A NEW ERA OF CRYPTOGRAPHY: QUANTUM CRYPTOGRAPHY

Sandeepak Bhandari

Aleksandras Stulginskis University, India

ABSTRACT

Security is the first priority in today digital world for secure communication between sender and receiver. Various Cryptography techniques are developed time to time for secure communication. Quantum Cryptography is one of the latest and advanced cryptography technique, it is different from all other cryptography technique and more secure. It based on the Quantum of physics since its name which make it more secure from all other cryptography and UN breakable. In this paper about quantum cryptography i.e working, limitation and advantages discussed.

KEYWORDS

Photon, Polarization filter, Advantage and Limitation of Quantum Cryptography.

1. INTRODUCTION

ID Quantique presents a quantum cryptography framework; will take after by the Magic innovations. These frameworks use photons to send mystery encryption keys, concealing every key behind the most well known tent of quantum mechanics, the Heisenberg vulnerability rule. This standard says, that it is difficult to know both an article's position and speed – in the meantime. Any email message, phone call or money related encoded with these keys will be protected.

Quantum cryptography utilizes current learning of material science to build up a cryptosystem that is not ready to be vanquished - that is, one that is totally secure against being traded off without information of the sender or the beneficiary of the messages. "Quantum" alludes to the essential thing conduct of the littlest particles of matter and vitality: quantum hypothesis clarifies everything that exists and nothing can be infringing upon it. Quantum cryptography's essentials is unique in relation to conventional cryptographic's basics is that, quantum cryptography depends more on material science, as opposed to arithmetic, as a key part of its security model.

Quantum cryptography was initially proposed by Stephen Wiesner, at Columbia University in New York in 1970s.The fundamental of Quantum cryptography is Photon. About photon, how it utilized as a part of Quantum Cryptography and what is its significance will be talked about in next area. Basic terms

1. **Photon:** A photon is a solitary quantum of light and in addition a solitary quantum of every single other type of electromagnetic radiation and can be alluded to as light quantum. It has no mass.
2. **Polarization:** In Quantum cryptography, there are four types of polarization of photon

namely diagonally, vertically and horizontally.

3. **Plain text***:* A message in its natural form which can be easily readable and understandable by anyone.
4. **Cipher text**: It is modified form of plaintext which is unreadable and understandable by anyone except the intended recipients.
5. **Key:** It is a bit of data that decides the practical yield of cryptography calculation or figure. A key is a number that the figure as a calculation, works on. To secure a message, we require an encryption calculation, an encryption key and plaintext. To unscramble a message we require a decoding calculation, an unscrambling key and figure content**.**
6. **Encryption**: It is a procedure of changing the plaintext into figure content in a manner that exclusive approved gatherings can read it.
7. **Decryption**: It is the converse procedure of encryption that is the changing of figure content into plaintext. As such, it is the way toward disentangling encoded data with the goal that it can be gotten to again by approved clients.

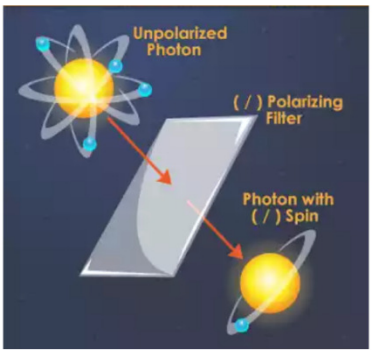

Figure 1:Photon Polarization

2. WORKING OF QUANTUM CRYPTOGRAPHY

Quantum Cryptography utilizes the information of material science to create and transmit a secured key amongst sender and recipient. In quantum Cryptography, for producing secured key the quantum of light is utilized called photon since its name is quantum cryptography.

Working of Quantum Cryptography can be explained in following four steps:

1. Creation of Photon.
2. Polarization of photon.
3. Attachment of information to photon.
4. Generation of Secured Key.

3. CREATION OF PHOTON

1. The initial phase in Quantum Cryptography is production of photon which is utilized to create and transmit secured key amongst source and goal.

2. For making the photon, quantum cryptographer use LEDs i.e. light Emitting Diode. LEDs are fit for making one photon at once which is the way strings of photon can be made.

4. POLARIZATION OF PHOTON

1. A photon can be in any structure or state to be specific corner to corner, on a level plane and vertically.

2. By utilizing polarization channels, the photon can be placed in one frame or state. Assume we utilize vertical polarization filter beyond a LEDs that photons will be polarized which will emerge. The photons that are not consumed will rise on the opposite side with vertical twist (/).

3.The thing about photon is that once they are captivated, they can't be measured once more, with the exception of by a channel like the one that at first delivered their present twist.

4. Its imply that if a photon with a vertical twist is measured through an inclining channel either the photon won't go through the corner to corner channel or the channel will impact the conduct of photon, making it take an askew turn.

5. In this sense, the data on photon's unique polarization is lost thus too is any data joined to the photon's twist.

5. ATTACHMENT OF INFORMATION TO PHOTON

1. The third step in quantum cryptography is connection of data to photon. Quantum Cryptography utilizes photons to transmit key amongst sender and beneficiary. Once the key is transmitted, coding and disentangling utilizing the ordinary mystery key technique can take place, but how data can append to a photon.

2. Every sort of photon's twist speaks to one bit of data either a 1 or a 0 to speak to parallel code. This double code utilizes series of 1s and 0s to make a cognizant message.

3. For example, a photon that has a vertical twist (/) speak to double piece 1.Alice, a sender sends her photon through haphazardly pick channel and record the polarization of every photon. At that point she will realize that what photon polarizations weave, a beneficiary ought to get.

4. At the point when Alice send to Bob her photons utilizing LEDs, she will arbitrarily energize the photons either through the X or + channels. So every photon has conceivably four states.

5. On the recipient side, the Bob gets these photons, he chooses to quantify the got photon by utilizing his X or + channel yet he can't have utilized both channel together at the same time. Weave has no learning which channel used to quantify the got every photon. Weave simply foresee the channel for each got photon.

6. Presently Bob calls Alice and advises her channel that he used to gauge each got photon and she will answer whether he utilized right or off base channel to quantify the photon. The

discussion amongst sender and beneficiary like:

Bob:PlusAlice:incorrect
Bob:XAlice:correct
Bob:PlusAlice:correct

So from above conversation between sender and receiver, if third party listening on their conversation, the third party can't determine the actual sequence of photon because the receiver, Bob is not saying what his measurements he just say the type of filter.

6. GENERATION OF SECURED KEY

1. The last stride of Quantum Cryptography is producing a secured key amongst sender and recipient. The key depends on the examination of polarization of photon amongst sender and collector.

2. On the off chance that the polarization of photon amongst sender and collector is right, then that photon will be utilized to produce key. The era of secured key will clarify in point of interest with case in next segment.

7. EXAMPLE OF QUANTUM CRYPTOGRAPHY

1. In the past segment the working of Quantum Cryptography is talked about, how the Quantum cryptography is worked and how it utilized the quantum of light called photon to produce and transmit key amongst sender and recipient.

2. In this segment a case is talked about so that working of Quantum Cryptography can be portray.

3. In this case Alice, a sender and Bob, receiver. The photons are made by utilizing LEDs since LED is equipped for making one photon at once. Alice send her photon through haphazardly pick channel and record the polarization of every photon. At that point she will realize that what photon polarizations sway, a beneficiary ought to get. At the point when Alice send her photon to Bob she haphazardly spellbinds the photon utilizing X or + channel. So every photon have four diverse conceivable state.

4. On the collector side, the Bob gets these photons, he chooses to gauge the got photon by utilizing his X or + channel however he can't have utilized both channel together at the same time. Bounce has no learning which channel used to gauge the got every photon. Sway simply anticipate the channel for each got photon.

5. Presently Bob calls Alice and advises her channel that he used to gauge each got photon and she will answer whether he utilized right or off base channel to quantify the photon.

6. For instance, Alice sent one photon as a (/) and bounce says he utilized a + channel to gauge it. Then Alice will say INCORRECT to Bob. But if Bob say he utilized X channel to quantify that specific channel then Alice say CORRECT to Bob.

7. On the premise of correspondence amongst source and goal the key will produce which is just known by sender and beneficiary.

8. Assume ‐ and \ speak to parallel 0 and/and | Represent double 1.If Alice send ‐ to Bob utilizing + channel and if Bob process that specific photon utilizing + channel, then that photon will be utilized to create a secured key on the grounds that the both sender and collector utilizes same channel for that specific photon.

9. Generally, if Bob utilized X channel to register that specific photon then that photon won't be utilized to create key.

The first Quantum Cryptography framework worked by **Charles Bennett Gilles Brassard and John Smolin in 1989 sent** a key more than 36 centimetres.

However, now-a-days the new models of Quantum Cryptography have achieved a separation of more than 150 kilometers. Yet at the same time it is insufficient to transmit data with present day PCs and media transmission frameworks.

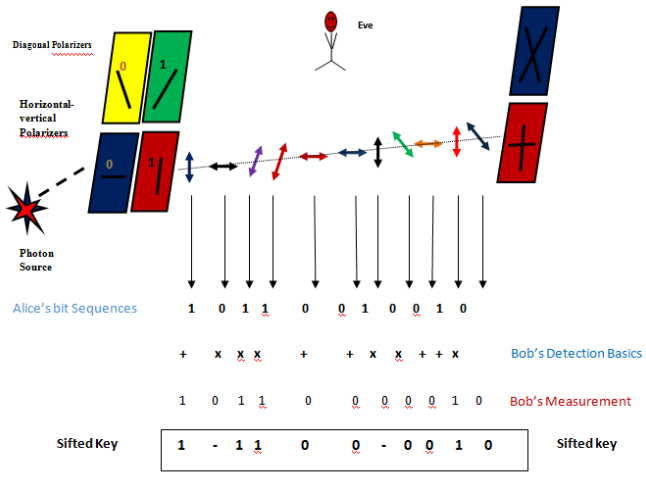

Figure 2: Illustrate the Working of Quantum Cryptography

Above (Figure 2) delineates the working of Quantum Cryptography which indicates how key is created amongst sender and collector.

In the above figure the secured key amongst sender and collector is 111000010.The idea driving the secured key is that both sender and recipient must utilize same polarization channel to register that specific photon. On the off chance that sender and collector use distinctive channel to process that specific photon then that photon cannot be utilized to produce channel on the grounds that either the data on the first polarization of photon is demolished on the other hand changed or the photon does not go through wrong polarization channel. The primary advantage of Quantum Cryptography is that it is unthinkable for middle or interloper amongst sender and beneficiary to break the secured key. Since the Quantum Cryptography depends on the most renowned tent of quantum mechanics, the Heisenberg vulnerability standard. This standard says, that it is difficult to know both an item's position and speed.

8. ADVANTAGES OF QUANTUM CRYPTOGRAPHY

The Quantum Cryptography is another zone of examination in the field of Cryptography. Firstly, the Quantum Cryptography will be broadly utilized as a part of future. The purpose for that the Quantum Cryptography will defeat the confinement of Public Key Cryptography (PKC) and Secured Key Cryptography (SKC). Also, the Quantum cryptography is more secured when contrasted with PKC and SKC. Since it depends on the quantum mechanics which says that it is impractical to know both of an item's position and speed.

Third is that in Quantum Cryptography if a middle of the road or gate crasher amongst sender and beneficiary attempt to adjust the data or wrongfully attempt to take data can be effectively identified.

9. LIMITATION OF QUANTUM CRYPTOGRAPHY

Like other Cryptography techniques namely PKC and SKC, the Quantum Cryptography has also some limitations but it is more secured as compared with all other cryptography techniques

10. CONCLUSION

In this paper, the new territory of examination Quantum Cryptograph is talked about. Quantum Cryptography depends on the Quantum of Physics since its named. Quantum Cryptography is contrast from all other cryptography strategies since it taking into account material science as opposed to on arithmetic. Quantum cryptography use photon to create and transmit key amongst sender and collector, which makes it more secure when contrasted with all other cryptography systems. It likewise defeats the confinement of PKC and SKC cryptography. Quantum Cryptography is difficult to break due to the novel property of photon. Yet, quantum cryptography is exceptionally hard to execute in long separations which is critical for cutting edge media transmission framework. In future, a compelling technique ought to be produced so that quantum cryptography can be utilized as a part of long separations.The distance covered by Quantum Cryptography is still in hundred Kilometres distance Which is not enough for modern telecommunication system.The reason is that when photon travels long distance the original polarization of photon is changed which cause the information destroyed. So long distance is the major limitation of Quantum Cryptography.

REFERNCES

[1] Pranab Garg,jaws, “A Review Paper on Cryptography and Significanceof Key length” JCSCESpecial issue on “Emerging Trends in Engineering” ICETIE 2012.

[2] Dripto Chatterjee, Joyshree Nash, Suvadeep Dasgupta, Asoke Nath ―A new Symmetric key Cryptography Algorithm using extended MSA method:DJSA symmetric key algorithm‖ published in 2011,International Conference on Communication Systemsand Network Technologies, 978-0-7695-4437-3/11$26.00 © 2011 IEEE.

[3] Md. Nazrul Islam, Md. Monir Hossain Mia,Muhammad F. I. Chowdhury, M.A. Matin ―Effect ofSecurity Increment to Symmetric Data Encryptionthrough AES Methodology‖ Ninth ACIS InternationalConference on Software Engineering, ArtificialIntelligence, Networking, and Parallel/DistributedComputing978-0-7695-3263-9/08DOI10.1109/SNPD.2008.101 IEEE 2008.

[4] Swati Paliwal, R.G" A Review of Some Popular Encryption Techniques"ISSN: 2277 128X, Volume 3, Issue 2, February 2013.
[5] Nitin Jirwan, A.S, Dr. S.V "Review and Analysis of Cryptography Techniques"ISSN 2229-5518,International Journal of Scientific &engineering research volume 4,issue 3,march 2013.
[6] J.Black,P.Rogaway, and T.Shrimpton Black-boxanalysis of the block-cipher-based hash function.
[7] Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.
[8] P. Rogaway, T. Shrimpton,‖ Cryptographic Hash-Function Basics:Definitions, Implications, andSeparations for Preimage Resistance, Second-PreimageResistance, and Collision Resistance‖ (FSE 2004).
[9] Tarun Sharma, Sandeepak Bhandari,Jagpreet Singh, Sarabjit Kaur,"Cryptography", Conference on Business Studies,Amritsar,India,2014.