IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 3, Issue 2 (July-Aug. 2012), PP 41-43
www.iosrjournals.org

Quantum Cryptography Using Past-Future Entanglement

[1]Smriti Jha
[1](Computer Science, Pune University, India)

Abstract: *Quantum Entanglement is an important principle on which Quantum Key Distribution is based. However, observations of measurements are discussed over a classical channel. Communication using entangled states is facilitated by Quantum Teleportation and has been the basis for various protocols. The purpose of this paper is to study the past protocols and present a security perspective on a novel quantum protocol which modifies the process of Quantum Teleportation. This paper explores the methodology of Quantum Teleportation and applies the concept to modern cryptographic applications.*

Keywords: *Entanglement, Past-Future Vacuum Entanglement, Quantum Cryptography, Quantum Teleportation, Quantum Channel, Ekert Protocol, Qauntum Key Distribution*

I. INTRODUCTION

Quantum Cryptography's essence lies in its use of quantum channels instead of classical channels. These quantum channels are based on the laws of quantum-mechanics, mainly underlining Heisenberg's uncertainty principle, superposition principle and the EPR paradox. Over the years, various quantum protocols have been proposed for Quantum Key Distribution (QKD), which aim to ensure secure communication of the key between users, Alice and Bob. [1]

In this paper, we take a brief look at the tested methods of Quantum Cryptography, their mechanism and introduce recent research done on the subject. A security perspective is provided on the mentioned Quantum protocol along with future scope of the same.

II. HISTORY OF QUANTUM PROTOCOLS

2.1 BB84 Protocol

BB84 protocol was proposed by Charles Bennett and Gilles Brassard in 1984 for Quantum Key Distribution. This protocol is based on Heisenberg's uncertainty principle and has since been of prominent use. BB84 protocol realizes a quantum channel which transport polarized photon states from one user to another, without making any use of entanglement. [2]

As a prerequisite to the BB84 protocol, measurement is exercised in two different orthogonal bases. The first orthogonal base is called the rectilinear base with horizontal axis signifying the bit 0 and vertical axis signifying the bit 1. The second orthogonal base is the diagonal basis with 45^{o} as bit 0 and 135^{o} as bit 1.

Alice and Bob communicate over this quantum channel with the purpose of fixing a common secret key. First, Alice chooses a random number of bits, and for each bit chooses a random basis, rectilinear or diagonal. These photons are then sent to Bob, who is unaware of the basis Alice has chosen for each bit. Bob then proceeds to measure each photon in a random basis. After this, Alice and Bob compare with each other, over a public channel, the bases they chose to measure each bit and discard any bit where Bob's basis of measurement does not match the one Alice used for that bit.

In this scenario, if any eavesdropper, say Eve, tries to secretly spy on the channel, it would cause detectable disturbance in the channel as she would have to measure the photon sent by Alice before sending it to Bob. This is in conformity with the no cloning theorem which states that Eve cannot replicate a particle of unknown state. Hence, Eve is forced to guess, which if incorrect would lead to loss of information, by Heisenberg's uncertainty principle with Bob having a 50-50 chance of measuring a bit value different from Alice. This would alert both Alice and Bob and they can drop their communication for ensuring safety of information.

2.2. Ekert's protocol

Artur Ekert introduced a novel approach to quantum key distribution, using entangled states and the concept of Quantum Teleportation. In Ekert's implementation, one source of entangled polarized photon is used to emit pairs of photons which are split between Alice and Bob, with each receiving one photon from the entangled pair. The rest of the process is almost similar to BB84 protocol, with Alice and Bob independently choosing their bases of measurements and then keeping the bits which are measured on a common basis. [3] Different angular orientations can be used for measurements, results of which are then used to determine the

Svalue in Clauser-Horne-Shimony-Holt inequality. Any attempt by eavesdropper to spy on the communication between Alice and Bob would destroy the entanglement shared between them and hence can be easily detected. Entanglement is an effective way for QKD as it does not require a random number generator. Recent experiments have achieved QKD using entangled photons proving their credibility. These attributes make entanglement of great significance in modern quantum cryptography techniques.

2.3. Quantum Teleportation

Quantum Teleportation is a technique of transporting quantum state from one location to another without disobeying the no cloning theorem.

Alice has a quantum state that she wants to send to Bob:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1)$$

But she cannot send the quantum state by measuring it, as it would not give her the value of α or β, but instead would result in the state |0> with probability $|\alpha|^2$ and in state |1> with probability $|\beta|^2$.

To circumvent this issue, Alice and Bob share a Bell state between each other. With the measurements made on Alice's quantum state and Bell state, Alice gathers two values b_1 and b_2 by measuring her qubits, though her qubits are destroyed in the process. This information is passed onto Bob, who then receives the quantum state. It is to be noted that without the classical information b_1 and b_2 from Alice's end, Bob will fail to reconstruct the desired quantum state.

III. RELATED WORK

In a recent paper published by Carlos Sabin, Borja Peropadre, Marco del Ray, and Eduardo Martin-Martinez from the Institute of Fundamental Physics in Madrid [4], a new kind of entanglement has been proposed in which two qubits become entangled with each other without ever physically interacting with each other.

The qubit P interacts with the quantum field along an open transmission line for an interval T_{on} and then, after a time-lapse T_{off}, the qubit F starts interacting for a time T_{on} in a symmetric fashion. After that, past-future quantum correlations will have transferred to the qubits, even if the qubits do not co-exist at the same time.

The physicists have successfully realized this experiment using current technology. The paper puts forward the idea of quantum teleportation "in time" where information about the quantum state of qubit P^1 is codified in the field during time T_{off} and recovered in F using classical information stored in the past. Special care has been taken in the experiments to disallow any photon exchange which could contribute in correlations, making the qubits entangled entirely using transference of vacuum correlations. The physicists have shown that if qubits are separated by given distance r and the interaction can be switched on and off fast enough to have finite interaction times, then past-future entanglement is possible for qubits with constant energy gaps.

The paper explores the example of Paula in possession of P, and another qubit P^1 which she wants to teleport to Frank. After the interaction with vacuum field is turned off at $-t_1$, she carries out measurements on her qubits. After t_2, Frank can use the results of Paula's measurements (stored as classical information) and manipulate his qubit F, to transfer the state of P^1 to F. The fidelity is a function of quantum correlations between P and F. The information of P^1 is coded in the field during T_{off} irrespective of the resultant state of qubit P after its interaction and measurement. The information is then recovered during T_{on} in F.

IV. PROPOSED APPLICATION

The proposed method focuses on a security technique which is based on the Past-Future Entanglement where the source of entanglement is neither Alice nor a third-party source which emits pairs of entangled particles. The source of Entanglement here is the vacuum field, which is the transmission line itself.

This novel quantum protocol has presented Quantum Teleportation "in time", which points to the fact that the quantum state of P is transferred to F in a time interval when none of them were coupled to the field. This time interval is denoted by Toff.

Communication faces the possibility of an eavesdropper listening on the channel in order to decipher the messages exchanged between two users. It is a well-known fact that one-time pad is considered the most secure way of encryption as it has a unique key for each message, though has its own disadvantages due to long key value.

The Past-Future Entanglement can serve as a potential technique for Quantum Cryptography. Here P interacts with the field for T_{on} before F couples to the field, there is a time interval T_{off} which is devoid of any interaction occurring with the vacuum field.

Let's say an eavesdropper wants to spy on Alice and Bob's communication, and interacts with the transmission line. This would disturb the correlation as T_{off} requires absolutely no interacting till F is coupled to the field. Hence, such an intrusion can be detected by the parties. Another thing of notice here is that as none of

the qubits are interacting with the vacuum field during Toff, the eavesdropper cannot have any knowledge of the qubits, which would be eventually required to crack the encrypted key.

In a scenario where an eavesdropper interferes with the field during $T_{on,}$ it would still disturb the entanglement, decreasing the fidelity of the quantum correlations. This would cause Alice and Bob to detect an intrusion.

The quantum channel has also proven to support Quantum Teleportation through time where the classical bits stored in the field are used by qubit F to replicate the quantum state of P^1. Though classical bits can be extracted by an eavesdropper, say Eve, she would still not know the entangled qubit F, which is required to derive the quantum state.

V. CONCLUSION

This paper has explored the security applications of the novel quantum protocol with respect to Past-Future Entanglement. Future Scope of the method lies in practical realization of Past-Future Entanglement and making it accessible. The paper is only focused on the security applications of the quantum channel, which can be equally applied in various other quantum information processing tasks. Another field of research could be implementation in device independent quantum cryptography.

REFERENCES

[1] Lomonaco, S., J., "A Quick Glance at Quantum Cryptography", November, 1998. http://xxx.lanl.gov/abs/quant-ph/9811056.

[2] Bennett, C. H. and Brassard, G., "Quantum Cryptography: Public key distribution and coin tossing.", International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10-12 December 1984, pp. 175-179

[3] Ekert, A. K., "Quantum cryptography based on Bell's theorem", *Physical Review Letters, vol. 67, no. 6*, 5 August 1991, pp. 661 - 663M

[4] Carlos Sabín, Borja Peropadre, Marco del Rey, Eduardo Martín-Martínez, "Extracting Past-Future Vacuum Correlations Using Circuit QED", *Phys. Rev. Lett. 109, 033602*