ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Quantum Key Distribution

Shaunak Shah[1], Mrinalini Shah[2], Ayush Shah[3], Rishi Shah[4]

Student, Information Technology, DJSCOE, Mumbai, India [1]

Student, Electronics, DJSCOE, Mumbai, India [2,3,4]

Abstract: Data security in present age of cutthroat competition is a dire necessity. With present encryption methods to keep pace with hackers, the algorithms for encryption are getting more complicated with day. It is only a matter of time before this equation is reverse engineered, to successfully decrypt it. Thus a need for more secure means of communication is realized. To address this, quantum key distribution is a front-runner. Although it is still in its infancy, this technology has the potential to become a secure means of communication. Here data is encrypted with a private shared key, which changes every minute, possession of source and receiver. This key is sent by encrypting of selectively polarized photons, in form of binary. A hacker can intercept both but interception changes polarization, alerting both involved parties and rendering the message inaccessible. This has wide applications in ever expanding field of communication and could prove to be the future.

Keywords: Security, Cryptography, Symmetric Key, and Quantum Cryptography.

I. INTRODUCTION

Encryption is the technique of securing data by scrambling information and generating a key, which can only be accessed by the authorized parties. Encrypted or encoded texts are called CipherText. Encryption process basically deals with converting a PlainText into a CipherText. A security key is generated once the data conversion process is successful and is shared only with the intended recipient. To reverse engineer or decrypt the message the receiver must have the relevant decryption key. Encryption is the building block of security and is constructed using complex mathematical models. The CIA triad stands for Confidentiality, Integrity and Availability of data and is done in order to ensure Information Security. Encryption fortifies the data and makes attempt at preserving the data integrity. Encryption Key safeguards the authenticity of the receiver, hence ensuring that data is available only to a legatee. Over the years encryption techniques have evolved immensely and many more sophisticated schemes are employed. But the question arises that why is it needed? Encryption is the need of the hour with the upsurge of communicating devices. It is similar to protecting a house from burglars.

- A message can be safeguarded from an intruder trying to invade our privacy.
- With the increase in e-commerce websites and monetary dealings over the Internet, Security is a primary concern. Encryption ensures that our credit and debit cards details are disclosed only to online shop.
- It helps to keep our anonymity intact. The business class uses it to protect corporate secrets, government uses it to secure classified information, and many individuals use it to protect personal information to guard against things like identity theft.
- It makes sure that even if invaders drive down and latch the data it is obsolete without a key [1].

Cryptography techniques are basically of 2 types. **Symmetric Key cryptography** and **Asymmetric Key cryptography**. **Symmetric-key algorithms** are those algorithms that use same cryptographic keys for both encryption of plaintext and decryption of the encrypted text. The Keys are identical or there may be a simple transformation between the two. This key is a secret-code shared between two or more parties involved in the information transfer [2] .

Public-key cryptography/Asymmetric Cryptography is often used to secure electronic communication over an open networked environment such as the internet. This avoids relying on a hidden channel even for a key exchange. Each party has a pair of cryptographic keys – a public encryption key and a private decryption key. For example, a key pair used for digital signatures consists of a private signing key and a public verification key. Maybe the Public key is known to all, but the private key is only known to the concerned party. However the drawback of this technique is that the keys are related mathematically, but due to the way the parameters are chosen, calculating the private key from the public key is unfeasible [3]. One of the most upcoming cryptography technique is 'Quantum Key Distribution [4]. It is a symmetric Key algorithm wherein the involved parties share identical keys. It is a random key generated every second. Unlike other common encryption techniques, which rely on complex computational models, QKD depends on laws of quantum physics. If an eavesdropper tries to intercept the message, the polarized photons change polarity in turn changing the binary pattern. Therefore in this paper we provide a brief overview of what is quantum key distribution. Section II contains the definition of QKD. Section III contains the fundamentals of QKD and Section IV contains the protocols used in QKD.

II. WHAT IS QUANTUM KEY DISTRIBUTION?

Quantum Key Distribution (QKD) is a technology, based on the quantum laws of physics, rather than the assumed

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

computational complexity of mathematical problems, to generate and distribute provably secure cipher keys over unsecured channels. It does this using single photon technology and can detect potential eavesdropping via the quantum bit error rates of the quantum channel. QKD uses photons that denote a bit (1 or 0), which is determined by polarization or spin for exchange of cryptographic key data between the users [5]. At senders end, a series of photon stream is generated which is aligned either Horizontally or Vertically. The polarization of the photon is measured at the receiver's end. If an eavesdropper intercepts the photon to determine its polarization, the photon polarization changes in the process, and the eavesdropper would have to generate a new, duplicate photon to pass on to the receiver. The uncertainty principle of quantum physics makes it impossible for the eavesdropper to determine both properties of the photon, so it would be impossible for him to send along an accurate duplicate [6] .The model of QKD is shown in figure 1.

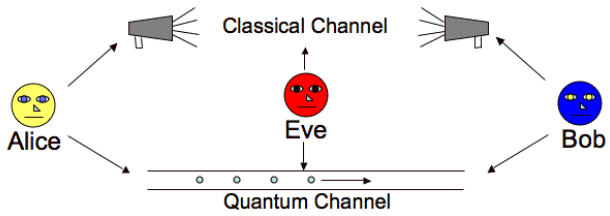

Figure 1:QKD Model

Now lets understand the fundamentals of quantum key distribution.

III. FUNDAMENTALS OF QUANTUM KEY DISTRIBUTION

Public Key Cryptography is the system presently in vogue. As established earlier, it isn't a very reliable means of communication. The need for a reliable Symmetric key algorithm has been realized. A system, which is faster and more reliable in terms of security, is required. That's why we turn towards QKD. This is a Symmetric key Cryptographic approach that employs the use of Quantum laws. Quantum Key Distribution primarily takes into account the Heisenberg Uncertainty Principle and the Quantum Entanglement laws into consideration. Heisenberg's uncertainty principle (1984) established that, if the position of some particle is determined more precisely, its momentum can be known less precisely, and vice versa. Thus, at a time only one of the quantities can be measured with absolute certainty. This is the most crucial aspect of QKD. Quantum entanglement is observed when 2 quantum particles are a part of one quantum system and share the same quantum state, no matter the separation. Now let's understand this concepts in brief.

a) Uncertainty Principle

The uncertainty principle also called as Heisenberg Uncertainty principle as it was articulated first by the German Physicist Werner Heisenberg states that the position and the velocity of an object cannot be measured exactly, at the same time. The complete rule as shown in figure 2 stipulates that the product of the uncertainties i.e. Position and Velocity is greater than or equal to the quantity h (where h is Planck's constant). According to the principle any attempt made to precisely measure the velocity of a subatomic particle will knock it about in an unpredictable way or vice versa. It is therefore impossible to simultaneously know both properties with certainty. Quantum cryptography can leverage this principle but generally uses the polarization of photons on different bases as the conjugate properties in question [7]. This is because photons can be exchanged over fiber optic links and are perhaps the most practical quantum systems for transmission between two parties wishing to perform key exchange.

$$\Delta x \Delta p \geq \frac{h}{4\pi}$$

Figure 2: Formula For Heisenberg's Uncertainty Formula

b) Quantum Entanglement

The other important principle on which QKD can be based is the principle of quantum entanglement. According to this principle it is possible for a two particles to become entangled in such a way that when a property in one particle is measured in the other particle the opposite state will be observed instantaneously. This principle is true without the consideration of the distance between the two particles [7].

However one of the limitations in the principle is that it is not possible to communicate via entangled principles without discussing the observations over a classic channel. Therefore this process of communicating using entangles particles and a classic information channel is known as Quantum Teleportation**.**

IV. PROTOCOLS OF QUANTUM KEY DISTRIBUTION

a) The BB84 Protocol

The BB84 was the first protocol for quantum cryptography and Charles H. Bennett and Gilles Brassard proposed it, therefore the name "BB84". The protocol uses the pulses of polarized light where each pulse contains a single photon. In order to provide a secure communication, the sender can choose between four non-orthogonal states.

The sender has two bases with polarized photons [8].

The horizontal-vertical basis ⊕
- Horizontally polarised | ↔⟩
- Vertically polarised | ↕⟩

and the diagonal basis ⊗
- +45○ polarised | ⤡⟩
- −45○ polarised | ⤢⟩

In this system to send information, a coding system is needed. Therefore | ↕⟩ and |⤢⟩ code for 0, while | ↔⟩ and |⤡⟩ code for 1.The sender chooses at random one of the polarization states and sends it to the receiver. The receiver now measures the incoming state out of the two

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

bases. If the basis match then they get the perfectly correlated results and if the basis doesn't match the receiver will not get any information about the polarisation state of the photon. Lets consider an example to understand this protocol:

In this example lets consider that Alice is the sender and bob is the receiver.

- Alice randomly chooses the basis and the polarization of each photon and sends it to bob.
- Now, bob on receiving it randomly measures the basis of the photon. As he chooses it randomly it can either be perfectly correlated or the opposite of what Alice had sent.
- As bob selects the basis he tells Alice about it via the public channel and on comparing the selected basis, they both keep only those bits that correspond to each other. Therefore we get a short secret key called as the sifted key.
- Alice and Bob choose at random some of the remaining bits which they discard later to check the error rate. To ensure a secret key, Alice and bob must correct the errors. With the help of this procedure they reduce Eve's knowledge of the key. The remaining string of bits is the secret key.
- Once the secret key is obtained the actual process of securely encrypting a message can begin.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 3:Example Of BB84 Protocol

b) BB92 Protocol

The BB92 protocol is quite similar to the BB84 protocol however, after the BB84 protocol was published, Charles Bennett realized that it was not necessary to use two orthogonal basis and that a single non-orthogonal basis can be used without affecting the security of the protocol. In this protocol 2 quantum states are used instead of 4, this is what was proposed in the BB92 protocol [9].

c) SARGO4 protocol

The SARG04 protocol was built when researcher noticed that by using the four states of BB84 with different information encoding they could develop a new protocol which would more robust when attenuated laser pulses are used instead of single- photon sources.

The first phase of this protocol is quite similar to that of BB84. In the second phase when client A and client B determine which of their bases matched, A does not directly announce her bases rather it reveals the state she has sent and one of the states which code for the other value of the bit, which are not orthogonal to the first one. The receiver will either have guessed correctly or incorrectly and depending on it the qubits(quantum bit) are discarded accordingly.

The SARG04 protocol provides more security in the presence of PNS attack [9].

d) E91 protocol: Artur Ekert (1991)

The main difference from the BB84 Protocol here is that this method employs the use of quantum entanglement with the principles used earlier. Here a quantum pair of photons is polarized along a basis according to a randomly generated key separate from both the source and recipient. Thus, one photon from each pair goes to Alice and the other to Bob. Here both Alice and Bob measure the state at the same time. They compare the states of the shared key, which is generated randomly in the same manner as before. If the states of the photons where they have chosen the same polarization is different, the communication line has been compromised, otherwise the communication continues with the public key generated randomly. The advantage is that the random bit sequence is not generated at the source, which reduces the chances of compromising at the source. It is independent of the control of Alice and in case of no involvement of Eve, makes sure that probability of Alice and Bob having the same answer if they measure the same polarization is 100%. The presence of Eve destroys the correlation between the entangled pair and can be detected.

V. CONCLUSION

Encryption techniques have steadily improved with the advent of technology. However an algorithm, no matter how complex, can be possibly be cracked. Therefore to find the solution to this seemingly hapless pursuit QKD was developed. The advantage of this technique is that it is not governed by math, but by uncertainty, which cannot be predicted under any circumstance. Thus, randomness coupled with Quantum physics gives us a solution, which makes the communication absolutely uncrackable, and by extension one can make a claim that unhackable as well; since an attempt to hack can be detected and subsequent communication terminated. On paper it sounds very peachy, however, this method hasn't yet delivered to the promise it holds. Practically is still faults sometimes, attributing to equipment error or other errors. With time, as we develop equipment that physically deliver on the promise on paper, we will achieve absolutely secure communication. QKD is unarguably the future of communication.

REFERENCES

[1]. http://www.netaction.org/encrypt/need.html
[2]. https://en.wikipedia.org/wiki/Quantum_key_distribution
[3]. http://science.opposingviews.com/advantages-disadvantages-symmetric-key-encryption-2609.html
[4]. http://www.computerweekly.com/feature/The-future-of-secure-comms-quantum-key-distribution
[5]. http://www.idquantique.com/resource-centre/quantum-key-distribution/
[6]. https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/CSA_What%20is%20Quantum%20Key%20Distribution_QSS.pdf
[7]. Mart Haitjema, 'A Survey of the Prominent Quantum Key Distribution Protocols' [Online]. Available: http://www.cse.wustl.edu/~jain/cse571-07/index.html
[8]. Petra Paji, " Quantum Cryptography" [Online]. Available: http://homepage.univie.ac.at/reinhold.bertlmann/pdfs/dipl_diss/PetraPajic_BA _QuantumCryptography.pdf
[9]. Hitesh Singh, D.L. Gupta, A.K Singh," Quantum Key Distribution Protocols: A Review", IOSR Journal of Computer Engineering (IOSR-JCE)