IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 1)
Available online at: www.ijariit.com

A survey on quantum cryptography and quantum key distribution protocols

Maithili S. Jha
jhamaithili999@gmail.com
Manipal University, Jaipur, Rajasthan

Manish Kumar Nirmal
manishn@cdac.in
Centre for Development of Advanced Computing, Pune, Maharashtra

Samrit Kumar Maity
samritm@cdac.in
Centre for Development of Advanced Computing, Pune, Maharashtra

Jaya Krishna
jaya.krishna@jaipur.manipal.edu
Manipal University, Jaipur, Rajasthan

ABSTRACT

As quantum computing matures, it's going to bring unimaginable increases in computational power along with the systems we use to protect our data (and our democratic processes) will become even more vulnerable. It is often said that the power of quantum computer comes from the quantum parallelism, which means instead of processing each input one by one, processor process each input parallelly. Quantum mechanics allow us to do an operation on a superposition of all the possible inputs at the same time. The classical computers have enabled amazing things, but there are still some problems we can't easily solve like-2^N(optimization problems where it grows exponentially).For transferring the information the protocols are very essential for security. Example is quantum key distribution, and its protocols are like -BB84,SA RG04,B92 etc. Moreover, quantum cryptography has proved its standing against many weaknesses in the classical cryptography. One of these weaknesses is the ability to copy any type of information using a passive attack without an interruption, which is impossible in the quantum system.

Keywords— *Quantum cryptography, Quantum-key-distribution, Quantum-key-distribution protocols*

1. INTRODUCTION

Recently we have the cyber-attacks on the business world, the data breaches that lead to losses of hundreds of millions and in some cases billions of dollars at different companies like Home Depot, JP Morgan, Yahoo, and Target. It wouldn't take many large attacks to ravage the world economy. And the public sector has not been immune either there was a significant data breach at the US Office of Personnel Management. Security clearance and the fingerprint were compromised affecting 22 million employees. And the attempt by state-sponsored hackers to use stolen data to influence election outcomes in several countries.

Cryptography is considered as the art of producing a code, where encoding and decoding a plaintext by a secret key are the main process of the security operation. Cryptography has existed for a long time and encoding, and decoding messages were just used by military communications or as a highly secure connection between countries. After spreading out the communication technologies and sharing secure information between legitimate parties, the cryptography became the main goal in many experimental labs and institutions.

There are three main important things for encryption.

1. The Code (Encryption key or Password)
2. The Exchange
3. Encryption Algorithm

What makes encryption key and encryption algorithm so important that, if someone even captures the data or information, without having an encryption key or algorithm, they won't be able to read the data.

Consider one of the most widely used systems today- RSA. In 1977 it was invented, it was guessed that it would take 40 quadrillion years to crack a 426-bit RSA key. In 1994, just 17 years later, the code was ruptured. As computers become more and more powerful, we had to use larger and larger codes. Today we use 2048 or 4096 bits of RSA. Then introduce the law of Quantum cryptography system, which can block any eavesdropping attempt by the law of physics, compare to regular information exchange for daily life important data such as financial data in banking and sensitive information in the companies are generally been encrypted using the pre-determined secrete key before transmission over the network. Insecure communication to protect data, the sender uses secrete key to embed the data in a secure shell and receiver uses a same or different key to retrieve data from the secure shell. However, with the current communication, the eave's dropper can easily copy the transmitted data in the secure shell and there are many ways to find out the secrete keys and principles, so they can easily retrieve the original data. So, there is impossible to protect the data from eave's dropper.

Quantum cryptography system (QCS) is a perfect solution to protect such kind of eave's dropping attempt. In QCS banks and company distribute the secrete key using a quantum signal which is fragile like a bubble If the eave's dropper tries to find out the secrete key the quantum signal will be destroyed like a bubble and therefore eave's dropping is impossible in QCS. Also compare with the current encryption system, where the secrete key is been reused repeatedly .where as in QCS the new secrete key is generated continuously, we can refresh the secrete key within a second. Therefore, we can rest assured, our sensitive data will be securely transmitted by our QCS.QCS secret key will be guaranteed to be unique unlike RSA or other encryption keys.

The cutting edge of QCS will bring the revolutionary in the communication system by providing the perfect safety to the communication infrastructure for military, government, financial and medical institute.

1.1 Problems

- Keys based on pseudo-random numbers
- Current key exchange techniques will not stand up to a quantum computer.

2. QUANTUM CRYPTOGRAPHY

In 1970, Quantum Cryptography was first to forge by Stephen Wiesner and later his ideas were enlightened by Bennett in 1984. [3] This Quantum Cryptography is conscience on the values of quantum mechanics, the least level of matter and on the concept of using lightweight particles called photons or electron. Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best example of quantum cryptography is quantum key distribution which offers an information-theoretically secure solution to the key exchange problem, currently use popular public key encryption and signature schemes for RSA and EL Gamal can be broken by quantum adversaries and the advantage of quantum cryptography lies in the fact that allows the completion of many cryptographic tasks that are proven or conjectured to be impossible using only classical, that is non quantum communication. Recent hacking and data leak even in the top tech titans like Yahoo data hack, Facebook data leak and many other, has time and again proved that the current methods are inefficient and unreliable for the security of our most asset.

Advantages

- It is impossible to copy data encoded in a quantum state.
- It uses a Heisenberg's uncertainty principle.
- Cannot record any of the characteristics of a quantum system, before any of its characteristics are measured.

2.1 Quantum Key Distribution (QKD)

Advancement in communication technology has created a world of agile and more conducive exchange of information. Data that is essential to business operations needs to be accessible across departments and transferable to other companies that work within a network. QKD is the only transfer method that is provable secured by the laws of physics to help secure the sensitive data to deliver. QKD allows us to generate a secure key, so secret information can be sent securely from one location to another. It guarantees security where classical cryptography system cannot do.

2.2 How it works

1. The QKD relies on generating a random key and securely transmitting it separate from the encrypted data.
2. Key data is created by a quantum engine and transmitted as a stream of photons through a fiber optic quantum link.
3. Key is completely random and contains quantum information that can only be successfully read by the intended recipient.
4. If anyone tries to intercept the photon stream in the quantum link, any interruption or modification to the photons will alert the system to the unauthorized access.
5. The benefits of using secure fiber lines make sense in all protected communication.
6. Photo transmission is limited to about 60 miles, so this limitation is solved by creating a chain of QKD trusted nodes, spread across the country.

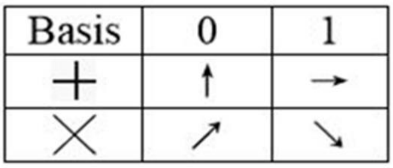
3. ANALYSIS OF KEY PROTOCOLS OF QUANTUM CRYPTOGRAPHY

3.1 BB84 Protocol

Bennet and Brassard proposed the quantum key distribution protocol for the first time in 1984 and familiarized as the BB84 protocol depended on Heisenberg Uncertainty principle. The components of the BB84 protocol are two bases that are to specify rectilinearly (R) and diagonal (D) and four states of polarized photons. A 0° polarization of photon in the rectilinear basis or 45° in the diagonal basis is used to represent a binary 0. A 90° Polarization in the rectilinear basis or 135° in diagonal basis is used to represent a binary 1 [4] [5].

Consider two individuals conventionally entitled Alice and Bob want to communicate and exchange information or message and an eavesdropper named Eve intercepts their communication.

When sender Alice A wants to send the key generated by the light particles of polarized photons to Bob B. receiver. She transfers each particular photon bit in an arbitrary way by selecting the two-arbitrary basis of polarized Photons either rectilinear or diagonal. Receiver Bob B may choose randomly the rectilinear or diagonal polarizer to calculate the photons received and inform the result to the sender through any insecure channel. After comparing the received bits from the receiver, finally, they discard the incorrect bits and make the right one as key.



Basis	0	1
+	↑	→
×	↗	↘

Fig. 1: BB84 Bit encodings

Bennett and Brassard in 1984, mentioned that the BB84 protocol involves the four states of polarization: Horizontal |h>, Vertical |v>, left circle polarized |lcp>, right circle polarized |rcp>. In these four states of polarization, Horizontal State of Polarization and the left circle state of polarization indicates a '0' and the Vertical state of polarization and right circle polarization indicate a'1'. [6].

3.2 BB92

The key difference in BB92 is that only two states are necessary rather than the possible 4 polarization states in the BB84 protocol. Figure 2: BB92 2-State Encoding, 0 can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis. The B92 protocol uses the same steps as of the BB84 based upon the Polarization of the states but uses only two non-orthogonal quantum state |h> represent a '0' and |rcp> represent a '1', half of the BB84 protocol to transmit the key. [6]

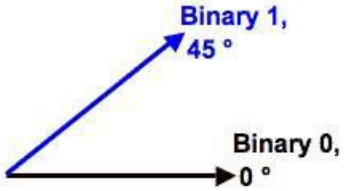


Fig. 2: BB92 Photon Polarization 2-State Encoding

3.3 SARG04 Protocol

The SARG04 protocol is built when a researcher noticed that by using the four states of BB84 with different information encoding them could develop a new protocol which would more robust when attenuated laser pulses are used instead of single-photon sources. SARG04 protocol was proposed in 2004 by Scarani et.al [7]. The SARG04 protocol shares the exact same first phase as BB84. In the second Phase when Client A and Client B determine for which bits their bases matched, Client A does not directly announce her bases rather than Client A announces a pair of non-orthogonal states one of which she used to encode her bit. If Client B used the correct basis, he will measure the correct state. If he chose incorrectly he will not measure either Client A states and will not be able to determine the bit. If there are no errors, then the length of the key remaining after the sifting stage is ¼ of the raw key.

The SARG04 protocol provides almost identical security to BB84 in perfect single-photon implementations: If the quantum channel is of given visibility (i.e. with losses) then the QBER of SARG04 is twice that of BB84 protocol and is more sensitive to losses.

However, SARG04 protocol provides more security than BB84 in the presence of PNS attack, in both the secret key rate and distance the signal can be carried (limiting distance).

3.4 Other Protocols

There are many other protocols in existence, both prepare, and measures and entanglement based. They are as follows:

3.4.1 KMB09 protocol: KMB09 protocol is an alternative quantum key distribution protocol [40]. Where Alice and Bob use two mutually unbiased bases with one of them encoding a “0” and the other one encoding a “1”. The security of the scheme is due to a minimum index transmission error rate (ITER) and quantum bit error rate (QBER) introduced by an eavesdropper. The ITER increase significantly for higher dimensional photon states. This allows for more Noise in the transmission line, thereby increasing the possible distance between Alice and Bob Without the need for intermediate nodes

3.4.2 S09 protocol: S09 protocol is quantum protocol based on public-private key cryptography for secure transmission of data over a public channel [9]. The security of the protocol derives from the fact that Alice and Bob each use secret keys in multiple exchanges of the qubit. Unlike the BB84 protocol [1] and its many variants. Bob Know the key to transmit, the qubits are transmitted in only one direction and classical information exchanged thereafter, the communication in the proposed protocol remains quantum in each stage. In the BB84 protocol, each transmitted qubit is in one of four different states in this protocol transmitted qubit can be in any arbitrary states.

3.4.3 S13 protocol: S13 protocol is a new quantum protocol [10] that is identical to the BB84 protocol for all the quantum manipulation, but differs from it by using Private Reconciliation from a Random Seed and Asymmetric Cryptography, thus allowing the generation of larger secure keys. The S13 protocol contains two communication channels, and these channels are the quantum and classical channels.

Table 1: Comparision table

Parameter	BB84	BB92	SARG04	KMB09	S09	S13
Founder	C.H.Bennett and G.Brassard	C.H. Bennett	Scarani.V, A. Acin, Ribordy G, Gisin N.	Muhammad Mubashir Khan, Michael Murphy and Almut Beige	Eduin Esteban Hernadez Serna	Eduin Esteban Hernadez Serna
Year	1984	1992	2004	2009	2009	2013
Number of states	4	2	4	2	Arbitrary states	4
Principals	Heisenberg	Heisenberg	Heisenberg	Heisenberg	Public private key	Heisenberg
Polarization	Orthogonal	Non-orthogonal	Orthogonal	Arbitrary	Bit-Flip Phase-Flip	2 orthogonal
DoS attack	Vulnerable	Vulnerable	Vulnerable	Vulnerable	N/A	N/A
Middle-Man attack	Vulnerable	Robust	Robust	Robust	Robust	N/A
PNS attack	Vulnerable	Vulnerable	It's better than BB84	Robust	N/A	N/A
Beam-Spilter attack	Vulnerable	Vulnerable	Robust	Robust	N/A	N/A
Security	Good for long distance	Average	Average	Average	Best for a small distance	Average
Efficiency	Low	Best	Average	Low	Good	Average

4. CONCLUSION

Here we have reviewed, why QKD is most reliable and how it can be implemented with the help of various protocols. QKD scheme is one of the most reliable QKD protocols as well as the most secure algorithm. In this survey show that the QKD protocol can stand against most of the well-known quantum attacks. In the comparison table, we can see that BB84 is more secured than any other protocols in terms of attacks and security, but S09 is more secured for short distance, while BB84 is more preferred for long distance communication. As compared to the efficiency, BB92 is best as compared to others. The encryption and decryption codes will be extracted by using a secure channel (entangled states) in a short time of processing. In the end, the QKD protocol provides authentication between any end users, and the quantum mechanics roles will be utilized during transferring the data.

5. REFERENCES

[1] Ms V. Padmavathi, Dr B. Vishnu Vardhan and Dr A. V. N. Krishna, “Quantum Cryptography and Quantum Key Distribution Protocols: A Survey” in 2016 IEEE.

[2] Hitesh Singh, D.L. Gupta, A.K Singh, “Quantum Key Distribution Protocols: A Review” in IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014).

[3] Subhashree Basu, and Supriyo Sengupta, “A Novel Quantum Cryptography Protocol”, in 2016 IEEE.

[4] C. Guenther, "The Relevance of Quantum Cryptography in Modern Cryptographic Systems" in SANS Institute, 2004.

[5] A. Abushgra and K. Elleithy, "QKDP’s Comparison Based upon Quantum Cryptography Rules," in IEEE, 2016.

[6] P. Techateerawat, "A Review on Quantum Cryptography Technology" International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, vol. Volume 1, 2010.

[7] Scarani, A. Acin, Ribordy, G. Gisin. N, “Quantum Cryptography protocols robust against Photon number Splitting attack.” Physical Review Letters, vol.92.2004 http://www.qci.jst.go.jp/eqsi03/program/papers/O26-Scarani.pdf

[8] Muhammad Mubashir Khan et al. “High error-rate quantum key distribution for long distance communication” New J. Phys. 11 063043 http://iopscience.iop.org/1367-2630/11/6/063043/

[9] Eduin Esteban, Hernandez Serna, “Quantum Key Distribution protocol with private-public key” arXiv: 0908.2146v4 quant-ph 12th May 2012.

[10] Eduin H. Serna, “Quantum Key Distribution from a random seed” arXiv: 1311.1582v2 quant-ph 12th Nov 2013.