A Secure Communication through Quantum Key Distribution Protocols

P.Satya Sai Teja
Kakatiya Institute of Technology and Science, Hanamkonda, Warangal, India
Satyateja401@gmail.com

P.Mounika Lakshmi
TechMahindra
Hyderabad, Telangana, India
pmounikalakshmi401@gmail.com

K.Vinay Kumar
Kakatiya Institute of Technology and Science, Hanamkonda, Warangal, India
kotte.vinaykumar@gmail.com

Abstract - Quantum cryptography is a new method of communication offering the security of the inviolability by using Law of Nature.Quantum Cryptography uses different secure communication by applying the phenomena of quantum physics. Unlike traditional classical cryptography, which uses mathematical techniques to restrict eavesdroppers, quantum cryptography is focused on the properties of physics of light for information. Quantum cryptography depends only on the validity of quantum theory, i.e., it is guarantied directly by the laws of physics. This is a different from any classical cryptographic techniques. This paper summarizes the current state of quantum cryptography and provides potential extensions of its feasibility as a mechanism for securing existing communication systems.

Keywords: Cryptography, Classical Cryptography, Quantum Cryptography, Qubits, Quantum Key Distribution, QKD Protocols

I. Introduction

The physics of quantum cryptography helps in achieving the possibilities for strong cryptography. The characteristics of quantum mechanics include the existence of indivisible quanta and of entangled systems, both of which are present at the root of quantum cryptography (QC). QC is one of the few best commercial applications of quantum physics at the single quantum level for achieving the secure communication.

Other applications of quantum mechanics to cryptography, which tend to come in three flavours:

- ✓ Quantum mechanism helps in breaking classical cryptography protocols.
- ✓ Quantum states are undetective which helps them to stay secure when classical cryptography methods are breakable y eavesdroppers.
- ✓ Cryptography is used to protect the information stored in quantum instead of classical information.

II. Classical Cryptography

Cryptography is method of design and analysis of mathematical techniques that enable secure communications in the presence of malicious eavesdroppers. It aims to send information to a proper receiver without giving any information to a third party for misuse of data.

Cryptography is method of protecting sensitive information as it is stored and transmitted through network communication channel. Cryptography operates by a sending scrambling or encrypting the original data by using different ways that obscures its meaning. The encrypted message is transmitted, and the receiver will recovers the message by using the same way the sender scrambled unscrambling or decrypting the transmission.

Today, ciphers are used where the algorithm for encryption and decryption which could be revealed to anybody without compromising the security of a particular message to third parties.So, in such cases ciphers provides a set of specific parameters, called a key, is used along with the data as an input to the encrypting algorithm. This encrypted data along with the key serves as the inputs for the decrypting algorithm. The encrypting and decrypting algorithms mainly depends on the secrecy of the key. To prevent the key from being discovered by accident or systematic search, the key is must be chosen as a very large number. When the connection is established and Once the key is established, at same time secure communication can take place by sending converted crypto text, even over a public channel that is vulnerable to total passive eavesdropping.

The main problem in cryptography is the maintain key distribution, for which there are essentially two solutions: one based on classical that is mathematical logics, and one based on Physics (quantum cryptography).But classical cryptography depends on the computational difficulty of factoring large integers, quantum cryptography relies on what we believe to be the universal laws of quantum mechanics.

The classical cryptography is divided into two types-symmetric and asymmetric systems.

The main aim of the secret key is to protect the data from eavesdroppers. The mathematical methods help the present cryptography methods to stay secure. For instance, an overnight breakthrough in mathematics or logics could make electronic money instantly worthless. To avoid such major economic and social risks, there is no alternative but to turn to symmetrical cryptosystems.

IRJECE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

2.1 Symmetrical (secret key) cryptosystems

Symmetrical ciphers are one of the classical cryptography method that use of a single key for both encryption and decryption. The symmetrical cryptosystems is used for routine applications such as e-commerce, bussines employ rather short keys. Asymmetrical cryptosystems, they offer only computational security unlike the symmetric cryptosystems. However, for a given key, symmetrical cryptosystems are more secure than their asymmetrical counterparts. In practical implementations, asymmetrical algorithms are not much used for encryption, because of their slowness, but rather for distribution of session keys for symmetrical cryptosystems such as DES. Because the security of those algorithms is not proven and not widely accepted, thus due to lack of this the security of the whole implementation can be compromised. If these algorithms were broken by mathematical advances, QC will constitute the only way to solve the key distribution problem.

III. Quantum Computing

Today's computers systems applies the laws of classical physics and Moore's law 2 which states that

Computers speed will be increased twice and capacity every 18 months due to chip makers are able to squeeze double as many transistors onto a computer chip. Due to these improvements transistors becomes much smaller.

But physics laws present a barrier that size of transistor shrunks to size of single atom which will not have any improvements to transistors to make them smaller in size. But what happens if the transistor could be replaced with a much better technology, a technology that allows for a new paradigm of computing?

In classical computing, information is stored in fundamental units called bits, where a bit can hold a binary digit with the value of 0 or 1.In quantum computing it provides a flexibility to hold both 0 or 1 value at same time depending on data, this is known as superposition of two states. These quantum bits are known as qubits and measuring the state of a qubit causes it to select or "collapse into", being a 0 or a 1. These properties make the quantum computers and advantage over the classical computers which helps them in rapid parallel computations which makes easier and efficient. For some unsolved mathematical equations and logics, quantum computers are able to perform computational tasks with efficiencies that are not known to be possible with classical computers. The design, development and analysis of patterns of computation carried out by using the quantum computers is a field known as quantum algorithms, and the most well-known quantum algorithms – Shor's algorithm and Grover's algorithm. These algorithms posses threat for many widely used cryptosystems that base their security on the premises that certain computational problems are difficult to solve by classical computing techniques. Quantum computers, developing quantum algorithms, can solve these different type classes of problems quickly enough to jeopardize the security of the information that is encrypted. Classical public-key cryptography relies on the assumption that some problems take an much long time to solve, that it would take a very long time for messages to be decrypted - but with technology changes the speed with which quantum algorithms can solve some of these problems severely challenges that assumption.

IV. Quantum Cryptography

The concept of quantum cryptography[2][11] was first proposed in the 1970s. One of the main aim of quantum cryptography is to create cryptographic protocols to protect quantum States whose properties cannot be copied. Advantages of quantum cryptography are that it gives more secure data transfer than classical cryptography. The first successful quantum cryptographic device could translate a secret key over 30 centimeters using polarized light, calcite crystal(s), and other filters, electro-optical devices.

Based on the laws of physics, quantum cryptography allows to exchange cryptographic key between two remote connected systems with unconditional security protocol. The foundation of quantum cryptography was laid by the concept of Heisenberg uncertainty principle, which describes that it can interpret as certain pair of physical properties that are related to each other in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. This law uses the quantum states of photons to transfer cryptographic key material via polarized photons to represent bits either 0 or 1. Each photon, is known as Qubit, carries only one bit of quantum information. To receive those qubits, the recipient must have determine the photon's polarization. The act of an eavesdropper intercepting a photon in this transmission will irreversibly change the information encoded on that photon, thereby detecting any security breach.

Quantum cryptography has great potential to become the most secure, confidentiality and privacy of communication in the future ICT world and also becomes the driver for the success of a series of services in the field of e-government, business, e-commerce, e-health, transmission of biometric data, intelligent transport systems and many others.

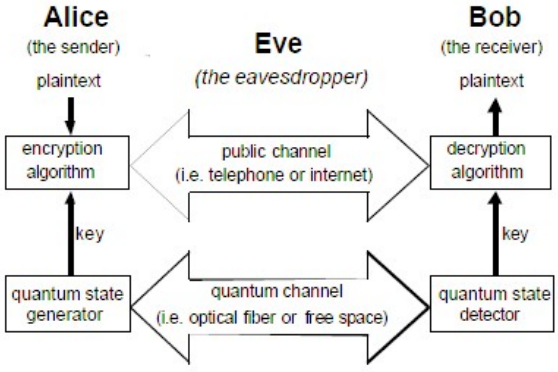

Fig 1: A Quantum Cryptographic communication system for secure transferring of random key.

IRJECE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

V. Why Quantum Cryptography Is So Secure

Quantum cryptography is verified to be secure[5][6][7] for three main reasons. One, the quantum no cloning[14] theorem states that without knowing properties of quantum it can be cloned. In Theory when a message is sent its unknown properties helps it in restrict copy or sent on. Two, in a quantum system, which can be in one of two states, any attempt to measure the quantum state will disturb the system. When quantum message is sent and eavesdropper intercepted and read will become garbled and useless. Three, the effects produced by measuring a quantum property are irreversible, which means when eavesdropper intercepted and changes the quantum properties and it can be reversible or change. These three properties provide the power of quantum cryptography fro secure communication. No amount of effort or genius can alter the fact that observing a quantum property irrevocably alters the object being observed. This is why quantum cryptography is so powerful in distributing the keys used to encrypt messages. A advanced knowledge eavesdropper could intercept a quantum encrypted message, and if he made the correct measurement for each bit of the message he would have the key, But although the likelihood of making the correct measurements is extremely very low for longer messages. But where as keys are random strings of characters, so even a eavesdropper successes could not tell if he had successfully intercepted a key. For all of his work, the eavesdropper is still becomes unsuccessful – But he has altered the key by reading it, and the acknowledgement can see that it has been tampered by eavesdroppers, and new keys are sent until one is received that has not been tampered with.

VI. Quantum Key Distribution

The method of by which a secret key is distributed using quantum cryptography is known as Quantum Key Distribution.Quantum Key Distribution (QKD), based on quantum cryptography. QKD enables two systems to distribute a shared random bit string generated by quantum cryptography known only to them, which can be used as a key to encrypt and decrypt messages.

QKD is a means of distributing keys[1] from one system to another, and detecting eavesdropping. It allows two parties to establish a common random secret key by taking advantage of the fact that quantum mechanics does not allow for distinguishing non-orthogonal states with certainly changes. since eavesdropping is also governed by the laws of quantum mechanics, these changes cause errors in transmissions and reveal the eavesdropper.QKD helps only in identifying the eavesdroppers in the communication channel. If any eavesdropping is detected in the channel, the key is simply thrown away i.e it is useless, and a new one is generated. No leakage of information occurs in this.

The primary application of QKD is to create a secret key, which is then with help of the one-time pad to send unconditionally secure messages. By Conjunction of quantum key distribution and one-time pad we ensure the connection is secure. The drawback for classical one-time pads is the distribution of encryption/decryption keys, and this is solved in the quantum cryptography as we can transfer key data in a totally secure fashion.

There also exist alternative key distribution algorithms using public key schemes that which are not in RSA or ECC.In contrast to these public key schemes, QKD as a cryptographic primitive key offers security that is guaranteed by using the laws of physics. QKD is a method for secure key establishment [GIS02] and proven to be information theoretically secure against many arbitrary attacks caused by third parties, including quantum attacks. Consequently, quantum key distribution provides the means to securely distribute secret keys that can be used with quantum safe symmetric key algorithms like Advanced Encryption Standard (AES), or one-time pad encryption.

Conceptually, the security of QKD is achieved by transforming the encoding information in quantum states of light. Using quantum states which allows security to be based on fundamental laws in quantum physics and quantum information theory. There are three deeply related notions from quantum physics that illustrate the source of the unique security properties of QKD[3][4]:

1. The Heisenberg uncertainty principle states that while measuring the unknown quantum-mechanical state, it is physically changed.
2. The no cloning[14] theorem states that it is highly impossible to make duplicate of unknown quantum state.
3. There exist properties of quantum entanglement that set fundamental limits on the information leaked to unauthorized third parties.

Interestingly, due to the laws of quantum mechanics, It is impossible for eavesdroppers to physically find the quantum key distribution. Looking at the quantum information encoded in quantum states actually changes the information in ways that can be detected by the legitimate parties. Even eavesdropper single change in the quantum key distribution it is irreversible so bit of information changes and detects the eavesdropper in the channel of communication. The percentage of attempts made by eavesdroppers results in errors which an eavesdropper necessarily introduces allow the sender and recipient to calculate it, not only whether an eavesdropper was present, but also it gives the precise how much of the information about the key the adversary could have gained access in the worst possible case with the most powerful quantum algorithms and hardware.

An important characteristic of quantum key distribution is stated that any attack (e.g. any attempt to exploit a flaw in an implementation of transmitters or receivers)from third parties must be carried out in real time. In Classical cryptography temporary stores the message for later decryption but in quantum message it is not possible. This greatly reduces the window of opportunity for performing an attack against QKD; this window is much wider for classical cryptography.

The security of QKD has been proven in a number of frameworks that including the universal computability [BHL05, Sca09], the abstract cryptography framework

IRJECE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

[MAU11], or the authenticated key exchange framework [MSU13]. The composability of QKD as a cryptographic primitive allows safely combining the distributed keys with other provably secure schemes such as Wegman-Carter authentication or onetime pad encryption while maintaining quantifiable long-term security.

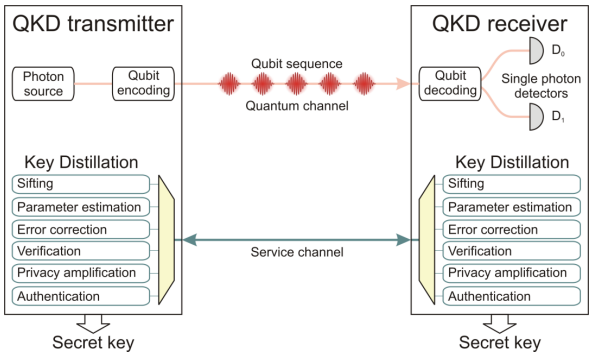

Fig. 2: Illustration of a typical prepare-and-measurement QKD setup

VII. How Quantum Key Distribution Works

Quantum key distribution[8] is a process that is used for authenticated communication channel together with a quantum communication channel in order to establish a secret key. There are many different protocols for implementing quantum key distribution, all of which require both a quantum channel, and an authenticated classical channel. The quantum channel uses optical fibres or free space/ satellite links to send photons between Alice and Bob, whereas the classical channel could be a simple (authenticated) telephone line that Alice and Bob use to communicate with each other. Interestingly, both of these can be public. It is described in section 3.2.1 that the quantum channel necessarily shows Alice and Bob when an eavesdropper has been listening in, and it is a fact of the QKD protocols that the classical channel will provide a broadcast publicly without compromising security to third parties.

Quantum Key Distribution begins from Alice deciding to distribute some cryptographic key to Bob or not. Both Alice and Bob have the specific specialized optical equipment necessary for establishing the quantum communication channel, as well as access to a classical channel where Alice and Bob can communicate with one another. Alice uses a laser light source to send a stream of photons one-at-a-time. Each photon consists of one bit of information. As each photon is sent, she randomly chooses to prepare it in one of two ‘’bases’’ i.e for bit information 0 or 1. Basis can be described as a perspective from which a photon is measured.

As the recipient, Bob needs to store values for each of the photon he receives via the quantum communication channel. To do this, he must, first like Alice, make a measurement of each photon, and he then therefore chooses one of the two possible ‘’bases’’ and stores which one he measured in. These choices are random and do not require any information about the bases that Alice chose when she was sending each bit to the bob. Afterward, Alice and Bob communicate over the classical channel to compare which basis each bit was measured in at each end of the quantum channel. Sometimes Alice and Bob will randomly choose the same basis, and these are the bits for which they will get the same value for the photon (which is useful, so they will keep this bit as part of the key). When Alice and Bob measure the photon using different bases, they throw this bit away and do not use it in the final key.

After each bit has been sent and received, Alice and Bob can speak publicly about which basis they used to measure each photon, and this can provide enough information for each of them to generate key from the received quantum states, but not enough information for an adversary to reconstruct the key. Thus, an eavesdropper will not be able to discover the transmitted key for two important reasons. Firstly, the adversary cannot directly observe the photon without changing them, therefore being detected and having these bits discarded by Alice and Bob. Secondly, the adversary cannot indirectly observe the photon through observing the measurements of Alice and Bob, either, since Alice and Bob do not disclose the final measurement result for each quantum state. Rather, they only disclose which basis they used to measure it. By this time, it is too late for the adversary to measure the photon, because it has already been received by Bob, so knowing the basis that Alice used is not useful. It is well-established using information theoretic proofs that the measurement information is inadequate for an adversary to use to reconstruct the generated key.

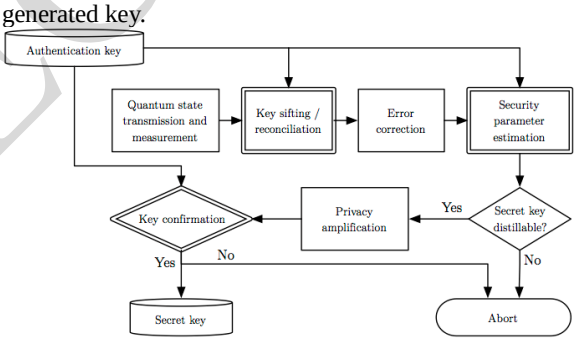

Fig. 3: Flow chart of the stages of a quantum key distribution protocol

VIII. Authenticating QKD Channel

An important aspect of consideration in quantum key distribution[13] is how to authenticate the classical communication channel to ensure that the two people communicating are actually Alice and Bob. The authenticated classical communication channel applies different methods to realize.

The most secure method for authentication does not require any computational assumptions and uses a small amount of random secret key or data that is initially shared between Alice and Bob. By combining this form of authentication with QKD may be expressed as an expansion of the initial secret data without sacrificing randomness or secrecy key. Subsequent communication using QKD

IRJECE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

normally uses part of the generated classical key material for authenticating subsequent QKD sessions, and part of the keying material for encryption.

At initial Alice and Bob do not share an authentication key, a natural alternative is to communicate using the public key signatures to authenticate their initial QKD session. Provided the public key signature will not be terminated during the QKD session, the resulting key is information theoretically secure and thus cannot be broken by future algorithmic advances, even if the public key signature is later terminated [PPS07, IM11, MSU13]. Subsequent QKD sessions between Alice and Bob may be authenticated with the help of previous QKD keys, so that they only need to rely on the short-term security of the public key signature once.

IX. QKD PROTOCOLS AND THEIR IMPLEMENTATIONS

Several QKD protocols[10] have been successfully implemented in business and commercial research labs, transmitting keys over long distances through either optical fibres or free space up to 150m. These protocols divided into two categories, and while theoretically identical in their analysis, are differentiated experimentally in part by how eavesdropping is detected:

1. Prepare-and-measure QKD allows authorized parties to detect eavesdroppers by comparing the amount of error i.e change in state of quantum they might expect in their communications to the actual error of their measurements. This technique depends upon the fact that an adversary intercepting a quantum state must measure it, and in this adversary attempting to guess and records the original state to forward it to the recipient, they will introduce a percentage of identifiable error occurred in the communication channel.

2. Entanglement-based QKD allows legitimate parties to detect eavesdroppers by virtue of the fact that if the sender and recipient each have a photon the two of which are related by quantum-mechanical entanglement-interception or measurement by an malicious third parties will change the two-photon system in a way that the legitimate parties can readily detect the error and presence of eavesdroppers.

One example of a QKD protocol is the BB84 protocol [BB84], which was the first protocol proposed for quantum key distribution and remains one of the most widely implemented protocols which is used for commercial products and within research labs.

The SARG protocol [SARG04] is similar to BB84 and has been used over a period of 21 months of continuous operation on the international Swiss Quantum network [STU11].

More recent protocols which aim to have convenient implementations while still enabling long-distance and high transmission rate QKD are the Differential-Phase-Shift protocol [WAN12] and the Coherent One Way protocol [STU09], which both have exceeded 250 km transmission distance in optical fibre.

There is also Continuous Variable QKD protocol that is the only QKD protocol that does not require single-photon detectors.

In addition to the above commonly used protocols, there is on-going research into protocols that aim to reduce the security assumptions of the actual implementation of the QKD devices. For example, Another possibility exists in the Ekert protocol [EKE91], which proposes the use of quantum entanglement to implement QKD with complete device-independent security. Once implemented, this would ultimately mean that trust assumptions of the QKD system implementation by a manufacturer could be reduced to a minimum.

Quantum key distribution penetration testing and security research ('quantum hacking') is an active area of academic and commercial work, and has identified some implementation specific vulnerabilities in QKD systems, leading to improved system designs.

X. HOW QUANTUM PROPERTIES OF LIGHT ARE USED TO PRODUCE KEYS

The quantum properties of light[15] used to send secret messages. Light has wavelike properties, and the waves can be aligned, or polarized, in any direction. Normal sunlight consists of varying wavelengths of light(which produce the colors in a rainbow) polarized in a random fashion. But in Laser light consists of only wavelength and it is polarized in only one direction. These characteristics are what make lasers so powerful – the individual waves of light, since the properties of they are equal, combine to produce one most powerful wave of light. These made Lasers to use to produce photons with a given polarization in quantum key distribution. Polarization can simply be thought of as the "tilt" of the light wave.

XI. QUANTUM CODING SCHEMES

As described in the previous section[12], polarization and measurement of polarization of photons can be done with the use of Polaroid. For the purpose of evaluating simple coding scheme, let us consider only the two filters rectilinear and diagonal polarization schemes. This gives us 4 different directions of polarization of a photon. See figure below.

The 4 different possible quantum states (shown in the figure) give us 4 quantum bits or 'qubits'. With these 4 qubits we can represent the classical bits 1 and 0 as follows.

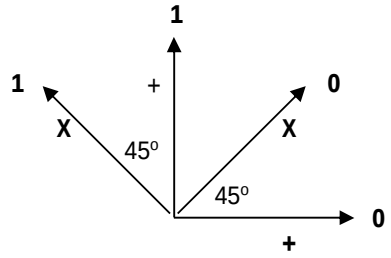

Fig 4: Mapping of quantum digits to binary digits

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

Bit 0 = photon with horizontal polarization or by a photon with polarization at 45 degrees to the horizontal direction.

Bit 1 = photon with vertical polarization or by a photon with polarization at 135 degrees to the horizontal direction.

The above scheme, by Charles H. Bennett and Gilles Brassard, was the first proposed quantum encoding of classical bits and is referred to as the BB84 coding scheme.

We shall use the following notations:

'+' to represent the rectilinear scheme

'X' to represent the diagonal scheme

'-' to represent 0 (Horizontal polarization quantum state)

'/' to represent 0 (45 degrees to horizontal polarization state)

'|' to represent 1 (Vertical polarization quantum state)

'\' to represent 1 (45 degrees to vertical polarization state)

So, using the above qubit representations, a BB84 transmission for the binary 11010011 could look like this:

TABLE 1: QUBIT TRANSMISSION & BINARY DIGIT SELECTION

Alice : Bits	1	1	0	1	0	0	1	1
Alice : Qubit	↕	↕	↔	↕	/	/	\	↕
Bob : Scheme	+	X	X	+	+	X	X	+
Bob : Qubit	↕	\	\	↕	↔	/	\	↕
Bob : Bits	1	1	1	1	0	0	1	1
Key Selection	√			√		√	√	√

Alice sends the 1st 1 using the + scheme, the 2nd one using the X scheme, 1st 0 using the X scheme and so on.

XII. CONCLUSION

As this quantum cryptography is a new science in a cryptosystem technology and many researchers from around the world are discovering a way of incorporating some new devices and have already made a breakthrough, it looks quantum cryptography will be an advanced code- making technology which is theoretically uncrackable. This is because of the laws of quantum physics that dictate an eavesdropper could not measure the properties of a single photon without the risk of altering those properties. In other words, even if an eavesdropper is able to listen in on a line, he/she could be unable to learn much about the communications traversing it.

REFERENCES

[1] Bennett, C. H., and Brassard,G.Quantum public key distribution reinvented.Sigact News 18(4) (1987), 51–53

[2] Bennett,C.H., Brassard, G., and Ekert, A. K.Quantum cryptography.Sci.Am.267,4(Oct.1992), 50.

[3] Bennett, C. H., and DiVincenzo, D. P. Quantum information and computation.Nature 404 (2000), 247–55.

[4] Bennett, C. H., and Shor, P. W. Quantum information theory. IEEE Transactions on Information Theory 44, 6 (1998), 2724–42

[5] Brassard, G. Cryptology column -25 years of quantum cryptography. Sigact News 27(3) (1996), 13–24.

[6] Gottesman, D., and Lo, H.-K. From quantum cheating to quantum seurity.Physics Today 53,11 (Nov. 2000), 22.

[7] Lo, H.-K. Quantum Cryptology. World Scientific, 1998.

[8] Singh, S., 1999, The Code Book: The Science of secrecy from Ancient Egypt to Quantum Cryptography(Fourth Estate,London).

[9] Brassard, G., 1988, Modern Cryptology: A Tutorial, Lecture Notes in Computer Science, Vol. 325 (Springer, New York).

[10] Shannon, C. E., 1949, ''Communication theory of secrecy systems, '' Bell Syst. Tech. J28, 656–715.

[11] Stallings, W., 1999, Cryptography and Network.

[12] Wiesner, S., 1983, ''Conjugate coding,'' SIGACT News, 15,78–88.

[13] Bennett, C. H., and G. Brassard, 1985, ''Quantum public key distribution system,'' IBM Tech. Discl. Bull. 28 , 3153–3163.

[14] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature 299, 802 (1982).

[15] BBN Technologies. "Quantum Cryptography." URL:http://www.bbn.com/networking/quantumcryptography.html

[16] Meystre, Pierre. "Future Issues in Theoretical Quantum Cryptography."15Feb1995.URL:http://www.aro.army.mil/phys/proceed.htm#Future%20Issues (10 Nov. 2002).

IRJECE

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)