A Survey on Quantum Key Distribution

Mr. Abhishek Sharma[1], Dr Amit Kumar[2]
[1]SRM Institute of Science and Technology, Delhi – NCR Campus, [2]KIET, Ghaziabad

***Abstract*-Quantum key distribution is a catchword among industry specialist now a day.It is arising an alarming situation to all the current network security techniques. These are the basic properties of Quantum Mechanics, which makes a combination with network security. At present there are so many companies out there in market which are making progress it this fields day by day.Quantum cryptography is a very important technology now days as it is helping a lot to secure the future network communication. This particular field has gained the attention from industry as well as from academics. Here we are writing this paper to provide the general review of various fields belongs to Quantum Computing, but our main aim is to provide a brief review and analysis of recent development in the field of Quantum Key Distribution, most famous and developed field of Quantum Computing. This paper presents review of Quantum Computing including different application fields like Quantum public key cryptography, QKD, Quantum Authentication.**
First we discuss the basics of Quantum Cryptography then we discuss the definition of Quantum key Distribution, Various protocols of this field. Then after we discuss the opportunities in this field.

Keywords: QKD, Quantum Computing, Neatwork Security, Cryptography, Quantum authentication, Quantum public key cryptography.

I. INTRODUCTION

Quantum computing is a wide area, which actually belongs to Quantum Physics, which is a part of Applied Physics. The term Quantum actually represents the use of tiny particle Quantum for the purpose of communication. Quantum actually represents the source of energy which can be charged positively and negatively, which could be used for communication as we use bits for representing 1 and 0 in classical communication.

Definition of Qubit

A qubit is a quantum bit, which is the counter representation of a classical bit in quantum computing. As we use binary 0,1 for information in classical computing, we use quantum binary 0 and 1 in quantum computing. So this quantumbinary number 0 and 1 is actually a charged photon generated from some source. We use a different notion notation known as Bra-Ket notation to represent a Qubit.
So the advantage of using Quantum Bits known as Qubits that is prone to classical attacks which is used in classical communication and in classical cryptography as quantum physics provide some special properties to those Qubits as they are prone to those attacks.

The rest of this paper is composed as pursues. In Section II, we characterize Quantum Cryptography and a presentation of the essential focuses identified with quantum data preparing. In Section III, we give a nitty gritty history of the QKD conventions. In Section IV, we talk about some open issues and practical research bearings. At long last, we outline this paper in Section V.

II. BASICS PRINCIPLE OF QUANTUM KEY DISTRIBUTION

Definition of Quantum Cryptography
Quantum Cryptography is the advanced form of cryptography as it is one step ahead from classical cryptography. It is a combination of two fields, “Quantum Physics” and “Network security”. In more simple words we can say “Quantum Cryptography is a application of Quantum Physics which serves the purpose of Cryptography”. Here we can take the advantages of following principles of Quantum physics.

Quantum Entanglement
Entanglement is a basic property of Quantum Physics. According to this principle two microscopic particles from a common source shows a relationship to each other. With the help of this relation ship we can find the state of one particle by measuring another particle whether they are near to each other or very far from each other. Albert Einstein called this phenomenon "spooky action at a distance."

Quantum Superposition
This feature of a quantum mechanics states that a Qubit can hold multiple states in parallel. In simple words we can say that without measuring the state of a qubit we cannot say it is holding what state, as to determine the state of qubit is known as qubit measurement. So before performing measurement on qubit its states cannot be determined so at present it is in a super position of all its possible states.

Quantum principle of uncertainty and non cloning
The no cloning theorem prevents the duplicate copies of an un-known quantum state. It was stated by Wootters, Zurek, and Dieks in 1982[20]. As per this theorem we can easily detect the presence of any unwanted person in the nwtwork. This ensures the security of the key or the information passed to it.

Quantum-measurement
it is the process of coding and decoding the information through qubits. It is a very important and critical process during quantum communication, as the integrity of the information highly depends on this. Modification and evolution are two sub processes of Quantum Measurement.

III. QUANTUM CRYPTOGRAPHY

The term cryptography is not new in the field of information security. Converting an information with the help of a

978-1-7281-1772-0

another piece of information popularly known as Key is a very classical idea of cryptography.

We can categories the current cryptography techniques according to the following fig.

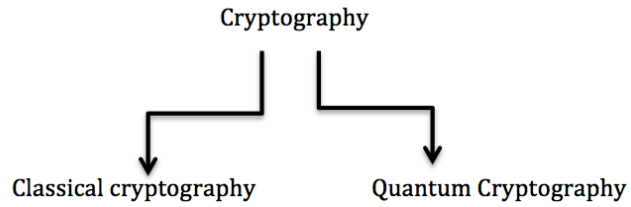

Fig. 1: categorization of cryptographic techniques

We can further sub divide Classical techniques in to Symmetric and Asymmetric Techniques as it depends on the number of keys required for encryption. But in the core they both depends on the complex mathematical Factorization problems. But in this era of high computing devices specially for Quantum computers, it is not a big task for them to solve this type of complex problems whichactually takes years to solve can be solved in few minutes only.

So here a new technique, which is actually a part of quantum physics, called as Quantum cryptography came into the picture.Due to its physical properties we can use it for cryptographic purposes and ensure the safety of information. Quantum Computing can be categorized into Quantum Key Distribution, quantum teleportation,quantum dense coding and so on.

Quantum Key Distributionworks on the principle of Key Distribution. Key distribution is a process of sharing a common key between sender and receiver with the guarantee of that the key is not compromised in any way. So basically the key distribution is the first and most important part of the encryption process.

1. Quantum key distribution

The basic of Quantum Key Distribution is to use non-cloning of non-orthogonalsingle quantum state to complete the key distribution.

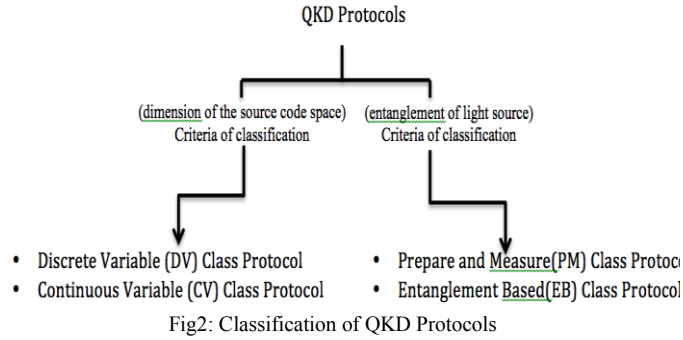

Fig2: Classification of QKD Protocols

TheQKD protocol can be classified into few categories on the basis of their physical properties. If we consider the dimension of the source code space as the criteria for classification, they can be classified as Discrete variable (DV) class protocol and Continuous variable (CV) class protocol.If we consider entanglementod light source is there or not, then we can further divide them as Prepare-and-measure (PM) protocol and Entanglement-based (EB) protocols.

The introductions of the above categorized protocols are as follows.

I. Discrete variable Quantum Key Distribution (DVQKD)

In this category of protocols we use Hilbert space as the criteria for classification. According to the definition of this category we use quantum states for coding are finite dimentional for the whole QKD process. Phase of the photon or Polarization direction of the information carrying photon could be used to distinguish states. The most basic protocol of QKD known as BB84 is an example of this category. But this normal DV-Protocols likewise incorporates Distributed stage reference (DPR) convention that is fundamentally the same as the traditional correspondence protocols.

DV- Protocols using only One Photon

These protocols uses different states of single photon for conveying information. So throughout the complete process different states are used for coding and encoding for key distribution. Here we are listing few protocols which belongs to this class of QKD protocols.

- BB84 – in 1984 by C.H. Bennett and G. Brassard[1]
- B92 – in 1992 by C.H. Bennet[2].
- Six-State Protocol – in 1998 by D. Bru[3].
- SARG04 – in 2004 by V. Scarani et al[4].

DV- Protocols based on Entanglement of Photon

This category of protocol refers such protocols which uses entanglement of photons for encoding and decoding instead of state of photon. Here we are listing few protocols which belongs to this class of QKD protocols.

- E91 – by ArturEkert in 1991[5].
- BBM92 – by C.H. Bennett et al. in 1992[6].

Some other DV Protocols

Except this there are few more protocols are also thereproposed by various authors at various time spans. They can be further categorized as One way Protocols or Two way Protocols. Below we are listing few of them from each category.

One –Way Protocols

- DPS(Differential phase reference) – protocols – By byKyo Inoue et al. in 2002[7].
- RRDPS Round-robin differential phase shift (RRDPS)[8] – proposed by T. Sasaki et. Al. in 2014.
- Coherent one-way (COW) protocol - by D. Stucki et al. in 2005[9].

Two-Way protocol

- Ping-Pong[10]
- LM05[11].

Distace is also a measure concern regarding QKD protocols. Most of the protocols doesn't support very long distance travel.till now the maximum distance coveed by DV category protocols is 300km.[12]

II. Continuous Variable Quantum Key Distribution (CVQKD)

In this category of protocols quantum states used for representation of information are continuous and infinite dimensional unlike DVQKD. The protocols fron this categories can be further subcategorized as squeezed state protocol, coherent state protocol, entangled state protocol.

Here we are listing few CVQKD protocol

- GMSSP(Gaussian-modulated squeezed state protocol) - by N.J. Cerf et al. in 2001[13].
- GG02(coherent state balanced homodyne detection protocol) – by F.Grosshans and P. Grangier in 2002[14].
- Coherent state heterodyne detection protocol – by C. Weedbrook et al. in 2004[15].
- CV two-way protocol - by S. Pirandola et al. in 2008[16].

CV-QKD can achieve a maximum transmission distance of 120km[17].

III. Measurement-device-independent QKD (MDIQKD)

As the name of this section define, the protocols which comes in this section are actually designed to be device independent because in theory the process of Key Distribution is perfect in terms of ideal conditions, But the devices(Photon Source or Photon Detector) used in processing could be intercepted for the purpose of attack. To solve the security issues related to this a new approach is used to design QKD protocols known as DI(Device Independent)-Protocols. A. AcÅLın et al. proposed this approach in 2007[18].The throughput of DI Protocols is measured by LFBT-Test(Loophole-free bell test). The devices used in Quantum Information Processing are complex and not very efficient in terms of reliability. But this issue can be resolved by changing the architecture of original protocols. If we reduce the dependency on the measurement devices, in will increase the efficiency of the protocol.

DI- Protocols could be further categorized as 1sDI (one-side Device independent) protocol[19] and semi-DI (semi-Device independent) protocol[20]. detectortimeshift attack[21], faked states attack[22], detector blind attack[23], wavelength-dependent attack[24]are few types of attacks on used to breach the security of QKD protocols. So the MDI protocol are very important for the implementation[25]. The security of these protocols are proven and they are being used in application as well as in experiment[26].

Now the maximum transmission distance is 400km.

Other fields of Quantum cryptography

Except Quantum Key Distribution we have few other fields of application for information security.

1. *Quantum Authentication*

Authentication is a process of identity verification of the sender and the integrity verification of the send message. And further ensure the security of the communication.

1) Quantum Authentication

Quantum Authentication needs to achieve the following purposes.

- First, the user caneffectively prove her self-identity, that is, Alice can prove to Bob “she” is Alice.
- Second, the user cannot beimitated, that is, after Alice completing the verification,Bob cannot claim to others that he is Alice using the information provided by Alice.

2) Quantum signature

The main purpose of Digital signature is to ensure the purity of the data and the validity of the sender in the communication. This is the combination of theasymmetric key encryption technology with digital abstract technology.

There are three kinds of representative quantum signature protocols:
Arbitrated quantum signature
Quantum blind signature
Quantumgroup signature.

Quantum Public Key Cryptography

With the recent development in various fields of computing, the classic cryptographic techniques based on complex mathematical problems like finding factors of a number are not secure any more for cryptography, so we immediately need a new cryptography system to fill the gap. QPKC(Quantum public key cryptography) is that techniques that can be used to fill this gap. In this cryptographic system, the physical properties of photons are used to ensure the security of this techniques.

Post Quantum Cryptography

With the advancement in the field of quantum computing, it has created a question mark on current cryptographic system. So to solve this issue a new approach is being developed known as Post Quantum Cryptography. Theoretically it ensures the safety of information against Quantum attacks .

Quantum A.I.

Quantum A.I. is the implementation of Quantum processing in implementation of Artificial Intelligence**.** It is a research effort ofGoogleCorporation. Quantum AI by googleisdedicated to improve quantum computing by developing quantum processors and novel quantum algorithms.It will help researchers and developers to solve near-term problems.

IV. CHALLENGES AND OPPORTUNITIES

1. Challenges of QC

With the development of Quantum Cryptography, the challenges have also increased. QKD, which is the most important component of QC, is also one of the important components of secure quantum communication. It has passed through the fear that quantum computer will use the Shor secure algorithm to nullify the existing public key cryptography.
Theoretical challenges
Except the theoretical challenges, physical application of

Quantum Computing is also a measure issue. Here we have listed few of they which are worth of discussion. These issues are true random number, light source, detection, post-processing, authentication, repeater, etc.

Experimental challenges

QKD experimental systems are also improved a lot with its time span. As we are having many QKD protocols based on physical properties to apply and observe on recent cryptographic applications. Few categories of our QKD protocols are listed as here.

- Discrete variable Quantum Key Distribution (DVQKD)
- Continuous Variable Quantum Key Distribution(CVQKD)
- Prepare and Measure Quantum Key Distribution (PMQKD)
- Entanglement Based Quantum Key Distribution(EBQKD)
- Measurement Device Independent Quantum Key Distribution(MDIQKD)

Each category is a large set of protocols to experimented and observe to find new results. So the overall output of this fields is very satisfactory till now but still there is a long distance to be travelled along with it.

VI. Summary

Quantum Cryptography has shown its potential as per the expectation of its observers. As Quantum Cryptography was expected as the perfect cryptography, with its development and challenges it has faced, it has proved itself.

Quantum Cryptography just not proved itself more secure it has also promised to exhibit the goal of classical cryptography. With its properties which it has derived from Quantum physics, it can ensure that sender and receiver can detect eavesdropping and take appropriate measures and the second objective is that the anybody cannot break the quantum key.

So we can make sure that QC can achieve its targets as promised theoretically. In its journey it has achieved many milestones in this short period of time and expected to achieve many others targets with the recent developments which are taking place in this field. So we can make sure that this research fields has a bright future for research and development and the upcoming time will we known as the quantum computing era.

References

[1] C.H. Bennett and G. Brassard, “Quantum cryptography: Publickey distribution and coin tossing”, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, IEEE, New York, pp.175–179, 1984.

[2] C.H. Bennett, “Quantum cryptography using any two nonorthogonal states”, Phys. Rev. Lett., Vol.68, No.21,pp.3121–3124, 1992.

[3] D. Bru., “Optimal eavesdropping in quantum cryptography with six states”, Phys. Rev. Lett., Vol.81, No.14, pp.3018–3021, 1998.

[4] V. Scarani, A. AcÅLın, G. Ribordy, et al., “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations”, Phys. Rev. Lett., Vol.92, No.5, Article ID 057901, 4 pages, 2004.

[5] A.K. Ekert, “Quantum cryptography based on Bell’s theorem”, Phys. Rev. Lett., Vol.67, No.6, pp.661–663, 1991.

[6] C.H. Bennett, G. Brassard and N.D. Mermin, “Quantum cryptography without Bell’s theorem”, Phys. Rev. Lett., Vol.68, No.5, pp.557–559, 1992.

[7] K. Inoue, E. Waks and Y. Yamamoto, “Differential phase shift quantum key distribution”, Phys. Rev. Lett., Vol.89, No.3, Article ID 037902, 3 pages, 2002.

[8] T. Sasaki, Y. Yamamoto and M. Koashi,“Practical quantum key distribution protocol without monitoring signal disturbance”, Nature, Vol.509, No.7501, pp.475–478, 2014.

[9] D. Stucki, N. Brunner, N. Gisin, et al., “Fast and simple one-way quantum key distribution”, Appl. Phys. Lett., Vol.87, No.19, Article ID 194108, 3 pages, 2005.

[10] K. BostrÅNom and T. Felbinger, “Deterministic secure directcommunication using entanglement”, Phys. Rev. Lett., Vol.89,No.18, Article ID 187902, 4 pages, 2002.

[11] M. Lucamarini and S. Mancini, “Secure deterministic communicationwithout entanglement”, Phys. Rev. Lett., Vol.94, No.14,Article ID 140501, 4 pages, 2005.

[12] B.J. Xu, W.L. Liu, J.Q. Mao, et al., “Research on developmentstatus & existing problems of quantum communication technology”,Communications Technology, Vol.47, No.5, pp.463–468, 2014.

[13] N.J. Cerf, M. LÅLevy and G.V. Assche,“Quantum distribution ofGaussian keys using squeezed states”, Phys. Rev. A, Vol.63,No.5, Article ID 052311, 5 pages, 2001.

[14] F. Grosshans and P. Grangier, “Continuous variable quantumcryptography using coherent states”, Phys. Rev. Lett., Vol.88,No.5, Article ID 057902, 4 pages, 2002.

[15] C. Weedbrook, A.M. Lance, W.P. Bowen, et al., “Quantumcryptography without switching”, Phys. Rev. Lett.,Vol.93,No.17, Article ID 170504, 4 pages, 2004.

[16] S. Pirandola, S. Mancini, S. Lloyd, et al., “Continuous-variablequantum cryptography using two-way quantum communication”,Nature Phys., Vol.4, No.9, pp.726–730, 2008.

[17] P. Jouguet, S. Kunz-Jacques and A. Leverrier, “Long-distancecontinuous-variable quantum key distribution with a Gaussianmodulation”, Phys. Rev. A, Vol.84, No.6, Article ID 062317, 7pages, 2011.

[18] A. AcÅLın, S. Massar and S. Pironio, “Efficient quantum key distributionsecure against no-signalingeavesdroppers”, New J.Phys., Vol.8, No.8, Article ID 126, 11 pages, 2006.

[19] C. Branciard, E.G. Cavalcanti, S.P. Walborn, et al., “One-sideddevice-independent quantum key distribution: Security, feasibility,and the connection with steering”, Phys. Rev. A, Vol.85,No.1, Article ID 010301, 5 pages, 2012.

[20] M. Pawlowski and N. Brunner, “Semi-device-independent securityof one-way quantum key distribution”, Phys. Rev. A,Vol.84, No.1, Article ID 010302, 4 pages, 2011.

[21] Y. Zhao, C.H.F. Fung, B. Qi, et al., “Quantum hacking: Experimentaldemonstration of time-shift attack against practicalquantum-key-distribution systems”, Phys. Rev. A, Vol.78, No.4,Article ID 042333, 5 pages, 2008.

[22] V. Makarov and D.R. Hjelme, “Faked states attack on quantumcryptosystems”, J. Mod. Opt., Vol.52, No.5, pp.691–705, 2005.

[23] V. Makarov, “Controlling passively quenched single photon detectorsby bright light”, New J. Phys., Vol.11, No.6, Article ID065003, 18 pages, 2009.

[24] H.W. Li, S. Wang, J.Z. Huang, et al., “Attacking a practicalquantum-key-distribution system with wavelength-dependentbeam-splitter and multiwavelength sources”, Phys. Rev. A,Vol.84, No.6, Article ID 062308, 5 pages, 2011.

[25] H.K. Lo, M. Curty and B. Qi, “Measurement-device independentquantum key distribution”, Phys. Rev. Lett., Vol.108, No.13, Article ID 130503, 5 pages, 2012.

[26] Y. Liu, T.Y. Chen, L.J. Wang, et al., “Experimental measurement-device-independent quantum key distribution”, Phys. Rev. Lett., Vol.111, No.13, Article ID 130502, 5 pages, 2013.

[27] Z. Tang, Z. Liao, F. Xu, et al., “Experimental demonstration ofpolarization encoding measurement-device-independent quantumkey distribution”, Phys. Rev. Lett., Vol.112, No.19, ArticleID 190503, 5 pages, 2014.

[28] H. Inamori, N. LÅNutkenhaus and D. Mayers, “Unconditional security of practical quantum key distribution”, Eur. Phys. J. D,Vol.41, No.3, pp.599–627, 2007.

[29] D. Gottesman, H.K. Lo, N. LÅNutkenhaus, et al., “Security ofquantum key distribution with imperfect devices”, QuantumInf. Comput., Vol.4, No.5, pp.325–360, 2004.

[30] W.Y. Hwang, H.Y. Su and J. Bae, “Improved measurement device-independent quantum key distribution with uncharacterizedqubits”, Phys. Rev. A, Vol.95, No.6, Article ID 062313,4 pages, 2017.