard (AES) and the Data Encryption Standard (3DES).

B. Asymmetric Cryptography

Asymmetric cryptography or public key cryptography (PKC) is a form of encryption in which keys are provided in pairs. Each party must have its own private and public key. For example, if Bob wants to encrypt a message, Alice will send her public key to Bob then Bob can encrypt the message using Alice's public key. Bob then transmits the encrypted message to Alice, who can decrypt the message with her private key. Therefore, we encrypt the message with the public key, and only the person with the private key can decrypt the message.

Asymmetric cryptography is also used for digital signatures. For example, Alice can digitally sign a document with her private key, and Bob can verify the signature with a public key that Alice already knows. The security of PKC depends on computational problems such as the difficulty of computing large primes and the discrete logarithm problem. These types of algorithms are called one-way functions because they are easy to compute in one direction but difficult to invert.

i. *Factorization Problem*- RSA Cryptosystem: One of the most important public key schemes is RSA invented in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman. RSA exploits the difficulty of computing bireme numbers. According to Paar and Pelzl, RSA and asymmetric algorithms in general are not intended to replace symmetric algorithms because they are computationally expensive. RSA is mainly used for secure key exchange between end nodes and is often used with symmetric algorithms such as AES, where the symmetric algorithm performs data encryption and decryption. Kirsch states that RSAis theoretically vulnerable if a fast factorization algorithm is introduced or if a large increase in

computing power can exist. The latter can be achieved with the use of quantum mechanics on computers, known as quantum computers.

ii. *Discrete Logarithm Problem (DLP)-* Asymmetric cryptographic systems such as Diffie Hellman (DH) and Elliptic Curve Cryptography (ECC) are based on DLP. The difficulty in breaking these cryptosystems is based on the difficulty of determining the integer r such that gr = x mod p. The integer r is called the discrete logarithm problem of x with base g, and we can write it as r = log x mod p The discrete logarithm problem is a very difficult problem if the parameters are sufficient. large.

C. Desirable QKD Attributes

Essentially, QKD offers a technique for reaching agreement on a random bit sequence shared in two separate devices, with a very low probability that other devices (spies) will be able to infer succeed on the value of these bits [11]. In effect, such strings are then used as secret keys to encrypt and decrypt messages between the two devices. Seen from this perspective, QKD is clearly a key distribution technique and one can judge the strengths of QKD against some of the important purposes of key distribution.

- Confidentiality of Keys
- Authentication
- Sufficiently Rapid Key Delivery
- Robustness
- Distances and Location Independence
- Resistance to Traffic Analysis

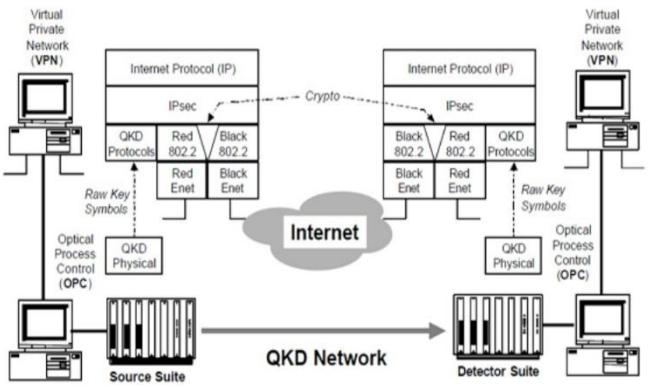

Figure 2- QKD Protocols

D. QKD Protocols Implementation

Quantum cryptography involves a surprisingly elaborate suite of specialized protocols, which we term "QKD protocols." Many aspects of these protocols are unusual – both in motivation and in implementation – and may be of interest to specialists in communications protocols.

i. *Sifting-* Filtering is the process by which Alice and Bob remove all obvious "q bits in error" from a sequence of pulses, photons are lost during transmission, and so on. They also include symbols where Alice chooses one base to transmit but Bob chooses the other to receive.

ii. *Error Correction-*Error correction allows Alice and Bob to identify all the "error bits" among their shared and filtered bits, and corrects them so that Alice and Bob share the same sequence of corrected bits. Error bits are those that Alice transmits as 0 but Bob receives as 1, or vice versa. These bit errors can be caused by noise or by the gutter. Therefore, there is a very strong incentive to design error detection and correction codes that reveal as little as possible in the public control traffic between Alice and Bob.

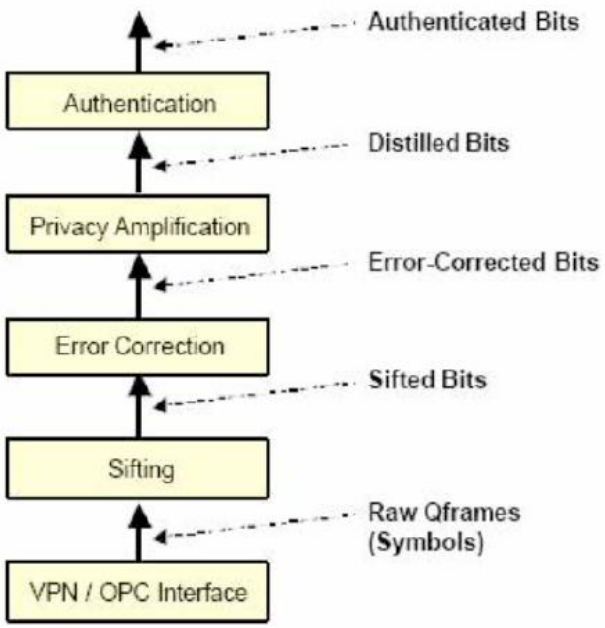

Figure 3- The QKD protocol Stack

iii. *Privacy Amplification-* Privacy enhancement is the process by which Alice and Bob reduce Eve's knowledge of their shared bits to an acceptable level. This technique is also commonly referred to as benefit distillation.

iv. *Authentication-* Authentication allows Alice and Bob to guard against "man-in-the-middle attacks", i.e., allows Alice to ensure that she is communicating with Bob (not Eve) and vice versa.[12]

Authentication must be ongoing for all traffic key management, since Eve can join the conversationbetween Alice and Bob at any stage in their communication. BB84's original paper described the authentication problem and outlined a solution based on popular families of hash functions, introduced by Wegman and Carter. Another important point: just authenticating the QKD protocols is not enough; We also need to apply these techniques to authenticate VPN traffic.

5.APPLICATIONS OF QUANTUM COMPUTING

Well, we know quantum computer systems are fantastic due to their houses like superposition and entanglement. However, it's miles critical to recognize that we stay in a quantum global and that quantum computer systems will permit us to higher simulate the conduct of nature, right all the way down to the molecular stage. For example, we will now make inroads in drug improvement and medicinal drug, have a take a observe the caffeine molecule. For scientists, it presently calls for an excessive amount of processing energy to nicely simulate this molecule and examine its structure. With quantum computing, scientists ought to higher simulate the caffeine molecule and its actual conduct on the molecular stage withinside the presence of quantum factors. In addition to medicinal drug and chemical analysis, quantum computing is likewise beneficial for packages in lots of different fields. used to boost up synthetic intelligence and gadget mastering to higher apprehend records models. It may be utilized in finance to construct extra best portfolios and determine the market. It may be utilized in robotics and precision manage principle to navigate complicated spaces. Overall, quantum computing is right for optimization and modelling in general. Therefore, whilst we aren't but fault tolerant (mentioned below), because the variety of qubits increases, quantum computer systems can enlarge their packages to many industries

6.FUTURE SCOPE AND CONCLUSION

In today's world, where information plays a particularly important role, the transmission and storage of data must be as secure as possible. algorithm (3DES, AES). Year after year, it looks like we're getting closer to to create a fully functional General Purpose Quantum Computer that can use powerful quantum algorithms like the Shor Algorithm and Grover Algorithm. DARPA is now starting to build multiple QKD links that weave into the global QKD network connecting its QKD endpoints through a grid of QKD relays or routers. When a certain point-to-point QKD link in the relay grid fails - fibre optic cutting or too much tone or noise reduction causes the connection to drop and be replaced by another. This emerging DARPA quantum network can be designed to be resilient even in the face of active listening or other denial of service attacks. Although there have been significant advances in the field of quantum cryptography over the past few decades, there are still challenges ahead before quantum cryptography can become an implemented key distribution system. widely available to governments, businesses and citizens.

Specifically, these challenges include the development of more advanced hardware to enable better quality and longer transmission distances for quantum key exchange. However, advances in computing power and the threat of obsolescence of today's cryptographic systems will remain the driving force behind the continued research and development of quantum cryptography. In fact, nearly $50 million in public and private funds is expected to be invested in quantum crypto technology over the next three years. Quantum cryptography is still in its infancy and so far, looks very promising. This technology has the potential to make a valuable contribution to e-commerce and business security, personal security, and the security of government organizations. If quantum cryptography finally lives up to some of its expectations, it will have a profound and revolutionary effect on all of our lives.

REFERENCES

[1] L. Pashaie, M. Bahrami, J. Karimpour and M. Jamali. “An Introduction to Distributed Cryptography Based on Quantum Cryptography.” International Journal of Soft Computing and Software Engineering, 2(8), 2012, pp.61-71.

[2] V.Mavroeidis, K.Vishi, M. D. Zych and A.Jøsang.“The Impact of Quantum Computing on Present Cryptography (IJACSA)”. International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018.

[3] J. Singh, M. Singh. " Evolution in Quantum Computing ", 5th International Conference on Systems Modeling & Advances in Research Trends, 2016.

[4] M.Steffen, D. DiVincenzo, J. Chow, T.Theis and M.Ketchen, "Quantum Computing: An IBM Perspective", IBM J.Res. and Dev.2011, and Réseau, 2014.
[5] M.Dyaknov."The Case Against Quantum Computing IEEE Spectrum.", 2019.
[6] G. Arun and V. Mishra. "A Review of Quantum Computing and Communication", International Conference on Trends Emerging technologies in electronics, communication and networking, 2014.
[7] Y. Cao, J. Romero and A.AspuruGuzik, "The Potential of Quantum Computing for Drug Discovery", IBM J.Res. & Dev. 62 (6): 16, 2018.
[8] S. Gupta, K. Sau, J. P.Swarnava, R. Ahamed and Rahul Biswas, "Quantum Computing of Perfection Eavesdropping in Place and Electromechanical Engineering", Conference (IEMECON), 2017.
[9] S. Singhal, A. Jain, A.Gankotiya and k. Aggarwal, "An Survey of Quantum Teleportation", Second international conference on advanced computer and communication technologies, 2012.
[10] C. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.
[11] C. Doyle. In: The adventure of the dancing men, Strand Magazine, 26, 602-617; reprinted in W. S. Baring-Gould (ed), The Annotated Sherlock Holmes, Vol. I1 (New Jersey: Wings Books), 1992, pp. 527-545.
[12] D. Deutsch, A.Ekert, R.Jozsa, C.Macchiavello, S. Popescu, and Anna Sanpera"Phys. Rev. Lett. 77, 2818 – Published 23", 1996.