Random Photon Key Pasting (RPKP) for Secure Optical Data Transport in Quantum Key Distribution

T.M Bhraguram
Asst.Professor, Department of IT
Adi Shankara Institute Of Engineering
And Technology, Kalady

S.Shermin
Asst.Professor, Department of CSE
Musaliar College of Engineering
And Technology, Pathanamthitta,

ABSTRACT
In this paper we proposed a new mutually authenticated method, ie Random Photon Key Pasting (RPKP) for secure data transmission which is already running under Quantum key distribution. RPKP is method which is trying to paste randomly generated number to the private key as log form and invoked from a trusted third party. The random numb will be completely based on the System level and it is highly depending on the time of the transmission, properties of the Source and destination and also the priority level. We are proposing separate protocol for Priority level key generation and property level communication establishment. The Time module is controlling the key pasting strategy. Quantum cryptography capitalizes on the inherent random polarization state of single photons, which are associated with binary logic values. Because the polarization state of a photon is not reproducible by an eavesdropper between the source and the destination, polarized photons are used with an intelligent algorithm to disseminate the cryptographic key with high security from he source to the destination, a process known as quantum key distribution. However, although the polarization state of a photon remains intact in free-space propagation, it does not remain so in dielectric medium and thus quantum cryptography is not problem-free.

Keywords- Quantum key distribution; Entanglement swapping; Authentication; Bell-basis measurement

1. INTRODUCTION
Quantum computation, with an offspring applicable to secure data communications, known as quantum cryptography. The key element of quantum computation is based on a quantum system that can not only be in two states but also in a superposition of state. Such system may be the two spin eigenstates of a particle, +1/2 and -1/2 or the polarization states of a photon. The two eigenstates are associated with the logic value "1" and "0". The superposition of two states is a concept that is explained only with quantum mechanics. Mathematically, this concept is linked with two complex coefficients α and β, such that, in a quantum mechanical notation:

$$|\psi> = \alpha|0> + \beta|1>, (|\alpha|2 + |\beta|2 = 1)$$

The term "quantum cryptography" does not really mean that cryptography is quantized, or that quantized quantities are cryptographic; they are merely a combination of two key words "quantum" and "cryptography" to describe that this is a technology that uses polarized photon explained by quantum mechanics and hence "quantum", and also a sophisticated scheme to transmit a secret code using a sequence of randomly polarized photons (to an external viewer) from which an encryption/decryption key is constructed, hence "cryptography". The method that a secret key is generated and distributed between the two ends of a communications link is known as quantum key distribution (QKD) [1]. With this secret quantum key, messages are encrypted and decrypted. Quantum cryptography, and particularly QKD, uses the polarization states of photons and a binary system. According to it, a subset of photon polarization states corresponds to logic "0", whereas another subset of states corresponds to logic "1".

2. POLARIZATION AND THE POINCARE SPHERE
When an electromagnetic wave propagates in a linear medium (e.g., non-crystalline), the electric polarization is expressed as

$$\mathbf{P} = \varepsilon o \chi \mathbf{E}$$

Where χ is the electric susceptibility of the medium. When it propagates in non-linear medium, then χ is expressed by a tensor, the dielectric constant ε = εo (1+χ) is also a tensor, and thus the polarization is not the same in every direction of the Cartesian or polar coordinate system.

Consequently, when a polarized photon travels in a non-linear birefringent medium, the interaction of light with matter affects the state of polarization (SoP). The SoP change is visualized if we consider a sphere and each point on its surface representing a state of polarization (SoP). Then, each point S represents a SoP defined in terms of an azimuth α and an ellipticity ε as:

1+cos(2α)cos(2ε)

SOP = cos(2α)sin(2ε)+isin(2α).

The azimuth α and ellipticity ε of the Poincaré sphere are related to Stokes parameters:

S1 = cos(2ε) cos(2a)

S2 = cos(2ε) sin(2a)

S3 = sin(2ε)

S0 = sqrt (S12 + S22 + S32)

Poincaré sphere mapping the polarization states of a photon. Some states are used to represent a logic "1" and some others a logic "0".

A moving point S on the surface of the Poincaré sphere defines a trajectory [2,3]; the trajectory is directly related to the retardation experienced by the field components. For example, if the sphere is defined by the three Cartesian axes x, y and z, then a linear retardation without axis rotation moves S on a circle with plane perpendicular to the x-axis; the arc traveled on the circle due to polarization rotation is equal to the amount of linear retardation. A linear retardation with axis rotation by θ corresponds to a movement of S on a circle having a plane perpendicular to an axis at an angle 2θ with the x-axis. Similarly, a circular retardation corresponds to a movement of S along a circle on a plane perpendicular to y-axis. In this case, the rotation angle is

equal to the amount of circular retardation. Two mutually orthogonal SoPs, both at equal intensity, result to a depolarized field. Furthermore, how the Poincaré sphere [2,3] is cut in halves and what the logic association is are kept a secret.

3. PICKING A RELIABLE QUANTUM QUANTITY

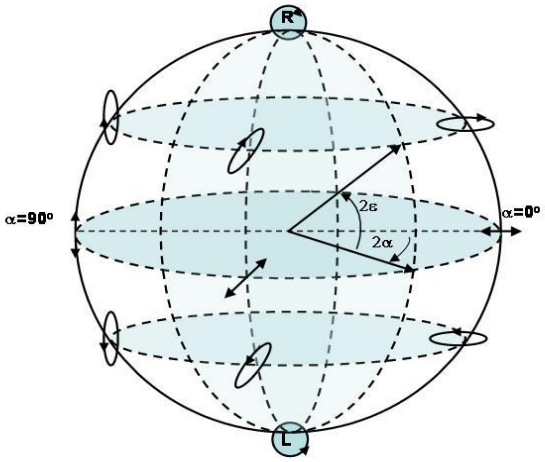

Figure 1:-Poincaré sphere logical association

QC takes advantage of the polarization property of photons, and particularly of polarized single photons that propagate in an optical medium such as glassy fiber (or air), in conjunction with polarizing filters, the polarization state of which varies either according to a program or randomly. Thus, if polarized photons are transmitted and received through polarizing filters from one end of a fiber link to the another end, then a secret key can be defined according to an algorithm that only the two ends can know, a concept that was proven by Charles Bennett, John A. Smolin and Gilles Brassard of IBM Thomas J. Watson Research Laboratory in 1989. However, single polarized photons are not easily generated and they cannot travel far in a lossy, dispersive and birefringent medium; loss attenuates photonic power, dispersion affects the propagation characteristics of photons, and birefringence, B=k|n2-n1|, affect the polarization orientation of travelling photons.

To overcome the shortcomings of polarization, other quantum methods have been devised. One of them uses phase shift of single photons instead of polarization. According to it, the wave nature of a photon is passed through a splitter with unequal lengths and the two halves are recombined in a Mach-Zehnder [4] interferometer to introduce a phase shift. However, the phase shift within a propagating photon that travels through the non-linear fiber cannot be sustained reliably for long lengths due to self modulation.

Another method uses entangled states of a photon pair. According to it, a high energy single photon, such as 405nm, is passed through a strong birefringent crystal to generate two orthogonally polarized photons each at 810nm, thus preserving the total energy. The method of entangled photons capitalizes on the aforementioned property that two mutually orthogonal SoPs, both at equal intensity, result to a depolarized field. As a result, the entangled photon-pair with orthogonal polarization may n theory travel longer distances than a single polarized photon, However, this method depends on the uniformity of medium non-linear properties, and thus like the other two it also has its own ramifications.

4. QUANTUM KEY DISTRIBUTION PROCESS

Quantum cryptography requires that there is a secret key known only to the processing computers at the end points of a link, point A and point B, and not to anyone else including human operators and any third party (human or computer) that may have tapped the link; this key will be used by end-point A to encrypt a message and by end-point B to decrypt or decipher it. Based on this, assume a transmitter at point A , receiver at point B and an eavesdropper at the transmitting medium between A and B. The two points A and B are connected with an optical fiber and also with a separate public channel, such as the Internet or the public wireless network. The task in hand is to make known to B of the secret key so that eavesdropper cannot understand it even if he has tapped the optical fibre. Although several protocols to accomplish this have been devised.

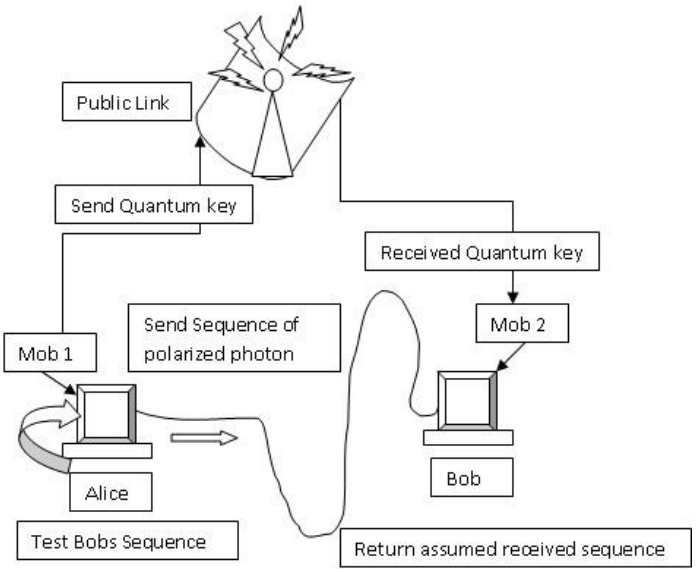

Figure 2:- Quantum key distribution process

Quantum Cryptography" (QC) is a process that consists of two major parts, the Quantum Key Distribution (QKD), and the message encryption/decryption process. The key point in both processes is the polarization state of photons and the variable polarization filter. In addition, because the polarization of single photons is not readable without altering it and because it is not reproducible, Evan the eavesdropper cannot read the polarization of single photons, reproduce it and send it to B. This is the key point in quantum cryptography.

5. QUANTUM CRYPTOGRAPHY TECHNICAL ISSUES

In a general applicability of QC, there will be many issues, which deserve to be identified and examined. These issues are:

1. Single photon generation with the desired polarization state; there are no "off-the-self" sources with controllable single photon rate generation and controllable photon polarization.

2. Polarization does not remain constant but it changes as photons propagate in the fiber medium due to medium non-linearity.

3. Polarizing filters; there are no "off-the-self" fast tunable polarizing filters with zero insertion loss that can control photon polarization reliably; certain clever method based on Faraday

mirrors have been developed but they seem complex and impractical in long length fibres.

4. Single photon source that is synchronized with the polarization state of an external filter; this is not known yet.

5. Point-to-point direct fiber link; the link should remain intact without splices, connectors and other optical components that may alter the polarization state of the propagating photon. This imposes a challenge as the fiber over time does not remain intact in its integrity and its performance.

6. Single wavelength channels; QC and particularly QKD is limited to single wavelength. Photons and thus to a single optical channel, thus underutilizing the full bandwidth capacity of fibre. To date, only dedicated point-to-point solutions are contemplated and no solutions have been reported in multichannel transmission.

7. Synchronized polarization [5] filters at both end A and B, polarization states of the filters at either end need to be synchronized and also to take into account the propagation speed of photons in the fiber medium. This is a very delicate issue as temperature drifts cause delays thus changing the synchronization between the two filters.

8. A not-perfectly coupled single photon source onto optical fibre; typical photonic power coupled onto fibre suffers from loss. There is no reason to believe that coupling a single photon source onto fibre will not suffer from similar loss which may result in photon loss and thus increased qu-bit error rate.

9. Optical fibre maintains the polarization state of photons; manufactured fibre must comply with tight physical, optical and mechanical specifications. The variability of these specifications is real and so are attenuation, birefringence, dispersion, and other non-linearity that affect the properties of propagating photons in the fibre.

10. Optical fibre has absorption or scattering centres; at about 1400nm, absorption peaks due to OH-, below 1300nm and above 1620nm increases due to absorption and Raleigh scattering. Currently, there is no zero-loss fibre in any part of the useful spectrum. In fact, to overcome this, researchers are thinking of quantum repeaters; that is, subsystems that will receive the polarized signal, restore its strength, and retransmit it. This of course may defeat the purpose of QKD because eavesdropper can also have the same subsystem which with minor modification can receive the signal, copy the polarized key, restore the polarization state of photons and retransmit it to B.

11. A very long bit sequence is required to warranty good encryption key. Because the two filters, one at each end, are randomly and independently polarized, the number of bits from A sequence that will pass through B filter are fewer; it is those bits that constitute the encryption key. Thus, in order to warranty a relatively long encryption key (few hundred bits), long sequences must be used.

12. Low bit rate transmission results in significant latency in key identification and encrypted message transmission. Because the process of transmitting photons is very slow, few hundred bits per second, and the bit sequence is too long, see issue #10, the process is comparatively slow.

13. Single chance to successfully negotiate the encryption key. If after a QKD [1,6,7,8] process a key is erroneously identified by A, or erroneously executed by B, neither side will know. This may create an important issue as it defeats the robustness of the encryption purpose.

14. There is no mechanism to confirm that the key has been correctly constructed and that the encrypted message has been correctly received and decrypted. This is similar to issue #12, yet it identifies a potentially serious issue with the robustness of QC and a lack of verification.

15. No acknowledgment by B that the negotiated encryption key works reliably or correctly. B must know if his polarizing filter behaves as prescribed by A, and should also know this from the first arriving photon in the encrypted message. Deciding when the first photon arrives is a task with its own.

16. The quantum cryptographic process of key distribution must frequently repeat itself to reinstate possible de-encrypting misalignments.

17. An eavesdropper may easily attack the transmitted polarization states on purpose. The focus in QKD so far to prevent from eavesdropping. However, it is equally important to prevent or countermeasure attacking.

An attacker may tap the medium and maliciously destroy the QKD process and thus hamper transmission of the encrypted message. In such case, an eavesdropper is not only a person that needs to "listen" but also one that hinders and deters successful communication between point A and point B; jamming is a well known form of communication deterrence.

18. If multiphoton bit transmission is contemplated, then a small part of the photonic pulse may be extracted from the fibre (by sophisticated tapping) and thus break the encrypted message.

6. OPTICAL COMMUNICATIONS PHOTON SOURCES

Solid state laser devices do not generate single photons but a multiplicity. In addition, the polarization state of photons emanating from the laser device is not easily controlled.

6.1 Absorption and Scattering

The fibre medium cannot be entirely free from absorption and scattering centres and thus attenuation. To overcome this, some researchers have tried transmitting a laser beam from one mountain top to another, a method known as free-space optical transmission (FSO) [1,6,7]. The FSO method is known to be more secure than fibre-optic transmission because it is not easy to intercept a thin beam in space without severely attenuating it or interrupting it. In fact, the notion of using the FSO method in deep space in optically interconnected satellite networks [1, 2] has been recognized and gained momentum for inter-satellite communications.

6.2 Fibre medium

The typical fibre medium cannot be polarization free. There is a residual birefringence that is measured as the difference of refractive indices in the x and y direction of the fibre (z is the transmission direction). Even small pressure and temperature points and tensile stress will vary the fiber birefringence significantly to distort the polarization state of propagating photons, and thus the quantum cryptographic process and the fiber medium cannot be of very long lengths as optical amplification will be required every 60-100 km. However, amplification cannot warranty that the polarization state will be maintained, and opaque repeaters that may restore polarization defeat the purpose as themselves become vulnerable to eavesdropping.

6.3 The receiver

The receiver in quantum cryptography consists of a random polarizing filter, which exhibits the same symptoms of polarizing filters described above, an ultra-sensitive photo detector, and of a

synchronizing clock. The sensitivity of the detector must be such that it detects single photons; such receivers are not trivial to cost-efficiently construct. Similarly, because the clock is not in synchronism with the source (but it relies on the accuracy of a free running clock) the bit rate cannot be too fast. Indeed, bit rates are in the order of few kilobits per second, which is a million times slower than typical optical transmission rates at gigabits per second.

6.4 Network topologies

Typical network topologies are the ring with several optical add-drop multiplexing nodes, the mesh topology with several interconnected nodes, and the point-to-point with optical add-drop multiplexing nodes. As such, any of the three topologies assumes that the optical signal will travel through a node, which even if it is all-optical or optically transparent, it does not warranty that the polarization of the transmitted photons will be maintained. Consequently, end-to-end quantum cryptography, as currently defined cannot be used in any of these topologies if one or more nodes are on the path between A and B.

6.5 WDM Fibre Communications

Currently, the typical optical communications technology is dense wavelength division multiplexing (DWDM) [4,5,8].

This is a technology with a well defined standard grid of optical channels and has successfully transmitted several Terabits per second of aggregate traffic in a single fiber. However, the success of the DWDM technology is not the result of single photons or the polarization states of photons but in its ability to transport high speed data over many optical channels that are multiplexed in the fiber. As a consequence, any new cryptographic technology should stay in step with DWDM and solve the data security issue for each channel and on the aggregate. Moreover, a more complex and pragmatic network topology should be considered, as well as that photons travel in a not so perfect fiber for hundreds of kilometres through optical components that may affect the properties of the optical signal. Finally, it should also be considered that the photonic signal will suffer from linear and non-linear phenomena that are typical in fiber communication. Such phenomena that emanate from the photon-matter interaction are four wave mixing, polarization mode dispersion, cross-phase modulation, instability modulations, polarization state rotation, phase shift, and so on, have an effect on photons and the photonic signal. Therefore, if single photons of different wavelength would be transmitted to comply with DWDM technology, their interactions would affect their polarization state, their logic value (1 or 0), and even more, their existence. Photonic quantum cryptography in its current state is so vulnerable that may be eventually proven disastrous, if widely used.

7. QUANTUM KEY GENERATION PROCESS

A sends a random association of polarization states for “1” and “0”.

B uses a random polarization filter for the arriving polarized photons.

Some pass successfully and some not. B, not knowing the successes and failures, tells A the sequence of polarization directions he used. A tests its original sequence of “1” and “0” with B’s filter. It then tells B which polarizations were successful the new sequence determines the quantum key.

Eavesdropper has changed the correct delivery of states so that when B tells A, the sequence of polarization directions he used, A determines a quantum key which turns out to be wrong as it will not decrypt correctly the encrypted messages.

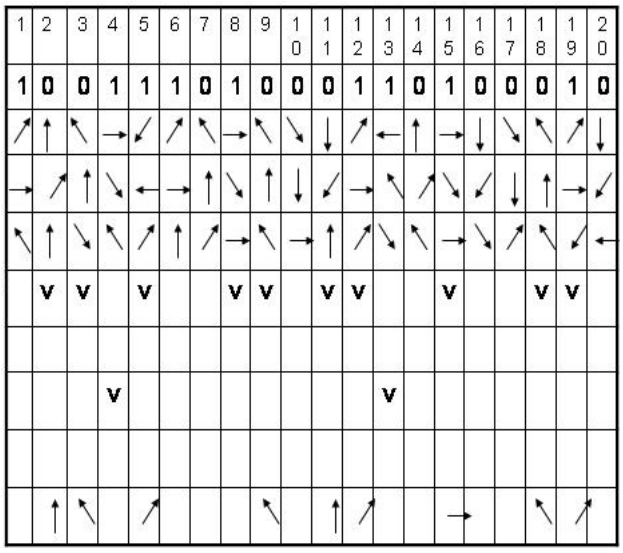

Figure 3:- Attacking the quantum key generation process.

8. PROPOSED MODEL: RANDOM PHOTON KEY PASTING (RPKP)

Assume that A and B are the legitimate anticipators who share two keys A SK and B SK and a one-way hash function h :{0,1}* □ {0,1}l →{0,1}m , where * means an arbitrary length, l is the length of a counter, and m is a constant. Then, authentication key can be generated by a hashed value, which includes the number of calling the one way hash function. Our QKD protocol contains two phases, one for mutual authentication between two legitimate users, and the other for key distribution. The detailed procedures are described as follows.

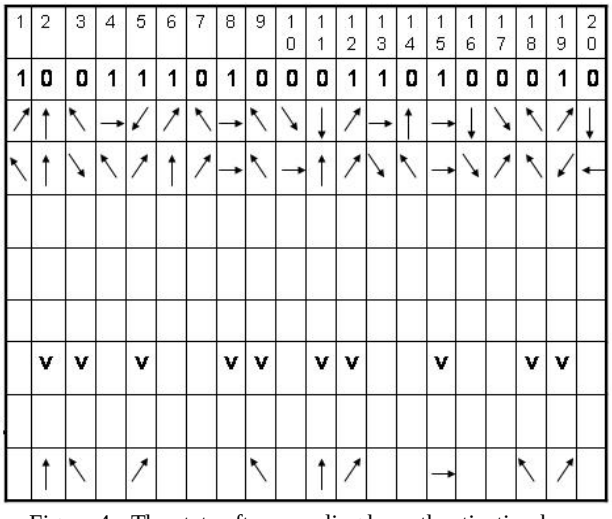

Figure 4:- The state after encoding by authentication key

According to Stinespring dilation theorem eavesdropping can be realized by a unitary operation, say, E # on a larger Hilbert space Beta=0.

$$\hat{E}|0\rangle_A|e\rangle_E = \alpha|0\rangle_A|e_{00}\rangle_E + \beta|1\rangle_A|e_{01}\rangle_E$$

$$\hat{E}|1\rangle_A|e\rangle_E = \beta`|0\rangle_A|e_{00}\rangle_E + \alpha|1\rangle_A|e_{01}\rangle_E$$

Where $|\alpha|^2 + |\beta|^2 = 1, |\alpha^e|^2 + |\beta^e|^2 = 1,$

and $\alpha\beta^e + \alpha^{e^1}$.

If a bit of the authentication key *h SK c* is 0 then,The total states ε0 and ε1 and the total probe of the system of evesdropping is the existing Stinespring dilation theorem [3,4,5]. When the probability of 0 and 1 in an authentication key is the same, Eve can be detected with probability 1/4 $(1+\beta^2+\beta'^{2)}$ in the authentication phase.

The source and destination can find out the existence of eavesdrop by the following probability.
$1-[1/4(1+alpha^2\ 1+alpha'^2)]^m$

If M is enlarged, the detected probability of eavesdrop is increased; therefore, eavesdrop will always be exposed when M is large enough. Hence source and Destination can trust each other are the expected user and the quantum tunnel is secure when the authentication is passed. In the key distribution phase, there is no qubits transmitted and source and Destination easurement results are random and secret to eavesdrop center.

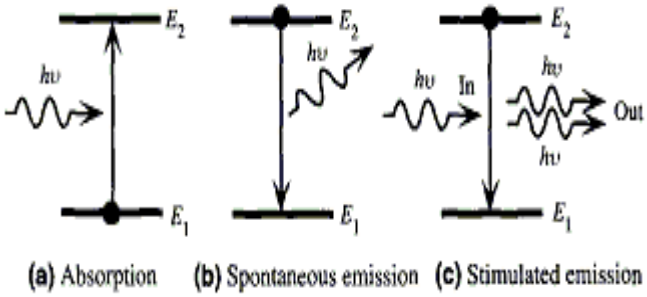

Figure 5:- Emission of Random Photon

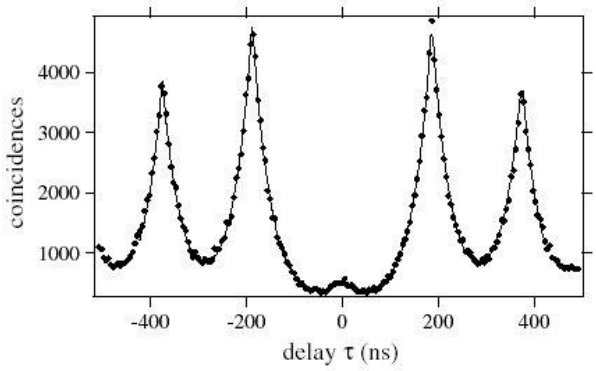

Figure 6:- Photon Pasting during delayed Transmission

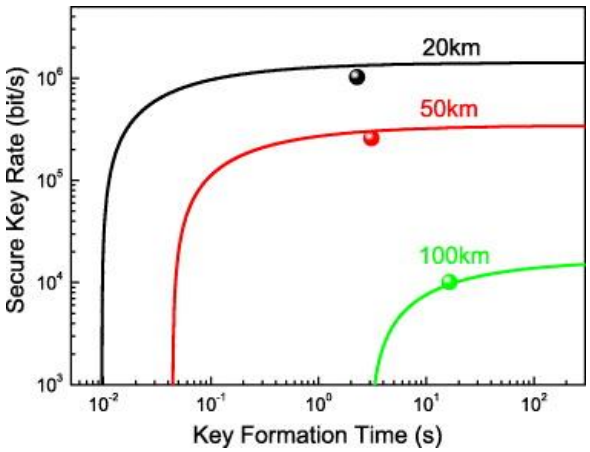

Figure 7:- Secure Key rate for a single Transmission

9. EFFICIENCY ANALYSIS

In 2000, Cabello defined the efficiency (∑) of a QKD protocol from the information theory point of view and ∑ is defined as follows,

$$\sum=(Bs/qi+bi)$$

Where *Bs* represents the expected number of secret bits received by destination or vice versa. and *qi* and *bi* are the number of qubits and bits source and destination interchanged in procedure of distributing the shared key, respectively. As discussed above, every transmission of two qubits can generate two bits of the shared key without classical information exchange, that is to say, the efficiency of our scheme is 100%. In fact, the particles transmitted in quantum tunnel between source and destinations are entangled ones which are different from single particle.

The newly introduced complementary definition of efficiency of a QKD protocol as

$$Nt=(Bs/Qt'+Bt')$$

Where *Qt'* is number of total quits used (not the ones transmitted; this is different from the definition proposed by Cabello's). In the presented QKD scheme, *Bs* =2, *Qt'*=4, *Bt* =0, thus its total efficiency is 50%.

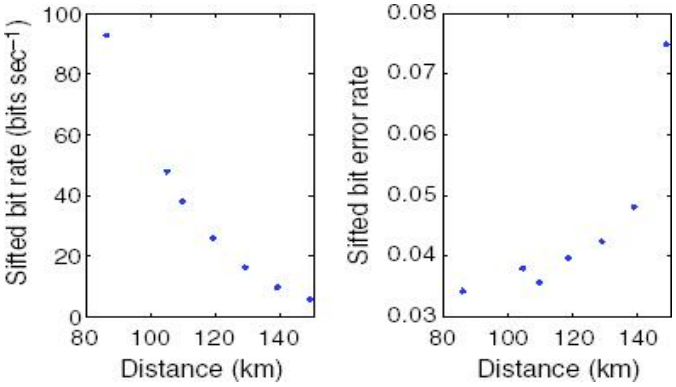

Figure 8:- Bit Error Rate during Photon Pasting

As almost all the quantum source (except for the particles used for eavesdropping check) can be used to carry the secret message, the intrinsic efficiency Nq for quits in our protocol approaches 100%. Here,

$$Nq=(Qu/Qt')$$

Where Qu is the number of useful quits in QKD.

10. CONCLUSIONS

In summary, a mutually authenticated QKD protocol based on RPKP (ie Random Photon Key Pasting) based on entanglement swapping is put forward. Communication participants ie source and Destination can ensure the security of the sequences, and authenticate each other to prevent illegal users gaining the session key, so an eavesdropper will be detected if there is an eavesdrops in the quantum channel. An original key is generated only by performing Bell-basis Measurements, without classical information exchange. After the key is generated, there is no need to compare sample bits to check eavesdropping. Furthermore, the secret key is randomly produced by Source and Destination rather than one part shares secret key with the other, so this is theoretically more secure. Except a few particles consumed for eavesdropping checking, most particles make contribution to generate the shared key, and two pairs of Entangled particles can provide two bits of the session key. Efficiency of the scheme is 100% according to Cabello's definition. According to modified definition, the efficiency of our protocol comes up to 50%, and the efficiency for quits is 100%. However, there are some future works to study, such as how to combine quantum error correction methods with our work, applying entanglement swapping mechanism.

11. REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE Press, 1984, pp.175-179.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett, vol. 67, pp. 661-663, 2008.

[3] C. H. Bennett, G. Brassard, N. D.MERMIN, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett, vol. 68, pp. 557-559, 2007.

[4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett, vol. 68, pp. 3121-3124, 2007.

[5] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett, vol. 81, pp. 3108-3021, 2008.

[6] G L Long, and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," Phys. Rev. A, vol. 65, 032302, 2003.

[7] Y. Guo, and G. H. Zeng, "Deterministic quantum key distribution using two non-orthogonal entangled states," Commun. Theor. Phys, vol. 47, pp. 459-463, 2007.

[8] X. L. Zhang, Y. X. Zhang, and K. L. Gao, "Quantum key distribution Phys, vol. 47, pp. 459-463, 2006.