Quantum Cryptography - The Future of Communication and Internet Security

Author

Kumari Neha
Assistant Professor / PhD. Research Scholar
B.R.M.College , Munger/ Patna university
Email ID: singh.neha624@gmail.com
Phone no.: 7300080964, 8789662562

Mailing Adress:
Kumari Neha
Department of Physics
B.R.M. College, Madhopur
Munger, Bihar
Pin – 811201

Co-Author

Dr. Amrita
Assistant Professor
Patna Women's College
Patna University
Email ID: amrita.phy@patnawomenscollege.in
Phone no: +91 93341 61253

Mailing Adress:
Dr. Amrita
Department of Physics
Patna women's College
bailey road, Patna
800001 Bihar

Abstract

Cyberspace has become the most popular carrier of information exchange in every corner of our life, which is beneficial for our life in almost all aspects. With the continuous development of science and technology, especially the quantum computer, cyberspace security has become the most critical problem for the Internet in near future. In this paper, we focus on analyzing characteristics of the quantum cryptography and exploring its advantages of it in the future Internet. It is worth noting that we analyze the quantum key distribution (QKD) protocol in the noise-free channel. To include real practical stimulators, there are developed various QKD Schemes for the noisy channels. Here we develop the unconditional security of quantum cryptography theoretically, which is suitable for the Internet as ever-increasing challenges are inevitable in the future.

Quantum key distribution (QKD) uses individual light quanta in quantum superposition states to guarantee unconditional communication security between distant parties. In practice, the achievable distance for QKD has been limited to a few hundred kilometers, due to the channel loss of fibers or terrestrial free space that exponentially reduced the photon rate. Also experimentally it is proved that the Satellite-based QKD promises to establish a global-scale quantum network by exploiting the negligible photon loss and decoherence in the empty space.

In this paper, we also give some introduction to various public-key cryptography and also touch on the various functions, advantages, and disadvantages of quantum cryptography and the need for quantum cryptography in the future as in data encoding, and digital signatures, and many more. It also covers the various securities issue of our current cryptography system. Different protocols BB84 i.e., the first QKD protocol also some other protocols, and finally the future directions of quantum cryptography followed by the conclusion of the paper.

Keywords: Quantum Cryptography, Cyberspace, Quantum key distribution, Digital signatures, Decryption, Encryption, Protocol, Internet security.

1. Introduction

Stephen Wiesner initially proposed the notion of quantum cryptography in the early 1970s. Quantum cryptography is centered on Heisenberg's uncertainty concept, which is one of quantum physics' foundational concepts. Our most well-known scientist demonstrated in 1900 that power in nature occurs as discrete little packets rather than a consistent flow, and every separate tiny pack is referred to as a quanta. Following that, Young demonstrated that light has a wave in nature. In addition, Einstein discovered that light acts like a particle in nature. Following that, Heisenberg introduced the Heisenberg Uncertainty Principle, stating that it is difficult to precisely know an electron’s motion and location. Einstein, Rosen, and Podolsky discovered that one of a pair's electrons may instantly and more quickly restore the state of the other electron.

Classical cryptography was the technique of concealed writing in the early years of cryptology. In traditional cryptography, the transmission of a message is safe till the encryption technique is not safe. The fundamental problems of classical cryptography are reverse engineering ideas and the hacking of encryption algorithm code. It is only used for the transmission of sensitive data along with military or government financial data. Classical procedures have a fairly restricted scope, but current cryptography is used by everybody and deals with safe online transactions, safe polling, and safe cloud services, among other things. All of these flaws in classical cryptography are being addressed in modern cryptography. With the expansion of the area of access keys and

advanced mathematical calculations, modern cryptography is always making strenuous efforts to limit the risk of eavesdropping. However, since the discovery of the quantum computer, the computing time has been drastically decreased, from millions of years in today's computers to seconds in quantum computers. The truth is that, in practice, security is a big concern for us in relati0on to the extremely restricted field of cryptographic technology. As a result, we must develop a powerful, safe master property that is less reliant on mathematical calculation and has a high number of keys. Quantum cryptography is defined as "unconditional security" constrained by a few hypotheses. Quantum key distribution is almost impenetrable to quantum computers. The mathematical complexity of a quantum key distribution model has no bearing on its level of security.

2. Quantum Cryptography

Quantum cryptography ensures the complete confidentiality of information. It is an encryption method in which the secret key is distributed completely out of secret communication.it uses principles of Quantum mechanics to generate the key by using the concept of entanglement of photons. This is not a complex mathematical problem but a sophisticated algorithm, or a unique form of hardware design that one or more mathematicians or specialist engineers can decipher.

2.1 Quantum bits (Qubits)

Quantum cryptography works through a quantum channel, which transports a physical item known as Quantum Bits also known as Qubits. Optical fiber cable is one form of a quantum channel, whereas the environment surrounding us is another. Qubits have a significant benefit over conventional bits in that they may be stated as a probabilistic intermediate between two boundaries of 0 and 1, whereas traditional bits can only be conveyed as 0 or 1. Quantum computers can

calculate orders of magnitude quicker than conventional computers. With the growth of high-speed laser optoelectronics, high-speed photons, wavelength, and time-division multiplexing, quantum cryptography becomes a quicker cryptosystem.

2.2 Quantum computing

The operation of quantum computers is based on the superposition principle of Quantum Physics to solve complex problems which are tough to solve through classical computing. Quantum computers use parallel computation, which involves scheduling and selecting a large number of microscopic processes focused on randomizing probability.

Quantum algorithms take a new approach to these sorts of complex problems by creating multidimensional spaces where the patterns linking individual data points emerge. Classical computers cannot create these computational spaces, so they cannot find these patterns, that's why quantum computers are faster than classical ones.

2.3 Quantum Key Distribution (QKD)

With the use of quantum physics, QKD creates a powerful safe key distribution strategy with limitless compute capacity, It implies cryptographic protocols involving quantum mechanics. The state of a system cannot be copied in quantum key distribution. Although a collective assault is a sort of collaborative attack, the Quantum key distribution technique is secure in opposition to such attacks.

2.4 BB84

The first quantum cryptography protocol is developed in 1984 by Charles Bennett and Gilles Brassard based on Heisenberg's Uncertainty Principle, and the name of the protocol is based on the author's name and the year of publication. As it is indicated in figure 1, Alice can transmit a

random secret key to bob, via QKD protocol, by sending photons and the secret key is encoded in their polarization. The no-cloning theorem guarantees that the eavesdropper eve cannot able to measure these photons and the photon transmits to the bob without any disturbance, which is not at all possible in classical cryptography or classical mode of transmission of information.

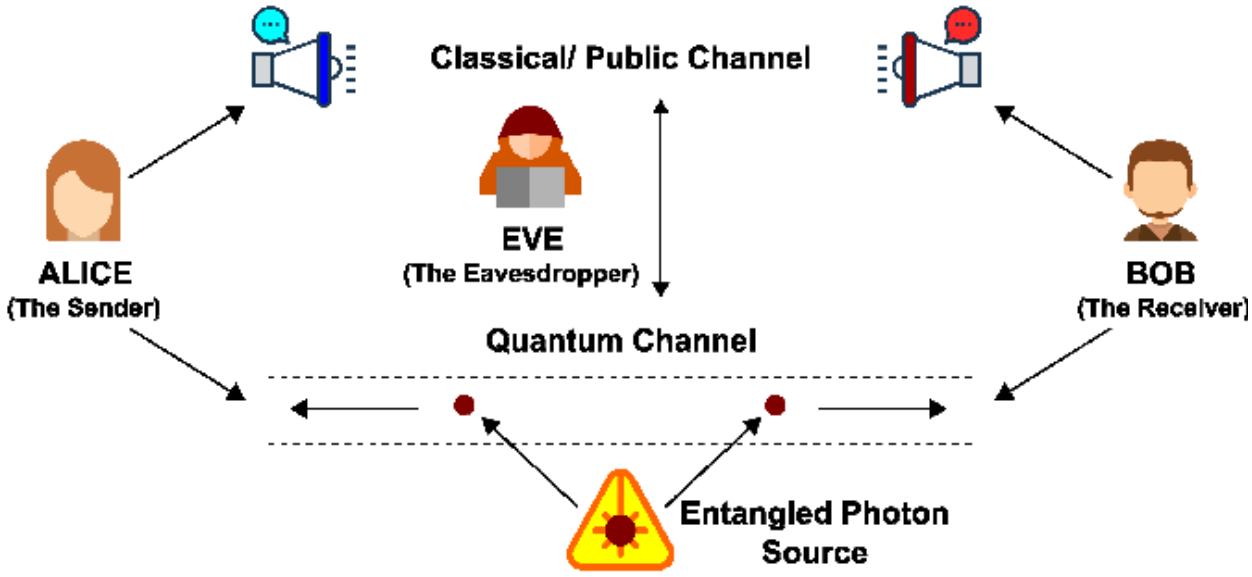

Figure 1

3. Modern Cryptography

One of the most basic requirements of our everyday lives is data security. Cryptography is a layer of data protection that protects secret information from being exposed to dangers. We require data protection while transmitting information across telecommunication networks. In symmetric-key cryptography, we have a number of strong methods for maintaining the secrecy and integrity of secret data throughout data transmission. IBM invented the first encryption algorithm in contemporary cryptography, known as the Data encryption standard (DES), for a symmetric cipher during the mid-1970s. Because the key size is very modest, DES has the benefit of being able to easily encrypt large amounts of data. However, DES was no longer regarded as secure since its weakest link is its short key size, which may be broken in as little as 24 days with dedicated gear.

Because the DES algorithm is employed 3 times, Triple DES (3DES) was designed for enhanced security in practice. Triple DES employs 3 keys, every one of which is 56 bits long. In 3DES, brute force search is nearly impractical and difficult to strike. For DES and triple DES, a larger block size is necessary for terms of efficiency, and there are currently no economical software codes accessible for DES or 3DES. Because the calculation time in DES is around 256, big memory space is necessary. Then, in 2000, Rijndael released another improved symmetric cipher called Advanced encryption standard (AES), which uses a larger key size for encryption. As a result, AES is becoming increasingly more secure than DES in terms of key size. The Rijndael cipher is used in AES. For 128-bit blocks of data, AES employs a key size of 192 bits, 128 bits, or 256 bits. In comparison, AES is quicker and more powerful. In the event of a birthday problem attack, AES is more secure than 3DES because AES utilizes 128-bit blocks whereas 3DES uses 64-bit blocks. However, a significant brute force assault weakens all symmetric keys. As a result, symmetric cryptosystems have the following advantages: they are quicker, they employ password authentication to confirm the receiver's identity, and only the sender has access to the secret key that can decode the messages. Although there are certain advantages, the cryptosystem is less safe when transmitting secret keys. Because symmetric cryptosystems do not give digital signatures, messages can be revoked, but asymmetric cryptosystems do not exchange keys; instead, the sender and recipient merely exchange two session keys. A one-time pad is a theoretically unbreakable encryption system that generates a real random key whose size is determined by the amount of the data to be encrypted. However, one of the most difficult issues is securing key sharing between two or more parties. Each end of a public-key cryptosystem (PKC) releases a pair of keys, one of which is the private key, and the other is the public key. The messages are encrypted into ciphertext by the public key, and the ciphertext is decrypted into plain text by the private key. It is not

computationally difficult to generate a public-private key combination, but it is computationally difficult to compute a private key using a public key.

Another property of PKC is the usage of a one-way function, which indicates that there is a unique inverse mapping from a domain to range. PKC's methods can all be solved in polynomial time. R. Rivest, A. Shamir, and L. Adleman created the RSA (Rivest-Shamir-Adleman) cryptosystem in 1977, where the block cipher employs integers in the range 0–n-1 and the block size $k < \log_2 n$. RSA is one of the most efficient and quick exponentiation methods. In terms of security, RSA can be harmed by a brute force assault. Table 1 shows how crypto techniques are classified based on the security services they provide. There are numbers of public-key cryptosystem developed so far;

3.1 Rabin cryptosystem

The Rabin cryptosystem is an asymmetric technique whose security depends upon the integer factorization. The decryption method is done by using the Chinese Remainder method. In a selected plaintext attack, the technique is secure, but in a chosen ciphertext attack, it is completely unsecure.

3.2 Knapsack cryptosystem

Knapsack algorithm is the first public key cryptosystem developed in 1978. In this algorithm, there are two different knapsack problems in which one is easy and the other one is hard. The easy knapsack is used as the private key and the hard knapsack is used as the public key. The easy knapsack is used to derive the hard knapsack. Although the procedure is a subset sum problem, it can be done in polynomial time. In 1984, Shamir already broke the knapsack system.

3.3 Elliptic curve cryptosystem (ECC)

Elliptic curves cryptosystem is a substitute to other main public key cryptosystems founded on integer or polynomial computing, which run out of memory while storing or processing big keys and messages. As a result, ECC has one of the most important computational benefits. When compared to any comparable public-key cryptosystem, like RSA (Rivest–Shamir–Adleman), elliptic curve cryptography can give a similar degree of security with smaller key sizes that are vulnerable to factoring.

See table 2

Despite all of the security concerns raised, key distribution, key creation, public key certifications, and key management are all infeasible in the public-key cryptosystem. Another option to protect our message-by-message authentication technique is to use a digital signature scheme that contains a MAC (message authentication code), hash functions (SHA, RIPEMD-160, HMAC, MD4, MD5, MD2), and a digital sign.

3.4 Cryptographic Hash function

A Cryptography hash function is the latest cryptosystem which is used by researchers, it is an algorithm that takes an arbitrary amount of input and produces a compact (fixed-sized) output in the form of coded text known as “hash value” or simply “hash”. The hash function may be used to achieve authentication and secrecy. Table-3 lists several known attacks on the hash function.

Security: All hash algorithms are connected to HMAC (Hash message authentication code), which is a type of MAC that provides client and server a shared private key that only known to them. In terms of security restrictions, the hash function is chosen based on processing speed.

The formula for HMAC:

HMAC = hashFunc(secret key + message).

3.5 MD5 (Message Digest 5)

MD stands for message digest, and Ronald Rivest invented MD5 in 1991. MD5 is broken cryptographically but still used for producing128-bit hash values, and the method comprises four rounds of 16-bit operations in the message block and buffer. MD4 and MD2 are two more MD series. MD5 is vulnerable to known attacks.

3.6 SHA-1 (Secure Hash Algorithm 1)

SHA was created by NIST and the NSA in 1993, and it was improved in 1995 to become SHA-1. SHA1 uses 160-bit hash values, with every set consisting of 20 stages. As a result, it is slower than MD5 and more difficult to brute force attack than MD5 (160: 128-bit hash values).

3.7 RIPEMD (RIPE Message Digest)

When several researchers in Europe were assaulted by MD4 or MD5, they created RIPEMD in 1992 which uses 2 equivalent lines of five rounds each with 16 stages and a 160-bit hash value. There are family of five functions in RIPEMD: - RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256 and RIPEMD-320. Of which RIPEMD-160 is the most common cryptosystem. The Corresponding to its computational complexity, RIPEMD-160 is both slower and more difficult to brute force.

3.8 Digital signature

During message transmission, a digital signature eliminates forgery and rejection. It is a mathematical technique used to verification and authenticity of any message. It is equivalent to a handwritten signature but in a proper manner and more secure. In a digital signature, the messenger first signs and encrypts the message based on the outcome of signing, then verifies the signature.

The advantage of RSA is that it can validate quicker in signing, but the downside is that the signer's processing capability is restricted. It works through public-key cryptography, The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key. But there are some limitations with the public key cryptography and confront certain difficulties also like random number generators, Advances in Quantum computers, Advances in computation power of CPU, and New attacks strategies.

4. Applications And Significance

The Quantum Cryptosystem outperforms symmetric and other public-key cryptosystems. Quantum cryptography is used in the majority of digital communication in our daily lives.

4.1 Advantages

Quantum cryptosystem is user friendly and because of its uniqueness very less resources are required for the operation of data transmission. As it is working in the principle of quantum mechanics it is nearly impossible to digitally destruction of the cryptosystem.

4.2 Disadvantages

In a recent scenario the reach of the quantum signal is restricted to around 90 miles and when we talk in terms of occupations quantum cryptography has the potential to eliminate a large variety of occupations and also actual resources.

4.3 Purpose of Quantum Cryptography

It is believed that by developing quantum cryptography researchers will be able to secure the confidentiality of the information, it will help in several methods like data encoding, Digital Signature, and Quantum internet. It will also be helpful in the advancement of the power grid,

ultra-secure voting, and also in the medical field like for the analysis of brain functions and also in the analysis and prediction of DNA structure.

5. Security Issues

5.1 How much secure is our current cryptography?

Security shelf lifetime(x-years), migration time(y-years), and collapse time(z-years) have a relationship that can forecast the cryptosystem state.

The term "security shelf lifespan" refers to how long our cryptographic keys must remain safe. The term "migration time" refers to the amount of time it will take to retool current infrastructure with a large-scale quantum-safe solution. The time it will take to build a large-scale quantum computer or make other advancements is referred to as the collapse time.

1: if $x + y > z$, then we will not be able to provide the required x years security.

2: if $y > z$, then the cyber system will collapse in z years with no quick.

5.2 Necessary condition for unconditional secrecy

Within the rules of Quantum Mechanics, a cryptosystem can be attacked by any third-party opponent for an indefinite amount of time or by computational equipment for an unlimited amount of time. The criterion for unconditional secrecy, according to the concept of privacy amplification, is that two end spots of a safe transmission channel exchange some unconditional secret bits. Sopt > 0, where Sopt is the ideal effective secrecy capacity, is the minimum requirement for sharing certain secret bits.

5.3 Common cryptographic attacks

Side-channel attacks are one of the most significant challenges to both conventional and quantum cryptography. Controlling the execution time and power consumption of cryptographic devices based on semiconductor logic gates and transistors are two key difficulties in modern cryptography.

A differential power analysis (DPA) attack is a form of passive attack that is based on a crypto device's power usage. At DPA, the protection of a smart card implementation by AES with 100 traces may be broken in a matter of minutes by around 50000 power traces. AES128 may be cracked in a matter of seconds, according to this assault.

In classical cryptography, a Passive side-channel attack is the same as a side-channel attack. A passive listener disrupts the quantum signal in QKD. Because it is a passive attack, it has no direct impact on security implementation. Listeners are looking for flaws in the current security system.

In an Active side-channel attack, the adversary attempts to directly change the security implementation and seeks to take advantage of the assumptions of the security proofing process.

Alice sends a quantum signal to Bob, light is reflected during transit across the quantum channel, it may be possible that the eavesdropper receives this reflected light. As a result, the knowledge about the key can be learned by the opponent. This type of attack is known as trojan horse attack. To counteract such attacks, spectral filters and optical isolators are utilized.

A single-photon detector is known as avalanche photodiodes (APDs). A photo detector's typical behavior can be changed or modified by a modest amount of light. The impact of this assault is that the detectors are changed into a counterfeit state that mimics the normal response. This is termed an attack on single-photon detectors.

6. Future of Digital Cryptography

Quantum cryptography can offer us more security, but it has one big drawback: it cannot be employed in the situation of private document signing with authentication. Quantum cryptography, it seems evident, could not have provided us with entirely secure communication. Currently, quantum cryptography cannot solve any of the traditional encryption techniques. Although the exchange of photons in key distribution gives unconditional security, safe encryption is achieved via traditional mathematical calculation approaches. NIST's (National Institute of Standards & Technology) future instruction to agencies is that they can employ NIST-recommended methods until new standard quantum resistance algorithms are implemented.

7. Conclusion

Quantum cryptography is a new type of encryption that works based on quantum mechanics and classical cryptography. Its most significant benefits over classical cryptography are unconditional security and sniffer detection. These qualities can solve significant cyberspace security challenges for the future Internet. Quantum cryptography ensures the security of many cyberspace applications (such as the Internet of Things and smart cities) for the future Internet. Quantum cryptography's unconditional security and sniffer detection are demonstrated in our experimental investigation as well. In the future it will help us to maintain cybersecurity.

References

1. Abbasi, F., & Singh, P. (2021). Quantum Cryptography: The Future of Internet and Security Analysis. *Journal of Management and Service Science*, *1*(1), 4.
2. Bedington, R., Arrazola, J. M., & Ling, A. (2017). Progress in satellite quantum key distribution. *npj Quantum Information*, *3*(1), 1-13.
3. Bhatt, A. P., & Sharma, A. (2019). Quantum cryptography for internet of things security. *Journal of Electronic Science and Technology*, *17*(3), 213-220.
4. Chen, C. Y., Zeng, G. J., Lin, F. J., Chou, Y. H., & Chao, H. C. (2015). Quantum cryptography and its applications over the internet. *IEEE Network*, *29*(5), 64-69.
5. Djordjevic, I. B. (2020). On global quantum communication networking. *Entropy*, *22*(8), 831.
6. Ekert, A. K. (1992). Quantum Cryptography and Bell's Theorem. In *Quantum Measurements in Optics* (pp. 413-418). Springer, Boston, MA.
7. Geihs, M., Nikiforov, O., Demirel, D., Sauer, A., Butin, D., Günther, F., ... & Buchmann, J. (2019). The status of quantum-key-distribution-based long-term secure internet communication. *IEEE Transactions on Sustainable Computing*, *6*(1), 19-29.
8. Kumar, A., Ottaviani, C., Gill, S. S., & Buyya, R. (2022). Securing the future internet of things with post-quantum cryptography. *Security and Privacy*, *5*(2), e200.
9. Liao, S. K., Cai, W. Q., Liu, W. Y., Zhang, L., Li, Y., Ren, J. G., ... & Pan, J. W. (2017). Satellite-to-ground quantum key distribution. *Nature*, *549*(7670), 43-47.
10. Lim, C. C. W., Xu, F., Pan, J. W., & Ekert, A. (2021). Security analysis of quantum key distribution with small block length and its application to quantum space communications. *Physical Review Letters*, *126*(10), 100501.
11. Mitra, S., Jana, B., Bhattacharya, S., Pal, P., & Poray, J. (2017, November). Quantum cryptography: Overview, security issues and future challenges. In *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)* (pp. 1-7). IEEE.
12. Muruganantham, B., Shamili, P., Ganesh Kumar, S., & Murugan, A. (2020). Quantum cryptography for secured communication networks. *International Journal of Electrical & Computer Engineering (2088-8708)*, *10*(1).
13. Petrache, A. L., & Suciu, G. (2020). Security in Quantum Computing. *Annals of Disaster Risk Sciences: ADRS*, *3*(1), 0-0.

14. Sasirekha, N., & Hemalatha, M. (2014). Quantum cryptography using quantum key distribution and its applications. *Int. J. Eng. Adv. Technol.(IJEAT)*, *3*(4).

15. Sharbaf, M. S. (2011, November). Quantum cryptography: An emerging technology in network security. In *2011 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 13-19). IEEE.

16. Singh, S. K., Azzaoui, A. E., Salim, M. M., & Park, J. H. (2020). Quantum communication technology for future ICT-review. *Journal of Information Processing Systems*, *16*(6), 1459-1478.

17. Zhang, D. Cyberspace Security for Future Internet.

18. Zhou, T., Shen, J., Li, X., Wang, C., & Shen, J. (2018). Quantum cryptography for the future internet and security analysis. *Security and Communication Networks*, *2018*.

Table-1: Security Service Vs. Mechanism

Services	Mechanism
Confidentiality	Encryption, Routing protocol
Authentication	Digital signature and encryption
Integrity	Encryption and Digital signature
Nonrepudiation	Digital signature and notarization
Access control	Access control mechanism and interactive poofs

Table-2: Comparison of the level of security in conventional computer and quantum computer

The algorithm in modern cryptography	Key size (in bits)	Level of security in bits (Conventional Computer)	Level of security in bits Quantum Computer)
RSA-1024	1024	80	~0
RSA-2048	2048	112	~0
ECC-256	256	128	~0
ECC-384	384	192	~0
AES- 128	128	128	~64
AES-256	256	256	~128

Table-2: Ratio of some Known attack

Hash function	Collision attack	(2nd) Preimage attack
MD2	$2^{63.3}$	2^{72}
MD4	3 operations	2^{102}
MD5	2^{18}	$2^{123.4}$
SHA-0	$2^{33.6}$	2^{160}
SHA-1	$2^{60.3}$	2^{160}
RIPEMD-160	2^{80}	2^{160}
SHA2-256	2^{128}	2^{256}
SHA2-512	2^{256}	2^{512}