IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 3 (March. 2019), ||S (II) || PP 37-41

Quantum Entanglement and Unbreakable Security In The Near Future

Bipul Sarkar[1] andShyamal Kumar Pal[2]
[1.]*Department of Physics, Bankura Christian College, Bankura, WB-722101, India.*
[2.]*Department of Physics, Bankura University, Bankura, WB-722101, India.*
Corresponding Author:Dr. Bipul Sarkar

Abstract: In this paper we highlight some special properties of quantum entanglement and quantum cryptography which is useful for recent security when data is transmitting over the network. In classical cryptography, bits are used to encode information whereas quantum cryptography uses photon or quantum particles (qubits) to encode the information. The emphasis of this paper is to rise of Quantum Cryptography and specially lighting on Quantum key distribution (QKD) techniques which ensure the unbreakable security in near future.

Key Word: Quantum Entanglement, Quantum Cryptography, Qubits, QKD.

Date of Submission: 01-03-2019 Date of acceptance: 18-03-2019

I. INTRODUCTION

Among the other activities communication is the prime activity to develop and growth a society since the time of civilization started. It is the activity of exchange information by various signals, visuals, writing something or behavior. A letter to friend, international confidential report or emergency information to government or organization, online banking transaction, online personal data sharing, war time military strategic information transaction have always essential strong security for protecting information and cryptology was developed. Cryptology studies contained with two opposite related disciplines, one is cryptography and the other is cryptanalysis. Cryptography is a method concerned with encoding a message in such a way that is provide authentication and confidentiality [1], so that only the sender and the particular recipient can decode it. In contrast, cryptanalysis is the science of decoding the encoded message without the key and without the permission of the sender or the receiver.

Many years ago(400 B.C.) the Spartan military commanders used scytale (a device) to write messages on strips of paper twirled around a baton; The technology behind it that after wrapped around the proper-sized baton to the strip the said massage could be decoded.Modern cryptography, like Web-standard RSA(initial letters of the surnamesof *Ron Rivest*, *Adi Shamir*, and *Leonard Adleman*)public key data encryption,public-key cryptosystem etc. is now an elegant concept invented by Diffie and Hellman [2]. In this technique, basically relies on keys created by multiplying two gigantic prime numbers together. A securityhacker should need to create the prime factors of thesecurity key to break the particular code or cipher, which are very much difficult to calculate on bound time.But with enough computational strength, these prime factors of the cipher could be calculated in finite time. Ifthe security hackerseeks out an easy way to calculate prime factors of the cipher then RSA encryption security would be invalid.

In theory, any classical private channel can be easilymonitored inertly, without the knowledge to sender or receiverthat the eavesdropping has been done. Classical physics is thetheory of macroscopic bodies and phenomena such as radio signals that allows a physical property of an object to be measured without disturbing other properties. Cryptographic key like information is encoded in computable physical properties of some object or signal. Thus there is open possibility of passive eavesdropping in classical cryptography.

On the other hand, the encryption securities of the above techniques are needs to be examined thoroughlysinceit's based on computational complexity [3]and speed of encrypting of text is becomes slow. With the approach of quantum computing, the scenario of cryptography gradually changed its paradigm. Once quantum computation is used in cryptography on a physical scale, the computational complexity of the present cryptosystems will be vanished [4]. For this reason, quantum mechanics plays an important role in cryptography. Basically, quantum cryptography incorporates many aspects of quantum entanglement together with Heisenberg uncertainty principle toobtain completely secure communications.

II. QUANTUM ENTANGLEMENT:

The basic idea of quantum entanglement is that two particles can be intimately linked to each other even it detached by billions of light-years of space and a change induced in one will affect the other. It is one of the most passionate and counter-intuitive aspects of Quantum Mechanics which enable completely accurate predictions of measurements that customarily would be of a statistical nature, even if the subsystems are detached by an arbitrary distance. Its existence was first recognized in early work of the pioneers of quantum mechanics[5]. It is the basis of the Einstein-Podolsky-Rosen (EPR) argument[6] which argued that its predictions are incompatible with locality. Foran example, a system consisting of two qubits (spin- $\frac{1}{2}$particles) with a basis of states $\left(\left|\uparrow\right\rangle_A , \left|\downarrow\right\rangle_A \right) \times \left(\left|\uparrow\right\rangle_B , \left|\downarrow\right\rangle_B \right)$. Let Alice observes qubit-A,Bob observes qubit-B. Now, the state $\left|\psi\right\rangle = \frac{1}{2}\left(\left|\uparrow\right\rangle_A \left|\uparrow\right\rangle_B + \left|\downarrow\right\rangle_A \left|\downarrow\right\rangle_B \right)$ is entangled. BeforeAlicemeasuresσ_A^z,Bob can obtain either result$\sigma_B^z = \pm 1$. But after Alice makes the measurement,the state in B collapses and Bob can only get one result.However, if the subsystems A and B are far apart the result is same (EPR paradox). Thus, a pair of quantum systems which is entangled can be used as a cryptographic task.

An entangled state is not exact with a classically correlated state. For the density matrix

$$\rho = \frac{1}{2}\left(\left|\uparrow\right\rangle_A \left|\uparrow\right\rangle_B \left\langle\uparrow\right|_A \left\langle\uparrow\right|_B + \left|\downarrow\right\rangle_A \left|\downarrow\right\rangle_B \left\langle\downarrow\right|_A \left\langle\downarrow\right|_B \right)$$

We have, in both cases,$\langle\sigma_A^z \sigma_B^z\rangle = 1$, but for the entangled state,$\langle\sigma_A^x \sigma_B^x\rangle = 1$and it vanishes for the classically correlated state i.e., $\langle\sigma_A^x \sigma_B^x\rangle = 0$.

2.1. Pure State Entanglement

A pure state is a quantum state which can be described by a single state vector. For pure states, it is rather easy to find out if a given state is separable or entangled. Any given pure state $\left|\psi\right\rangle$ is entangled if S(ρ^A) > 0, where S is any suitable entropy like Von-Neumann Entropy i.e., $S(\rho) = -Tr\rho \ln \rho$ and ρ^A is the reduced density matrix . The entropy of a pure state always vanishes and entanglement can be considered as information about a composite state, which does not apply to any one of the single parties but only to the composite system [7].

2.2. Mixed State Entanglement

The mixed state is a more general state than a pure state.Mixed states are in fact the most frequently encountered states in real experiments, since hardly any quantum system can be isolated completely from its surrounds.For mixed states; this task is much more complicated. Since up to now new method was found capable of distinguishing between entangled or separable states in general, one has to settle with necessary separability criteria. If one of these is violated by a state, is has to be entangled, while non-violation does not represent a conclusive result.It is in general not possible to keep track of the many environmental degrees of freedom, and the state of the system is given bythe partial trace over the environment. This reduced state is then typicallymixed.*Mixed entangled states*, in turn, are defined by the non-existence of decomposition into product states[8].

2.3. Measure of entanglement

Entanglement can be used to perform various tasks which are otherwise impossible. To apply this resource perfectly the quantification is very much necessary. However there is no measure of entanglement which satisfies all the properties of a good measure of entanglement. One of important measures of entanglement is Von-Neumann entropy and pure state entanglement.

2.3.1. Von-Neumann entropy and Pure state entanglement

If we have a mixture of quantum states $\left|\psi_i\right\rangle$ with probability,P_i. Thus, the density matrix of the mixture$\left\{P_i , \left|\psi_i\right\rangle\right\}$is

$$\rho = \sum_i P_i |\psi_i\rangle\langle\psi_i| \qquad (1)$$

Now, Von-Neumann entropy, S(ρ) = - Tr (ρ ln ρ).

Thus, the Von Neumann entropy of a quantum ensemble with density matrix ρ with eigenvalue λ_i is,

$$S(\lambda_i) = -\sum_i \lambda_i \ln \lambda_i \quad (2)$$

in two-party system with subsystems A and B.

III. QUANTUM CRYPTOGRAPHY

The Heisenberg uncertainty principle and Quantum entanglement can be exploited in a system of secure communication, often referred to as Quantum cryptography [9,10]. It is a recent technique that can be used to ensure the confidentiality of information transmitted between two parties [11]. The mid-twentieth century was marked by the creation of a new discipline called information theory. Information theory is aimed at defining the concept of information and mathematically describing tasks such as communication, coding and encryption. Pioneered by famous scientists like Turing and von Neumann and formally laid down by Shannon.Shannon was also interested in cryptography and in the way we can transmit confidential information. He proved that a perfectly secure cipher would need a secret key that is as long as the message to encrypt. But he does not say how to obtain such a long secret key.

Quantum cryptography devices only work if the devices that generated the code for encryption were completely reliable. To generatea secure encryption the only condition is that the random numbers generated for the one-time pad are surely random and the device should be some quantum entanglement, which can be determined by running a statistical test. According to quantum mechanics, certain properties of subatomic particles can't be measured without disturbing the particles and changing the outcome. i.e., a particle exists in a state of indecision until a measurement is made, forcing it to choose one state or another. Thus, if anyone made a measurement of the particle, it would firmly change the particle.If an encryption key were encoded in bits represented by particles in different states, it would be immediately obvious when a key was not secure because the measurement made to hack the key would have changed the key.

Quantum Cryptographic methods of information security based on quantum technologies,
(i) Quantum digital signature (QDS)
(ii) Quantum key distribution (QKD):
(iii) Quantum stream cipher (QSC)
(iv) Quantum secret sharing (QSS)
(v) Quantum secure direct communication (QSDC)

CRYPTOGRAPHIC METHOD OF INFORMATION SECURITY BASED ON QUANTUM TECHNOLOGY							
QUANTUM DIGITAL SIGNATURE		QUANTUM KEY DISTRIBUTION		QUANTUM SECRET SHARING		QUANTUM SECURE DIRECT COMMUNICATION	
QDS using single qubits	**QDS** using Entanglement states	**QKD** using single qubits	**QKD** using Entanglement states	**QSS** using single qubits	**QSS** using Entanglement states	**QSDC** using single qubits	**QSDC** with block transfer

Fig. 1 Quantum Cryptographic methods of information security.

3.1. Quantum key distribution (QKD)

Quantum key distribution (QKD) [12] is a technique that allows two parties, to share a secret key for cryptographic purposes.To ensure the confidentiality of communications, let us suppose Alice and Bob agree on a secret key i.e., a piece of information.Encryption is performed by combining the message with the particular key in such a way that the result is unimaginable by an observer who isunaware about the key. The recipient of the message uses his part of the key to decrypt the real message. The goal of QKD is to guarantee the confidentiality of a particular distributed key.The secrecy of the transmitted data is then ensured by a chain with two links- (i) the quantum-distributed key and (ii) the encryption algorithm. If one of these two links is broken, the whole chain is endangered; hence we have to examine the strengths of both links. The laws of quantum mechanics have strange properties, with the nice property of making the detectable of spy. If a spy,

conventionally called Eve, tries to know the key by hacking, she will be detected. The legal parties will then cast away the key and thus no confidential information has been transmitted yet. If, on the other hand, no tapping is detected, the secrecy of the distributed key is out of danger.

On the other hand, second link of the chain, the encryption algorithm must also have strong properties. The secrecy of data is absolutely safe if the encryption key is as long as the message to transmit and is not reused for subsequent messages. This is where quantum key distribution is particularly useful, as it can distribute long keys as often as needed by legitimate parties.

Quantum key distribution requires a transmission channel on which quantum carriers are transmitted from one legitimate party to another. If any particle obeying the laws of quantum mechanics can be apply for this type of security purpose. In the quantum carriers, Alice encodes random pieces of information that will compose the key. These key may be, for instance, random bits or Gaussian-distributed random numbers. During the transmission between Alice and Bob, Eve might listen to the quantum channel and therefore spy on potential secret key bits. This does not pose a fundamental problem to the legitimate parties, as the spy is detectable by way of transmission errors. In the case where errors are detected, Alice and Bob may decide to stop the protocol in the preliminary stages. At least, this prevents the creation of a key that can be known to the opponent. Furthermore, the secret-key distillation techniques allow legitimate partiesto recover from such errors and create a secret key out of the bits that are unknown to spy.

After the transmission of massage, Alice and Bob can verify a fraction of the exchanged information to see if there are any transmission errors caused by Eve. For this process, QKD requires the use of a public classical authenticated channel, as shown in Fig. 2.

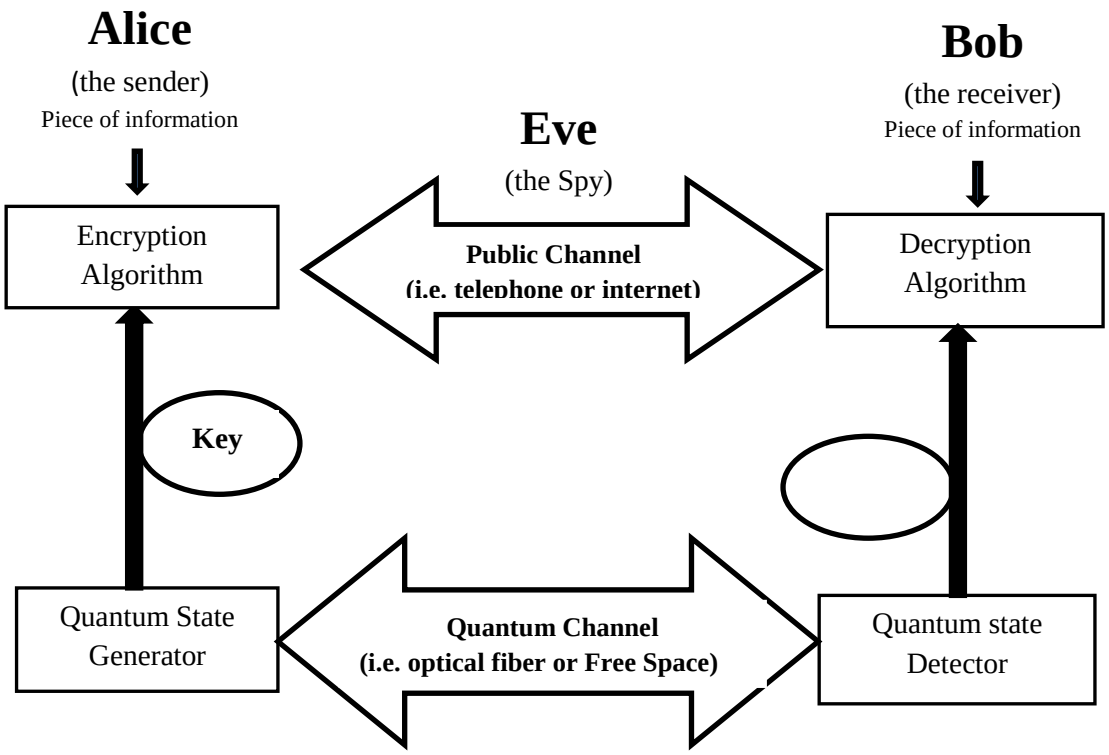

Fig.-2 Quantum key distribution comprises a quantum channel and a public classical authenticated channel.

This classical channel has two important characteristics, namely, publicness and authentication. It is not required to be public, but if Alice and Bob had access to a private channel, they would not need to encrypt messages; hence the channel is assumed to be public. As an important consequence, any message exchanged by Alice and Bob on this channel may be known to Eve. The authentication feature is necessary so that Alice and Bob can make sure that they are talking to each other. We may think that Alice and Bob know each other and will not get fooled if Eve pretends to be either of them.

As a cryptographic tool, QKD is unconditionally secured, able to deliver provable security even in the face of attackers with unlimited computational power. QKD is vastly superior to current key systems such as in the Secure Socket Layer (SSL) protocol and the Internet Key Exchange protocol (IKE). Used in end to end schemes, QKD can formed the essential building block for unconditionally secure communication.

IV. CONCLUSION

Entanglement is a fascinating and useful property of quantum mechanics. In quantum mechanics, entropy is a useful measure of entanglement for characterizing many-body ground states (and also in quantum information theory) in principle it can be measured in condensed matter or cold atom experiments. QKD offers the ultimate security assurance in communicationworld.The QKD protocol has been widely adopted gradually in the fields of e-governances, e-commerce, e-health, and transmission of biometric data, intelligent transport systems and many others. Thus, Quantum entanglement promises to be an unbreakable, eavesdropping-proof security measure in the future communication.

REFERENCES

[1]. N Garg, P Yadav, "Comparison of AsymmetricAlgorithms in Cryptography",IJCSMC, Vol 3, Issue. 4, page 1190 – 1196, 2014.

[2]. WDiffie, M Hellman, "New directions in cryptography" IEEE Trans. Inform. Theory, Vol 22, No 2,Page644-654, 1976.

[3]. R L Rivest, A Shamir, LAdleman"A method for obtaining digital signatures and public-key cryptosystems" Communications of the ACM, Vol 21, No 2, Page120–126, 1978.

[4]. P W Shor "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer",SIAM journal on computing, Vol 26, No 5, Page 1484–1509, 1997.

[5]. E Schrödinger,"Discussion of probability relations between separated systems",Mathematical Proceedings of the Cambridge Philosophical Society,Vol 31, No 4, Page 555-563. 1935.

[6]. AEinstein, BPodolsky, NRosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?", Phys. Rev.,Vol 47 No 10, page 777-780, 1935.

[7]. D Cavalcanti, M O Terra Cunha, A. Ac´ın, "Multipartite entanglement of superpositions", Physical Review A, Vol 76, No 042329, 2007.

[8]. R F Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admittinga hidden-variable model", Phys. Rev. A, Vol**40**, No 4277, 1989

[9]. C H Bennett, G Brassard, A K Ekert,"Quantum Cryptography, scientific American" ,Vol 267, No 4, 1992.

[10]. C Elliot, "Quantum Cryptography", IEEE Security & Privacy Journal, Vol 2, No 4, Page 57-61,2004.

[11]. C Elliot, "The DARPA Quantum Network, Quantum Communications and cryptography", CRC Press/Taylor & Francis, Boca Raton/London, Page 83-102, 2005.

[12]. A Poppe, MPeev, O Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna", International Journal of Quantum Information, Vol 6, No 2, Page 209-218, 2008.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Dr. Bipul Sarkar. "Quantum Entanglement and Unbreakable Security In The Near Future."IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 03, 2019, pp. 37-41.