A Comprehensive Survey: Quantum Cryptography

Mohammed Moizuddin[1], Dr.Joy Winston[2]
[1, 2] Department of Computer Skills,
King Saud University,
Riyadh, Saudi Arabia.
moimohammed.c@ksu.edu.sa,
joywinston47@gmail.com

Mohammed Qayyum[3]
[3] Department of Computer Engineering,
King Khalid University,
Abha, Saudi Arabia
mdqayyum.se@gmail.com

***Abstract*—Internet has become a global means of communication, turned our reality upside down. It has transformed communications, to the level that it is now our chosen standard of communication. Although there are many ways to protect information from undesired access, Quantum cryptography can be used to unconditionally secure data communications by applying the laws of quantum physics which overcomes the drawbacks of traditional classical cryptography, which depends on mathematical methods to limit attacks such as eavesdroppers. Quantum cryptography is considered to be a future replica of classical cryptography. In this survey paper, we will discuss about various protocols of cryptography. Also discussing about their vulnerabilities**

Keywords—Cryptography, Communication, Quantum Cryptography, Security attacks.

I. INTRODUCTION

Cryptography is defined as the system by which the normal records can be turned to the unreadable form, so that the unlawful persons cannot access the plain or the normal records. While developing cryptography algorithm the developer must consider the three golden objectives Confidentiality, Integrity, Availability (CIA) [1]. To provide (CIA) to all types of network, requires a special key called the secret key. A key is a piece of information (a parameter) that defines the efficient productivity of a cryptographic algorithm. A key advances the conversion of plaintext into cipher text. Quantum Cryptography rationally Quantum key Distribution (QKD) provides the security to the network communications and important aspect to the distribution of the key. Stephen Wiesner devised this cryptography in the year 1970.It is one of the advanced element in the field of cryptography. [2].

This paper will emphasis on the quantum cryptography protocols on various parameters and summaries the importance of Quantum over traditional cryptography.

This paper is structured in the following manner: Section 3 presents the attributes of both the traditional as well as Quantum Cryptography and its importance. Section 4 deals with the analysis of various Quantum Cryptography protocols. Section 5 compares the various Quantum Cryptography protocols. This paper concludes with Section 6 Conclusion and Future work.

A. Classical Cryptography

Based on Mathematical techniques and the unproven computational rules, this traditional cryptography is applied to send secret messages and the main problem in this traditional cryptography is the key distribution. Cryptography is classified as two types based on their requirement and applications. They are Symmetric Key Cryptosystem (Traditional Cryptography) and Asymmetric Key Cryptosystem. The Symmetric Cryptography has the same key at both the sides for encryption and decryption of the communications.

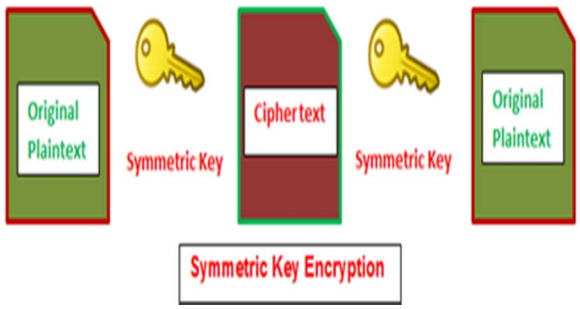

Fig. 1. Symmetric Key Encryption

The Asymmetric Cryptography has two variant keys, one key functional for encryption and the other for decryption.

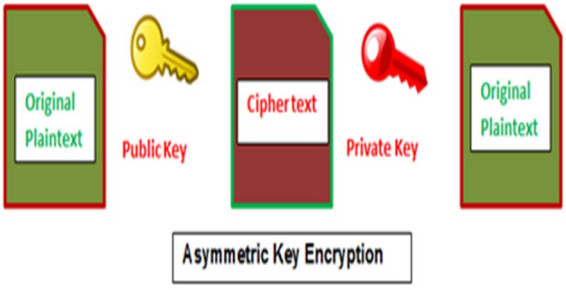

Fig. 2. Asymmetric Key Encryption

978-1-5090-5814-3/17/$31.00 ©2017 IEEE

B. *Quantum Cryptography*

In 1970, Quantum Cryptography was first devised by Stephen Wiesner and later his ideas were elucidated by Bennett in 1984. [3] This Quantum Cryptography was based on the values of quantum mechanics, the least level of matter and on the concept of using light weight particles called photons.

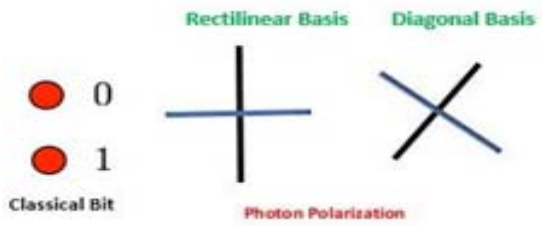

Fig. 3. Classical and Quantum Cryptography

Quantum systems designed in such a way that it uses quantum mechanics and depends greatly on the classical physics. This proves that these quantum systems are classical in nature [4] [5]as well. It depend on the Heisenberg principle of uncertainty and polarization of photons. The basic concept is that it is difficult to calculate the quantum states of any system such as energy, momentum of the particles without disturbing that system. The main aim of QKD is to create a key that is used in encryption system to transfer data with light weight photons through either fiber optics or free space.

At present many researchers agree that these quantum computers will replace with the desktop computer and with built-in-features quantum computer will enhance the global communications in coming years, possibly 2050^{13}. [6]

C. *Importance of Quantum Cryptography*

Even in a secure network there is no security assured. In theory of ordinary scale bodies permits the physical factors to be measured without disturbing those properties, hence leading to the passive attacks which are highly observed in traditional system, sender and receiver are not aware of eavesdropping which taken place and this situation does not happen in quantum theory.

Eavesdropping: Getting access to the communication without the consent of the sender or the receiver, and intercepting the data transmitted over a network. This is an important issue in the Quantum Key distribution networks.

II. ANALYSIS OF KEY PROTOCOLS OF QUANTUM CRYPTOGRAPHY

A. *BB84 Protocol*

In this paper, consider two individuals conventionally entitled Alice and Bob wants 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 transfer 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 chose randomly the rectilinear or diagonal polarizer to calculate the photons received and informs the result to 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.

TABLE I. RECTILINEAR AND ORTHOGONAL

Basis	0	1
+	↑	→
×	↗	↘

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 this 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'. [7]

B. *BB92:*

It is not important to use two orthogonal bases for encrypting and decrypting the data. [8] 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. [7]

C. *EPR:*

In 1991, Artur Ekert has elaborated a quantum protocol based pair of particles (called pair EPR). It states that there exit pair of particles that are spatially detached, named EPR pairs, these particles situations remain interrelated as if selected and measured one particle leads to the direction and the dimension of the auxiliary particle. This conduct is termed as "action at a distance" as the particles are separated at far distances. [9]

TABLE II. STATES OF PAIR OF PARTICLES AT ANY GIVEN TIME

Pair of Particles in the form of photons at any observable time	Measured State
photon 1	$\|0\rangle$
photon 2	$\|1\rangle$

D. SARG 04:

In BB84 protocol where four states of polarization used, if these four states are encoded with variant records it gives the new protocol called SARG04,which is vigorous against the photon-number-splitting attack, when attenuated pulses of laser are used as a substitute of single-photon sources.
Alice sends single particular photon bits of length 'a' to Bob over a public channel to Bob. Bob chooses his basis when calculating the qubits communicated by Alice. If Bob matched the same bits as sent by Alice, then Bob announces openly that he has received Alice's transmission. If there are errors in the length of the key at both sides then Alice and Bob cancel the process and start over.

As per the simulations done for this protocol and the results published earlier [10] the average 'Quantum Bit Error Rate' for N = 2 is around 75 % which is greater than 50% for the BB84 protocol. The possibility of transmission distance up to 144 km free space link is expected. [10]

E. COW Protocol

In this Coherent One-Way Protocol, by using the calculated photons arrival time on the detector data-line, a key developed and an interferometer is assembled on an extra observing line. The purpose of this line is to permit to detect the occurrence of a secret agent who would halt consistency by attack. [9]

F. S13:

Eduin H.Serna, presented this protocol in 2013,to prevent the loss of data packets over the transmission channels.S13 is constructed on a seed state called random seed and public key cryptography. It is proven to be secured by generating same size of the secret keys at many interactions. This protocol varies from BB84 just in the traditional techniques. [11]

G. SIX-STATE Protocol

Pasquinucci and Gisin designed SSP protocol which has the added two states of polarization. The polarization states of this protocol has three bases: with x, y and z basis. It is similar to the popular four states of BB84 (0°, 90°, +45°, -45°) with [2] the supplementary of two polarized basis.
Nicolas Gisin in 2001, stated that this protocol is significantly safe and diminishes the interference caused by the Eve's accessing the information. Even if calculates every single photon, the QBER is 33%, compared to 25% in the case of the BB84 protocol [12] [13]

H. One Time Pad-OTP (The Unbreakable encryption Method):

In this protocol, truly random key pairs which is equally long as the plain text is used to send the plain text to the receiver Bob B and the keys are known to each other before encryption takes place. The key is mixed by (XOR-ing) bit by bit, constantly a bit of the key with a bit of the plain text is blended to create a bit of cipher text. Later, the encrypted message is mixed (XOR-ed) with the duplicate copy of the One Time Key and the plain text is restored. [14]

I. AK15:

The data send using decoy states into stream of qubits can get more secured, and makes an eavesdropper more difficult to depend on the content. The receiver can easily get the sequence of qubits sent through the narrow classical channel without any additional support of communication. Hence this protocol is robust against Intercept –Resend - Attack (IRA), MIMA, and wasting time. [15].

J. Three Stage Quantum:

This quantum cryptographic protocol was first proposed in 2006 and implemented in 2012.It is asymmetric cryptography based protocol, each participant use their own private key to encode the communications sent over public channels.
Contrasting the BB84 protocol, where the stream of quantum bit are transferred in single direction [16] and classic data switched subsequently, the message remains quantum in each stage. There is probability of the multi-photon quantum cryptography, as this protocol, procedures multiple photons to interchange the information or messages between sender Alice A and Bob B the receiver which improve the transmission of data. [17]

K. DPS Protocol:

It was proposed by Kyo Inoue in 2003 [18]demonstrated on two non-orthogonal states.
Sender Alice A sends a randomly modulated coherent train of pulses between $\{0,\pi\}$ to Bob the receiver B using a Poisson distribution, Bob divides every pulse into two routes and then recombines them using a beam splitter ,when the beams are recombined the phase difference between the two pulses will either be 0 or π.Depending on the instances of the detector of the correct results, Alice A and Bob B can then decide their key bits and discard all other bits. The DPS protocol also provides robustness against a PNS attack. [19]

L. KMB09

This protocol uses two sets of basis and it is called prepare and measure [10] type of cryptography protocol. Alice sends the photons in one of the chosen states to Bob, and Bob calculate the arriving photons in an arbitrarily selected basis. To generate a strong association Alice disclose some information related to the index of the basis state through a traditional passage, which she used for the encryption of the photon and without uncovering the information of the key.
As per the results published earlier [10] KMB09 also delivers simply 25% of transmission rate of key, but on the payoff of

high error rate in the existence of an eavesdropper. Bit error rate of KMB09 is approximately 50%. [10]

M. S09:

Eduin Esteban Hernandez Serna presented S09 protocol with the combination of private key and public key cryptography. [20]

This protocol provides the safe transmission of information through the open mode of network. At each stage the communication remains quantum. The colossal key distribution in this protocol takes place between the n-1 computers and a key distribution center. It does not run-through on the classical channels so it is invulnerable against the middle-in-the-man attack and other similar attacks In this protocol transmission of qubits can be done in any arbitrary states. [19]

N. E91:

It uses the principle quantum entanglement where Alice A produce the pair of photons and these pairs are distributed by both and they get single photon at the end. These entangled photons are logically connected, if both calculate their particles of photons have either vertical or horizontal states of polarizations they get 100% possibility of the equivalent outcome [8]

Information mentioned in the below table were gathered from many resources like articles, journals, published papers and conference papers).These analysed data and processed information depends on the published books of various authors. Here in this paper, we focused on the key protocols and compared other protocols for future references.

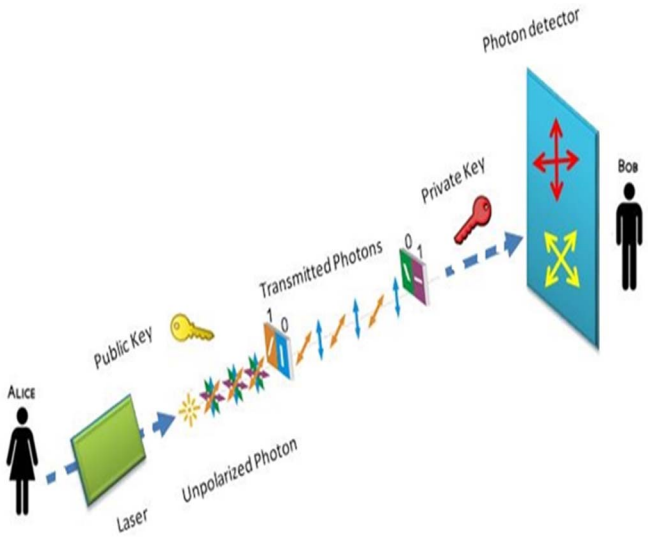

Fig. 4. Alice sending photons to Bob

TABLE III. THE COMPARISON OF VARIOUS QUANTUM CRYPTOGRAPHY PROTOCOLS

Properties	Year	Principles	No. of States	Polarization Situation	Classical channels	Bell's-in-equality	Man-In The-Middle attack	Protocol Used/ Manufacturer/ Product
BB84	1984	Heisenberg Uncertainty	4 states	2 orthogonal	yes	no	Vulnerable	BB84/IDQuantique/Cerberis
BB92	1992	Heisenberg Uncertainty	2 States	1 non orthogonal	yes	no	Robust	-
SAR04	2004	Heisenberg Uncertainty	4 states	coded bits	yes	no	Robust	SARG 04/ IDQuantique/ Clavis2
COW	2004	Quantum Entanglement	Time slots	No, using DPS	yes	no	Robust	-
KMB09	2009	Heisenberg Uncertainty	2 states	no	yes	no	Robust	-
EPR	1935	Quantum Entanglement	3-state	no	yes	yes	Robust	-
DPS	2003	Quantum Entanglement	4 States	4 non orthogonal	yes	no	Robust	-
S13	2013	Heisenberg Uncertainty	4 states	2 orthogonal	yes	no	N/A	-
SSP	1999	Heisenberg Uncertainty	6 states	-	-	no	-	-
E91	1991	Quantum Entanglement	3states	-	-	no	-	E91/ SeQureNet/ Cygnus
S09	2012	Public private key	-	-	-	no	-	-
OTP	1917	Quantum Entanglement	-	-	-	no	-	AES with OTP/Toshiba QKD GHz Sys.
Three State Quantum	2006		3states	-	-	no	-	-
AK15	2015	Heisenberg	n states	2 orthogonal	no	Yes	Robust	-

III. CONCLUSION AND FUTURE WORK

In Quantum Cryptography probabilities of data being intercepted and modified are very low compared to the classical cryptography. QKD is established on values of the quantum physics and can be thoroughly proven by generating secret keys. In this paper, it has been surveyed that quantum cryptography is preeminent optimal to provide secure delivery of authenticating data, and prevents unauthorized users from accessible or making undetectable alterations to the data by solving the key management issues which is an important aspect to attain the security. Lots of research work is ongoing to extend the scope and increase the availability of the data of QKD. There is ample to define about quantum cryptography protocols and their applications.

IV. REFERENCES

[1] W. Stallings, cryptography and network security principles and practice, 2006. j. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] B. Charles H and Gilles Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Elsevier B.V*, 2014.K. Elissa, “Title of paper if known,” unpublished.

[3] N. Kaur, "Enhancement of Network Security Techniques using Quantum Cryptography," in *International Journal on Computer Science and Engineering (IJCSE)*, 2011.

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

[5] V. Ojha, A. Sharma, S. K. Lenka and S. R. Biradar, "Advantages of Classical Cryptography Over the Quantum Cryptography," in *World Applied Programming*, 2012.

[6] L. O. Mailloux , C. D. Lewis II , C. Riggs and M. R. Grimaila , "Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals," *IEEE,* vol. 18, no. 05 - Sept.-Oct., 2016.

[7] P. Techateerawat, "A Review on Quantum Cryptography Technology," *International Transaction Journal of Engg, Mangmt, & Applied Sciences & Technologies,* vol. Volume 1 , 2010.

[8] M. P. P. Wasankar and P. P. D. Soni, "An Invention of Quantum Cryptography over the Classical Cryptography for Enhancing Security," *International Journal of Application or Innovation in Engineering & Management (IJAIEM),* vol. Volume 2, 2013.

[9] M. Elboukhari, M. Azizi and A. Azizi, "Quantum Key Distribution Protocols: A Survey," *International Journal of Universal Computer Sciences,* vol. Vol.1, 2010.

[10] M. Lopes and D. Sarwade, "On the performance of quantum cryptographic protocols SARG04 and KMB09," in *IEEE*, 2015.

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

[12] P. Curtacci, F. Garzia, R. Cusani and E. Baccarelli, "Performance analysis of different multi-user optical passive networks for quantum cryptography applications," in *SPIE Digital Library*, 2006.

[13] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," *REVIEWS OF MODERN PHYSICS,* vol. 74, 2002.

[14] "mils electronic," mils electronic, 1947. [Online]. Available: https://www.mils.com/.

[15] A. Abushgra and K. Elleithy, "Simultaneous Initiating EPR and Quantum Channel by Quantum Key Distribution Protocol," *Global Journals Inc. (USA),* vol. Volume 16, 2016.

[16] S. Kak, "A Three-Stage Quantum Cryptography Protocol," *Foundations of Physics Letters,* vol. Vol. 19, 2006.

[17] W. O. Krawec , "Asymptotic Analysis of a Three State Quantum Cryptographic Protocol," in *IEEE*, 2016.

[18] K. Inoue, E. Waks and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *PHY REVIEW,* 2003.

[19] H. Singh , D. Gupta and A. Singh, "Quantum Key Distribution Protocols: A Review," *IOSR Journal of Computer Engineering (IOSR-JCE),* vol. Volume 16, 2014.

[20] E. E. H. Serna, "QUANTUM KEY DISTRIBUTION PROTOCOL WITH PRIVATE-PUBLIC KEY," *Cornell University.*