Volume 3, Issue 10, October 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Quantum Key Distribution Scheme with EPR Sequences

Ch.Krishna*, A.Sujith Kumar
M. Tech (SE) & SNIST.
India

Abstract— Since languages become the tool for communication, the desire and need to transmit secret messages from one person to another begin.The most important classic cryptographic scheme is public-key crypto-system its safety relies on the high complexity of the underlying mathematical problems, for instance the factorization of large numbers. But with the development of the quantum computation(QC), especially the Shor's algorithm for factoring big numbers, the systems once seemingly unbroken in practice will be aggressed easily. Now in the information community, the safety of transmission of secret information is becoming more and more concerned. One essential theme of secure communication is to distribute secret keys between senders and receivers. Quantum mechanics, one of the greatest discovery of the 20th century, has now entered the field of cryptography: if the key distribution makes use of quantum states, an eavesdropper can not measure them without disturbing them.The principle of the quantum mechanics can help to make the key distribution secure. A quantum key distribution scheme using EPR pairs is presented here. This scheme is efficient in that it uses all EPR pairs in distributing the key except those chosen for checking eavesdroppers.

Keywords— Bell States,EPR pairs,Quantum Entanglement,Quantum Key Distribution.

I. INTRODUCTION

Quantum cryptography is an arising technology which emphasizes the phenomena of quantum physics in which two parties can have secure communications over network is based on the invulnerability of the laws of quantum mechanics. Quantum mechanics is a mathematical framework or set of rules for the construction of physical theories. The two important elements of quantum mechanics on which quantum cryptography depends are Heisenberg Uncertainty principle and photon polarization principle. The Heisenberg Uncertainty principle refers that, certain pairs of physical properties are pertained in such a way that measuring one property prevents the eavesdropper from simultaneously knowing the value of the other. The principle of photon polarization refers that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem. If an attempt is made to measure the property, it disturbs the other.

II. QUBIT

A qubit is a two-state quantum-mechanical syste, such as the polarization of a single photon: here the two states are vertical polarization and horizontal polarization. In a classical system, a bit would have to be in one state or the other, but quantum mechanics allows the qubit to be in a superposition of both states at the same time, a property which is fundamental to quantum computing.

A qubit has a few similarities to a classical bit, but is overall very different. Like a bit, a qubit can have two possible values—normally a 0 or a 1. The difference is that whereas a bit *must be* either 0 or 1, a qubit *can be* 0, 1, or a superposition of both.

Representation of Qubit

The two states in which a qubit may be measured are known as basis states (or basis vectors). As is the tradition with any sort of quantum states, Dirac, or bra-ket notation, is used to represent them. This means that the two computational basis states are conventionally written as $|0\rangle$ and $|1\rangle$ (pronounced "ket 0" and "ket 1"). A pure qubit state is a linear superposition of the basis states. This means that the qubit can be represented as a linear combination of $|0\rangle$ and$|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are probability amplitudes and can in general both be complex numbers.When we measure this qubit in the standard basis, the probability of outcome $|0\rangle$ is $|\alpha|^2$ and the probability of outcome $|1\rangle$ is $|\beta|^2$. Because the absolute squares of the amplitudes equate to probabilities, it follows that α and β must be constrained by the equation

$$|\alpha|^2 + |\beta|^2 = 1$$

III. QUANTUM KEY DISTRIBUTION

Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. An important and unique property of quantum distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental aspect of

quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure (i.e. the eavesdropper has no information about it), otherwise no secure key is possible and communication is aborted. The security of quantum key distribution relies on the foundations of quantum mechanics, in contrast to traditional key distribution protocol which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security. Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key. Quantum communication involves encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum key distribution exploits certain properties of these quantum states to ensure its security. There are several different approaches to quantum key distribution, but they can be divided into two main categories depending on which property they exploit.

Prepare and measure protocols

In contrast to classical physics, the act of measurement is an integral part of quantum mechanics. In general, measuring an unknown quantum state changes that state in some way. This is known as quantum indeterminacy, and underlies results such as the Heisenberg uncertainty principle and no cloning theorem. This can be exploited in order to detect any eavesdropping on communication (which necessarily involves measurement) and, more importantly, to calculate the amount of information that has been intercepted.

Entanglement based protocols

The quantum states of two (or more) separate objects can become linked together in such a way that they must be described by a combined quantum state, not as individual objects. This is known as entanglement and means that, for example, performing a measurement on one object affects the other. If an entangled pair of objects is shared between two parties, anyone intercepting either object alters the overall system, revealing the presence of the third party (and the amount of information they have gained).

IV. QUANTUM ENTANGLEMENT

Quantum entanglement is a physical phenomenon that occurs when pairs (or groups) of particles are generated or interact in ways such that the quantum state of each member must subsequently be described relative to each other. The state of each member is indefinite in terms of important factors such as position, momentum, spin, polarization, etc. in a manner distinct from the intrinsic uncertainty of a quantum superposition. Quantum entanglement is a product of quantum superposition, i.e., of the fundamental aspect of quantum mechanics where the complete state of a system is expressed as a sum of basis states, or eigenstates of some observable(s). Though it is common to speak of single quantum systems as existing in superpositions of basis states, the same is also valid for the quantum state of a pair or group of quantum systems. If the quantum state of a pair of particles is in a definite superposition, and that superposition cannot be factored out into the product of two states (one for each particle), then that pair is entangled. When a measurement is made on one member of such a pair and the outcome is known (e.g., clockwise spin), the other member of this entangled pair is at any subsequent time always found (when measured) to have taken the appropriately correlated value (e.g., counterclockwise spin). Thus, there is a correlation between the results of measurements performed on entangled pairs, and this correlation is observed even though the entangled pair may be separated by arbitrarily large distances.

Quantum systems can become entangled through various types of interactions. If entangled, one constituent cannot be fully described without considering the other(s). They remain entangled until a measurement is made and they decohere through interaction with the environment (i.e. measurement device). Upto now, there have already been several quantum key distribution(QKD) schemes: BB84 protocol , the B92, the 4+2
protocol , the six-state protocol.

V. THE PROPOSED WORK

An EPR pair is one of the 4 Bell states

$| \Phi^{+}> = 1/\sqrt{2}(|00> + |11>)$, (1)

$|\Phi^{-}> = 1/\sqrt{2}(|00> - |11>)$, (2)

$|\Psi^{+}> = 1/\sqrt{2}(|01> + |10>)$, (3)

$|\Psi^{-}> = 1/\sqrt{2}(|01> - |10>)$, (4)

After some of the people – Bell, Einstein, Podolsky and Rosen – who first pointed out the strange properties of states like these.

Our protocol is as follows:
Alice prepares an ordered 4-qubit state sequence $[p_1^1, p_2^1, p_3^1, p_4^1, p_1^2, p_2^2, p_3^2, p_4^2, p_1^3, p_2^3, p_3^3, p_4^3, p_1^4, p_2^4, p_3^4, p_4^4 \ldots\ldots, p_3^n, p_4^n]$.
Here, the subscripts 1, 2, 3 and 4 represent four different particles in one entangled state and the superscripts 1, 2, 3, . . ., *n* indicate the entangled pair orders in the sequence.
Then Alice takes one particle
from each entangled pair to form four ordered particle sequences:

S*i*: $[p_i^1, p_i^2, \ldots.. p_i^n]$, i=1,2,3,4.

$S_1=[p_1^1, p_1^2, p_1^3, p_1^4, \ldots\ldots. p_1^n]$

$S_2=[p_2^1, p_2^2, p_2^3, p_2^4, \ldots\ldots. P_2^n]$

$S_3=[p_3^1, p_3^2, p_3^3, p_3^4, \ldots\ldots. P_3^n]$

$S_4=[p_4^1, p_4^2, p_4^3, p_4^4, \ldots\ldots. P_4^n]$

Alice keeps particle sequences S1 and S3, and sends the particles in sequences S2 and S4 to Bob.

Eavesdropping check:
Bob randomly chooses a sufficiently large subset from the S2 and S4 sequences and measures these particles (sample particles) in the bases *BMB*1 or *BMB*2. He stores the rest of his particles and tells Alice the positions of the sample particles and his measurement basis through a classical channel. Then Alice measures the corresponding particles in the sequences S3 and S1 in the corresponding basis *AMB*1 or *AMB*2. Finally, Alice and Bob present their measurement outcomes to check quantum channels. If the error rate exceeds the threshold, Alice and Bob will discard these entangled particles and abort the protocol. Otherwise, they will securely use the remaining *N* pairs of entangled particles to communicate their secret message. Here,
AMB1 = $\{\Phi_1^{\pm}, \Psi_1^{\pm} |\Phi_1^{\pm} = 1/\sqrt{2}\ (|\Phi^+\rangle \pm |\Psi^-\rangle)$,
$\Psi_1^{\pm} = 1/\sqrt{2}\ (|\Psi^+\rangle \pm |\Phi^-\rangle)\}$,
AMB2 = $\{\Phi_2^{\pm}, \Psi_2^{\pm} |\Phi_2^{\pm} = 1/\sqrt{2}\ (|\Phi^+\rangle \pm |\Psi^-\rangle)$,
$\Psi_2^{\pm} = 1/\sqrt{2}\ (|\Psi^+\rangle \pm |\Phi^-\rangle)\}$,
BMB1 = $\{0+, 0-, 1+, 1- \mid |\pm\rangle = 1/\sqrt{2}\ (|0\rangle \pm |1\rangle)\}$,
BMB2 = $\{+0, -0, +1, -1 \mid |\pm\rangle = 1/\sqrt{2}\ (|0\rangle \pm |1\rangle)\}$.
Where AMB1=Alice measurement Base 1,

AMB2=Alice measurement Base 2,

BMB1=Bob measurement Base 1,

BMB2=Bob measurement Base 2.

The scheme is secure against direct measurement by Eve.If Eve make an attempt to measure the EPR sequences S2 and S4 then the the EPR pairs Will be collapsed (Heisenberg uncertainty principle).Then Bob will have only 50% probability of obtaining the right result when Bob uses Bell-basis measurement to read his EPR particle pairs. For instance,suppose $|00\rangle + |11\rangle$ is collapsed into $|00\rangle$ by Eve's interception. Since

$$|00\rangle = 1/\sqrt{2}\ |\Phi^+\rangle + 1/\sqrt{2}\ |\Phi^-\rangle$$

Bob has only 50% to obtain $|\Phi^+\rangle$ when he makes a Bell-basis measurement. In other words, the error rate will be as high as 50%, and this can be easily detected.

The scheme is secure against the intercept-resend attack. Suppose Eve intercepts the particle sequences S2 and S4 and keeps them. However she can not make Bell-basis measurement because she does not possess the other particle sequence. In order to obtain the other particle sequence, she must send a fake particle sequence to Bob so that Bob can notify Alice. However this can be detected easily. Bob chooses randomly a subset of particles and measures them. After Bob tells Alice what particles he has measured, Alice measures the corresponding particles at her hands.Then Alice and Bob publicly compare their results. If Bob's particle sequence is the fake particle sequence sent by Eve, half of his results will be inconsistent with that of Alice. This will easily detect Eve.

VI. CONCLUTION

This proposed scheme is secure and we can easily detect the presence of Eve.This scheme is very efficient.Here we are sending half the EPR sequences and upon receiving the authenticted acknowledgement from receiver we are snding the remaining half EPR sequences otherwise we are aborting the protocol.Even though Eve intercepts the first half EPR

sequence he can not make Bell measurement without other half EPR sequence.In that way this scheme became very efficient .

ACKNOWLEDGMENT

We would like to give our sincere gratitude to our guide Dr.Kumar Eswaran (*Prof. in CSE Dept)* who encouraged and guided us throughout this paper.

REFERENCES

[1] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proc. IEEE Int'l Conf. Computers, Systems, and Signal Processing, pp. 175-179, 1984

[2] C. H. Bennett, G. Brassard and N. D. Mermin, Phys. Rev. Lett.68 (1992) 557.

[3] W.K. Wootters and W.H. Zurek, "A Single Quantum Cannot Be Cloned," Nature, vol. 299, pp. 802-803, 1992.

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no.1, 3 - 28, 1992.

[5] M. Nielsen and I. Chuang, "Quantum computation and quantum information", London Cambridge University Press, 2000.

[6] Dan C.Marinescu , Gabriela M.Marinescu "Approaching Quantum Computing",Pearson Education,2009.

[7] T. Hwang, K. C. Lee, and C. M. Li, "Provably Secure Three- Party Authenticated Quantum Key Distribution Protocols", *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 1, pp. 71-80, 2007.

[8] W. Diffie and M. Hellman, IEEE Trans. Inf. Theory, IT-22, 644(1997).

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Rev. of Modern Physics*, vol. 74, pp. 145-190, 2002.

[10] G. Benenti, G. Casatti, and G. Strini, *Principles of Quantum computation, vol. I: Basic Concepts*, World Scientific Publishing, New Jersey, 2004.

